Carmelo Di Stefano

Introduzione alla Teoria dei numeri

Sommario

§1. L'insieme dei numeri naturali. 3
Esercizi. 7
§2. Numeri figurati 8
Esercizi. 11
§3. I numeri primi. 12
Esercizi. 15
§4. La distribuzione dei numeri primi. 16
§5. Il crivello di Eratostene. 18
Esercizi. 20
§6. Il metodo di Fermat per la fattorizzazione di un numero. 21
Esercizi. 24
§7. Alcuni problemi sui numeri primi. 25
Esercizi. 29
§8. La scomposizione di un numero in fattori primi. 30
Esercizi. 32
§9. Massimo comune divisore e minimo comune multiplo. 33
Esercizi. 35
§10. Il numero dei divisori di un numero. 36
Esercizi. 41
§11. Numeri perfetti e numeri amicabili. 42
Esercizi. 45
§12. Equazioni indeterminate. 46
Esercizi. 49
§13. Teoria delle congruenze. 50
Esercizi. 56
§14. Criteri di divisibilità. 57
Esercizi. 60
§15. Il teorema di Eulero. 61
Esercizi. 64
§16. Sviluppo decimale delle frazioni. 65
Esercizi. 71
§17. Principio di induzione. 72
Esercizi. 74
Esercizi svolti 76
Bibliografia 111

§1. L'insieme dei numeri naturali.

Si narra che il grande matematico Carl Friedrich Gauss abbia affermato: *La matematica è la regina delle scienze e la teoria dei numeri è la regina della matematica*. In effetti la teoria dei numeri, ossia la disciplina che si occupa di studiare le proprietà elementari dei numeri interi, è una delle discipline più affascinanti e difficili dell'intera matematica. Di contro è anche una delle parti più trascurate nell'insegnamento sia primario che secondario e talvolta anche universitario. Chi scrive ritiene invece che da tale disciplina possano trarsi molti spunti per far sì che lo studente possa appassionarsi alla matematica. In questi appunti vogliamo fornire diversi esempi per stimolare lo scarso interesse degli alunni verso la nostra disciplina.
L'insieme sul quale vogliamo operare è il cosiddetto insieme dei numeri naturali, solitamente indicato con il simbolo $\mathbb{N}$. Esso comprende i numeri {1, 2, 3, 4, ...} ossia quelli che solitamente vengono chiamati numeri interi positivi. Se lo zero sia o no da considerarsi un numero naturale è una questione dibattuta da secoli; allo stato attuale si è addivenuto ad una specie di compromesso, ossia ciascuna diversa teoria assiomatica di $\mathbb{N}$ stabilisce di considerare o no, zero un numero naturale. Per esempio Giuseppe Peano, il famoso matematico torinese della fine del secolo scorso, nelle prime edizioni del suo *Formulario matematico*, nel quale assiomatizzò appunto il sistema dei numeri naturali, considerò come elemento "minimo" di $\mathbb{N}$ il numero 1, nelle successive edizioni invece lo sostituì con lo 0. Per approfondimenti sull'argomento può consultarsi [D] e la bibliografia citata in quel lavoro. Cominciamo ricordando appunto i cosiddetti assiomi di Peano. I termini primitivi in tale assiomatica sono 0 (o 1 a seconda i casi), numero (intendendo con tale termine il numero naturale) e successivo:

Assiomi di Peano
1. 0 è un numero;
2. Se a è un numero anche a^+ (il successivo di a) è un numero;
3. Se $a = b$ allora anche $a^+ = b^+$, quali che siano i numeri a e b.
4. 0 non è successivo di alcun numero.
5. Se A è un insieme di numeri tale che $0 \in A$, e ogni volta che $a \in A$ anche $a^+ \in A$, allora A è l'insieme $\mathbb{N}$.

L'ultimo assioma, opportunamente modificato, costituisce il cosiddetto principio di induzione, mediante il quale potranno provarsi teoremi che riguardano sottoinsiemi infiniti di $\mathbb{N}$, come vedremo nel paragrafo 16.
I simboli utilizzati per indicare i numeri sono quelli cosiddetti *indo arabi* e a loro volta fra questi i primi dieci: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} vengono chiamati **cifre di un sistema di numerazione decimale**. Ovviamente potremmo considerare, come si è fatto nella storia e come si fa in molte applicazioni matematiche (per esempio in informatica) un sistema a base diversa da 10.
Una estensione dell'insieme $\mathbb{N}$ è l'insieme $\mathbb{Z}$[1] dei numeri interi relativi. Cioè l'insieme $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$. Per tale insieme viene a perdere di significato il quarto assioma, dato che non esiste un corrispondente di 0 (o 1), ossia non vi è un "primo elemento" nell'insieme. Quindi viene a cadere la necessità di stabilire il postulato 1 per l'esistenza dello zero.

[1] Il simbolo deriva dalla parola tedesca Zahlen che significa appunto Interi, è stato introdotto abbastanza recentemente dal fantomatico matematico Bourbaki, dietro il quale si sono celati alcuni fra i più importanti matematici del XX secolo

Definiti gli elementi detti numeri interi, nasce la necessità di definire le operazioni su di essi. Lo stesso Peano definisce intanto l'operazione di somma fra numeri interi utilizzando il principio di induzione. Ossia, dato il numero a definisce l'operazione $a + 1$ come la legge che associa al numero a il suo successivo, pone cioè $a + 1 = a^+$. Per definire $a + 2$ utilizza il successivo di $a + 1$, cioè pone $a + 2 = (a + 1)^+$ e via di questo passo. Quindi in generale pone $a + b + 1 = (a + b)^+$, quali che siano i numeri naturali a e b. A partire dalla somma definisce anche la moltiplicazione, così $a \cdot 1 = a$, $a \cdot 2 = a \cdot 1^+ = (a \cdot 1 + a) = a + a$, $a \cdot 3 = a \cdot 2^+ = (a \cdot 2 + a) = a + a + a$. In generale $a \cdot b^+ = (a \cdot b + b)$. Possiamo inserire queste due definizioni di operazioni come assiomi 6 e 7 del nostro sistema:

6. $a + 0 = a$, $\forall a \in \mathbb{N}$, $a + b^+ = (a + b)^+$, $\forall a, b \in \mathbb{N}$;
7. $a \cdot 0 = 0$, $\forall a \in \mathbb{N}$, $a \cdot b^+ = a \cdot b + b$, $\forall a, b \in \mathbb{N}$.

Adesso consideriamo quelle somme ottenute ripetendo più volte lo stesso addendo: $a + a + ... + a$, che grazie ai postulati 6 e 7 precedenti possiamo scrivere nel modo seguente $\underbrace{a + a + ... + a}_{n} = n \cdot a$. Poniamo la seguente definizione.

Definizione 1. Dato un numero intero a diciamo che esso è **multiplo** di un numero intero b, se esiste un terzo numero intero c tale che risulti $a = b \cdot c$.

È facile capire che i multipli di un numero naturale sono infiniti e che 0 è multiplo di qualsiasi numero, infatti $0 = a \cdot 0$ per tutti i numeri a. Ora il problema di ottenere un multiplo di un numero a secondo un dato fattore n è molto semplice; come spesso accade è invece molto più complicato determinare se un dato numero b è multiplo di un altro dato numero a. In particolare risulta interessante, dato un numero a, stabilire di quali altri numeri interi esso è multiplo. La prima considerazione che può farsi è che i numeri di cui a può essere multiplo sono, in valore assoluto, non maggiori di a. Un altro fatto interessante da notare è che nel momento in cui troviamo che $a = b \cdot c$, abbiamo trovato che a è multiplo di b ma anche di c, cioè i numeri di cui a è multiplo li troviamo a coppie. Poniamo adesso la seguente definizione.

Definizione 2. Se a è un multiplo del numero b, quest'ultimo numero si dice che è un **divisore** di a. Si dice inoltre che a è divisibile per b e che b divide a.

Risulta interessante determinare quanti e quali sono i divisori di un numero intero.

Esempio 1.

Vogliamo determinare i divisori del numero 24. Se ci atteniamo alla definizione 2, dobbiamo cercare di scomporre il numero 24 come somma di un certo numero di addendi tutti uguali fra di loro. La più semplice di queste uguaglianze è $24 = 24$, cioè $24 = 24 \cdot 1$, ciò vuol dire che 1 e 24 sono entrambi divisori di 24. Poi $24 = 12 + 12 = 12 \cdot 2$, quindi anche 2 e 12 sono divisori di 24. Ancora $24 = 8 + 8 + 8 = 8 \cdot 3$, quindi 3 ed 8 sono divisori di 24. Infine $24 = 6 + 6 + 6 + 6 = 4 \cdot 6$, cioè 4 e 6 sono divisori di 24. Non è possibile scrivere 24 come somma di cinque addendi fra di loro uguali. Se proviamo a scriverlo come somma di 6 addendi uguali, tali addendi sono evidentemente uguali a 4, ossia $24 = 4 + 4 + 4 + 4 + 4 + 4 = 6 \cdot 4$. Troviamo quindi la coppia (6, 4) che avevamo già trovata, anche se nell'ordine (4, 6). Possiamo perciò fermare il procedimento poiché continuando ritroveremo le coppie già trovate (8, 3), (12, 2) e (24, 1), anche se in ordine diverso. Infine i divisori di 24 sono 1, 2, 3, 4, 6, 8, 12, 24. Sono quindi 8.

Abbiamo visto nell'esempio precedente che 24 non può scriversi come somma di 5 addendi uguali, cioè 24 non è divisibile per 5. Quindi non possiamo scrivere $24 = 5 \cdot p$ quale che sia p. Possiamo però scrivere $24 = 5 \cdot 4 + 4$. Ciò ci permette di enunciare il seguente risultato.

Teorema 1. Dati due numeri interi m ed n, con $n \neq 0$, esistono sempre due numeri q ed r che rendono vera la seguente scritta: $m = n \cdot q + r$, con r: $0 \leq r \leq |n| - 1$.

Nel precedente teorema consideriamo il valore assoluto di n perché i numeri m ed n possono anche essere negativi.

Esempio 2.

Siano $m = 126$ e $n = 37$, abbiamo: $126 = 37 \cdot 3 + 15$. Quindi $q = 3$ e $r = 15$. Nel caso in cui $m = 12$ e $n = 43$, abbiamo: $12 = 43 \cdot 0 + 12$. Quindi $q = 0$ e $r = 12$. Infine se $m = 16$ e $n = -19$, abbiamo: $16 = -19 \cdot 1 + 3$, perciò $q = 1$ e $r = 3$.

Poniamo la seguente definizione.

Definizione 3. Dati due numeri interi m ed n, con $n \neq 0$, diciamo **divisione** di m per n l'operazione di determinare due numeri q ed r per cui si abbia $m = n \cdot q + r$, con r: $0 \leq r \leq |n| - 1$. Il numero q si chiama **quoziente** della divisione ed il numero r si chiama suo **resto**.

È chiaro che se nella divisione di m per n, il resto r è diverso da 0 vuol dire che m non è multiplo di n e che n non divide m.
Vediamo qualche esercizio da risolvere mediante la divisibilità negli interi.

Esempio 3.

Consideriamo i seguenti insiemi di frazioni, vogliamo sapere se fra di esse vi sono numeri interi.

- $\frac{n+2}{n+5}$. Se consideriamo n numero naturale, possiamo dire che tutte le frazioni sono proprie e quindi nessuna di esse rappresenta un numero naturale. Se però supponiamo che $n \in \mathbb{Z}$, allora ciò non è più vero, per esempio per $n = -2$, la frazione vale 0. È questo l'unico valore intero? Riscriviamo la frazione: $\frac{n+5-3}{n+5} = 1 - \frac{3}{n+5}$, in questo modo tutto dipende dal fatto che $n + 5$ sia un divisore di 3, ossia $n + 5 = -1 \Rightarrow n = -6$; $n + 5 = 1 \Rightarrow n = -4$; $n + 5 = -3 \Rightarrow n = -8$; $n + 5 = 3 \Rightarrow n = -2$. E adesso siamo sicuri che vi sono solo questi valori e i valori interi sono: 4; –2; 2 e 0.
- $\frac{n+6}{2n+1}$. Stavolta non possiamo ripetere il procedimento precedente, dividiamo i due polinomi, ottenendo: $\frac{11}{2\cdot(2n+1)} + \frac{1}{2} = \frac{1}{2} \cdot \left(\frac{11}{2n+1} + 1 \right)$, perché si ottenga un numero intero, all'interno della parentesi la frazione deve rappresentare un numero intero dispari, quindi $2n + 1 = \pm 1$ oppure $2n + 1 = \pm 11$, che hanno soluzioni $n = 0$, e si ottiene 6; $n = -1$, e vale –5; $n = 5$, otteniamo 1; e $n = -6$, per cui si ha 0.

Prima di procedere è opportuno precisare meglio cosa significa che operiamo in un sistema numerico posizionale a base 10. Lo vediamo meglio nel seguente esempio.

Esempio 4.

- Il numero 278 si può esprimere nella forma *polinomiale*: $2 \cdot 10^2 + 7 \cdot 10 + 8$.
- Il numero –4577 si può esprimere come: $-4 \cdot 10^3 + 5 \cdot 10^2 + 7 \cdot 10 + 7$.

Possiamo quindi affermare che un generico numero intero $a_n a_{n-1} \ldots a_2 a_1 a_0$ di $(n + 1)$ cifre, si esprime nella forma: $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \cdot 10^0$. Proprio a causa di questa modalità si hanno diverse proprietà dei numeri interi che a prima vista possono sembrare vere e proprie "magie".

Esempio 5.

Il seguente schema dovuto al matematico Edouard Lucas (1842 – 1891), che oltre ad essere un grande studioso di teoria dei numeri, si occupò di *matematica ricreativa*, scrivendo alcuni dei testi più importanti come *Récréations mathématiques* del 1894 e *L'arithmétique amusante* del 1895. Proprio nel primo presenta la seguente catena di uguaglianze:

$$1 \cdot 9 + 2 = 11$$
$$12 \cdot 9 + 3 = 111$$
$$123 \cdot 9 + 4 = 1111$$
$$1234 \cdot 9 + 5 = 11111$$
$$12345 \cdot 9 + 6 = 111111 \quad .$$
$$123456 \cdot 9 + 7 = 1111111$$
$$1234567 \cdot 9 + 8 = 11111111$$
$$12345678 \cdot 9 + 9 = 111111111$$
$$123456789 \cdot 9 + 10 = 1111111111$$

Osserviamo che in forma polinomiale $\underbrace{111\ldots1}_{n+1} = 1 \cdot 10^n + 1 \cdot 10^{n-1} + \ldots + 1 \cdot 10^2 + 1 \cdot 10 + 1 \cdot 10^0$. D'altro canto $[12345 \ldots (n-1)n] \cdot 9 + (n+1) = [1 \cdot 10^{n-1} + 2 \cdot 10^{n-2} + \ldots + (n-1) \cdot 10 + n \cdot 10^0] \cdot (10 - 1) + (n + 1) = 1 \cdot 10^n + 2 \cdot 10^{n-1} + \ldots + (n-1) \cdot 10^2 + n \cdot 10^1 - [1 \cdot 10^{n-1} + 2 \cdot 10^{n-2} + \ldots + (n-1) \cdot 10 + n \cdot 10^0] + (n + 1) = 1 \cdot 10^n + 1 \cdot 10^{n-1} + \ldots + 1 \cdot 10^2 + 1 \cdot 10^1 - n \cdot 10^0 + (n + 1) = \underbrace{111\ldots1}_{n+1}$

Esercizi.

1. Determinare per quali valori di n vi sono numeri interi nei seguenti insiemi di frazioni. a) $\frac{2n+11}{2n-3}$; b) $\frac{n+12}{n+15}$; c) $\frac{n^2+n+1}{n^2+n-1}$; d) $\frac{2n+1}{3n-1}$; e) $\frac{4-3n}{n^2+1}$

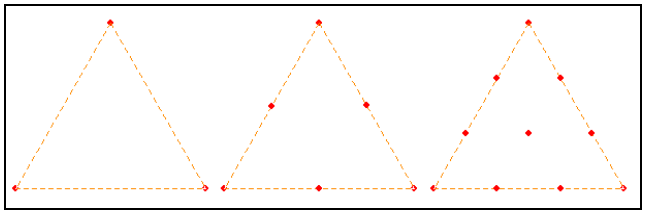
   [a) $n \in \{\pm 2; 1; 5\}$;
   b) $n \in \{-12; -14; -16; -18\}$; c) $n \in \{-2; \pm 1; 0\}$; d) $n \in \{0; 2\}$; e) $n \in \{-2; 0\}$]
2. Dimostrare la validità delle seguenti catene di uguaglianze.
   a) $9 \cdot 9 + 7 = 88$; $98 \cdot 9 + 6 = 888$; ...; $98765432 \cdot 9 + 0 = \underbrace{888...8}_{9}$.

   b) $1 \cdot 8 + 1 = 9$; $12 \cdot 8 + 2 = 98$; …
3. Possiamo generalizzare la 2a)? Se sì come?

   [Solo $987654321 \cdot 9 - 1 = \underbrace{888...8}_{10}$ e $9876543210 \cdot 9 - 2 = \underbrace{888...8}_{11}$]

§2. Numeri figurati

I cosiddetti pitagorici, cioè i seguaci di Pitagora, nato a Samo circa nel 569 a.C. e morto circa nel 475 a.C., avevano una vera e propria adorazione per i numeri interi. Arrivarono così al punto di associare dei numeri a certe figure geometriche, come mostrato nella figura seguente.



In questo caso ai triangoli, abbiamo associato i numeri 3, 6 e 10. Ma come si ottengono questi numeri *triangolari*? Non è difficile capire che ogni numero si ottiene dal precedente aggiungendo un numero naturale che è maggiore di 1 rispetto alla precedente somma. Cioè 6 = 3 + 3, 10 = 6 + 4, così il successivo numero sarà 10 + 5 = 15 e così via. Perciò in generale un numero triangolare è somma dei primi numeri naturali consecutivi. Infatti 1 + 2 = 3, 1 + 2 + 3 = 6, 1 + 2 + 3 + 4 = 10 e così via. Ora la somma di questi numeri si ottiene facilmente con una semplice operazione, che, secondo un aneddoto probabilmente falso, fu scoperta dal grande matematico tedesco Karl Friedrich Gauss (Brunswick 30/04/1777, Göttingen 23/02/1855) all'età di dieci anni. Per esempio supponiamo di volere sommare i primi dieci numeri naturali:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10$$

poiché la somma gode della proprietà associativa, possiamo sistemare gli addendi a nostro piacere e noi lo facciamo considerando il primo con l'ultimo, il secondo con il penultimo e così via: (1 + 10) + (2 + 9) + (3 + 8) + (4 + 7) + (5 + 6), in questo modo vediamo che le somme hanno tutte lo stesso valore: 11. e poiché queste somme sono in numero di 5, possiamo dire semplicemente che

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 11 \cdot 5 = 55.$$

Per trovare una formula generale dobbiamo però esprimere 11 e 5 in funzione dei dieci numeri. 5 è proprio la metà dei numeri, mentre 11 è il successivo di tale numero. Quindi possiamo scrivere: $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = (10+1)\cdot\frac{10}{2}$. Verifichiamo la nostra formula per la somma dei primi 12 numeri naturali:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 = (12+1)\cdot\frac{12}{2} = 13\cdot 6 = 78.$$

Potremmo pensare però che la formula valga solo se i numeri sono pari, dato che se fossero dispari non potremmo accoppiarli:

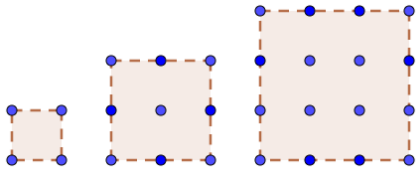
$$(1 + 11) + (2 + 10) + (3 + 9) + (4 + 8) + (5 + 7) + 6 = 12 \cdot 6 = (11+1)\cdot\frac{12}{2} = 72.$$

È facile trovare una formula generale: $1 + 2 + 3 + \ldots + n = \frac{n\cdot(n+1)}{2}$.

Anche se può sembrare strano, come primo numero triangolare non si considera 3, bensì 1. Ogni numero triangolare si indica con T_n, in cui n indica quanti addendi devono sommarsi per ottenerlo. Così $T_1 = 1$, $T_2 = 1 + 2 = 3$, $T_3 = 1 + 2 + 3 = 6$, e così via.

Esempio 6.

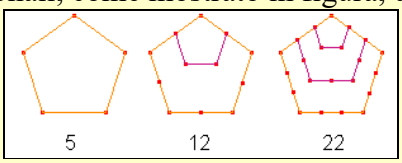
Fra i numeri triangolari alcuni sono dei quadrati perfetti, per esempio lo sono $T_1 = 1$, $T_8 = \frac{8\cdot 9}{2} = 36$ e $T_{49} = \frac{49\cdot 50}{2} = 1225$. Da quello che abbiamo visto possiamo dire che è un quadrato perfetto se è prodotto di un quadrato perfetto per il doppio di un quadrato perfetto. Dobbiamo perciò cercare i quadrati fra gli T_n, in cui n è un quadrato perfetto (come 1 e 9), o un numero che precede un quadrato perfetto, come 8.



Possiamo anche costruire numeri quadrati , che ovviamente rispondono alla sempice legge: $Q_n = n^2$. Più in generale possiamo considerare i numeri poligonali, che indichiamo con $P_n^{(r)}$, dove n indica il numero di lati del poligono, mentre r indica il cosiddetto *rango* del numero, ossia il passo che facciamo nella costruzione. Pertanto i tre numeri quadrati nella figura precedente li indicheremo con $P_4^{(2)}, P_4^{(3)}, P_4^{(4)}$, mentre un generico numero triangolare si indica con $P_3^{(n)}$. Per definizione abbiamo $P_n^1 = 1, \forall n \in \mathbb{N}, n \geq 3$.

Esempio 7.

Costruiamo i numeri pentagonali, come mostrato in figura, quanto vale il successivo?



Considerando il primo numero pentagonale uguale a 1, osserviamo che il terzo numero pentagonale si ottiene dal secondo aggiungendo altri 7 punti, quindi $P_5^{(2)} = P_5^{(2)} + 7 = 12$. Allo stesso modo $P_5^{(4)} = P_5^{(3)} + 10 = 22$, Non è difficile capire perciò che ogni numero pentagonale è uguale al precedente più un addendo che è 3 unità in più del precedente addendo, così $P_5^{(5)} = P_5^{(4)} + 10 + 3 = 35$.

Teorema 2. Si ha: $P_5^{(r)} = \frac{r\cdot(3r-1)}{2}$.

Dimostrazione.

Dall'esempio precedente possiamo scrivere:

$$P_5^{(2)} = P_5^{(1)} + (1+3\cdot 1); P_5^{(3)} = P_5^{(2)} + (1+3\cdot 2); P_5^{(4)} = P_5^{(3)} + (1+3\cdot 3); P_5^{(5)} = P_5^{(4)} + (1+3\cdot 4)$$

Per cui in generale possiamo dire che si ha: $P_5^{(r)} = P_5^{(r-1)} + [1+3\cdot(r-1)]$, quindi andando a ritroso:

$$P_5^{(r)} = P_5^{(r-2)} + [1+3\cdot(r-2)] + [1+3\cdot(r-1)] = P_5^{(r-2)} + 2 + 3\cdot[(r-1)+(r-2)] =$$

$$= P_5^{(r-3)} + 3 + 3\cdot[(r-1)+(r-2)+(r-3)] = \ldots = P_5^{(1)} + (r-1) + 3\cdot[(r-1)+(r-2)+\ldots+1] =$$

$$= 1 + (r-1) + 3\cdot\frac{r\cdot(r-1)}{2} = \frac{2+2\cdot(r-1)+3r\cdot(r-1)}{2} = \frac{3r^2-r}{2} = \frac{r\cdot(3r-1)}{2}$$

Più in generale vale il seguente risultato di cui omettiamo la dimostrazione.

Teorema 3. Si ha: $P_n^{(r)} = \dfrac{r\cdot\left[(r-1)n-2\cdot(r-2)\right]}{2}$.

Vi è anche un modo per determinare se un dato numero è poligonale di qualche rango.

Teorema 4. Se $8N\cdot(n-2)+(n-4)^2 = x^2$, allora $N = P_n^{(r)}$, con $r = \dfrac{x+n-4}{2\cdot(n-2)}$.

Dimostrazione.

Per il Teorema 3 si ha: $N = P_n^{(r)} = \dfrac{r\cdot\left[(r-1)n-2\cdot(r-2)\right]}{2}$, per un qualche n, da cui si ha: $\cancel{8}^{4}\cdot\dfrac{r\cdot\left[(r-1)n-2\cdot(r-2)\right]}{\cancel{2}}\cdot(n-2)+(n-4)^2 = (4nr^2 - 4nr - 8r^2 + 16r)\cdot(n-2) + n^2 - 8n + 16 = 4n^2r^2 - 8nr^2 - 4n^2r + 8nr - 8nr^2 + 16r^2 + 16nr - 32r + n^2 - 8n + 16 = (2rn - 4r - n + 4)^2$. Per determinare il rango abbiamo: $x = 2rn - 4r - n + 4$ e quindi ricavando rispetto ad r, otteniamo quanto voluto.

Esempio 8.

- 28 è un numero esagonale, infatti: $8\cdot 28\cdot(6-2)+(6-4)^2 = 30^2$, il suo rango è $r = \dfrac{30+6-4}{2\cdot(6-2)} = \dfrac{32}{8} = 4$, quindi $28 = P_6^{(4)}$.
- 100 non è un numero ottagonale: $8\cdot 100\cdot(8-2)+(8-4)^2 = 4816$, che non è un quadrato perfetto.

Esercizi.

1. Osserviamo che $1^3 = T_1^2$, $1^3 + 2^3 = 9 = T_2^2$, $1^3 + 2^3 + 3^3 = 36 = T_3^2$. Senza effettuare i calcoli, quanto fa $1^3 + 2^3 + 3^3 + 4^3 + 5^3$?
2. Osserviamo che $8T_1 + 1 = 9$, $8T_2 + 1 = 25$, $8T_3 + 1 = 49$. Senza effettuare i calcoli, quanto fa $8T_4 + 1$?
3. Quali fra i seguenti è un numero triangolare: 91, 106, 153, 170, 190, 231?
4. Osserviamo che $T_1 + T_2 = 4$, $T_2 + T_3 = 9$, $T_3 + T_4 = 16$. Senza fare conti possiamo ipotizzare quanto fa $T_{10} + T_{11}$?
5. Determinare i primi 5 numeri esagonali, verificando che confermano il Teorema 4.
6. Possiamo dire che $P_5^{(6)} = P_5^{(5)} + x$. Quanto vale x? **[16]**
7. Trovare altri due numeri triangolari che siano quadrati perfetti, oltre i tre da noi mostrati. $\left[P_3^{(288)}; P_3^{(1681)}\right]$

Esprimere le seguenti espressioni mediante un solo numero poligonale

8. a) $P_5^{(4)} - P_3^{(3)}$; b) $P_5^{(r)} - P_3^{(r-1)}$; c) $14P_3^{(2)} + 2P_3^{(3)} + 1$; d) $6P_3^{(r)} + r + 1$

$\left[\text{a)} P_4^{(4)};\ \text{b)}\ P_4^{(r)}; \text{c)}\ P_3^{(10)}; \text{d)}\ P_8^{(r+1)}\right]$

9. a) $P_3^{(r)} + P_3^{(r+1)}$; b) $8P_3^{(r)} + 1$; c) $3P_3^{(r)} + r + 1$; d) $3P_3^{(r)} + P_3^{(r+1)}$; e) $4P_3^{(r)} + r + 1$

$\left[\text{a)}\ P_4^{(r+1)};\ \text{b)}\ P_4^{(r+2)}; \text{c)}\ P_5^{(r+1)}; \text{d)}\ P_3^{(2r+1)}; \text{e)}\ P_6^{(r+1)}\right]$

10. Tenuto conto di alcuni degli esercizi precedenti esprimere $nP_3^{(r)} + r + 1, n \geq 2$.

$\left[P_{n+2}^{(r+1)}\right]$

11. Provare che $P_4^{(r)} + P_3^{(r-1)} = P_5^{(r)}$.
12. Determinare una relazione fra $P_n^{(r)}$ e $P_n^{(r-1)}$. $\left[P_n^{(r)} = P_n^{(r-1)} + (r-1)(n-1) - r + 2\right]$

§3. I numeri primi.

Vedremo in seguito di trovare una formula che ci permetta di calcolare quanti divisori ha un numero senza trovarli uno per uno. Intanto osserviamo che, come notato nell'esempio 1, ogni numero ha certamente almeno due divisori: l'unità ed il numero stesso. Risulta opportuno caratterizzare quei numeri che hanno solo due divisori.

Definizione 4. Un numero che ha solo due divisori distinti viene detto numero **primo**.

In seguito vedremo perché abbiamo aggiunto alla definizione precedente il fatto che i divisori debbano essere distinti.
Non è facile stabilire, in generale, se un dato numero è o no primo. È però vero che di numeri primi ve ne sono quanti ne vogliamo. Ciò è stabilito da un teorema che fu enunciato e dimostrato da Euclide, la cui dimostrazione rimane uno dei più bei esempi di eleganza nell'intero campo delle discipline matematiche.

Teorema 5. (di Euclide). Esistono infiniti numeri primi.
Dimostrazione. La dimostrazione avviene per assurdo. Supponiamo che i numeri primi siano finiti, li possiamo quindi ordinare nel modo seguente: p_1, p_2, p_3, ... , p_h. Consideriamo adesso il numero $p_1 \cdot p_2 \cdot p_3 \cdot \ ... \ \cdot p_h$. Esso è naturalmente divisibile per tutti i numeri primi, per la definizione stessa di divisori. Invece il numero $n = p_1 \cdot p_2 \cdot p_3 \cdot \ ... \ \cdot p_h + 1$ non è divisibile per nessuno dei detti numeri primi, dato che la divisione del numero n per uno qualsiasi dei numeri p_i ha per resto 1. Questo vuol dire che il numero n è a sua volta un numero primo o che è divisibile per un numero primo diverso dai p_i. Ciò è appunto assurdo, dato che abbiamo detto che non vi sono altri numeri primi tranne quelli scritti.

Esempio 9.
Costruiamo la seguente tabella utilizzando il procedimento usato da Euclide nella dimostrazione del teorema 5.

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 421$	Numero primo
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$	Numero primo
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$	Composto da $59 \cdot 509$
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511$	Composto da $19 \cdot 97 \cdot 277$
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1 = 9699691$	Composto da $347 \cdot 27953$

Notiamo che nei primi due casi abbiamo ottenuto due numeri primi, entrambi maggiori di quelli che li hanno "generati", negli altri due casi due numeri composti ma ciascuno contenente almeno un numero primo maggiore, quindi diverso, di tutti i numeri primi che lo hanno "generato".

In seguito fu provato, da Lejeune Dirichlet (1805 – 1859), un risultato ancora più interessante, la cui dimostrazione è però molto più complicata. Il grande matematico tedesco, noto soprattutto per la funzione che porta il suo nome e che costituisce un esempio di una funzione discontinua in ogni punto, dimostrò il seguente teorema.

Teorema 6. (di Dirichlet) Ogni progressione aritmetica di primo termine a e di ragione d, con a e d numeri interi privi di divisori comuni, contiene infiniti numeri primi.

Dimostrazione Dimostriamo solo il caso particolare della progressione di termine generale $4n - 1$, la dimostrazione generale è alquanto complessa. Operiamo ancora per assurdo, supponendo quindi che esistano solo un numero finito di primi, che indichiamo con $p_1, p_2, p_3, ..., p_n$, che hanno la forma predetta. Consideriamo quindi il numero $N = 4 \cdot (p_1 \cdot p_2 \cdot p_3 \cdot \ ... \cdot p_n) - 1$. Ragionando come abbiamo fatto nella dimostrazione del teorema di Euclide possiamo dire intanto che N non è divisibile per nessuno dei p_i e che tale numero o è primo, e abbiamo finito, o contiene un primo P diverso dai p_i. Tale numero deve certamente essere dispari perché N è dispari. Ogni numero dispari può scriversi come elemento della progressione $4n - 1$ o della progressione $4n + 1$, dato che la divisione di un numero dispari per 4 fornisce resto uguale a 1 o a 3 (che equivale a 4 – 1). Se P avesse la forma $4n + 1$ e se tutti gli altri fattori di N (potendo anche essere tutti uguali a P), hanno questa forma anche N deve avere tale forma, dato che $(4n + 1) \cdot (4m + 1) = 16mn + 4n + 4m + 1 = 4 \cdot (4mn + n + m) + 1$. Tale fatto è certamente assurdo.

Adesso consideriamo un procedimento simile a quello utilizzato da Euclide per la dimostrazione dell'infinità dell'insieme dei numeri primi. Consideriamo cioè non il prodotto dei soli primi consecutivi, ma il prodotto di tutti i numeri interi consecutivi fino ad un dato valore. Costruiamo cioè la tabella dei numeri esprimibili nella forma $n! + 1$ (ricordiamo che il simbolo $n!$ si legge n fattoriale e rappresenta il prodotto dei primi n numeri naturali. Per esempio $4! = 1 \cdot 2 \cdot 3 \cdot 4$).

n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
***n*! + 1**	3	7	25	121	721	5041	40321	362881	3628801
Fattori	3	7	5^2	11^2	$7 \cdot 103$	71^2	$61 \cdot 661$	$19 \cdot 71 \cdot 269$	$11 \cdot 329891$

La prima idea che poteva venirci è che $n! + 1$ potesse essere primo se lo era n, ma si nota che ciò è vero per $n = 2$ e 3 ma non per 7, continuando la tabella si vedrebbe che lo è anche per $n = 11$, ma non lo è per $n = 13$. Quindi dobbiamo abbandonare questa idea. Notiamo invece un altro fatto: se n è un numero primo $(n - 1)! + 1$ è divisibile per n (non abbiamo considerato $1! + 1$, ma vale anche per tale valore). Questa congettura è avvalorata da un ridotto numero di termini, costruiamo perciò la seguente tabella, con l'aiuto di un CAS (non dimentichiamo che $28! + 1$ ha 30 cifre!).

n	**3**	**5**	**7**	**11**	**13**
(*n* – 1)!+ 1	3	25	$7 \cdot 103$	$11 \cdot 329.891$	$13 \cdot A$
n	17	19	23	29	
(*n* –1)! + 1	$17 \cdot 61 \cdot 137 \cdot B$	$19 \cdot 23 \cdot 29 \cdot 61 \cdot 67 \cdot C$	$23 \cdot 521 \cdot D$	$29 \cdot E$	

Per semplificare abbiamo indicato con A = 2834329; B = 105951; C = 123610951; D = 93799610095769647; E = 10513391193507374500051862069

In effetti adesso la congettura è più ragionevole, possiamo quindi enunciare il seguente risultato.

Teorema 7. Ogni numero primo p è tale che $(p - 1)! + 1$ è divisibile per p.

Secondo Ore [O] questo teorema fu enunciato da Waring nel suo libro *Meditationes algebricae* del 1770, che però lo cita come risultato di un suo studente: John Wilson (1741 – 1793). In effetti era stato ipotizzato già da Leibniz e fu provato da Lagrange nel 1771. Per curiosità ricordiamo che Wilson abbandonò ben presto gli studi matematici a Cam-

bridge per quelli giuridici. In seguitò si laureò in legge e divenne giudice. Visto che anche Fermat e molti altri grandi matematici furono uomini di legge, sarebbe forse interessante stabilire delle connessioni fra le due discipline, soprattutto se pensiamo al fatto che in matematica si ragiona su mondi fantastici, stabilire che un teorema è errato o che un assioma non è ben scelto non riguarda quasi mai danni alla salute pubblica di alcuno, a parte di quella mentale del matematico che si occupa di tali fatti. Invece nella legge sbagliare una sentenza, o una ipotesi di colpevolezza ha ripercussioni molto forti e profonde sugli imputati e sulla società in generale.
Non lo dimostriamo ma nel paragrafo sulle congruenze forniremo una traccia su un caso particolare. Intanto costruiamo l'analoga tabella per i numeri non primi.

n	**4**	**6**	**8**	**9**
(*n* – 1)! + 1	7	11^2	71^2	$61 \cdot 661$
n	**10**	**12**	**14**	**16**
(*n* – 1)! + 1	$19 \cdot 61 \cdot 269$	39916801	$83 \cdot 75024347$	$59 \cdot 479 \cdot 46271341$

Questa tabella ci suggerisce di enunciare il seguente teorema.

Teorema 8. Ogni numero composto n è tale che $(n-1)! + 1$ non è divisibile per n.
Dimostrazione Consideriamo prima un caso particolare, per capire la struttura della dimostrazione. Consideriamo per esempio $60 = 2^2 \cdot 3 \cdot 5$ e consideriamo $59! + 1$. Ovviamente $59!$ contiene tutti i fattori di 60, anche più di una volta, quindi è divisibile per 60 e perciò $59! + 1$ non lo è. In generale se consideriamo $n = p_1^{a_1} \cdot p_1^{a_1} \cdot \ldots \cdot p_h^{a_h}$ e poi consideriamo $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$, possiamo dire che questo numero contiene almeno una volta tutti i fattori di n, quindi è divisibile per n e perciò $(n-1)! + 1$ non è divisibile per n.

Quindi possiamo riunire i precedenti risultati nell'unico seguente risultato:

Teorema 9. (di Wilson) Un numero p è primo se e solo se $(p-1)! + 1$ è divisibile per p.

Quindi il teorema di Wilson costituisce un criterio di primalità, ossia permette di stabilire se un numero è o no primo. Purtroppo, come succederà con altri test che presenteremo in seguito, esso è efficace ma non efficiente. Infatti per verificare che 29 è un numero primo dovremmo stabilire che $28! + 1$, un numero di ben 30 cifre, è divisibile per 29.

Esercizi.

1. Mediante un software di tipo CAS costruire una tabella del tipo di quella presentata nell'esempio 9.
2. Costruire una tabella analoga a quella da noi costruita considerando i numeri $p_1 \cdot p_2 \cdot p_3 \cdot \ ... \ \cdot p_h - 1$.
3. Osserviamo che le due tabelle di cui all'esercizio precedente forniscono numeri con cifra delle unità sempre uguale ad 1 e a 9 rispettivamente. Possiamo dire che ciò vale sempre? Giustificare la risposta.
4. Dimostrare il teorema di Dirichlet per la progressione di termine generale $6n - 1$.
5. Mostrare che la dimostrazione del teorema di Dirichlet utilizzata per la progressione $4n - 1$, non è utile per le progressioni $4n + 1$ e $8n - 1$.
6. Costruire una tabella dei primi 10 termini delle progressioni di termine generale $4n + 1$, $4n + 3$ e $6n + 5$, evidenziando i numeri primi.
7. Utilizzando un software di tipo CAS costruire la tabella dei valori $(n - 1)! + 1$ per n da 18 a 50.
8. Determinare se una proprietà analoga a quella stabilita dal teorema di Wilson vale anche per $(n - 1)! - 1$.
9. Provare che un numero primo della forma $p = 4n - 1$ non può esprimersi come somma di due quadrati.
10. Verificare sui numeri primi minori di 100 della forma $p = 4n + 1$ che possono esprimersi come somma di due quadrati in un solo modo. Esempio $5 = 1^2 + 2^2$.
11. Dato $n!$ possiamo stabilire qual è la massima potenza di un numero primo p che lo divide, provando che essa è data da $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ... + \left\lfloor \frac{n}{p^k} \right\rfloor, p^k \le n < p^{k+1}$, in cui il simbolo $\lfloor x \rfloor$ indica il cosiddetto *pavimento* del numero reale x, ossia il più grande numero intero minore o uguale a x. Provare questo fatto.
12. Stabilire la massima potenza di 7 che divide 1000!. [164]

§4. La distribuzione dei numeri primi.

Nonostante i numeri primi siano infiniti la loro distribuzione non segue una legge "regolare", per esempio nei numeri da 1 a 10 vi sono ben 4 numeri primi (2, 3, 5, 7), lo stesso accade nei numeri da 11 a 20 (11, 13, 17, 19) mentre nei numeri da 21 a 30 essi divengono solo 2 (23, 29). Nei primi 100 interi vi sono 25 numeri primi. Nei numeri da 200 a 300 ve ne sono 21. Da 300 a 400 ve ne sono 16. Andando di questo passo fino a 1000 troviamo in ogni centinaio 16, 17, 14, 16, 14, 15 e 14 numeri primi. Utilizzando un consueto procedimento induttivo potrebbe congetturarsi che *al limite*, ogni cento numeri interi ve ne saranno 14 o 15 che sono primi. Tutto falso! Infatti considerando i numeri da 10^7 a 10^8 di numeri primi ve ne sono solo 2. Ma vi è di più, possiamo trovare intervalli di grandezza arbitraria in cui non vi è neanche un numero primo. Per esempio nell'intervallo dei numeri che vanno dal numero immenso $10^7! + 2$ a $10^7! + 10^7$, che contiene ben 9999999 numeri interi, nessuno di essi è un numero primo! Infatti il generico numero $10^7! + n$ ha certamente come uno dei suoi fattori il numero n, cosi avremo: $10^7! + 2 = 2 \cdot (A + 1)$ in cui $A = 10^7!/2$; $10^7! + 3 = 3 \cdot (B + 1)$ in cui $B = 10^7!/3$ e in generale $10^7! + n = n \cdot (Z + 1)$ in cui $Z = 10^7!/n$. Visto che la matematica spesso "generalizza", riusciamo a trovare intervalli di ampiezza "grande" a piacere in cui non vi è neanche un numero primo. Basta considerare l'intervallo $[n! + 2, ..., n! + n]$, assegnando ad n il valore desiderato. A questo punto potremmo avere un'altra idea sbagliata, cioè che all'aumentare di n i numeri primi tendono a sparire, ma ciò è in contrasto con il teorema di Euclide.
In effetti Gauss (sempre lui!) pensò di valutare piuttosto che la quantità di numeri primi in un dato intervallo o più in generale di numeri primi minori di un dato numero, il rapporto fra tale quantità ed il totale degli elementi. Cioè, indicando con il simbolo $\pi(n)$ il numero dei primi minori di un dato numero intero n, Gauss pensò di valutare il rapporto $\pi(n)/n$. Così facendo ottenne delle tabelle simili a questa che qui presentiamo.

n	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$\pi(n)$	168	1229	9592	78498	664579	5761455	50847478
$\pi(n)/n$	0,168	0,1229	0,09592	0,078498	0,0664579	0,05761455	0,050847478

Qui la sensazione che la successione $\pi(n)/n$ sia convergente è più netta, anche se non appare ancora il limite a cui essa sembra convergere. Gauss però notò che i valori ottenuti erano "abbastanza" vicini a quelli della successione: $1/ln(n)$. Aggiungiamo allora una quarta colonna alla precedente tabella in cui inseriamo i valori della detta successione approssimati allo stesso numero di cifre dei valori della terza colonna. Nella quinta colonna tabuliamo le differenze fra i valori della terza e quarta colonna, che ci danno l'errore, con quattro cifre decimali, che si commette considerando il valore di $1/ln(n)$ come approssimazione di quello di $\pi(n)/n$.

n	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$\pi(n)$	168	1229	9592	78498	664579	5761455	50847478
$\frac{\pi(n)}{n}$	0,168	0,1229	0,09592	0,078498	0,0664579	0,05761455	0,050847478
$\frac{1}{ln(n)}$	0,144	0,1085	0,08685	0,072382	0,0620420	0,05428681	0,048254942
$\frac{\pi(n)}{n} - \frac{1}{ln(n)}$	0,0240	0,0144	0,0090	0,0061	0,0041	0,0033	0,0025

Notiamo che in effetti la tabella fornisce un ottimo punto di partenza per avvalorare la congettura di Gauss. Questa ovviamente è solo una verifica, una conferma che la congettur possa essere corrette e non una sua dimostrazione. Bisognò attendere il 1896 perché la congettura diventasse una verità matematica, ossia un teorema. Lo provarono due distinti matematici ciascuno indipendentemente dall'altro, Jacques Hadamard (1865 – 1963) a Parigi e Charles Jean Gustave Nicolas de la Vallée Poussin (1866 – 1962) a Lovanio.

Teorema 10. (di Hadamard – de la Vallée Poussin)

Vale la seguente uguaglianza: $\lim_{n\to\infty}\left[\frac{\pi(n)}{n}-\frac{1}{ln(n)}\right]=0$.

§5. Il crivello di Eratostene.

Un altro sogno dei matematici è stato quello di determinare una formula che potesse generare tutti i numeri primi. Ciò si è rivelato di una difficoltà enorme, tanto è che ancora ai giorni nostri uno degli algoritmi più efficaci (anche se la sua efficienza diminuisce per numeri molto "grandi") per determinare tutti i numeri primi è un risultato ottenuto nel III sec. a.C., il cosiddetto crivello di Eratostene. Esso è dovuto ad un matematico greco nato a Cirene nel 276 a.C. e morto nel 194 a.C., che fu bibliotecario della famosa biblioteca di Alessandria e che è noto anche per aver determinato con buona approssimazione la misura del raggio terrestre. È anche famoso poiché risulta il "destinatario" de *Il metodo*, opera minore di Archimede in cui questi descrive il suo metodo di scoperta di molte formule per il calcolo dei volumi di alcuni corpi rotondi.
Il metodo di Eratostene per la determinazione dei numeri primi, consiste in una vera e propria "decimazione" dei numeri naturali da cui eliminiamo i numeri composti. Esso parte dall'osservazione elementare che se n è un numero primo $m \cdot n$ è sempre un numero composto per ogni m numero intero maggiore di 1. Basta quindi, partendo dal numero 2 che risulta il primo numero primo, eliminare tutti i numeri che si trovano nelle posizioni 4, 6, 8, e via dicendo perché tutti divisibili per 2. Il primo numero non eliminato dopo questo procedimento, in questo caso il 3, deve essere per forza primo perché se non lo avremmo già eliminato, Quindi adesso togliamo tutti i numeri multipli di 3, che perciò occupano le posizioni 3, 6, 9, ecc. In questo modo ovviamente elimineremo numeri già eliminati in precedenza come il numero 6 e tutti i multipli pari di 3. Ancora una volta il primo numero non eliminato successivo al 3, cioè il 5, è primo. Elimineremo dunque ogni numero che occupa le posizioni 5, 10, 15 e via dicendo. L'algoritmo è certamente efficace, ma poco efficiente, poiché per determinare per esempio i 25 numeri primi contenuti nei numeri da 1 a 100 dobbiamo effettuare ben 146 fra eliminazioni e controlli, dato che ad ogni passo successivo al primo ci troveremo ad eliminare o comunque a controllare se lo sono, elementi già eliminati nei passi precedenti. Potremmo pensare di eliminare in modo definitivo i numeri già tolti, ma questo scombussola il metodo. Infatti se dopo il primo passaggio l'insieme su cui operare diventa {2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, …}, allora a partire da 3, ogni terzo numero sarà divisibile per 3 e va bene. Ma se poi l'insieme diventa {2, 3, 5, 7, 11, 13, 17, 19, …}, il quinto numero che segue 5 è 19, che non solo non è multiplo di 5, ma è primo e quindi non deve essere eliminato.
Nella seguente tabella consideriamo quante eliminazioni o controlli dobbiamo effettuare per determinare ciascuno dei primi 15 numeri primi. Per comodità indichiamo con $d(n)$ i numeri minori o uguali a 100 divisibili per n.

n	**2**	**3**	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	**31**	**37**	**41**	**43**	**47**
$d(n)$	49	32	19	13	18	6	4	4	3	2	2	1	1	1	1

Notiamo che nella tabella non abbiamo messo i successivi 10 numeri primi minori di 100 perché per essi non faremo alcun controllo, dato che nel momento in cui abbiamo trovato 47 abbiamo trovato anch'essi, perché $2 \cdot 47 = 98$ e quindi tutti i numeri rimasti se fossero composti sarebbero stati multipli di primi già trovati e quindi sarebbero stati eliminati. In effetti possiamo arrestare prima il nostro procedimento di selezione, precisamente possiamo fermarci alla determinazione del numero 7. Infatti l'ultimo numero composto che andremo a cancellare sarà $77 = 7 \cdot 11$, a questo punto possiamo affermare con certezza che non vi saranno più numeri composti da cancellare, per quanto abbiamo

già spiegato. In tal modo il numero di eliminazioni e controlli si riduce a 113, che è comunque un valore ugualmente elevato relativamente alla cardinalità (100) dell'insieme considerato, ed al fatto che di numeri dobbiamo eliminarne solo 74 (1 non va eliminato, anche se non è primo).
Come si vede il crivello di Eratostene è un metodo che in linea teorica funziona, ma per valori molto elevati può dare diversi problemi. Supponiamo allora di voler stabilire se un dato numero naturale n è o no primo. Applicando la definizione 4, dovremmo operare $(n - 1)$ divisioni e nell'ipotesi in cui nessuna di queste sia "esatta" (abbia cioè resto zero), concluderemmo che n è primo. In effetti, tenendo conto di quanto abbiamo già detto sui divisori di un numero, ossia che essi sono presenti sempre a coppie, potremmo limitare i controlli solo per i numeri fino a $\lfloor \sqrt{n} \rfloor + 1$. Il simbolo precedente indica il cosiddetto pavimento di un numero, ossia il più grande numero intero che contiene il numero. Per esempio $\lfloor 2{,}3 \rfloor = 2$. In questo modo siamo sicuri di stare considerando un numero intero, dato che in generale la radice quadrata di un numero naturale non lo è. Infatti, se dovessimo stabilire se il numero 293 è o no primo (in effetti lo è), verificato che fino alla divisione di 293 per $\lfloor \sqrt{293} \rfloor + 1 = 16 + 1 = 17$ non abbiamo ottenuto alcun resto nullo, concludiamo che 293 è primo. Ciò dipende dal fatto che, se esistessero divisori di 293 superiori a 17 essi dovrebbero avere associato un divisore inferiore a 17, che quindi dovremmo avere già trovato. Con questa osservazione abbiamo ridotto il numero dei controlli da $n - 1$ a $\lfloor \sqrt{n} \rfloor + 1$, che per valori di n elevati è un bel risparmio. Si pensi che per verificare che 4999 è un numero primo, con questa osservazione dobbiamo effettuare solo 71 controlli invece che 4998. Per valori di n molto grandi il vantaggio è irrilevante, infatti per verificare se un numero con 20 cifre, cioè dell'ordine di 10^{19}, è o no primo dobbiamo fare, nell'ipotesi in cui il numero sia primo, circa 10^{10} controlli che sono un numero considerevole anche per i velocissimi processori attuali. Dobbiamo quindi determinare dei metodi "migliori". Ne vedremo qualcuno nei prossimi paragrafi.

Esercizi.

1. Usando il crivello di Eratostene per determinare tutti i 168 numeri primi minori di 1000, qual è l'ultimo numero composto che andremo a cancellare? **[961]**
2. Determinare una formula che valuti il numero di eliminazioni da operare con il crivello di Eratostene, per ottenere tutti i numeri primi minori di n, senza contare numeri già controllati. **[$\lfloor n/2 \rfloor + \lfloor n/3 \rfloor + \lfloor n/5 \rfloor \cdot \ldots \cdot \lfloor n/p_k \rfloor$, con p_k il k– esimo numero primo tale che $(p_k)^2 < n < (p_{k+1})^2$]**

§6. Il metodo di Fermat per la fattorizzazione di un numero.

Consideriamo adesso un metodo dovuto al matematico che forse più degli altri ha contribuito allo sviluppo della teoria dei numeri: Pierre Fermat, il principe dei dilettanti come è stato battezzato dallo storico Eric Temple Bell. Tale metodo fu illustrato in una lettera all'abate Marin Mersenne (anche lui figura molto importante nello sviluppo della teoria dei numeri), scritta probabilmente nel 1643. Esso si basa su un fatto molto semplice, cioè sulla scomposizione dei polinomi in fattori. Infatti se un polinomio in una o più indeterminate è scomponibile in fattori, è evidente che il numero che esso rappresenta sostituendo alle sue incognite dati valori è anch'esso un numero composto. Tranne che il polinomio sia scomponibile nel prodotto di due soli fattori, uno dei quali con le sostituzioni risulta uguale ad 1. Vediamo un esempio.

Esempio 10.

Consideriamo il polinomio $x^2 - 5x + 6$. È facile vedere che esso può scomporsi nel prodotto dei due fattori di primo grado: $(x - 2) \cdot (x - 3)$. Sostituendo ad x valori interi superiori a 3 otteniamo sempre numeri naturali, essi risultano composti per ogni valore, tranne che per 4. Infatti per quest'ultimo valore otteniamo $4^2 - 5 \cdot 4 + 6 = (4 - 2) \cdot (4 - 3) = 2 \cdot 1 = 2$. In tutti gli altri casi entrambi i fattori sono diversi da 1, quindi il numero che il polinomio rappresenta è composto.

Pertanto dobbiamo intanto imparare a scrivere un dato numero in forma polinomiale. Il modo più semplice è quello di esprimere il numero mediante la sua espressione decimale. Cioè per esempio per vedere se il numero 319 è o no primo associargli il polinomio $3x^2 + x + 9$ e vedere se esso è o no irriducibile. Se lo è per ogni valore di x allora lo è anche per $x = 10$. Il problema non è però così semplice. Infatti se il polinomio è irriducibile in $\mathbb{Z}$ non significa che tutti i numeri interi che esso rappresenta siano primi per qualsiasi valore assegnato alla x.

Esempio 11.

Il polinomio $3x^2 + x + 9$ non è riducibile in $\mathbb{Z}$, addirittura è irriducibile in $\mathbb{R}$, dato che il suo discriminante è negativo. Ciononostante $319 = 11 \cdot 29$. Anche il polinomio $x^2 + 1$ è irriducibile in $\mathbb{R}$, eppure esso rappresenta numeri pari (quindi composti) per ogni valore dispari sostituito alla x. Ed anche per valori pari, come per esempio $x = 8$, esso rappresenta numeri composti.

Fermat pensò quindi di considerare un altro prodotto notevole: la cosiddetta differenza di quadrati. Se riuscissimo a provare che il numero in questione si può scrivere come differenza di due quadrati potremmo ottenere facilmente una sua fattorizzazione (in generale non di numeri primi). Ma ciò è sempre possibile? Supponiamo che sia $n = a \cdot b$, allora possiamo verificare facilmente che la seguente è una identità:

$$n = a \cdot b = \left(\frac{a+b}{2} - \frac{a-b}{2}\right) \cdot \left(\frac{a+b}{2} + \frac{a-b}{2}\right) = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Nel caso in cui il numero è primo, la precedente identità diviene la seguente:

$$n = 1 \cdot n = \left(\frac{n+1}{2} - \frac{n-1}{2}\right) \cdot \left(\frac{n+1}{2} + \frac{n-1}{2}\right) = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$$

Notiamo che poiché $\frac{n+1}{2}=\frac{n-1}{2}+1$, possiamo dire che ogni numero può esprimersi come differenza dei quadrati di due numeri consecutivi; anzi nel caso dei numeri primi questa è l'unica maniera per esprimerli come differenza di due quadrati.
Pertanto abbiamo trovato una condizione necessaria e sufficiente per determinare se un numero è o no primo ed in caso negativo per trovare una sua fattorizzazione. Il problema è quindi quello di vedere se un dato numero naturale è esprimibile come differenza di quadrati in un solo modo (nel qual caso il numero è primo) o in più di un modo. Vediamo un esempio.

Esempio 12.

Fattorizzare il numero 423877. Cerchiamo il massimo numero naturale il cui quadrato è minore di 423877. Abbiamo che $651^2 = 423801 < 423877 < 425104 = 652^2$. Adesso effettuiamo la differenza fra 652^2 ed il numero dato, ottenendo 425104 – 423877 = 1227. Se tale valore fosse un quadrato perfetto (in effetti non lo è), avremmo finito, diversamente passiamo a considerare la differenza del dato numero dal quadrato successivo a 652. Otteniamo così: $653^2 – 423877 = 2532$ che ancora non è un quadrato perfetto, continueremo questo procedimento, finché troveremo una differenza che sia quadrato perfetto. Nel nostro caso troviamo abbastanza presto che $659^2 – 423877 = 10404 = (10000 + 400 + 4) = 102^2$ e quindi: $423877 = 659^2 – 102^2 = (659 – 102) \cdot (659 + 102) = 557 \cdot 761$.
Osserviamo che con il metodo precedente non abbiamo bisogno di verificare che tutte le differenze ottenute siano quadrati perfetti, ciò in virtù del fatto che le possibili cifre delle unità dei quadrati perfetti, possono essere solo 0, 1, 4, 5, 6, 9[2]. Quindi delle 8 differenze di questo esempio ne verificheremo solo tre ($3839 = 654^2 – 423877$; $6459 = 656^2 – 423877$ e 10404). Anzi proprio per quanto detto potremo evitare di sviluppare certi quadrati; in particolare essendo 7 l'ultima cifra del numero in questione la differenza fra la cifra *u* delle unità di un quadrato e 7 fornirà un "potenziale" quadrato solo se $u \in \{1; 6\}$, quindi prenderemo in considerazione solo quei numeri la cui cifra delle unità appartiene all'insieme {1; 4; 6; 9}.

Visto quanto detto nell'esempio precedente, potremmo raffinare ancor più la ricerca stabilendo una proprietà riguardante le ultime due cifre di un potenziale quadrato e costruendo la seguente tabella, la cui giustificazione lasciamo al lettore[3].

00	01	04	09	16	21	24	25	29	36	41
44	49	56	61	64	69	76	81	84	89	96

Abbiamo prima notato che il procedimento avrà sempre una sua fine e siamo anzi in grado di stabilire il numero massimo di differenze che dobbiamo costruire per verificare se un numero è primo, ovvero per trovare una sua fattorizzazione. Saranno: $\frac{n-1}{2}-\lfloor\sqrt{n}\rfloor-2$. Infatti la prima differenza sarà: $\left(\lfloor\sqrt{n}\rfloor+1\right)^2-n$ e l'ultima, se *n* è primo,

[2] La cifra delle unità di un quadrato è ovviamente quella del quadrato della cifra delle unità dei numeri di una cifra, quindi $1^2 = 9^2 = \mathbf{1}$; $2^2 = 8^2 = \mathbf{4}$; $3^2 = 7^2 = \mathbf{9}$; $4^2 = 6^2 = \mathbf{6}$; $5^2 = \mathbf{5}$

[3] Basta effettuare i quadrati dei numeri da 00 a 99, considerando solo le ultime due cifre. E anche in questo caso possiamo risparmiare moltiplicazioni, osservando che, per esempio $10^2 = 20^2 = \ldots = 90^2 = \mathbf{00}$; $15^2 = 25^2 = 35^2 = \ldots = 95^2 = 25$; e altri

sarà appunto: $\left(\frac{n-1}{2}\right)^2 - n$. Quindi il precedente è sì un test di primalità ma di scarsa applicazione per numeri molto grandi. Per stabilire per esempio che il numero di Mersenne $2^{521} - 1$ (che ha 157 cifre[4]) è primo debbono calcolarsi circa $(10^{157} - 10^{79}) \approx 10^{157}$ differenze. Per inciso il precedente numero viene calcolato con tutte le sue cifre esatte in meno di un secondo e viene verificata la sua primalità, chiedendone la fattorizzazione da TI-nspire CX CAS. Vediamo invece un'applicazione su un numero di livelli "scolastici".

Esempio 13.

Verificare che 2423 è un numero primo. Tenuto conto di quanto già detto sulle cifre delle unità, stavolta considereremo solo le differenze $au^2 - 2423$ con $u \in \{2; 3; 7; 8\}$; costruiremo quindi: $52^2 - 2423$; $53^2 - 2423$; $57^2 - 2423$; $58^2 - 2423$; $62^2 - 2423$; ...; $1211^2 - 2423 = 1212^2$, così l'unica espressione di 2423 come differenza di quadrati sarà: $2423 = 1212^2 - 1211^2$. Il numero è primo.

Nota Biografica

Pierre de Fermat nacque il 17 Agosto 1601 a Beaumont – de – Lomagne e morì il 12 Gennaio 1665 a Castres. Era figlio di un mercante di pelli il cui cognome era semplicemente Fermat. Frequentò prima l'università di Tolosa e poi quella di Bordeaux dove cominciò a fare ricerca in matematica. Non conseguì però alcuna laurea. Poi si trasferì ad Orleàns dove si laureò in legge sul finire del 1630 e nel 1631 cominciò ad esercitare la professione di avvocato. Per tale motivo cambiò il proprio cognome aggiungendovi la particella onorifica de. Pur svolgendo per tutta la sua vita il giurista, si occupò con passione di matematica, tanto da ricevere l'appellativo di *principe dei dilettanti*.
Molto importanti per le sue ricerche furono gli scambi epistolari con l'abate Mersenne e con altri importanti personaggi della sua epoca, quali Pascal e Descartes. Durante la vita non pubblicò mai nulla, ma propose e risolvette importantissimi problemi, diffuse proprio mediante le sue corrispondenze. Il famoso teorema qui ricordato fu da Egli enunciato sul margine di una copia di un libro di un antico matematico: *l'Aritmetica di Diofanto*. È interessante il fatto che egli scrisse di aver trovato un'interessante e bella dimostrazione che non riportava a causa della ristrettezza del margine. In realtà per più di tre secoli le migliori menti non riuscirono a provare il teorema che solo per casi particolari, ossia per particolari valori dell'esponente. Infine nel 1994 l'inglese Andrew Wiles riuscì a dimostrarlo, ma in modo molto più complicato e lungo (la sua dimostrazione è contenuta in due volumi che raccolgono l'intera annata di una famosa rivista matematica) di quel che aveva "promesso" Fermat.

[4] Si ha $2^{521} = (2^{10})^{52} \cdot 2 > (10^3)^{52} \cdot 2 > 10^{156}$

Esercizi.

1. Utilizzare il metodo di Fermat per fattorizzare il numero n che lo stesso matematico francese pose ad esempio: 2027651281. **[44021 · 46061]**
2. Usando il metodo di Fermat determinare una fattorizzazione dei seguenti numeri:
   a) 24047; b) 123456789; c) 1234554321.
   [a) 139 · 173; b) $3^2 \cdot 3607 \cdot 3803$; c) 37 · 367;d) 3 · 7 · 11 · 13 · 37 · 41 · 271]
3. Utilizzando il metodo di Fermat verificare che i seguenti sono numeri primi:
   a) 197; b) 3121; c) 7919.
4. Scriviamo i numeri da 1 a 2023 uno di seguito all'altro. Dire perché l'enorme numero così ottenuto non può essere un quadrato perfetto. **[Finisce per 3]**

§7. Alcuni problemi sui numeri primi.

Dopo le enormi difficoltà di cui abbiamo parlato per la determinazione di formule che generassero solo numeri primi, i matematici abbassarono il tiro. Pensarono cioè di determinare almeno delle formule che generassero solo numeri primi anche se non tutti. Eulero pensò di avere ottenuto il risultato in un articolo del 1772 pubblicato sui *Nouveau Mémoires de l'Académie régal des Sciences*, proponendo l'espressione $x^2 + x + 41$. Infatti, sostituiamo al posto di x i numeri da 0 a 8, ottenendo la seguente tabella:

x	0	1	2	3	4	5	6	7	8
$x^2 + x + 41$	41	43	47	53	61	71	83	97	123

Notiamo che tutti i numeri ottenuti sono primi. Questo potrebbe suggerirci di enunciare il seguente fatto: *Se x è un numero intero positivo allora l'espressione* $x^2 + x + 41$ *rappresenta sempre un numero primo*. In effetti, anche continuando questo procedimento fino a $x = 39$, continuiamo a trovare sempre numeri primi e anche tutti distinti fra di loro. Ciononostante un attento lettore dovrebbe concludere che tale espressione non può generare solo numeri primi, poiché sostituendo alla x il numero 41 o un suo multiplo otterremmo un numero certamente divisibile per 41. Infatti $41^2 + 41 + 41 = 41 \cdot (41 + 1 + 1) = 41 \cdot 43 = 1763$. Ciò significa che affinché si possa trovare una espressione polinomiale che generi solo numeri primi essa deve avere termine noto uguale ad 1 o a –1. In realtà mostriamo che questo fatto è necessario ma non sufficiente.

Teorema 11. Nessuna espressione polinomiale può generare solo numeri primi.
Dimostrazione. Supponiamo che il polinomio $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ generi solo numeri primi quale che sia il valore intero assegnato alla sua variabile x. Supponiamo per esempio che $p(h) = a_0 + a_1 \cdot h + a_2 \cdot h^2 + ... + a_n \cdot h^n = k$, con k numero primo. Consideriamo adesso il valore di p calcolato in $h + m \cdot k$: $p(h + m \cdot k) = a_0 + a_1 \cdot (h + m \cdot k) + a_2 \cdot (h + m \cdot k)^2 + ... + a_n \cdot (h + m \cdot k)^n$, noi diciamo che tale numero non è primo ma è divisibile per k. Infatti consideriamo la differenza $p(h + m \cdot k) – p(h) = a_1 \cdot (h + m \cdot k – h) + a_2 \cdot [(h + m \cdot k)^2 – h^2] + ... + a_n \cdot [(h + m \cdot k)^n – h^n]$. Adesso pensiamo allo sviluppo del quadrato di un binomio, sappiamo che tutti i termini contengono una potenza di $m \cdot k$ tranne il primo che è una potenza "pura" di h. Osserviamo però che tale potenza va ad elidersi con il corrispondente termine posto all'interno della stessa parentesi quadra, che possiede $p(h)$. Quindi il polinomio differenza è divisibile per $m \cdot k$. Ma poiché $p(h)$ è divisibile per k anche $p(h + m \cdot k)$ deve esserlo.

Se la precedente dimostrazione può risultare complicata consideriamo un suo caso particolare.

Esempio 14.
Sia $p(x) = x^2 + x + 41$. Calcoliamo per esempio $p(5) = 25 + 5 + 41 = 71$. Facciamo vedere che $p(5 + 71m)$ è sempre divisibile per 71. Infatti

$$p(5 + 71m) = (5 + 71m)^2 + (5 + 71m) + 41.$$

Consideriamo adesso
$p(5 + 71m) – p(5) = (5 + 71m)^2 + (5 + 71m) + 41 – (25 + 5 + 41) = [25 + 71^2m^2 + 710m – 25] + (5 + 71m – 5) + 41 – 41 = 71m \cdot (71m + 10) + 71m = 71m \cdot (71m + 10 + 1) = 71m \cdot (71m + 11)$.

Poiché $p(5)$ è divisibile per 71 anche $p(5 + 71m)$ deve esserlo. Anzi
$p(5 + 71m) = p(5) + 71m \cdot (71m + 11) = 71 + 71m \cdot (71m + 11) = 71 \cdot (71m^2 + 11m + 1)$.
Verifichiamolo per $m = 2$.

$$p(5 + 142) = 147^2 + 147 + 41 = 21797 = 71 \cdot 307 = 71 \cdot (71 \cdot 2^2 + 11 \cdot 2 + 1).$$

Soprattutto nel '700 sono state ottenute altre espressioni che generano "molti" numeri primi, come per esempio $n^2 + n + 17$ che li genera per ogni n da 0 a 15, o $x^2 - 79x + 1601$ che fornisce numeri primi per ogni x da 0 a 79. Successivamente è stato provato che l'espressione $x^2 + x + 41$ è quella che genera il maggior numero di primi distinti, infatti nell'espressione $x^2 - 79x + 1601$ vi sono diversi numeri che si ripetono.
Nel 1967, H.M. Stork ha pubblicato sul Michican Mathematical Journal il seguente risultato.

Teorema 12.
Nessun trinomio $x^2 + x + a$, con $a > 41$ rappresenta numeri primi per $a - 1$ valori di x.

Visti i risultati del teorema precedente, si è perciò pensato di ricorrere a formule non polinomiali. Già Fermat nel '600 aveva proposto la formula $F_n = 2^{2^n} + 1$. Egli espresse la sua opinione in una lettera a Frénicle del 1640, basandosi sul fatto che la formula forniva valori corretti fino ad $n = 4$, come testimoniato dalla tabella seguente. Potrebbe obiettarsi che quattro valori erano pochi per avvalorare una tale congettura, non deve però dimenticarsi che il successivo valore è 4294967297, un numero molto elevato da trattare senza calcolatrici o senza particolari virtù calcolistiche. Fu infatti il grande Leonhard Euler a scoprire nel 1739 che il detto numero era scomponibile nel prodotto di 641 e 6700417.

n	1	2	3	4
$F_n = 2^{2^n} + 1$	5	17	257	65537

Successivamente, con metodi più raffinati e con l'utilizzo della calcolatrice e dei programmi di matematica simbolica, i quali utilizzano test molto raffinati e complicati, si sono fattorizzati molti altri numeri di Fermat. Allo stato attuale non si sono trovati numeri di Fermat primi per valori di n successivi a 4 e si crede che non ve ne siano altri.
Numeri la cui espressione è molto simile a quelli di Fermat sono quelli cosiddetti di Mersenne. Essi sono i numeri del tipo $M_n = 2^n - 1$. Il loro nome è dovuto al fatto che l'abate Mersenne, di cui abbiamo già parlato, pur non essendo il primo ad interessarsi di questi numeri, nel suo libro *Cogita physico – mathematica* del 1644, enunciò diverse congetture relativamente a tali numeri. Vediamo di costruire una tavola di alcuni di tali valori. Tralasciando $M_0 = 0$, abbiamo le seguenti fattorizzazioni:

n	2	3	4	5	6	7	8
M_n	3	7	15	31	63	127	255
Stato	Primo	Primo	$3 \cdot 5$	Primo	$3^2 \cdot 7$	Primo	$3 \cdot 5 \cdot 17$

Una prima cosa che si nota è che se n è pari, salvo $n = 2$, si ottengono numeri composti. In effetti ciò è vero ed è semplice da dimostrare. Vale cioè il seguente risultato.

Teorema 13. M_n è composto per ogni n composto.
Dimostrazione. Sia infatti $n = a \cdot b$. Abbiamo allora
$2^n - 1 = 2^{a \cdot b} - 1 = 2^{a \cdot b} - 1^b = (2^a - 1) \cdot (2^{a \cdot (b-1)} + 2^{a \cdot (b-2)} + 2^{a \cdot (b-3)} + ... + 2^a + 1)$.

Esempio 15.

Consideriamo $2^{24} - 1 = 2^{3 \cdot 8} - 1 = 2^{3 \cdot 8} - 1^3 = (2^8 - 1) \cdot (2^{2 \cdot 8} + 2^8 + 1)$.

Quindi i numeri di Mersenne possono essere primi solo se n è un numero primo. Nella tabella precedente si nota che in effetti tutti gli M_n sono primi se n è primo. La questione è: è sempre vero? In effetti esso è vero certamente per i primi inferiori a 23, dato che $M_{23} = 8388607 = 47 \cdot 178481$. Lo stesso Mersenne congetturò che, considerati gli esponenti primi minori o uguali a 257, tali numeri sono primi solo per i seguenti valori: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257. Questa congettura si è rivelata falsa, dato che M_{67} e M_{257} non sono primi, mentre lo sono M_{61} (trovato da Pervouchine nel 1883), M_{89} e M_{107} (verificati da Powers nel 1911 e nel 1914). Per curiosità M_{31} fu trovato da Eulero nel 1750 e M_{127} da un altro grande personaggio della teoria dei numeri: Edouard Lucas, nel 1876. In tempi recenti, con i computers sono stati trovati altri 25 numeri primi di Mersenne per valori di n superiori a 257. Il primo di questi è M_{521}, che è un numero di 157 cifre ed è stato trovato da Robinson nel 1952. Questo stesso matematico, sempre nel 1952 ha provato che sono primi M_{607} che ha 183 cifre, M_{1279} che ha 386 cifre, M_{2203} che ha 664 cifre e M_{2281} che ha 687 cifre. Nel 1998 uno studente americano Roland Clarkson, con l'aiuto di Woltman, Kurowski e di un considerevole aiuto di collaboratori sparsi per il mondo, ha trovato $M_{3021377}$, il 37° numero primo di Mersenne, un numero che ha 909526 cifre. Da allora sempre con la collaborazione di migliaia di calcolatori sono stati trovati altri numeri di Mersenne, il più grande, fino al 2022, è il 51° che ha ben 24862046 cifre (!!!!). Per chi volesse avere altre informazioni su tali numeri e sullo stato delle ricerche attorno ad essi vi è il sito internet: **www.mersenne.org/prime.htm**. Rimangono ancora congetture i seguenti fatti: *Vi sono infiniti primi di Mersenne? Vi sono infiniti composti di Mersenne?*
Altri problemi interessanti da poter presentare in classe, sia come curiosità che anche come spunti di lavoro sono i seguenti.
In una lettera datata 7 giugno 1742, Christian Goldbach (1690 – 1764) scrive a Leonhard Euler, che gli è capitato di notare che se prendiamo un numero pari questo può scriversi sempre come somma di due numeri primi. Goldbach e dopo di lui molti altri hanno verificato che questo è vero per tutti i numeri pari fino a 1000, ad un milione ad un miliardo e con l'avvento dei moderni e velocissimi computer anche a valori molto più grandi. Però fino ad oggi nessuno è riuscito a dimostrare la verità o falsità di questa affermazione, che quindi fino a tale data rimane una congettura. Sottolineiamo il fatto che l'aver verificato per un numero sempre maggiore di casi la congettura di Goldbach, ha solo aumentato la probabilità che essa sia vera. Se però un giorno qualcuno riuscisse a provare che essa è vera, per il principio di non contraddizione non si potrà mai dimostrare che essa è falsa. Se ciò dovesse accadere vuol dire che una delle due dimostrazioni (o anche tutte due) è sbagliata. Per il principio del terzo escluso però essa deve certamente essere vera o falsa.
Un'altra interessante congettura di Goldbach è che ogni numero dispari non primo possa esprimersi come somma di 3 numeri primi. Anzi la seconda congettura è una conseguenza della prima. Infatti se avessimo dimostrato che ogni numero pari è esprimibile come somma di due primi, consideriamo un numero dispari, sia per esempio $2n + 1$. Possiamo scrivere $2n + 1 = 3 + 2 \cdot (n - 2)$, essendo il secondo addendo pari, per la pre-

sunta validità della congettura di Goldbach possiamo scrivere $2n + 1 = 3 + p_1 + p_2$, con p_1 e p_2 numeri primi.

Infine un altro problema aperto è quello della infinità dei cosiddetti numeri primi gemelli.

Definizione 5. Due numeri primi p_1 e p_2 si dicono **primi gemelli** se $|p_1 - p_2| = 2$.

Esempi di numeri primi gemelli sono le coppie (3, 5), (5, 7), (11, 13), (17, 19). Una coppia di numeri primi gemelli "abbastanza" grande è 10006427 e 10006429. Nel 2016 è stata scoperta una coppia ciascuno dei quali componenti ha ben 388342 cifre.

Nota Biografica

Leonhard Euler nacque a Basilea il 15 Aprile 1707, figlio di un pastore protestante. Dall'intelligenza vivace e dagli interessi molteplici, è considerato uno dei più eminenti matematici di tutti i tempi. Per i suoi fondamentali risultati in diverse branche delle scienze è paragonato a Leonardo da Vinci ed è considerato l'ultimo grande uomo dagli interessi multiformi. Sin da giovane studiò matematica, teologia, medicina, astronomia, fisica, lingue orientali, sempre con brillanti risultati. Ebbe una famiglia numerosa, ben tredici figli. Fu scienziato di corte presso i più importanti regnanti della sua epoca, fra i quali Federico il Grande di Prussia e Caterina la Grande zarina di Russia. Durante la sua vita pubblicò più di 500 lavori ed è considerato uno degli scienziati più prolifici di tutti i tempi; la sua opera completa comprende più di settanta grossi volumi. Nonostante nel 1771 sia divenuto completamente cieco, grazie all'aiuto dei figli continuò a scrivere copiosamente fino alla morte avvenuta a San Pietroburgo il 18 Settembre 1783. Oltre all'idea dei cerchi per racchiudere gli insiemi, molti altri simboli sono stati da lui inventati: fra i quali quello per il numero e, e quello per l'unità immaginaria.

Esercizi.

1. Provare che l'espressione $n^2 + n + a$, con $a \in \mathbb{N}$, $a > 1$, è divisibile per $(a - 1)$.
2. Determinare una sequenza consecutiva di numeri primi per le espressioni seguenti a) $2n^2 + 29$; b) $6n^2 + 6n + 31$; c) $3n^2 + 3n + 23$.
3. Determinare una sequenza consecutiva di numeri primi per le progressioni aritmetiche seguenti: a) $7 + 30n$; b) $107 + 30n$; c) $7 + 150n$; d) $47 + 210n$; e) $71 + 2310n$.
4. Utilizzare la dimostrazione del teorema 11 per provare che $n^2 + n + 17$ e $n^2 - 79n + 1601$ non possono generare solo numeri primi.
5. Utilizzando un software di tipo CAS, tabulare per un centinaio di valori, facendo scrivere solo i valori per cui essi forniscono numeri primi. a) $n^2 + n + 41$; b) $n^2 + n + 17$; c) $n^2 - 79n + 1601$. **[a) 86 valori; b) 59 valori ; c) 95 valori]**
6. Verificare la congettura di Goldbach per tutti i numeri pari da 4 fino a 50.
7. Tenuto conto dell'esercizio precedente osservare che se $2n = p_1 + p_2$, anche $2n + 2$ e $2n + 4$ verificano certamente la congettura di Goldbach per opportuni valori di p_1 e p_2. Quali? **[$3 + p_2$, $5 + p_2$, e $7 + p_2$]**
8. Possiamo dire che se $2n = p_1 + p_2$ verifica la congettura di Goldbach, in quale caso certamente la verifica anche $2n + 2$?
   [Se almeno una coppia fra $(p_1, p_1 + 2)$ e $(p_2, p_2 + 2)$ e di primi gemelli]
9. Notiamo che alcuni numeri sono esprimibili anche in due modi diversi come somme di due numeri primi. Trovare tutti i numeri pari minori di 50 che non verificano quest'ultima proprietà. **[2, 4, 6, 8, 12]**
10. Trovare il primo numero pari esprimibile in tre modi diversi come somma di due numeri primi. **[22 = 3 + 19 = 5 + 17 = 11 + 11]**
11. Trovare il primo numero pari esprimibile in quattro modi diversi come somma di due numeri primi. **[34 = 3 + 31 = 5 + 29 = 11 + 23 = 17 + 17]**

§8. La scomposizione di un numero in fattori primi.

Dato che i numeri primi appaiono così importanti ed interessanti, pensiamo di utilizzarli nella scomposizione di un numero, cioè nella scrittura di un numero come prodotto di numeri non maggiori di esso. Abbiamo visto infatti che ogni numero non primo (composto) si può esprimere in più di un modo come prodotto di due o più fattori. Se però imponiamo che i fattori siano tutti potenze di numeri primi otteniamo un importantissimo risultato noto come teorema fondamentale dell'aritmetica.

Teorema 14. Ogni numero intero può scomporsi in un solo modo come prodotto di potenze di fattori primi.
Dimostrazione. Proviamo intanto che ogni numero intero può scomporsi come prodotto di numeri primi, poi proveremo che tale scomposizione è unica. Sia un numero composto n. Dato che esso non è primo potrà scriversi come prodotto di almeno due numeri entrambi diversi da 1 e da n. Supponiamo che sia $n = a \cdot b$, con $a < n$ e $b < n$. Se a e b sono entrambi primi abbiamo finito, diversamente ripetiamo il procedimento su a e b o solo su uno dei due se l'altro è primo. Così otteniamo per esempio $a = c \cdot d$ e $b = e \cdot f$, con $c < a < n$, $d < a < n$, $e < b < n$, $f < b < n$. Abbiamo così $a = c \cdot d \cdot e \cdot f$, ancora una volta se tutti i fattori sono primi abbiamo finito, diversamente ripetiamo il procedimento precedente sui numeri che non sono primi. Questo procedimento deve però concludersi perché ad ogni passo troviamo numeri naturali sempre minori, quindi dato che $\mathbb{N}$ è un insieme bene ordinato (cioè ogni suo sottoinsieme ha minimo), deve arrestarsi. Quindi otterremo $n = p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots \ \cdot p_h$, in questa espressione alcuni o tutti i simboli possono rappresentare numeri uguali, applicando quindi le proprietà sulle potenze aventi uguale base, scriveremo $n = \prod_{i=1}^{k} p_i^{a_i}$, in cui tutte le basi rappresentano numeri diversi. Proviamo adesso l'unicità del teorema. Supponiamo che esistano due diverse scomposizioni: $n = \prod_{i=1}^{k} p_i^{a_i} = \prod_{j=1}^{m} q_j^{a_j}$. Poiché ognuno dei numeri primi indicati con p_i divide n deve dividere qualcuno dei q_j, ma poiché entrambi sono numeri primi ciò significa che $p_i = q_j$. Cioè i fattori primi sono gli stessi, quindi entrambe le espressioni contengono le stesse basi. Potrebbe capitare che siano diversi gli esponenti di basi uguali. Ciò non è però possibile. Infatti se per esempio p_1 compare con potenza 3 al primo membro e con potenza 4 al secondo, eliminando il fattore comune $(p_1)^3$ da entrambi i membri ci troveremmo ad avere al secondo membro il fattore p_1 che però manca al primo membro. Fatto assurdo.

Consideriamo un curioso esempio.

Esempio 16.

- Il seguente è una variazione di un quesito proposto nel 1965 dall'Università di Stanford negli Stati Uniti, dove si sono tenuti per molti anni delle famose gare matematiche. Due amiche Anna e Bea si incontrano dopo tanto tempo. Anna chiede a Bea se ha figli e quanti anni ha ciascuno di essi. Bea risponde dicendo che ha tre figli e moltiplicando le loro età s ottiene 36 mentre se li sommiamo otteniamo il numero civico della porta davanti la quale le due sono ferme a parlare. Anna dice che, pur essendo brava in matematica, non riesce a determinare le tre età, allora Bea aggiunge dicendo che il maggiore dei suoi figli ha gli occhi azzurri. Quest'ultima affermazione

sembrerebbe priva di senso, vedremo invece che è effettivamente indispensabile per risolvere il quesito. La prima informazione ci dice che i figli possono avere una delle seguenti tre terne di età: (1, 1, 36), (1, 2, 18), (1, 3, 12), (1, 4, 9), (2, 2, 9), (1, 6, 6), (2, 3, 6), (3, 3, 4); dato che esse sono le uniche terne il cui prodotto fornisce 36. Se le sommiamo otteniamo sempre risultati diversi tranne nei casi $2 + 2 + 9 = 1 + 6 + 6 = 13$. Dato che Anna ha detto di non riuscire a determinare le età dei tre ragazzi esse devono essere ferme davanti ad una abitazione posta al numero 13. La terza informazione svela l'inghippo, dato che la mamma parla di un maggiore, i due gemelli che vi sono fra i tre figli non possono comprendere il primogenito, come accadrebbe nel caso (1, 6, 6). Quindi i bambini hanno 9, 2 e 2 anni.

- Vogliamo provare che $n^3 + 5n$ è divisibile per 6. Fattorizziamo: $n \cdot (n^2 + 11)$. Se n è pari, l'altro fattore è dispari e viceversa, quindi l'espressione è pari. Se n è multiplo di 3 abbiamo finito, se non lo è, vuol dire che diviso per 3 ha resto 1 o 2, cioè $n = 3h + 1 \vee n = 3h - 1$, quindi $n^2 + 11 = (3h + 1)^2 + 11 = 9h^2 + 6h + 1 + 11 = 9h^2 + 6h + 12 = 3 \cdot (3h^2 + 2h + 4)$, che è divisibile per 3. Analogo risultato nell'altra possibilità. Concludiamo perciò che in ogni caso $n^3 + 5n$ è divisibile per 6.

Il primo dei precedenti esempi è molto interessante per diversi motivi. Intanto perché mette in gioco delle informazioni apparentemente prive di senso: gli occhi azzurri del figlio maggiore (in effetti la vera informazione è che vi è un figlio maggiore, ma essa è sviata sul colore degli occhi, informazione effettivamente ininfluente). Poi perché è una applicazione che riesce a stimolare la curiosità dello studente.

Esercizi.

1. Il numero 12 si può scrivere come $2 \cdot 6$ o anche come $3 \cdot 4$, che sono fattorizzazioni distinte, anche se non formate da numeri primi. Esistono numeri che si possono esprimere in un solo modo come prodotto di due numeri nessuno dei quali è uguale a 1? Se la risposta è positiva quali sono? **[I numeri prodotto di due numeri primi]**
2. Con riferimento al quesito precedente, quali sono i numeri che hanno due sole fattorizzazioni? **[I numeri del tipo p^2q, con p e q numeri primi]**
3. Risolvere il problema degli "occhi azzurri" nella sua versione originaria, ossia con il prodotto delle età pari a 72 anni. **[3; 3; 8]**
4. Un quesito da Stanford 1958. Moltiplicando fra loro l'età del capitano, il numero dei suoi figli e la lunghezza della sua barca si ottiene 32118. Il capitano ha figli di entrambi i sessi, ha più anni che figli e ha meno di 100 anni. La barca è misurata in un numero intero di piedi, ed è più di 1 piede. Determinare i tre numeri. **[53 anni, 6 figli, 101 piedi]**
5. Un quesito da Stanford 1960. Delle penne a sfera venivano vendute a 50 cents, ma non avevano molti clienti, così il prezzo fu ridotto e si vendettero tutte quelle rimaste al prezzo complessivo di \$ 31.93. Qual era il prezzo scontato? **[31 cents]**
6. Un quesito da Stanford 1963. Provare che $n^2 \cdot (n^2 - 1) \cdot (n^2 - 4)$ è divisibile per 360 qualunque sia n numero naturale.
7. Provare che a) $n^2 \cdot (n^2 - 1)$ è divisibile per 12; b) $n^5 - n$ è divisibile per 30; c) $n^4 + 2n^3 + 3n^2 + 2n$ è divisibile per 8.
8. Provare che a) $n^3 + 11n$ è divisibile per 6; b) $7^n - 5^n$ è divisibile per 2; c) $n^3 + (n + 1)^3 + (n + 2)^3$ è divisibile per 9.
9. Provare che fra i numeri $(m^2 - n^2)$, $2mn$ e $(m^2 + n^2)$, con m, n numeri naturali, a) uno almeno è divisibile per 3; b) uno almeno è divisibile per 5; c) il prodotto di almeno due di essi è divisibile per 12; d) il loro prodotto è divisibile per 60.

§9. Massimo comune divisore e minimo comune multiplo.

Consideriamo adesso un'altra questione. Siano n ed m due numeri interi. Ciascuno di essi ha un certo numero di divisori, che inseriamo nei due insiemi D_n e D_m. Consideriamo adesso l'insieme $I = D_n \cap D_m$. Intanto osserviamo che I non è l'insieme vuoto perché contiene certamente almeno il numero 1. Inoltre I non può contenere più elementi di quanti ne contiene il più piccolo dei due insiemi di divisori. Infine il maggiore degli elementi di I non può essere superiore al minimo fra gli elementi massimi di D_n e D_m. Ciò significa che I contiene un elemento massimo. Poniamo allora la seguente definizione.

Definizione 6. Dati due numeri interi n ed m. Indichiamo con D_n e D_m gli insiemi dei loro divisori. Diciamo **massimo comune divisore** di m ed n, il massimo degli elementi dell'insieme $I = D_n \cap D_m$.

Un metodo per determinare il *MCD* di due numeri è quello di scomporre i numeri in fattori primi ed applicare la ben nota regola: *moltiplicare i fattori comuni con il minore esponente*. Infatti il prendere fattori comuni fa sì che prendiamo solo i numeri primi divisori comuni ai due numeri, il fatto che il loro esponente sia il minore fa sì che i divisori siano comuni compresi i loro esponenti.

Esempio 17.

Determinare $MCD(4752, 4536)$. Abbiamo $4752 = 2^4 \cdot 3^3 \cdot 11$, $4536 = 2^3 \cdot 3^4 \cdot 7$. Per quanto detto abbiamo $MCD(4752, 4536) = 2^3 \cdot 3^3 = 8 \cdot 27 = 216$.

Un metodo più antico del precedente fu esposto da Euclide nei suoi elementi ed è descritto nel seguente esempio.

Esempio 18.

Determinare $MCD(4224, 5040)$. Consideriamo la divisione di 5040 per 4224 Si ha: $5040 = 4224 + 816$. Adesso dividiamo 4224 per 816, ottenendo: $4224 = 816 \cdot 5 + 144$; continuiamo a dividere: $816 = 144 \cdot 5 + 96$, $144 = 96 + 48$, $96 = 48 \cdot 2$. Adesso scriviamo tutte queste disuguaglianze una di seguito all'altra. $5040 = 4224 + 816 = 816 \cdot 5 + 144 + 816 = 816 \cdot 6 + 144 = (144 \cdot 5 + 96) \cdot 6 + 144 = 144 \cdot 30 + 96 \cdot 6 + 144 = 144 \cdot 31 + 96 \cdot 6 = (96 + 48) \cdot 31 + 96 \cdot 6 = 96 \cdot 31 + 48 \cdot 31 + 96 \cdot 6 = 96 \cdot 37 + 48 \cdot 31 = 48 \cdot 2 \cdot 37 + 48 \cdot 31 = 48 \cdot 105$. Se le scriviamo a partire dalla seconda invece otteniamo: $816 = 144 \cdot 5 + 96 = (96 + 48) \cdot 5 + 96 = 96 \cdot 5 + 48 \cdot 5 + 96 = 96 \cdot 6 + 48 \cdot 5 = 48 \cdot 2 \cdot 6 + 48 \cdot 5 = 48 \cdot 17$. Quindi $MCD(4224, 5040) = MCD(48 \cdot 17, 48 \cdot 105) = 48$. In pratica il *MCD* è l'ultimo quoziente ottenuto nella sequenza di divisioni, che si interrompe quando otteniamo una divisione esatta, cioè con resto 0.

Quindi l'algoritmo di Euclide consiste nell'effettuare le divisioni successive dei primi due numeri e poi in successione di ogni divisore per il relativo quoziente, finché non si ottiene resto zero. Il precedente resto è perciò il massimo comun divisore. Vediamo di provare rigorosamente questo risultato.

Algoritmo di Euclide. Siano m ed n i numeri di cui vogliamo determinare il loro *MCD*. Sia per esempio $m > n$. Possiamo allora scrivere: $m = q_1 \cdot n + r_1$, con $r_1 < n$. Se $r_1 = 0$, m è multiplo di n che è perciò il *MCD* cercato. Se $r_1 \neq 0$, scriviamo $n = q_2 \cdot r_1 + r_2$, con $r_2 < r_1$. Se $r_2 = 0$, vuol dire che n è multiplo di r_1, ma anche m lo è, infatti $m = q_1 \cdot n + r_1 = q_1 \cdot q_2 \cdot r_1 + r_1 = (q_1 \cdot q_2 + 1) \cdot r_1$. Non solo, ma r_1 è anche il *MCD*, dato che m non è divisibile per q_2. Questo procedimento può continuarsi fino ad un certo punto, dato che ad ogni passo il resto ottenuto è un numero positivo inferiore al resto precedente, quindi ad un certo momento deve divenire zero.

Esempio 19.

Vogliamo dividere in pezzi più piccoli ma tutti di uguale peso tre forme di grana che pesano 52, 68 e 76 chilogrammi. Quanto deve pesare ciascuno dei pezzi in chili interi se il loro numero totale deve essere il più piccolo possibile? Scomponiamo i numeri dei pesi delle tre forme: $52 = 2^2 \cdot 13$, $68 = 2^2 \cdot 17$, $76 = 2^2 \cdot 19$. Poiché vogliamo dividere le forme in parti tutti uguali con il minor numero possibile di pezzi dobbiamo cercare il loro massimo comune divisore, che è 4. Quindi suddividiamo le tre forme in $(52 + 68 + 76) : 4 = 196 : 4 = 49$ pezzi da 4 Kg ciascuno.

Poiché risulterà interessante nel seguito stabiliamo il seguente concetto.

Definizione 7. Due numeri naturali m ed n si diranno **coprimi** o **primi fra di loro** se $MCD(m, n) = 1$.

Introduciamo adesso un altro concetto del tutto simile al *MCD*.

Definizione 8. Dati due numeri naturali m ed n, consideriamo gli insiemi M_n e M_m dei loro multipli. Diciamo **minimo comune multiplo** di m ed n il minimo elemento dell'insieme $M_n \cap M_m$.

La precedente definizione ha senso. Infatti gli insiemi M_n e M_m sono chiaramente infiniti e pure infinito è il loro insieme intersezione. Tale insieme è però un sottoinsieme di $\mathbb{N}$, quindi ammette minimo, dato che $\mathbb{N}$ è bene ordinato.
Per la determinazione del mcm di due numeri può applicarsi la ben nota regola: *moltiplicare i fattori comuni e non comuni con il maggiore esponente*. Infatti debbono considerarsi tutti i fattori primi di entrambi i numeri, per essere sicuri che il loro prodotto contenga tutti i fattori di entrambi i numeri. Il fatto di prendere i maggiori esponenti fa sì che si considerino degli effettivi multipli di m ed n.

Teorema 15. Dati due numeri naturali m ed n, vale la seguente uguaglianza:

$$MCD(m, n) \cdot mcm(m, n) = m \cdot n.$$

Esempio 20.

Tre navi il primo gennaio partono da A per andare a B dove effettuano un nuovo carico. Lo stesso giorno di arrivo ripartono per A dove scaricano e ripartono per B lo stesso giorno. Continuano questo andirivieni per tutto l'anno. Se la prima nave compie un tragitto di andata e ritorno in 12 *giorni, la seconda in* 16 *giorni e la terza in* 20*, fra quanti giorni ripartiranno da A lo stesso giorno*? In pratica vogliamo determinare un numero che deve essere multiplo di 11, 16 e 20. Poiché vogliamo sapere quando sarà la prossima volta, calcoleremo il mcm(12, 16, 20) = 240.

Esercizi.

1. Con l'algoritmo euclideo determinare il *MCD* dei seguenti numeri:
   a) (12345; 23456); b) (123321; 234432); c) (102132; 213243). **[a) 1; b) 1221; c) 3]**
2. Dal *Sun Tsu Suan Ching* un testo cinese del IV secolo. *Tre sorelle escono di casa rispettivamente ogni* 3, 4 *e* 5 *giorni. Se un certo giorno escono tutti e tre insieme dopo quanti giorni riusciranno insieme?* **[60]**
3. Nel gioco *Regina, reginella*, ciascuno deve arrivare dalla Regina facendo passi di animale. Sappiamo che Sharon arriva dalla regina con 10 passi da tartaruga, 2 da lepre e 1 da canguro. Sappiamo inoltre che un passo di canguro è lungo quanto 2 da lepre e quanto 6 da tartaruga. Se Stefania arriva dalla regina facendo solo passi da tartaruga, quanti passi fa? **[22]**
4. Caterina ha invitato 8 suoi amici per il giorno di Pasqua e a ognuno vuole regalare lo stesso numero di ovetti. Non tutti però sono certi di poter venire: Giulio verrà solo se lo farà Giada, mentre Anna, Carlo e Tommaso forse andranno insieme a Parigi. Quanti ovetti deve comprare almeno perché possa darne a tutti lo stesso numero, quanti che siano gli intervenuti? **[120]**
5. Erika ha più di 50 ma meno di 120 caramelle. Si accorge che mentre è insieme ad Alice e Bob potrebbe dividerle in parti uguali con loro. Nel frattempo arrivano Tom ed Erika e così non può più dividere le caramelle in parti uguali fra tutti. Dopo qualche minuto arrivano Dalila e Mirko, perciò lo può fare di nuovo. Quante caramelle ha Erika a) minimo? b) massimo? **[a) 63; b) 84]**
6. Generalizzare il Teorema 15 a più di due numeri.

§10. Il numero dei divisori di un numero.

Vediamo di parlare adesso di un problema che abbiamo già parzialmente trattato. Quanti sono i divisori di un numero? Cominciamo a considerare i casi più semplici. È chiaro che se il numero è primo per la sua stessa definizione ha solo due divisori. Quanti divisori ha se è il quadrato di un numero primo, come per esempio 25? Pensiamo che non vi siano problemi a dire che essi sono 3, cioè: 1, 5 e 25. Ciò è vero per ogni altro numero del tipo p^2, con p primo. Per il seguito indichiamo con il simbolo $\nu(n)$ il numero di divisori di n. Allora indicando con p un generico numero primo, abbiamo $\nu(p) = 2$ e $\nu(p^2) = 3$, dato che i divisori di p^2 saranno 1, p e p^2. Quanti sono i divisori di p^3? Anche qui pensiamo che la risposta sia semplice: essi sono 4, cioè 1, p, p^2 e p^3. A questo punto è semplice enunciare e provare il seguente risultato.

Teorema 16. Dato un numero primo p, si ha $\nu(p^n) = n + 1$.
Dimostrazione. I divisori sono: $1, p, p^2, \ldots, p^n$.

Il passo successivo sarà di considerare un numero che sia prodotto di due numeri primi, come per esempio $15 = 3 \cdot 5$. Quanti saranno i suoi divisori? 4, cioè 1, 3, 5 e 15. Ciò ci conduce a dire che se $n = p_1 \cdot p_2$, con p_1 e p_2 numeri primi distinti, si ha: $\nu(p_1 \cdot p_2) = 4$, dato che i divisori sono 1, p_1, p_2 e $p_1 \cdot p_2$. Se i fattori primi di n sono 3, p_1, p_2 e p_3, i suoi divisori saranno 1, p_1, p_2, p_3, $p_1 \cdot p_2$, $p_1 \cdot p_3$, $p_2 \cdot p_3$ e $p_1 \cdot p_2 \cdot p_3$. Sono cioè 8. Pensiamo allora che possa facilmente enunciare e dimostrare il seguente fatto.

Teorema 17. Dato un numero naturale $n = p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots\ p_h$, con p_i che indica un numero primo. Si ha $\nu(n) = 2^h$.
Dimostrazione. Il problema equivale a prendere intanto il numero 1, quindi i divisori formati solo dai numeri primi, che sono $p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots\ p_h$. Poi consideriamo i divisori ottenuti moltiplicando a due a due i detti numeri primi, che sono $\binom{h}{2}$, cioè quanto le combinazioni di h oggetti a due a due. I divisori prodotto di 3 di questi fattori sono quindi $\binom{h}{3}$ e così via fino allo stesso numero n. Quindi possiamo dire che in totale si ha: $\nu(n) = \binom{h}{0} + \binom{h}{1} + \binom{h}{2} + \ldots + \binom{h}{h} = 2^h$ (*). Ricordiamo che l'ultimo risultato dipende dallo sviluppo del binomio di Newton: $(x+y)^h = \binom{h}{0}x^h + \binom{h}{1}x^{h-1}y + \ldots + \binom{h}{h}y^h$, dove ponendo $x = y = 1$ otteniamo (*)

A questo punto manca il teorema generale, cioè il caso in cui i fattori primi possono avere potenze maggiori di 1: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_h^{a_h}$.
Enunciamo e proviamo il seguente fatto.

Teorema 18. Dato un numero naturale $n = \prod_{i=1}^{k} p_i^{a_i}$, con p_i che indica un numero primo. Si ha $\nu\left(\prod_{i=1}^{h} p_i^{a_i}\right) = \prod_{i=1}^{h}(a_i + 1)$.

Dimostrazione. Fra i divisori di n vi sono i divisori di $p_1^{a_1}$ che, per quanto visto nel teorema 16, sono in numero di $(a_1 + 1)$. Poi vi sono i divisori di $p_2^{a_2}$ che sono in numero di $(a_2 + 1)$. Vi sono poi anche i divisori ottenuti moltiplicando i divisori di $p_1^{a_1}$ per quelli di $p_2^{a_2}$, ottenendo quindi $(a_1 + 1) \cdot (a_2 + 1)$ divisori. Osserviamo che quando consideriamo 1 come divisore di $p_1^{a_1}$ moltiplicando per i divisori di $p_2^{a_2}$, otteniamo proprio i divisori di quest'ultimo, analogamente quando moltiplichiamo i divisori di $p_1^{a_1}$ per 1. Allo stesso modo, dati i divisori di $p_3^{a_3}$, che sono in numero di $(a_3 + 1)$, i divisori che contengono almeno uno dei divisori dei tre detti numeri primi sono $(a_1 + 1) \cdot (a_2 + 1) \cdot (a_3 + 1)$. Iterando il procedimento otteniamo la tesi del teorema.

Esempio 21.

Vediamo di capire meglio la dimostrazione precedente, calcolando quanti divisori ha il numero $180 = 2^2 \cdot 3^3 \cdot 5$. Vi sono i divisori di 2^2, che sono 3 (1, 2, 4), quelli di 3^3 che sono 4 (1, 3, 9, 27) e quelli di 5 che sono 2 (1, 5). Se ora consideriamo il prodotto dei divisori di 2^2 per quelli di 3^3 otteniamo i 12 divisori che contengono almeno uno dei fattori di 2^2 o (vel) di 3^3. Infine considerando il prodotto dei 3 divisori di 2^2 per i 4 divisori di 3^3 per i 2 divisori di 5, otteniamo i 24 divisori di 180. Ciò coincide con il risultato del teorema 18: $(3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 4 \cdot 3 \cdot 2 = 24$.

Collegato a questo problema vi è quello di determinare la somma dei detti divisori, che indichiamo con $\sigma(n)$. Procediamo come abbiamo visto in precedenza. Cominciamo quindi a determinare $\sigma(p)$, con p numero primo. Sarà chiaramente $\sigma(p) = p + 1$. Altrettanto facilmente abbiamo che $\sigma\left(p^h\right) = \sum_{m=0}^{h} p^m = \frac{p^{m+1} - 1}{p - 1}$. Quest'ultima uguaglianza discende dal fatto che stiamo calcolando la somma di una progressione geometrica di ragione p. Il passo successivo sarà quello di calcolare $\sigma(p_1 \cdot p_2)$. Dato che abbiamo visto che i divisori di $p_1 \cdot p_2$ sono 1, p_1, p_2 e $p_1 \cdot p_2$, abbiamo $\sigma(p_1 \cdot p_2) = 1 + p_1 + p_2 + p_1 \cdot p_2 = 1 + p_1 + p_2 \cdot (1 + p_1) = (1 + p_1) \cdot (1 + p_2) = \sigma(p_1) \cdot \sigma(p_2)$. È facile generalizzare questo risultato e dire che se $MCD(m, n) = 1$, allora $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$. Da qui il passo è breve per enunciare e dimostrare il seguente teorema generale.

Teorema 19. Dato un numero naturale $n = \prod_{i=1}^{k} p_i^{a_i}$, con p_i che indica un numero primo. Si ha $\sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \sigma\left(p_i^{a_i}\right) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$.

Esempio 22.

La formula precedente assume una forma particolarmente semplice per le potenze di 2. Infatti si ha: $\sigma\left(2^n\right) = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$.

Dato che nel seguito useremo tale argomento, indichiamo con $\sigma_0(n)$ la somma dei divisori di n inferiori a n. Poniamo cioè $\sigma_0(n) = \sigma(n) - n$.
In qualche modo legata a questi problemi è un'altra funzione.

Definizione 9. Dato un numero naturale $n > 1$, chiamiamo sua **funzione di Eulero** o anche **funzione toziente**, e la indichiamo con $\phi(n)$, la funzione che determina quanti numeri minori di n sono primi con n.

La prima questione riguarda il numero 1, esso non è primo, quindi nel calcolo di $\phi(n)$ si considera sempre. Un'altra questione riguarda $\phi(1)$. Tenuto conto della definizione esso dovrebbe essere 0 perché 1 non ha numeri naturali a esso inferiori; ma nella definizione il numero 1 è escluso, quindi si definisce a parte come $\phi(1) = 1$, ciò per fare sì che si possano enunciare regole generali in modo più semplice.
La funzione toziente, o anche *fi* dal simbolo greco con cui si indica, è associata ad Eulero che propose per primo la questione nel 1760 fornendo anche la soluzione.
Noi, come ormai abbiamo fatto con altre questioni, costruiamo una tabella che possa servirci poi da suggerimento per stabilire una congettura sull'espressione di $\phi(n)$.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18

Una prima cosa che si nota e che era anche immediato osservare è che se p è un numero primo allora $\phi(p) = p - 1$. Invece non risulta semplice stabilire una relazione per n composto, tranne il fatto che $\phi(n)$ è pari per $n > 2$, dato che ovviamente se $h < n$ è primo con n, anche $(n - h)$ lo è, dato che diversamente da $n = h + (n - h)$ avremmo $h = n - (n - h)$, ma il secondo membro è una differenza fra due numeri divisibili per n e quindi è anch'esso divisibile con n, il che è contro l'ipotesi. Notiamo però che si ha per esempio $\phi(6) = \phi(2) \cdot \phi(3)$, $\phi(12) = \phi(3) \cdot \phi(4)$, $\phi(15) = \phi(3) \cdot \phi(5)$, mentre $\phi(16) \neq \phi(2) \cdot \phi(8)$.
Cerchiamo di capire perché la proprietà moltiplicativa a volte funziona e a volte no.

Esempio 23.

- I numeri coprimi con 3 sono A = {1, 2}, quelli coprimi con 5 sono B = {1, 2, 3, 4}, quelli coprimi con 15 sono: C = {1, 2, 4, 7, 8, 11, 13, 14}. Come possiamo legare questi numeri con quelli dei singoli fattori di 15? Consideriamo l'insieme A × B, ed effettuiamo gli 8 prodotti fra gli elementi delle sue coppie, ottenendo: {1, 2, 3, 4, 2, 4, 6, 8}. Intanto alcuni prodotti si ripetono e quindi riduciamo a {1, 2, 3, 4, 6, 8}. Di questi prodotti a noi interessano solo quelli che sono coprimi con entrambi 3 e 5, quindi solo {1, 2, 4, 8}. D'altro canto però 15 ha 14 numeri minori di esso, quindi dobbiamo considerare quelli che sono coprimi con 3 e 5 maggiori di 8. Questi sono {7, 11, 13, 14} e sono altri 4. Il perché dipende dal fatto che gli altri contengono divisori di 3 o di 5.
- Per quanto riguarda invece $\phi(16)$ abbiamo A = {1} e B = {1, 3, 5, 7}, C = {1, 3, 5, 7, 9, 11, 13, 15, 17}. Stavolta A × B ha meno elementi di C, quindi ecco perché non vi è l'uguaglianza.

Tenuto conto dell'esempio precedente enunciamo e dimostriamo allora il seguente risultato.

Teorema 20. Se MCD(n, m) = 1 allora $\phi(nm) = \phi(n) \cdot \phi(m)$.
Dimostrazione.
Se MCD(h, mn) = 1 si ha anche MCD(h, m) = 1 e MCD(h, n) = 1, diversamente avremmo per esempio $h = tm$, ma allora anche $h = tmn$ e perciò h ed mn non sarebbero coprimi. Per il Teorema cinese del resto possiamo dire che l'insieme $\{p: \text{MCD}(p, nm) = 1\}$ ha la stessa cardinalità di $\{(i, j) \in \mathbb{N}^2 : 1 \le i \le m, 1 \le j \le n, \text{MCD}(i, m) = \text{MCD}(j, n) = 1\} = \{i \in \mathbb{N} : 1 \le i \le m, \text{MCD}(i, m) = 1\} \times \{j \in \mathbb{N} : 1 \le j \le n, \text{MCD}(j, n) = 1\}$, il che equivale alla tesi.

Un altro caso semplice da calcolare è quando n è una potenza di un numero primo: $n = p^h$. Infatti in questo caso i suoi divisori sono 1 e tutti i multipli di p, sono cioè: 1, p, $2p$, $3p$, ..., $(p^{h-1} - 2) \cdot p$, $(p^{h-1} - 1) \cdot p$. Questi sono chiaramente in numero di p^{h-1}. Quindi possiamo dire che $\phi(p^h) = p^h - p^{h-1} = p^{h-1} \cdot (p - 1) = p^h \cdot \left(1 - \frac{1}{p}\right) = p^{h-1} \cdot (p - 1)$. A partire da questo fatto enunciamo il risultato generale.

Teorema 21. $\phi\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1)$, con p_i che indicano numeri primi.

Già nella tabella precedente si vede che fissato un certo numero naturale h vi possono essere più naturali n per i quali si ha $\phi(n) = h$. In realtà una congettura afferma che non esiste nessun numero h per cui l'equazione $\phi(n) = h$, ha una sola soluzione.

Esempio 24.
Quanti e quali sono i numeri naturali n soluzioni di $\phi(n) = 6$? Tenuto conto del Teorema 21 deve essere $\prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1) = 6$ e dato che $6 = 1 \cdot 6 = 2 \cdot 3$, abbiamo solo le seguenti possibilità: $6 = 7^0 \cdot (7 - 1)$, $6 = 3^1 \cdot (3 - 1)$, $6 = 2^0 \cdot (2 - 1) \cdot 7^0 \cdot (7 - 1)$, $6 = 2^0 \cdot (2 - 1) \cdot 3^1 \cdot (3 - 1)$. Cioè $\phi(7) = \phi(9) = \phi(14) = \phi(18) = 6$.

L'esempio precedente suggerisce il seguente risultato.

Corollario 1. $\phi(2n + 1) = a \Rightarrow \phi(4n + 2) = a$.
Dimostrazione.
Ciò dipende dal fatto che se $\phi(2n+1) = \phi\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1) = a$ allora, dato che si ha $2^0 \cdot (2 - 1) = 1 \Rightarrow \phi(4n+2) = \phi\left(2 \cdot \prod_{i=1}^{k} p_i^{a_i}\right) = 2^0 \cdot (2-1) \cdot \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1) = a$.

Notiamo che non tutte le equazioni $\phi(n) = h$, hanno soluzioni. Per esempio non ce l'ha $\phi(n) = 14$, dato che $14 = 1 \cdot 14 = 2 \cdot 7$. Nel primo caso $14 + 1 = 15$ non è un numero primo, nel secondo caso non lo è $7 + 1$. Quindi non possiamo scrivere 14 nella forma prevista dal Teorema 21.

Concludiamo il paragrafo con un nuovo problema.

Esempio 25.

Scriviamo tutte le frazioni proprie, ridotte ai minimi termini, il cui denominatore non superi 5. Esse sono: ½, 1/3, ¼, 1/5, 2/3, 2/5, 3/5, 4/5. Ordiniamole in modo crescente: {1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 4/5}. Vogliamo risolvere i seguenti problemi:

1) Fissato il massimo denominatore, per esempio n, possiamo stabilire una regola per determinare quante frazioni come quelle viste vi sono?
2) Vi è una qualche relazione che permette di passare da una frazione alla successiva?

Prima di risolvere i problemi posti poniamo una definizione.

Definizione 10. Dato un numero naturale $n > 1$, chiamiamo **serie di Farey di ordine *n***, la totalità di frazioni proprie ridotte ai minimi termini di denominatore minore o uguale ad n, ordinate in modo crescente.

Adesso veniamo alle questioni poste. La prima si risolve facilmente.

Teorema 22. Le frazioni della serie di Farey di ordine n sono in numero di $\sum_{h=2}^{n} \phi(h)$.

Dimostrazione. Dato che le frazioni sono ridotte ai minimi termini le frazioni della serie di Farey di ordine n sono del tipo m/p con MCD$(m, p) = 1$ e $2 \le p \le n$ e quindi sono proprie tanto quanto i numeri primi con p, ossia $\phi(p)$.

Per quanto riguarda il problema 2) consideriamo qualche caso.

Esempio 26.

Data la serie di Farey di ordine 5: {1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 4/5}, osserviamo che ¼ = (1 + 1)/(5 + 3); 1/3 = (1 + 2)/(4 + 5); 2/5 = (1 + 1)/(3 + 2) e così via.

Tenuto conto dell'esempio precedente, ci limitiamo ad enunciare il seguente risultato, che non dimostriamo.

Teorema 23. Se a/b e c/d sono termini consecutivi di una serie di Farey è $bc - ad = 1$.

Dimostriamo invece il seguente risultato.

Teorema 24. Detti a/b, c/d, e/f tre termini consecutivi di una serie di Farey, si ha $c/d = (a + e)/(b + f)$.

Dimostrazione. Per il teorema 23 si ha: $bc - ad = 1$ e $de - cf = 1$, da cui: $bce - ade = e$ e $ade - acf = a$. Sommiamo termine a termine: $bce - ade + ade - acf = a + e \Rightarrow c(be - af) = a + e$ (1). Analogamente abbiamo: $bcf - adf = f$ e $bde - bcf = b \Rightarrow bcf - adf + bde - bcf = b + f \Rightarrow d(be - af) = b + f$ (2). Si ha $be - af \neq 0$ perché si ha $e/f > a/b$ e quindi $(be - af)/bf > 0 \Rightarrow \ be - af > 1$. Quindi dividendo termine a termine (1) e (2) otteniamo: $c/b = (a + e)/(b + f)$, ossia la tesi richiesta.

Esercizi.

1. Tenuto conto dei risultati del teorema 18, determinare per quali numeri $\nu(n)$ è un numero dispari. **[Quando tutti i suoi fattori primi hanno esponenti pari]**
2. Verificare il teorema 18 calcolando a) $\nu(124)$; b) $\nu(123456)$; c) $\nu(12345678)$. **[a) 6; b) 28; c) 24]**
3. Verificare il teorema 19 calcolando a) $\sigma(124)$; b) $\sigma(123456)$; c) $\sigma(12345678)$. **[a) 224; b) 327152; c) 27319968]**
4. Osservato che $\sigma(3) = 1 + 3 = 2^2$, determinare tutti gli $n \leq 100$, per cui $\sigma(n) = m^2$. **[1, 3, 22, 66, 70, 81, 94]**
5. Determinare tutti gli $n \leq 20$, per cui $\sigma(n^2) = m^2$. **[1, 9, 20]**
6. Determinare tutti gli $n \leq 50$, per cui $\sigma_0(n^2) = m^2$. **[1, 3, 49]**
7. Trovare i minimi numeri naturali che hanno a) 2; b) 3; c) 4; d) 5; e) divisori. **[a) 2; b) 4; c) 8; d) 16; e) 32]**
8. Tenuto conto del precedente quesito, qual è il minimo naturale che ha n divisori? **[2^{n-1}]**
9. Trovare i minimi numeri naturali, con almeno 2 fattori primi, che hanno 10 o 20 divisori. **[48; 240]**
10. a) Quanti fattori primi può avere al massimo un numero che ha 34 divisori? b) Per avere lo stesso risultato con n divisori, quanto vale n? **[a) 2; b) n è prodotto di due primi]**
11. Quanti fattori primi distinti può avere al massimo un numero con 12 divisori? **[3]**
12. Quanti divisori minimo ha un numero che ha a) 5; b) n fattori primi distinti? **[32; 2^n]**
13. Trovare tutti i numeri minori o uguali a 30 (in effetti sono gli unici possibili) i cui numeri a essi inferiori con i quali sono coprimi sono tutti numeri primi. **[2, 3, 4, 6, 8, 12, 24, 30]**
14. Verificare il risultato del teorema 21 per $n = 35, 40, 123$ **[24, 16, 80]**
15. Determinare tutti i numeri naturali n per cui si ha $\phi(n) = 8$. **[15, 16, 20, 24, 30]**
16. Provare che non esistono numeri naturali per cui $\phi(n) = 34$.
17. Trovare tutti i numeri $h < 100$ per cui $\phi(n) = h$ non ha soluzione. **[14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98]**
18. Provare che $\phi(n^2) = n \cdot \phi(n)$, $\forall n \in \mathbb{N}$.
19. Costruire una tabella per $\phi(n)$, per tutti gli n inferiori a 50.
20. Provare che $\sum_{i=0}^{h} \phi\left(p^i\right) = p^h$, per ogni numero primo p.
21. Provare che dato un numero naturale n, e indicati con d_i $1 \leq i \leq h$, tutti i suoi divisori allora $\sum_{i=1}^{h} \phi\left(d_i\right) = p^h$.

Quesiti sulle serie di Farey

22. Costruire quelle di ordine n: $6 \leq n \leq 10$.
23. Provare che i termini sono sempre in numero dispari e il termine centrale è sempre ½.
24. Enunciare una congettura relativa alla somma delle frazioni di posto simmetrico rispetto al centro. **[È uguale a 1]**
25. Enunciare una congettura relativa alla differenza fra due termini consecutivi. **[È uguale al reciproco del prodotto dei loro denominatori]**

§11. Numeri perfetti e numeri amicabili.

Strettamente legati agli argomenti che abbiamo trattato in questi ultimi paragrafi sono i cosiddetti numeri perfetti. È dire comune che il numero perfetto è 3 poiché nella religione cristiana esso rappresenta la divina trinità. Invece in matematica i numeri perfetti sono stati considerati altri. Già Euclide nei suoi elementi tratta di questi numeri e trova un'interessante formula che li riguarda. Vediamo di definirli.

Definizione 12. Un numero naturale n, per cui si ha $\sigma_0(n) = n$, si dice **numero perfetto**.

È evidente che nella somma dei divisori dobbiamo escludere lo stesso n, se no non accadrebbe mai ciò che impone la definizione. Se vogliamo considerare tutti i divisori di n, potremmo modificare la definizione 10, nel modo seguente.

Definizione 12′. Un numero n, per cui $\sigma(n) = 2n$, si dice numero perfetto.

Dal punto di vista storico la definizione 12 è più efficace, infatti la pretesa perfezione dei detti numeri consiste nel fatto che essi risultano somma delle loro "parti". A questo fatto nei secoli si sono sommate diverse altre giustificazioni mistiche. Infatti come è facile notare il numero $6 = 1 + 2 + 3$ è un numero perfetto. Nella religione cristiana Dio creò l'universo in 6 giorni. Ma anche il numero $28 = 1 + 2 + 4 + 7 + 14$, è un numero perfetto e la luna gira attorno alla terra in un periodo all'incirca di 28 giorni. Addirittura Alcuino (735 – 804), che fu il tutore di Carlo Magno, disse che la prima creazione del mondo fu perfetta perché compiuta appunto in 6 giorni; la seconda, quella avvenuta dopo il diluvio universale, fu invece imperfetta poiché tutti gli esseri umani furono creati a partire dagli 8 sopravvissuti. Ora $\sigma(8) - 8 = 1 + 2 + 4 < 8$. La somma delle parti di 8 non raggiunge 8, quindi affinché la seconda creazione potesse essere considerata perfetta, ad essa "manca" qualcosa. Alcuino, da buon fanatico, adattò le cose ai suoi interessi; infatti non disse perché se la prima creazione era da considerarsi perfetta, Dio la eliminò parzialmente annegando quasi tutti gli esseri viventi.
Comunque a partire anche da tali considerazioni, stabiliamo la seguente ulteriore definizione.

Definizione 13.
- Un numero n, per cui $\sigma(n) < 2n$, si dice **numero deficiente**.
- Un numero n, per cui $\sigma(n) > 2n$, si dice **numero abbondante**.

Torniamo ai numeri perfetti. Possiamo farci aiutare da un CAS oppure scrivere un programma in un qualche linguaggio, per calcolare i numeri perfetti inferiori a 10.000. Sorprendentemente ne troveremo solo in 4: 6, 28, 496 e 8128.

Teorema 25. Se $(2^p - 1)$ numero primo allora $n = 2^{p-1} \cdot (2^p - 1)$, è un numero perfetto.
Dimostrazione. Notiamo che nell'enunciato abbiamo indicato l'esponente con p, infatti abbiamo già notato che i numeri del tipo $(2^p - 1)$, che abbiamo chiamato numeri di Mersenne, non sono primi se p è composto. Abbiamo $\sigma(n) = \sigma(2^{p-1}) \cdot \sigma[(2^p - 1)]$, dato che $(2^p - 1)$ è un numero primo, abbiamo che $\sigma[(2^p - 1)] = 1 + 2^p - 1 = 2^p$. Abbiamo anche osservato che $\sigma(2^{p-1}) = 2^p - 1$. Quindi $\sigma(n) = (2^p - 1) \cdot 2^p = 2 \cdot [(2^p - 1) \cdot 2^{p-1}] = 2n$. Questa uguaglianza costituisce la tesi.

Molto tempo dopo Euclide il solito Eulero provò che la precedente condizione non è solo sufficiente ma è anche necessaria a far sì che un numero **pari** sia perfetto. Vediamolo.

Teorema 26. Ogni numero perfetto pari è della forma $n = 2^{p-1} \cdot (2^p - 1)$, con $(2^p - 1)$ numero primo.
Dimostrazione. Poiché n è un numero pari esso avrà la forma seguente: $n = 2^{p-1} \cdot m$, con m numero dispari (anche uguale ad 1). Per provare il teorema dobbiamo quindi far vedere che $m = 2^p - 1$. Dato che n è prodotto di due fattori coprimi avremo $\sigma(n) = \sigma(2^{p-1}) \cdot \sigma(m) = (2^p - 1) \cdot \sigma(m)$. Dato che n è un numero perfetto si ha $\sigma(n) = 2n = 2^p \cdot m$. Quindi possiamo dire che la seguente è una uguaglianza vera: $(2^p - 1) \cdot \sigma(m) = 2^p \cdot m$. Indichiamo con $\sigma_0(m)$ la somma dei divisori di m escluso m. La precedente uguaglianza diviene quindi: $(2^p - 1) \cdot [\sigma_0(m) + m] = 2^p \cdot m \Rightarrow (2^p - 1) \cdot \sigma_0(m) + 2^p \cdot m - m = 2^p \cdot m \Rightarrow (2^p - 1) \cdot \sigma_0(m) = m$. Ciò significa che $\sigma_0(m)$ è un divisore di m. Ciò può accadere solo se $\sigma_0(m) = 1$. Ma allora $\sigma(m) = m + 1$, cioè m è un numero primo. Non solo, ma l'ultima uguaglianza adesso diviene: $2^p - 1 = m$. Cioè la tesi.

Il teorema precedente mette in relazione i numeri perfetti pari con i numeri di Mersenne. Visto quello che abbiamo finora detto i numeri perfetti pari finora conosciuti (settembre 2022) sono 51, il più grande dei quali è $2^{82589933} \cdot (2^{82589933} - 1)$.
Un problema tuttora aperto consiste nello stabilire se possano esistere numeri perfetti dispari. I risultati finora ottenuti fanno propendere per una risposta negativa, dato che se esistessero dovrebbe verificare delle condizioni molto restrittive. È stato infatti stabilito che se un tale numero esiste deve essere divisibile almeno per otto primi distinti, avere almeno 29 fattori primi, avere almeno 300 cifre ed avere un divisore primo superiore a 10^{20}.
Infine un'altra classe di numeri che è stata presa in considerazione sempre per le sue presunte proprietà mistiche, è quella dei numeri amici.

Definizione 14. Due numeri naturali m ed n si dicono **amici** se $\sigma_0(n) = \sigma_0(m)$.

La giustificazione della terminologia è la seguente: dato che ciascun numero è somma delle parti dell'altro vuol dire che i due sono parte uno dell'altro, sono quindi come amici fraterni. Sembra che i primi ad indagare su tali numeri siano stati i Pitagorici. Comunque anche nella matematica araba essi hanno giocato un ruolo molto importante. In [O] è riportata una citazione di un passo di Ibn Khaldun, vissuto nella seconda metà del 1330, in cui egli dice: «*Persone che si occupano di magia assicurano che questi numeri hanno una particolare influenza nello stabilire unione ed amicizia fra due individui.* [...] *Essi stabiliscono un legame così forte fra due persone che esse non possono essere più separate. L'autore di Ghaïa e di altri capolavori in quest'arte* [la magia] *dichiarano che ciò è stato confermato dalla loro esperienza personale».* Nonostante questo interesse della numerologia, per molti secoli l'unica coppia di numeri amici conosciuta è stata (220, 284). Si ha infatti $\sigma_0(220) = \sigma_0(2^2 \cdot 5 \cdot 11) = (2^3 - 1) \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{11^2 - 1}{11 - 1}$ $= 7 \cdot 6 \cdot 12 = 504$, si ha inoltre $\sigma_0(284) = \sigma_0(2^2 \cdot 71) = (2^3 - 1) \cdot \frac{71^2 - 1}{71 - 1} = 7 \cdot 72 = 504$.
Si dovette arrivare al solito Fermat per ottenere altre coppie di numeri amici. Il fatto è alquanto strano, poiché il matematico francese determinò una formula utilizzando dei risultati che l'arabo Abu'l Hasan Thabit ben Korrah aveva stabilito nel IX secolo. Ve-

diamo il risultato di Fermat.

Teorema 27. Sia $p_n = 3 \cdot 2^n - 1$ e sia $q_n = 9 \cdot 2^{2n-1} - 1$. Se esiste un numero naturale n per cui p_{n-1}, p_n e q_n sono tutti numeri primi, allora i numeri $2^n \cdot p_{n-1} \cdot p_n$ e $2^n \cdot q_n$ sono amici.

Dimostrazione. Verifichiamo la proprietà dei numeri amici sulla data coppia.

$$\sigma_0\left(2^n \cdot p_{n-1} \cdot p_n\right) = \left(2^{n+1}-1\right) \cdot \frac{p_{n-1}^2 - 1}{p_{n-1} - 1} \cdot \frac{p_n^2 - 1}{p_n - 1} = \left(2^{n+1}-1\right) \cdot \frac{\left(3 \cdot 2^{n-1} - 1\right)^2 - 1}{\left(3 \cdot 2^{n-1} - 1\right) - 1} \cdot \frac{\left(3 \cdot 2^n - 1\right)^2 - 1}{\left(3 \cdot 2^n - 1\right) - 1} =$$

$$= \left(2^{n+1}-1\right) \cdot \frac{9 \cdot 2^{2n-2} - 3 \cdot 2^n + \cancel{1-1}}{3 \cdot 2^{n-1} - 2} \cdot \frac{9 \cdot 2^{2n} - 3 \cdot 2^{n+1} \cancel{+1-1}}{3 \cdot 2^n - 2} =$$

$$= \left(2^{n+1}-1\right) \cdot \frac{3 \cdot 2^n \cdot \cancel{\left(3 \cdot 2^{n-2} - 1\right)}}{2 \cdot \cancel{\left(3 \cdot 2^{n-2} - 1\right)}} \cdot \frac{3 \cdot 2^{n+1} \cancel{\left(3 \cdot 2^{n-1} - 1\right)}}{2 \cdot \cancel{\left(3 \cdot 2^{n-1} - 1\right)}} = \left(2^{n+1}-1\right) \cdot 3 \cdot 2^{n-1} \cdot 3 \cdot 2^n =$$

$$= 9 \cdot 2^{2n-1} \cdot \left(2^{n+1} - 1\right)$$

Si verifica che anche $\sigma_0(2^n \cdot q_n) = 9 \cdot 2^{2n-1} \cdot (2^{n+1} - 1)$. Quindi il teorema è vero.

Esempio 27.

Utilizzando il teorema 27 troviamo la prima coppia di numeri amici che Fermat determinò nel 1636. Visto che $p_3 = 3 \cdot 2^3 - 1 = 23$ è primo, che $p_4 = 3 \cdot 2^4 - 1 = 47$ è primo e $q_4 = 9 \cdot 2^7 - 1 = 1151$ è primo, stabiliamo che i numeri $2^4 \cdot 23 \cdot 47 = 17296$ e $2^4 \cdot 1151 = 18416$ sono amici.

In una lettera a Mersenne del 1638 Descartes annunciò di essere arrivato autonomamente allo stesso risultato e fornì la terza coppia di numeri amici: 9363584 e 9437056. Nel 1747 ancora Eulero diede una lista di 30 coppie di numeri amici, che successivamente aumentò a 60. Un fatto alquanto strano è che tutti questi grandi matematici, per aver guardato troppo lontano non videro ciò che era sotto i loro occhi. Andati cioè alla ricerca di coppie di numeri amici molto "grandi" non si avvidero della coppia 1184 e 1210. Essa fu ottenuta nel 1866 da un giovane italiano: Niccolò Paganini, per diversi anni scambiato per il grande musicista.

Esercizi.

1. Provare che tutte le potenze dei numeri primi rappresentano numeri deficienti.
2. Determinare tutti i numeri abbondanti minori di 100.
   [12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96]
3. Verificare che 945 è un numero abbondante. In effetti è il più piccolo fra i dispari.
4. Provare che i numeri perfetti pari possono esprimersi nel modo seguente: $\frac{M(p)+1}{2} \cdot M(p)$, dove $M(p)$ indica il numero di Mersenne di esponente p.
5. Utilizzando un CAS e mediante il teorema 27, trovare la coppia 9363584 e 9437056 di numeri amici, Per quale valore di n si trova? [7]
6. Verificare che le seguenti sono coppie di numeri amici, e che non si trovano con la formula di Thabit ben Korrah. a) (2620; 2924), b) (5020; 5564), c) (6232; 6368).
7. Provare che ogni numero perfetto $n = 2^{p-1} \cdot (2^p - 1)$, con $p > 2$, è somma dei cubi dei primi $2^{(p-1)/2}$ numeri dispari, per esempio $28 = 2^2 \cdot (2^3 - 1) = 1^3 + 3^3$. Ricorda che si ha: $\sum_{k=1}^{n} k^3 = \left[\frac{n \cdot (n+1)}{2}\right]^2$.
8. Il numero 120 si dice molteplicemente perfetto perché la somma dei suoi divisori, esso compreso, è multipla di 120 ($1 + 2 + \ldots + 120 = 3 \cdot 120$). Trovare tutti i numeri molteplicemente perfetti minori di 1000. **[120; 672]**
9. Il numero 12 ha la proprietà che il prodotto dei suoi divisori propri è uguale al suo quadrato, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 = 144 = 12^2$. Trovare tutti i numeri minori di 50 che verificano questa proprietà. **[12, 18, 20, 28, 32, 44, 45]**

§12. Equazioni indeterminate.

Uno degli argomenti per così dire "stabili" delle scuole secondarie superiori è quello delle equazioni polinomiali in una incognita quasi sempre solo di I e II grado e dei problemi che con esse possono risolversi. In particolare quando le incognite sono più di una si ricorre alla risoluzione di sistemi di equazioni che hanno tante incognite quante equazioni. La ricerca della soluzione unica viene vista come unico problema degno di essere affrontato. In effetti nei problemi per così dire pratici la soluzione unica non esiste. Molti problemi hanno più di una soluzione, per cui il compito del risolutore è quello di andare a determinare la soluzione "migliore", dove il precedente aggettivo dipende dagli scopi che intendono perpetrarsi. Così può cercarsi la soluzione minima o quella che verifica una data proprietà. In effetti nella storia delle matematiche soprattutto in certi periodi è stato profuso un notevole impegno anche nella risoluzione delle equazioni cosiddette indeterminate. Vediamo un esempio di un problema enunciato e risolto, senza alcuna giustificazione, dal già citato Alcuino: *Si distribuiscono* 100 *covoni di grano fra* 100 *persone, in modo che ogni uomo ne riceva* 3*, ogni donna* 2 *ed ogni bambino mezzo. Si vuol saper equanti sono gli uomini, quante le donne e quanti i bambini.* Alcuino fornisce la risposta: 11 uomini, 15 donne e 74 bambini. Una semplice verifica, $11 \cdot 3 + 15 \cdot 2 + 74 \cdot \frac{1}{2} = 33 + 30 + 37 = 100$, ci convince della correttezza del risultato. Se però andiamo ad impostare il sistema risolvente $\begin{cases} u + d + b = 100 \\ 3u + 2d + \frac{b}{2} = 100 \end{cases}$, ci accorgiamo di avere una condizione in meno di quelle necessarie affinché possiamo dire che la soluzione, se c'è, sia unica. Molti di questi problemi si trovano in opere indiane (per esempio il *Lilavati*[5] di Bhaskara scritto nel XII secolo, o il *Ganita – Sara – Sangraha* scritto da Mahaviracarya nel IX secolo). Vediamo come possiamo affrontare in modo rigoroso problemi del genere. Iniziamo al solito da quelli più semplici, ossia equazioni indeterminate in due incognite.

Esempio 28.

- Il seguente problema è tratto dal *Ganita – Sara – Sangraha*. *Vi erano* 63 *mucchi di datteri, ciascuno contenente lo stesso numero di frutti e* 7 *frutti isolati. Tutti i datteri furono divisi esattamente fra* 23 *marinai. Quanti frutti vi erano in ogni mucchio?* Impostiamo l'equazione risolvente $63n + 7 = 23m$, in cui n indica il numero dei datteri in ogni mucchio ed m il numero di datteri che toccò a ciascun marinaio. Dalla precedente uguaglianza ricaviamo $n = \frac{23m - 7}{63}$. Quindi le soluzioni dell'equazione sono infinite ma noi cerchiamo solo le soluzioni intere positive, può quindi essere che di tali soluzioni ve ne siano un numero finito. Dato che n deve essere positivo deve essere $23m - 7 > 0$, cioè $m > 7/23 > 1$. Inoltre n deve essere intero, quindi il numeratore deve essere un multiplo del denominatore e poiché esso si esprime come differenza di due numeri, uno dei quali è 7, ciò significa che m deve essere multiplo

[5] A proposito di quest'opera vi è un curioso aneddoto, si dice che il suo autore l'abbia scritto per confortare una delle sue figlie. Infatti egli aveva molta fiducia nella numerologia, pertanto aveva programmato nei minimi particolari il matrimonio della figlia, non solo nella scelta dello sposo, ma anche del luogo e dell'ora. Purtroppo l'orologio ad acqua che doveva stabilire l'esatto momento del matrimonio, si inceppò. Quando ci si accorse del fatto era troppo tardi, le congiunzioni astrali che avrebbero garantito l'eterna felicità del matrimonio erano svanite, quindi svanì anche il matrimonio.

di 7, cioè $m = 7h$. Quindi: $n = \frac{23 \cdot 7h - 7}{63} = \frac{7 \cdot (23h - 1)}{7 \cdot 9} = \frac{23h - 1}{9}$. Possiamo allora dire che $23h - 1$ deve essere un multiplo di 9, cioè $23h$ diviso per 9 deve avere per resto 1. Ossia $23h = 9k + 1$ che può anche scriversi $18h + 5h = 9k + 1$ o anche $9(k - 2h) = 5h - 1$. Quindi dobbiamo trovare qualche valore di h compreso tra 0 e 8 per cui $5h - 1$ sia multiplo di 9. Basta provare i diversi valori, trovando così $h = 2$. Otteniamo così $n = \frac{23 \cdot 2 - 1}{9} = \frac{45}{9} = 5$, da cui $m = \frac{63 \cdot 5 + 7}{23} = \frac{322}{23} = 14$. Naturalmente vi sono infinite altre soluzioni $h = 2 + 9t$, infatti anche in questo caso $5h - 1 = 10 + 45t - 1 = 9(5t + 1)$. Quindi $n = 5$ è solo la soluzione minima, le altre soluzioni sono $n = 5 + t$, t numero naturale.

- Rispetto al precedente il problema di Alcuino ha 3 incognite con 2 equazioni, ma il modo di risolvere è analogo: $\begin{cases} u = 100 - d - b \\ 300 - 3d - 3b + 2d + \frac{b}{2} = 100 \end{cases} \Rightarrow \begin{cases} u = 100 - d - b \\ d = \frac{400 - 5b}{2} \end{cases}$.

  Anche stavolta dobbiamo effettuare delle verifiche che quindi dobbiamo ridurre al minimo. Imponiamo allora le condizioni "nascoste":

$$\begin{cases} 0 < u < 100 \\ 0 < d < 100 \end{cases} \Rightarrow \begin{cases} 0 < b + d < 100 \\ 0 < \frac{400 - 5b}{2} < 100 \end{cases} \Rightarrow \begin{cases} 0 < \frac{400 - 3b}{2} < 100 \\ 40 < b < 80 \end{cases} \Rightarrow \begin{cases} \frac{200}{3} < b < \frac{400}{3} \\ 40 < b < 80 \end{cases} \Rightarrow 66 \le b < 80$$

Inoltre b deve essere un numero pari perché d deve essere un numero naturale, quindi $66 \le b \le 78$. Quindi vi sono un numero finito di soluzioni, che scriviamo nella seguente tabella, perché poi Alcuino abbia scelto la soluzione (74, 15, 11) non è dato di sapere:

b	68	70	72	74	76	78
$d = 200 - 5/2b$	30	25	20	15	10	5
$u = 100 - d - b$	2	5	8	11	14	17

Definizione 15. Una equazione polinomiale con due o più incognite a coefficienti interi e per la quale si ricercano soluzioni intere, si chiama **equazione diofantea**.

Le precedente definizione è dovuta al fatto che Diofanto nella sua famosa *Aritmetica*[6], trattò molti di questi problemi. Vogliamo adesso ricercare un risultato che ci permetta di dire se una equazione diofantea ammette o no soluzioni. Abbiamo il seguente risultato.

Teorema 28. L'equazione diofantea di I grado a due incognite $ax + by = 1$ ammette soluzioni solo se $MCD(a,b) = 1$.

Dimostrazione. Supponiamo che sia $a > b$, calcoliamo $MCD(a, b)$ applicando l'algoritmo euclideo. Otteniamo la seguente successione di uguaglianze $a = b \cdot q_1 + r_1$, $b = q_2 \cdot r_1 + r_2$, $r_1 = q_3 \cdot r_2 + r_3$, ... , $r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}$, $r_{n-2} = q_n \cdot r_{n-1} + r_n$. Visto che $MCD(a,b) = 1$, si ha $r_n = 1$. Partendo dall'ultima di tali uguaglianze ed otteniamo: $r_n = 1 = r_{n-2} - q_n \cdot r_{n-1}$, cioè 1 è combinazione lineare di r_{n-2} e r_{n-1}. Adesso possiamo scrivere $1 = r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) = (1 + q_n \cdot q_{n-1}) \cdot r_{n-2} - q_n \cdot r_{n-3}$, cioè 1 è combinazione lineare di r_{n-3} e r_{n-2}. Continuando questo processo di sostituzione, otterremo alla fine che 1 è combinazione lineare di a e b. Il che significa che esistono due numeri x ed y per cui si può scrivere $1 = ax + by$. Ossia la tesi del nostro teorema.

[6] Per curiosità ricordiamo che proprio su una copia di tale opera, Fermat appuntò la sua famosa osservazione sull'equazione $x^n + y^n = z^n$.

Esempio 29.

Risolvere l'equazione diofantea $17x + 19y = 1$. Abbiamo $19 = 17 \cdot 1 + 2$, da cui $17 = 8 \cdot 2 + 1$, $8 = 8 \cdot 1 + 0$. Ma allora $1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (19 - 17 \cdot 1) = 17 - 8 \cdot 19 + 8 \cdot 17 = 17 \cdot 9 - 8 \cdot 19$. Quindi $(x = 9, y = -8)$ è una soluzione dell'equazione data.

Vale anche il seguente risultato.

Teorema 29. L'equazione diofantea di I grado a due incognite $ax + by = c$ ammette soluzioni solo se $MCD(a, b)$ è un divisore di c.

Esempio 30.

- L'equazione $4x - 6y = 3$ non ha soluzioni intere perché $MCD(4, 6) = 2$ non divide 3.
- L'equazione $24x + 40x = 48$ ammette soluzioni intere perché $MCD(24, 40) = 8$ che è un divisore di 48. Essa equivale quindi all'equazione $3x + 5y = 6$ che ha soluzioni perché $MCD(3, 5) = 1$ che divide 6. Vediamo di trovare una soluzione. Applichiamo l'algoritmo euclideo per determinare il $MCD(3, 5)$. $5 = 3 \cdot 1 + 2$, $3 = 2 \cdot 1 + 1$, $2 = 2 \cdot 1 + 0$. Allora $1 = 3 - 2 \cdot 1 = 3 - 1 \cdot (5 - 3) = 3 \cdot 2 - 5 \cdot 1$. Quindi $(x = 2, y = -1)$ è una soluzione dell'equazione $3x + 5y = 1$, che non è l'equazione data. Ma possiamo determinare facilmente una soluzione di tale equazione. Infatti da $1 = 3 \cdot 2 - 5 \cdot 1$ si ha $6 = 3 \cdot 12 - 5 \cdot 6$, quindi una soluzione è $(x = 12, y = -6)$.

Siamo adesso interessati a determinare la soluzione generale dell'equazione $ax + by = c$. Vale il seguente fatto.

Teorema 30. L'equazione diofantea di I grado a due incognite $ax + by = c$, nell'ipotesi in cui ammette una soluzione $x = x_0$ e $y = y_0$, tutte le sue soluzioni si ottengono dalla formula: $x = x_0 + t \cdot b$ e $y = y_0 - t \cdot a$, al variare del parametro t in $\mathbb{Z}$.
Dimostrazione. Supponiamo che $x = x_0$ e $y = y_0$ sia una soluzione di $ax + by = c$, ciò vuol dire che possiamo scrivere $ax_0 + by_0 = c$. Sottraiamo membro a membro le precedenti uguaglianze, ottenendo: $a \cdot (x - x_0) + b \cdot (y - y_0) = 0 \Rightarrow a \cdot (x - x_0) = -b \cdot (y - y_0)$. Quindi $a(x - x_0)$ è divisibile per b e poiché a non è divisibile per b vuol dire che lo è $(x - x_0)$. Quindi possiamo scrivere $x - x_0 = t \cdot b$. Ma allora è vero che $a \cdot t \cdot b = -b \cdot (y - y_0) \Rightarrow a \cdot t = -y + y_0$. Possiamo quindi scrivere: $x = x_0 + t \cdot b$ e $y = -a \cdot t + y_0$. Queste due scritte costituiscono la tesi cercata.

Esempio 31.

La soluzione generale dell'equazione $3x + 5y = 6$ è $x = 12 + 5t$, $y = -6 - 3t$. In particolare potrebbe interessarci stabilire qual è la minima soluzione positiva dell'equazione. Ora $12 + 5t > 0 \Rightarrow t > -12/5 \Rightarrow t > -2$. Così la minima x positiva è $x = 12 + 5 \cdot (-2) = 2$. Allo stesso modo $-6 - 3t > 0 \Rightarrow t < -2$ e la minima soluzione positiva di y si ottiene per $t = -3$ ed è $y = 3$. Non esiste alcuna soluzione con entrambi i valori positivi.

Esercizi.

1. Se il 55% degli agnelli nati in un gregge sono maschi ed il 90% sopravvive il primo anno, qual è il minimo numero di agnelli maschi nati affinché alla fine del primo anno ve ne siano 100 vivi? **[203]**
2. Da un manoscritto arabo del 1200: Un'oca costa 5 dracme, una gallina 1 dracma e 20 pulcini 1 dracma. Avendo 100 dracme e volendo comprare 100 animali, quanti dovrai prenderne di ciascun tipo? **[19 oche, 1 gallina, 80 pulcini]**
3. Da un manuale tedesco del 1526: In una taverna, 20 persone pagano un conto di 20 dobloni. Vi sono uomini, donne e bambini. Sapendo che gli uomini pagano 3 dobloni, le donne 2 ed i bambini ½ doblone, determinare quanti erano gli uomini, quante le donne e quanti i bambini. **[$u = 1$, $d = 5$, $b = 14$]**
4. Dal *Lilavati* di Bhaskara: O matematico, rispondi rapidamente. Qual è il minimo numero naturale che moltiplicato per 221 ed aumentato di 65 diviene un multiplo di 195? **[5]**
5. Un anno fa Alex aveva un età il cui valore numerico era reversale (per esempio 27 e 72) di quella di sua madre Xela. Quest'anno invece la sua età è reversale di quella di suo padre Eric. Se la somma delle età dei suoi genitori, oggi, è di 93, determinare l'età attuale di Alex. **[15]**
6. Un teatro ha 100 posti. Il proprietario vuole incassare 100 euro facendo pagare 5 euro il prezzo intero, 2 euro il ridotto militari e per ogni 10 ragazzi al di sotto dei 12 anni farà pagare 1 euro. Quanti adulti, militari e ragazzi devono entrare? **[11 adulti, 19 militari e 70 ragazzi]**
7. Dall'Algebra di Eulero. Dividi 100 in due addendi, uno divisibile per 7 e l'altro per 11. **[44 e 56]**
8. Da Mahaviracarya. Furono raccolte delle mele, che furono sistemate in 37 cassette, ciascuna contenente lo stesso numero di frutti. Ogni cassetta conteneva più di 100 e meno di 200 mele. Sapendo che i raccoglitori erano 79 e che quando si divisero le mele in parti uguali ne avanzarono 17, si vuol sapere quante mele ebbe ciascun raccoglitore e quante ne conteneva ciascuna cassetta. **[78 e 167]**
9. Risolvere le seguenti equazioni diofantee, determinando la minima soluzione positiva, se esiste. a) $37x - 41y = 11$; b) $23x + 15y = 24$; c) $123x + 35y = 15$; d) $43x - 71y = 2$; e) $132x + 61y = -4$. **[a) (25; 28); b) ∅; c) ∅; d) (3; 5); e) ∅]**
10. Un quesito da Stanford 1957. Bob tiene i suoi francobolli in tre album. Due decimi sono nel primo album, alcuni settimi nel secondo e 303 nel terzo. Quanti francobolli ha Bob? **[3535]**

§13. Teoria delle congruenze.

Abbiamo trattato più volte con le divisioni fra numeri interi, ci sembra perciò opportuno porre alcune definizioni al riguardo.

Definizione 16. Due numeri interi m ed n si dicono **congruenti modulo *r*** se $m - n$ è divisibile per r. Indichiamo questo fatto scrivendo $m \equiv n \bmod r$ o anche $m \overset{r}{\equiv} n$[7]

Esempio 32.

I numeri 7 e 3 sono congruenti modulo 2 e anche modulo 4, dato che 7 – 3 = 4. Quindi $7 \overset{2}{\equiv} 3$ e anche $7 \overset{4}{\equiv} 3$.

Il precedente concetto è dovuto, almeno nella sua sistemazione organica, a Carl Friedrich Gauss, che lo presentò nella sua opera *Disquisitiones arithmeticae* del 1801. Vediamo adesso di introdurre delle operazioni sulle congruenze.

Esempio 33.

Sappiamo che $7 \overset{2}{\equiv} 3$ e $11 \overset{2}{\equiv} 5$, cosa possiamo dire di (7 + 11)? O meglio, possiamo dire che $(7+11) \overset{2}{\equiv} (3+5)$? Una semplice verifica ci convince di sì. Anzi, almeno nel caso del modulo 2, possiamo dire che se $m \overset{2}{\equiv} n$, vuol dire che m ed n sono entrambi pari od entrambi dispari. Allora da $m \overset{2}{\equiv} n$ e $p \overset{2}{\equiv} q$, possiamo dire che vale anche $(m+p) \overset{2}{\equiv} (n+q)$, dato che anche $m + p$ e $n + q$ saranno numeri entrambi dispari o entrambi pari.

L'esempio precedente ci suggerisce di tentare di provare il seguente risultato.

Teorema 31. $m \overset{r}{\equiv} n$ e $p \overset{r}{\equiv} q \Rightarrow (m \pm p) \overset{r}{\equiv} (n \pm q)$.

Dimostrazione. Le ipotesi possono scriversi nel seguente modo: $(m - n) = h \cdot r$, $h \in \mathbb{Z}$ e $(p - q) = k \cdot r$, $k \in \mathbb{Z}$. Ma allora possiamo dire che $(m \pm p) - (n \pm q) = (m - n) \pm (p - q) = h \cdot r \pm k \cdot r = (h \pm k) \cdot r$. Il che equivale alla tesi.

Da questo risultato segue quest'altro.

Corollario 2. $m \overset{r}{\equiv} n \Rightarrow m \cdot p \overset{r}{\equiv} n \cdot p, \forall p \in \mathbb{Z} \setminus \{0\}$.

Dimostrazione. È una immediata conseguenza del Teorema 31, dato che moltiplicare per p equivale a sommare algebricamente p volte la congruenza $m \overset{r}{\equiv} n$.

In generale invece non vale il viceversa, cioè $m \cdot p \overset{r}{\equiv} n \cdot p \not\Rightarrow m \overset{r}{\equiv} n, p \neq 0$.

[7] Questa notazione è esclusivamente mia, non viene usata, per quanto ne sappia, in alcun altro testo

Esempio 34.

Si ha $35 \overset{5}{\equiv} 20$, ma non è vero che $7 \overset{5}{\equiv} 4$. Invece è vero che $21 \overset{10}{\equiv} 6 \Rightarrow 7 \overset{10}{\equiv} 2$. È inoltre vero che $35 \overset{10}{\equiv} 25 \Rightarrow 7 \overset{2}{\equiv} 5$.

Quanto visto nell'esempio precedente permette di enunciare il seguente risultato.

Teorema 32. $m \cdot p \overset{r}{\equiv} n \cdot p \Rightarrow m \overset{r/MCD(r,p)}{\equiv} n$.

Dimostrazione. Supponiamo che, allora da $p \cdot (m - n) = h \cdot r$ segue che $h = p \cdot t$, quindi $p \cdot (m - n) = p \cdot t \cdot r \Rightarrow (m - n) = t \cdot r$, ossia $m \overset{r}{\equiv} n$. Adesso sia $MCD(r, p) = t > 1 \Rightarrow r = k \cdot t$ e $p = q \cdot t$, allora da $p \cdot (m - n) = h \cdot r \Rightarrow q \cdot t \cdot (m - n) = h \cdot k \cdot t \Rightarrow q \cdot (m - n) = h \cdot \frac{k \cdot t}{t} = \frac{r}{MCD(r,t)\, p} \Rightarrow m \overset{r/MCD(r,p)}{\equiv} n$.

Il seguente risultato è immediato.

Corollario 3. $MCD(r, p) = 1 \Rightarrow m \cdot p \overset{r}{\equiv} n \cdot p \Rightarrow m \overset{r}{\equiv} n, \forall p \in \mathbb{Z} \setminus \{0\}$.

Vale anche quest'altra proprietà.

Teorema 33. $m \overset{r}{\equiv} n$ e $p \overset{r}{\equiv} q \Rightarrow m \cdot p \overset{r}{\equiv} n \cdot q$.

Dimostrazione. Si ha $(m - n) = h \cdot r$ e $(p - q) = k \cdot r \;\; h, k \in \mathbb{Z}$. Moltiplicando membro a membro, abbiamo: $(m - n) \cdot (p - q) = h \cdot k \cdot r$. Possiamo anche scrivere: $(m - n) \cdot (p - q) = m \cdot p - n \cdot p - m \cdot q + n \cdot q = m \cdot p - n \cdot q + n \cdot q - n \cdot p - m \cdot q + n \cdot q = (m \cdot p - n \cdot q) - n \cdot (p - q) - q \cdot (m - n)$. Abbiamo ottenuto una uguaglianza in cui il primo membro è divisibile per r, mentre il secondo membro è formato da tre addendi, due dei quali sono divisibili per r, quindi anche il terzo addendo, cioè $(m \cdot p - n \cdot q)$ deve essere divisibile per r. Ciò equivale alla tesi.

Quest'ultimo teorema ci fornisce uno strumento molto potente per determinare la verità o meno di congruenze i cui termini sono "grandi".

Esempio 35.

Determinare il valore di n nella seguente congruenza: $13^{17} \overset{19}{\equiv} n$. Il numero 13^{17} ha ben 19 cifre, perciò non è opportuno calcolarlo e dividerlo per 19. Utilizziamo invece il teorema 32. Abbiamo: $13 \overset{19}{\equiv} -6$ (infatti $13 - (-6) = 19$), quindi $13^2 \overset{19}{\equiv} 36$, ma $36 \overset{19}{\equiv} -2$, perciò $13^2 \overset{19}{\equiv} -2$. Allo stesso modo: $13^{16} \overset{19}{\equiv} (-2)^8 = 256 \overset{19}{\equiv} 9 \Rightarrow 13^{16} \overset{19}{\equiv} 9$. Infine $13^{17} \overset{19}{\equiv} (-6) \cdot 9 = -54 \overset{19}{\equiv} 3 \Rightarrow 13^{17} \overset{19}{\equiv} 3$, quindi $n = 3$.

Torniamo al Teorema di Wilson e vediamo una struttura di dimostrazione ragionando su un caso particolare. Consideriamo per esempio $p = 19$ e consideriamo 19!. Abbiamo che si ha ovviamente $1 \overset{19}{\equiv} 1, 18 \overset{19}{\equiv} -1$. Ora consideriamo gli altri 16 numeri osservando che

possiamo accoppiarli in modo che il loro prodotto sia congruo a 1 modulo 19, infatti abbiamo: $2\cdot 10 \overset{19}{\equiv} 1, 3\cdot 13 \overset{19}{\equiv} 1, 4\cdot 5 \overset{19}{\equiv} 1, 6\cdot 16 \overset{19}{\equiv} 1, 7\cdot 11 \overset{19}{\equiv} 1, 8\cdot 12 \overset{19}{\equiv} 1, 9\cdot 17 \overset{19}{\equiv} 1, 14\cdot 15 \overset{19}{\equiv} 1$, ciò significa che $18! \overset{19}{\equiv} -1$, che quanto voluto.
Vi è un interessante corollario del Teorema di Wilson.

Corollario 4. Se un numero primo $p = 4n + 1 \Rightarrow \left[(2n)!\right]^2 \overset{p}{\equiv} -1$.

Dimostrazione Si ha $4n \overset{4n+1}{\equiv} -1, 4n-1 \overset{4n+1}{\equiv} -2, ..., 4n-(2n-1) = 2n+1 \overset{4n+1}{\equiv} -2n$, moltiplicando fra loro queste congruenze otteniamo $(2n + 1) \cdot (2n + 2) \cdot \ldots \cdot 4n \overset{4n+1}{\equiv} (-1)^{2n} \cdot 1 \cdot 2 \cdot \ldots \cdot (2n) = (2n)!$, il primo membro diventa il fattoriale di $4n$ se moltiplichiamo per il secondo membro, pertanto: $(4n)! \overset{4n+1}{\equiv} \left[(2n)!\right]^2$, che è la tesi, dato che per il Teorema di Wilson si ha: $(4n)! + 1 \overset{4n+1}{\equiv} 0 \Rightarrow (4n)! \overset{4n+1}{\equiv} -1$.

È semplice provare che la relazione di congruenza è una relazione di equivalenza su $\mathbb{Z}$, verifica cioè le proprietà riflessiva ($n \overset{r}{\equiv} n, \forall n, r \in \mathbb{Z}$), simmetrica ($m \overset{r}{\equiv} n \Rightarrow n \overset{r}{\equiv} m$) e transitiva ($m \overset{r}{\equiv} n, n \overset{r}{\equiv} p \Rightarrow m \overset{r}{\equiv} p$). Pertanto possiamo considerare l'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza, che è formato raggruppando in classi tutti i numeri la cui differenza è divisibile per i vari numeri interi. In particolare è interessante considerare gli insiemi $\mathbb{Z}_n$ formati raggruppando tutti i numeri interi in classi, a seconda del resto della divisione di essi per il numero dato *n*. Si prova che in questo caso $\mathbb{Z}_n$ è un anello rispetto alle operazioni di somma e prodotto fra congruenze che abbiamo introdotto, anzi se *n* è un numero primo rappresenta un campo. Questi sono i cosiddetti campi di Galois, esempi di campi finiti, ossia con un numero finito di elementi.
Ci interessa adesso risolvere equazioni con le congruenze, cioè equazioni del tipo $f(x) \overset{r}{\equiv} n$, in cui l'incognita è indicata con *x*, mentre *f*(*x*) indica una espressione contenente *x*.

Esempio 36.

- La congruenza $x \overset{3}{\equiv} 5$, ammette le infinite soluzioni $x = 5h + 3$, con *h* numero naturale.
- La congruenza $x^2 - 3 \overset{5}{\equiv} 3$, ammette le soluzioni $x = 5 + h$ e $x = 5 + 4h$. Infatti abbiamo $1^2 - 3 - 3 = -5$ e $4^2 - 3 - 3 = 10$ che sono entrambi multipli di 5, mentre la verifica con gli altri possibili resti della divisione per 5 non lo sono: $0^2 - 3 - 3 = -6$, $2^2 - 3 - 3 = -2$, $3^2 - 3 - 3 = 3$.
- Invece la congruenza $x^2 - 3 \overset{5}{\equiv} 4$, non ammette alcuna soluzione, come si verifica facilmente sostituendo i valori $x = 0, 1, 2, 3, 4$ (cioè tutti i possibili resti di una divisione con 5 come divisore).

Come si è visto nell'esempio precedente vi sono congruenze che hanno infinite soluzioni e congruenze che non hanno soluzioni. Nel primo caso, dato che in realtà tutte le soluzioni sono congruenti fra di loro si preferisce considerarne solo una di esse, per esempio la minore positiva. Così nell'esempio precedente la soluzione di $x \overset{3}{\equiv} 5$ è 5, mentre le

soluzioni di $x^2-3\overset{5}{\equiv}3$ sono 1 e 4 rispettivamente. In questo modo una congruenza del tipo $f(x)\overset{r}{\equiv}n$ non può avere più di *r* soluzioni. Vediamo di trattare i più semplici tipi di congruenze.

Definizione 17. Una congruenza del tipo $a\cdot x\overset{r}{\equiv}b$, si dice **congruenza lineare**.

Ci accorgiamo subito che risolvere la congruenza lineare $a\cdot x\overset{r}{\equiv}b$, equivale a risolvere l'equazione indeterminata $ax - b = ry \Rightarrow ax - ry = b$. Per quel che abbiamo visto nel paragrafo precedente possiamo dire che una congruenza lineare $a\cdot x\overset{r}{\equiv}b$, ammette soluzioni solo se $MCD(a, r)$ divide *b*. vale anzi il seguente risultato.

Teorema 34. La congruenza lineare $a\cdot x\overset{r}{\equiv}b$ ha soluzioni solo se $m = \text{MCD}(a, r)$ divide *b*, in questo caso ha *m* soluzioni distinte, date da $x_k=\bar{x}\cdot\frac{b}{m}+k\cdot\frac{r}{m}, 0\le k\le m-1$, con $\bar{x}$ tale che $\bar{x}\cdot\frac{a}{m}\overset{r/m}{\equiv}1$.

Definizione 18. Diciamo che $\bar{x}$ è inverso aritmetico di *x* modulo se $\bar{x}\cdot x\overset{r}{\equiv}1$.

Quindi nel Teorema 34 la soluzione dipende dall'inverso aritmetico di *a/m* modulo *r/m*.

Esempio 37.

- La congruenza lineare $6x\overset{3}{\equiv}5$ non ha soluzioni, perché $MCD(6, 3) = 2$ non divide 5.
- Invece la congruenza $18x\overset{10}{\equiv}8$ ha soluzione, perché MCD(18, 10) = 2 divide 8 e ha quindi due soluzioni. Poiché congruo a 8 modulo 10 significa che ha 8 come cifra delle unità si vede subito che le soluzioni sono solo $18\cdot 1 = 18 \overset{10}{\equiv} 8$ e $18\cdot 6 \overset{10}{\equiv} 8$. Potevamo trovarle applicando il teorema precedente. L'inverso aritmetico di 18/2 = 9 modulo 10/2 = 5 è soluzione dell'equazione $\bar{x}\cdot 9\overset{5}{\equiv}1$, che si trova essere $\bar{x}$ = 4. Quindi le due soluzioni sono: $x_1 = 4\cdot 4 + 1\cdot 5 = 21 \overset{10}{\equiv} 1$ e $x_2 = 4\cdot 4 + 2\cdot 5 = 26 \overset{10}{\equiv} 6$.
- Non sempre vi è l'inverso aritmetico di un numero modulo un altro numero. Per esempio non esiste l'inverso aritmetico di 15 modulo 12. Infatti $(4n)\cdot 15\overset{12}{\equiv}0;(4n+1)\cdot 15\overset{12}{\equiv}3;(4n+2)\cdot 15\overset{12}{\equiv}6;(4n+3)\cdot 15\overset{12}{\equiv}9$

Può capitare di dover risolvere sistemi di congruenze lineari.

Esempio 38.

Risolvere il seguente sistema di congruenze: $\begin{cases} x\overset{3}{\equiv}7 \\ x\overset{3}{\equiv}17 \end{cases}$. Risolviamo la prima congruenza, ottenendo: $x = 13y - 7$, per qualche $y\in\mathbb{N}$. La seconda congruenza invece fornisce le soluzioni: $x = 17z - 3$, per qualche $z\in\mathbb{Z}$. Devono quindi trovarsi due numeri interi *y* e *z*,

verificanti l'equazione diofantea $13y - 7 = 17z - 3$, cioè $13y - 17z = 4$. Poiché $MCD(13, 17) = 1$, che divide 4, l'equazione ammette soluzioni. Esse si ottengono mediante il seguente procedimento: $17 = 13 + 4$; $13 = 3 \cdot 4 + 1$. Quindi $1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 13) = 4 \cdot 13 - 3 \cdot 17$. Una soluzione di $13y - 17z = 1$ è $y = 4$, $z = 3$, perciò una soluzione di $13y - 17z = 4$ è $y = 16$, $z = 12$. Allora abbiamo $x = 13 \cdot 16 - 7 = 13 \cdot 17 - 20$. Perciò le soluzioni del sistema sono tutte le soluzioni di $x \overset{13\cdot 7}{\equiv} -20$.

In effetti alcuni sistemi si risolvono più facilmente, come afferma il seguente enunciato.

Teorema 35. Il sistema $\begin{cases} x \overset{r_1}{\equiv} n \\ x \overset{r_2}{\equiv} n \\ \dots \\ x \overset{r_h}{\equiv} n \end{cases}$ equivale a $x \overset{mcm(r_1, r_2, \dots, r_h)}{\equiv} n$.

Dimostrazione. Abbiamo $(x - n) = k_1 \cdot r_1 = k_2 \cdot r_2 = \dots = k_h \cdot r_h$. Cioè $(x - n)$ è multiplo di tutti gli r_i, quindi anche del loro minimo comune multiplo.

Esempio 39.

Per il Teorema precedente $\begin{cases} x \overset{3}{\equiv} 2 \\ x \overset{4}{\equiv} 2 \end{cases}$ equivale a $x \overset{12}{\equiv} 2$, quindi a $x = 12h + 2$. Infatti $12h + 2 - 2 = 12h$ che è multiplo di 3, ma anche multiplo di 4.

Per risolvere un sistema generico di h congruenze lineari, possiamo enunciare il seguente risultato.

Teorema 36. Un sistema di h congruenze lineari $\begin{cases} x \overset{r_1}{\equiv} n_1 \\ x \overset{r_2}{\equiv} n_2 \\ \dots \\ x \overset{r_h}{\equiv} n_h \end{cases}$, ammette un'unica soluzione solo se $n_i \overset{MCD(r_i, r_j)}{\equiv} n_j, \forall (i, j) \in \mathbb{N}^2, 1 \le i < j \le h$. Tale soluzione è $x \overset{M}{\equiv} \sum_{j=1}^{h} n_j \cdot m_j \cdot \frac{M}{r_j}$, con $M = mcm(r_1, r_2, \dots, r_h)$ e $\frac{M}{r_j} \cdot m_i \overset{r_j}{\equiv} 1$.

Il precedente teorema è noto sotto il nome di teorema cinese del resto, poiché anche se non sotto questa forma così rigorosa, esso è stato trovato in un'opera di un certo Sun – Tse, vissuto nei primi anni dell'era cristiana.

Esempio 40.

Consideriamo un antico problema di epoca medioevale: Al mercato un cavallo passò sopra il cestino pieno di uova di una donna distruggendole tutte. Il cavaliere si mostrò pronto a pagare il danno e chiese alla donna quante uova vi erano nel cestino. Lei rispose di non ricordare l'esatto numero. Ricordava però che aveva pensato di

raggrupparle a due a due e gliene era avanzato uno. Aveva allora tentato di raggrupparle a tre a tre ed ancora gliene avanzava uno. Le avanzò sempre un uovo raggruppandoli a gruppi di 4, 5 e 6. Finalmente li poté raggruppare a 7 a 7. Quante erano al minimo le uova? Praticamente dobbiamo risolvere il sistema di 6 congruenze lineari $\begin{cases} x \overset{2}{\equiv} 2 \\ x \overset{2}{\equiv} 3 \\ x \overset{2}{\equiv} 4 \\ x \overset{2}{\equiv} 5 \\ x \overset{2}{\equiv} 6 \\ x \overset{2}{\equiv} 7 \end{cases}$. In effetti le prime cinque congruenze possono essere sostituite dall'unica $x \overset{mcm(2,3,4,5,6)}{\equiv} 1 \Leftrightarrow x \overset{60}{\equiv} 1$. Quindi basta risolvere il sistema $\begin{cases} x \overset{60}{\equiv} 1 \\ x \overset{7}{\equiv} 0 \end{cases}$. Da cui $x = 60t + 1 \overset{7}{\equiv} 0 \Rightarrow 60t \overset{7}{\equiv} -1 \Rightarrow 4t \overset{7}{\equiv} -1$, abbiamo eliminato $56t$ perché multiplo di 7; $20t \overset{7}{\equiv} -5 \overset{7}{\equiv} 2 \Rightarrow -t \overset{7}{\equiv} 2 \Rightarrow t \overset{7}{\equiv} -2 \Rightarrow t = 7h - 2$, perciò $x = 420h - 119 \Rightarrow x \overset{420}{\equiv} -119$, con $420 = mcm(60, 7)$. Quindi le uova minimo erano $420 - 119 = 301$.

Esercizi.

1. Provare che la relazione di congruenza è una relazione di equivalenza.
2. Risolvere le seguenti equazioni: : a) $2^{27} \overset{23}{\equiv} n$; b) $3^{41} \overset{37}{\equiv} n$; c) $11^{125} \overset{41}{\equiv} n$; d) $5^{217} \overset{13}{\equiv} n$; e) $7^{276} \overset{29}{\equiv} n$. **[a) 9; b) 21; c) 3; d) 5; e) 24]**
3. Risolvere le seguenti congruenze: a) $x^2 \overset{13}{\equiv} 1$; b) $x^2 - x + 2 \overset{7}{\equiv} -1$; c) $2x^2 - x + 1 \overset{5}{\equiv} 0$; d) $x^3 - x - 2 \overset{12}{\equiv} 4$. **[a) ±1; b) ∅; c) ∅; d) x = ±2, 6]**
4. Trovare gli inversi aritmetici di 15 moduli a) 7; b) 10; c) 11. **[a) 1; b) ∅; c) 3]**
5. Risolvere le congruenze lineari: a) $3x \overset{11}{\equiv} 7$; b) $13x \overset{123}{\equiv} 17$; c) $144x \overset{36}{\equiv} 60$; d) $1234x \overset{12}{\equiv} 5678$. **[a) 6; b) 77; c) ∅; d) –1 ∨ 5]**
6. Risolvere il problema delle uova con la modifica seguente: raggruppando le uova a n a n ($2 \le n \le 5$) ne rimangono $n - 1$, mentre a 7 a 7 non vi sono rimanenze. Suggerimento: cercare di scrivere le congruenze in modo da potere applicare il Teorema 35. **[119]**
7. Un quesito da Stanford 1949. Provare che nessun numero della successione {11, 11, 1111, …} è un quadrato perfetto.
8. Un problema di Regiomontano. Risolvere $\begin{cases} x \overset{10}{\equiv} 3 \\ x \overset{13}{\equiv} 11 \\ x \overset{17}{\equiv} 15 \end{cases}$. $\left[x \overset{2210}{\equiv} 1103 \right]$
9. Un problema di Eulero. Risolvere $\begin{cases} x \overset{11}{\equiv} 3 \\ x \overset{19}{\equiv} 5 \\ x \overset{29}{\equiv} 10 \end{cases}$. $\left[x \overset{6061}{\equiv} -1993 \right]$
10. Dal *Sun Tsu Suan Ching*. *Un numero minore di* 100 *è tale che se lo dividiamo per* 3 *il resto è* 2; *dividendolo per* 5 *il resto è* 3; *dividendolo per* 7 *il resto è* 2. *Qual è questo numero*? **[23]**
11. Usando le congruenze provare che $2^{32} + 1$ è divisibile per 641.
12. Provare che $x + y + z$ è multiplo di 6 solo se lo è $x^3 + y^3 + z^3$.
13. Provare che $3^{2n+1} + 2^{n+2}$ è multiplo di 7, $\forall n \in \mathbb{N}$.

§14. Criteri di divisibilità.

Vediamo di utilizzare i precedenti concetti sulle congruenze per determinare i noti (ed i meno noti) criteri di divisibilità. Consideriamo un generico numero intero, la cui espressione in base 10 è $a_n a_{n-1} a_{n-2} ... a_1 a_0$, in cui a_i indica una cifra, ossia un numero intero compreso tra 0 e 9. Dal significato della notazione posizionale possiamo dire che il detto numero può anche esprimersi nella seguente forma "polinomiale": $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_1 \cdot 10 + a_0 \cdot 10^0$. È evidente che se un numero m è divisibile per un numero k, anche $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_1 \cdot 10 + a_0 \cdot 10^0$ è divisibile per 2. Dire che m è divisibile per 2, nella teoria delle congruenze significa dire che $m \overset{2}{\equiv} 0$. Cioè $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_1 \cdot 10 + a_0 \cdot 10^0) \overset{2}{\equiv} 0$. Ma i primi n addendi sono congruenti a 0 mod 2, sono cioè divisibili per 2, dato che contengono almeno un fattore 10. Ciò significa che $m \overset{2}{\equiv} 0 \Leftrightarrow a_0 \overset{2}{\equiv} 0$. Possiamo quindi enunciare il ben noto criterio seguente.

Criterio di divisibilità per 2. Un numero naturale m è divisibile per 2 se e solo se lo è la sua cifra delle unità.

A questo punto è molto semplice stabilire un criterio di divisibilità per 4, infatti $m \overset{4}{\equiv} 0 \Leftrightarrow (a_1 \cdot 10 + a_0) \; m \overset{4}{\equiv} 0$, dato che tutti gli altri addendi contengono almeno un fattore 10^2, che è divisibile per 2.

Criterio di divisibilità per 4. Un numero naturale $m > 9$, è divisibile per 4 se lo è il numero formato con le sue cifre della decina e delle unità.

Risulta immediata la seguente generalizzazione.

Criterio di divisibilità per 2^n. Un numero naturale $m > 10^{n-1}$, è divisibile per 2^n se lo è il numero formato con le sue ultime n cifre.

Esempio 41.

Il numero 12345678 è divisibile per 2 ma non per 4, perché 8 è divisibile per 2 ma 78 non è divisibile per 4. Il numero 12348840 è divisibile per 8, perché $840 = 8 \cdot 105$, ma non per 16, perché $8840 = 16 \cdot 552 + 8$.

Passiamo alla divisibilità per 3. Abbiamo $10 \overset{3}{\equiv} 1$, quindi $10^n \overset{3}{\equiv} 1, \forall n \in \mathbb{N}$. Ciò significa che $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_1 \cdot 10 + a_0 \cdot 10^0) \overset{3}{\equiv} 0 \Leftrightarrow (a_n + a_{n-1} + a_{n-2} \cdot \; + ... + a_1 + a_0) \overset{3}{\equiv} 0$. Da cui segue il ben noto criterio seguente.

Criterio di divisibilità per 3. Un numero naturale m è divisibile per 3 se lo è il numero formato sommando tutte le sue cifre.

Poiché si ha anche $10 \overset{9}{\equiv} 1$, il precedente criterio vale anche per tale numero.

Criterio di divisibilità per 9. Un numero naturale m è divisibile per 9 se lo è il numero formato sommando tutte le sue cifre.

Non possiamo generalizzare il precedente criterio di divisibilità perché si ha: $10^0 \overset{27}{\equiv} 1, 10 \overset{27}{\equiv} 10, 10^2 \overset{27}{\equiv} 19, 10^3 \overset{27}{\equiv} 1$. Possiamo però ottenere un altro criterio.
La divisibilità per 5 è molto facile da ottenere poiché, come è accaduto per il numero 2, tutti gli addendi tranne l'ultimo, nell'espressione polinomiale del numero sono divisibili per 5, quindi tutto è delegato alla divisibilità di a_0. E poiché $a_0 \overset{5}{\equiv} 0 \Leftrightarrow a_0 = 0 \vee 5$, abbiamo il ben noto criterio seguente.

Criterio di divisibilità per 5. Un numero naturale m è divisibile per 5 se la sua cifra delle unità è 0 oppure 5.

Passiamo alla divisibilità per 7. Abbiamo la seguente catena di congruenze:

$$10^0 \overset{7}{\equiv} 1, 10 \overset{7}{\equiv} 3, 10^2 \overset{7}{\equiv} 2, 10^3 \overset{7}{\equiv} -1, 10^4 \overset{7}{\equiv} 4, 10^5 \overset{7}{\equiv} -2, 10^6 \overset{7}{\equiv} 1.$$

Possiamo perciò dire che $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_1 \cdot 10 + a_0 \cdot 10^0) \overset{7}{\equiv} 0 \Leftrightarrow (a_0 + 3a_1 + 2a_2 - a_3 + 4a_4 - 2a_5) + (a_6 + 3a_7 + 2a_8 - a_9 + 4a_{10} - 2a_{11}) + ... \overset{7}{\equiv} 0$.
Come si vede un criterio molto complicato da tenere a mente.
Riteniamo opportuno sottolineare che il criterio si ottiene nel momento in cui si trova il primo valore positivo di n per cui si ha $10^n \overset{m}{\equiv} 1$, dato che ovviamente a partire da questo valore si ripeteranno tutti i precedenti resti ottenuti.

Esempio 42.

86422 è divisibile per 7 perché $(2 + 3 \cdot 2 + 2 \cdot 4 - 6 + 4 \cdot 8) = 2 + 6 + 8 - 6 + 32 = 42$ è divisibile per 7. Invece 123456789 non è divisibile per 7 perché $(9 + 3 \cdot 8 + 2 \cdot 7 - 6 + 4 \cdot 5 - 2 \cdot 4 + 3 + 3 \cdot 2 + 2 \cdot 1) = 9 + 24 + 14 - 6 + 20 - 8 + 3 + 6 + 2 = 64$ non è divisibile per 7.

Lasciamo al lettore la dimostrazione del ben noto criterio per 11.

Criterio di divisibilità per 11. Un numero naturale m è divisibile per 11 se la differenza fra la somma delle sue cifre di posto dispari e la somma delle sue cifre di posto pari lo è.

Utilizzando le congruenze possiamo anche giustificare la cosiddetta prova del 9 per verificare se il risultato di un'operazione aritmetica è errato. Ricordiamo che la regola non permette di dire se il risultato è giusto. Infatti se eseguiamo $m + n$, allora se $m \overset{9}{\equiv} p$ e $n \overset{9}{\equiv} q$, allora $m + n \overset{9}{\equiv} p + q$. Se ciò non avviene l'operazione non è corretta, mentre se avviene non è detto che sia corretta. Potremmo anche stabilire una prova del 7 o del 19 o di quel che ci pare, ma il modulo 9 ovviamente crea una regola semplice da applicare. Dato che per determinare il resto della divisione di un numero per 9 basta sommare le cifre ed eliminare il massimo multiplo di 9 che contiene tale somma, in pratica sommare ripetutamente le cifre dei numeri ottenuti finché non si ottiene un numero di una cifra.

Esempio 43.

Consideriamo l'operazione: 123456 + 58749 = 182105. Abbiamo $123456 \overset{9}{\equiv} 3$ e $58749 \overset{9}{\equiv} 6$, se l'operazione è corretta dovrebbe aversi $182105 \overset{9}{\equiv} 3 + 6 \overset{9}{\equiv} 0$, mentre invece si ha $182105 \overset{9}{\equiv} 8$, quindi il risultato della somma è sbagliato. Si noti però che la prova del 9 "funziona" anche con i risultati errati 182106, 190105 e via di questo passo.

Esercizi.

1. Provare che un criterio di divisibilità per n coinvolge un'espressione che ha al massimo $(n - 1)$ termini.
2. Determinare un criterio di divisibilità per 25.
   [Le ultime due cifre devono essere divisibili per 25]
3. Determinare un criterio di divisibilità per 5^n.
   [Le ultime n cifre devono essere divisibili per 5^n]
4. Determinare un criterio di divisibilità per 13. Verificarlo sul numero 3195258885.
   [$(a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5) + ...$]
5. Determinare un criterio di divisibilità per 17. Verificarlo con 421361401347108.
   [$(a_0 - 7a_1 - 2a_2 - 3a_3 + 4a_4 + 6a_5 - 8a_6 + 5a_7 - a_8 + 7a_9 + 2a_{10} + 3a_{11} - 4a_{12} - 6a_{13} + 8a_{14} - 5a_{15}) + ...$]
6. Determinare un criterio di divisibilità per 27. Verificarlo sul numero 39363192.
   [$(a_0 + 10a_1 - 8a_2) + (a_3 + 10a_4 - 8a_5) + \ldots$]
7. Per numeri "grandi" conviene considerare prove con numeri superiori a 9, per esempio 99. Determinare una prova del 99 e verificarla per stabilire se può essere corretta la moltiplicazione $245678 \cdot 1357931 = 333613772218$.
   [$(a_0 + 10a_1) + (a_2 + 10a_3) + ...$]
8. Determinare i valori dell'incognita x in modo che siano veri gli enunciati seguenti:
   a) $123x456$ è divisibile per 3; b) $23456x78$ è divisibile per 8; c) $81y1058294x$ è divisibile per 33. **[a) 0, 3, 6, 9; b) Nessun valore; c) $x + y = 10$]**
9. Enunciare una prova del 9 per le altre operazioni aritmetiche elementari.
10. Provare che se alla somma delle cifre di un numero, applichiamo la procedura della prova del 9, e non otteniamo uno dei numeri dell'insieme $\{0, 1, 4, 7\}$, il numero non è un quadrato. Esempio $123456 \to 21 \to 3$.
11. Un quesito di Stanford 1947. Fra le carte del nonno ne è stata trovata una con la scritta 72 tacchini \$ _67.9_, in cui la prima e l'ultima cifra del prezzo sono incomprensibili. Qual era il prezzo di un tacchino? **[\$ 5.11]**

§15. Il teorema di Eulero.

Consideriamo qualche applicazione delle congruenze. Il solito Fermat, in una lettera indirizzata a Frénicle de Bessy e datata 18 Ottobre 1640, enunciò il seguente risultato, noto con il nome di Piccolo teorema di Fermat[8] (nel seguito ometteremo l'aggettivo piccolo).

Teorema 37 (di Fermat). Se p è un numero primo e $MCD(n, p) = 1$ allora $(n^{p-1} - 1)$ è divisibile per p.

Notiamo che lo stesso teorema potrebbe enunciarsi ricorrendo alle congruenze, dicendo cioè che $n^{p-1} \overset{p}{\equiv} 1$. Come è spesso accaduto Fermat non propose alcuna dimostrazione per questo fatto, la prima dimostrazione fu presentata invece da Eulero nel 1736. Si ha facilmente: $3^2 - 1 = 8 \overset{3}{\equiv} 1$. Costruiamo poi diverse tabelle per tutti i valori inferiori ai seguenti numeri primi: 5, 7, 11, per verificare tale enunciato.

n	2	3	4
$n^4 - 1$	**5** · 3	**5** · 16	**5** · 51

n	2	3	4	5	6
$n^6 - 1$	**7** · 9	**7** · 104	**7** · 585	**7** · 2232	**7** · 6665

n	2	3	4	5	6
$n^{10} - 1$	**11** · 93	**11** · 5368	**11** · 95325	**11** · 887784	**11** · 5496925
n	7	8	9	10	
$n^{10} - 1$	**11** · 25679568	**11** · 97612893	**11** · 316980400	**11** · 909090909	

In effetti notiamo che i valori crescono in modo considerevole, è perciò più comodo considerare l'enunciato del teorema nella sua forma in cui vengono utilizzate le congruenze.

Esempio 44.

- $10 \overset{11}{\equiv} -1 \Rightarrow 10^2 \overset{11}{\equiv} 1 \Rightarrow 10^{10} \overset{11}{\equiv} 1$.
- $28 \overset{37}{\equiv} -9 \Rightarrow 28^2 \overset{37}{\equiv} 7 \Rightarrow 28^4 \overset{37}{\equiv} 12 \Rightarrow 28^8 \overset{37}{\equiv} -4 \Rightarrow 28^{16} \overset{37}{\equiv} 16 \Rightarrow 28^{32} \overset{37}{\equiv} -3 \Rightarrow 28^{36} \overset{37}{\equiv} 1$

Il teorema di Fermat può anche enunciarsi nel seguente modo:

Teorema 38. Se p è un numero primo allora $(n^p - n)$ è divisibile per p.

Dimostrazione Per il teorema 37 si ha $n^{p-1} \overset{p}{\equiv} 1 \Rightarrow n^p \overset{p}{\equiv} n \Rightarrow n^p - n \overset{p}{\equiv} 0$.

[8] L'aggettivo piccolo viene usato per distinguerlo dal teorema più noto che è anche detto ultimo teorema di Fermat, ossia quello, provato solo nel 1995, che afferma che l'equazione $x^n + y^n = z^n$ non ha soluzioni intere non banali (diverse cioè da (0, 0, 0), (1, 0, 1), …) per $n > 2$.

Si noti che abbiamo eliminato la clausola che n e p siano coprimi, dato che se non lo sono allora n^p è divisibile per p, quindi lo è anche $(n^p - n)$.
Usando il teorema di Fermat in questa forma possiamo provare più facilmente alcune proprietà, come per esempio che ogni quinta potenza di un numero ha la stessa cifra delle unità della base. Ciò infatti equivale a provare che $n^5 \overset{10}{\equiv} n$. Ma per il precedente teorema noi abbiamo $n^5 \overset{5}{\equiv} n, n^5 \overset{2}{\equiv} n$, cioè $(n^5 - n)$ è divisibile per 2 e per 5, quindi per 10.
Se il Teorema 37 fosse una condizione necessaria e sufficiente sarebbe un criterio di primalità, ma purtroppo non lo è, nel senso che vi sono particolari valori di p composto per cui $(n^p - n)$ è divisibile per p.

Esempio 45.

- Si ha $4 \overset{15}{\equiv} 4; 4^2 \overset{15}{\equiv} 1; 4^3 \overset{15}{\equiv} 4; 4^{12} \overset{15}{\equiv} 1; 4^{15} \overset{15}{\equiv} 4 \Rightarrow 4^{15} - 4 \overset{15}{\equiv} 0$ e $(4^{15} - 4) = 15 \cdot 71582788$.
- Si ha $13 \overset{21}{\equiv} -8; 13^2 \overset{21}{\equiv} 1; 13^3 \overset{21}{\equiv} -8; 13^4 \overset{21}{\equiv} 1; 13^7 \overset{21}{\equiv} -8; 13^{21} \overset{21}{\equiv} -512 \overset{21}{\equiv} 13 \Rightarrow 13^{21} - 13 \overset{21}{\equiv} 0$.

Lo stesso Eulero, nel 1760, generalizzò il teorema 36 nel modo seguente.

Teorema 39 (di Eulero). Se m e n sono due numeri naturali tali che $MCD(m, n) = 1$ allora $(n^{\phi(m)} - 1)$ è divisibile per m o anche che $n^{\phi(m)} \overset{m}{\equiv} 1$.

Dato che abbiamo già visto che $\phi(p) = p - 1$, per p numero primo, il teorema di Fermat diviene un caso particolare di questo teorema di Eulero.

Esempio 46.

Poiché $m = 12$ e $n = 25$ sono primi fra di loro dovrebbe accadere $12^{\phi(25)} \overset{25}{\equiv} 1$ e anche $25^{\phi(12)} \overset{12}{\equiv} 1$. Intanto $\phi(25) = \phi(5^2) = 5 \cdot \phi(5) = 5 \cdot 4 = 20$. Mentre $\phi(12) = \phi(2 \cdot 3^2) = 4$. Dobbiamo quindi verificare che $12^{20} \overset{25}{\equiv} 1$ e $25^4 \overset{12}{\equiv} 1$. Ora $12 \overset{25}{\equiv} 12 \Rightarrow 12^2 \overset{25}{\equiv} -6 \Rightarrow$ $\Rightarrow 12^4 \overset{25}{\equiv} 11 \Rightarrow 12^8 \overset{25}{\equiv} -4 \Rightarrow 12^{16} \overset{25}{\equiv} -9 \Rightarrow 12^{20} \overset{25}{\equiv} -99 \overset{25}{\equiv} 1$. Passiamo alla seconda verifica, che risulta immediata: $25 \overset{12}{\equiv} 1 \Rightarrow 25^4 \overset{12}{\equiv} 1$.

Abbiamo visto che $12^{\phi(25)} \overset{25}{\equiv} 1$ e non vi sono esponenti n minori di $\phi(5)$ per cui si abbia $12^n \overset{25}{\equiv} 1$, mentre ciò non accade per 25. Poniamo allora la seguente definizione.

Definizione 19. Si dice che x è una **radice primitiva** di un numero n, con MCD(x, n) = 1, se $m < \phi(n) \Rightarrow x^m \overset{n}{\not\equiv} 1$. Scriviamo $x = Rp(n)$.

Chiaramente 1 è radice primitiva solo di 2, dato che si ha $1 \overset{n}{\equiv} 1, \forall n \in \mathbb{N} \setminus \{1\}$, pertanto nella ricerca delle radici primitive di un numero non consideriamo mai 1.

Esempio 47.

- Abbiamo $\phi(11) = 10$, l'equazione $x^{\phi(11)} \overset{11}{\equiv} 1$ è ovviamente verificata per tutti i naturali da 2 a 10, però abbiamo $3^5 \overset{11}{\equiv} 1$, $4^5 \overset{11}{\equiv} 1$, $5^5 \overset{11}{\equiv} 1$, $9^5 \overset{11}{\equiv} 1$. Quindi 11 ha 5 radici primitive (2, 6, 7, 8, 10).
- Abbiamo $\phi(8) = 4$, ma abbiamo $3^2 \overset{8}{\equiv} 1$, $5^2 \overset{8}{\equiv} 1$ e $7^2 \overset{8}{\equiv} 1$, quindi 8 non ha radici primitive.

Poniamo un'ulteriore definizione, nella quale sottintendiamo che x ed n siano coprimi.

Definizione 20. Se $x^h \overset{n}{\equiv} 1$ e $m < h \Rightarrow x^m \overset{n}{\not\equiv} 1$ diciamo che x ha **ordine *h* modulo *n***, o anche che ***x* appartiene all'esponente *h***. Scriviamo $ord_n(x) = h$.

Quindi abbiamo $ord_{11}(3) = ord_{11}(4) = ord_{11}(5) = ord_{11}(9) = 5$, mentre $ord_8(3) = ord_8(5) = ord_8(7) = 2$. Da quanto mostrato nell'esempio 47, non è difficile capire che vale il seguente risultato.

Teorema 40. $Ord_n(x)$ è un divisore di $\phi(n)$.
Dimostrazione.
Se avessimo $x^h \overset{n}{\equiv} 1$ con h: MCD(h, $\phi(n)$) = $t < h$, allora $hy \overset{\phi(n)}{\equiv} t$ ha almeno una soluzione w e si ha: $t = a\phi(n) + hy$, ma allora $x^t \overset{n}{\equiv} x^{a\phi(n)+hy} \overset{n}{\equiv} \left(x^{\phi(n)}\right)^a \cdot \left(x^h\right)^y \overset{n}{\equiv} 1^a \cdot 1^y \overset{n}{\equiv} 1$, ma questo è assurdo perché allora l'ordine di x dovrebbe essere $t < h$. Quindi MCD(h, $\phi(n)$) = h.

Sempre considerando l'esempio 47, enunciamo quest'altro risultato.

Teorema 41. Il numero di basi appartenenti ad un esponente h sono in numero di $\phi(h)$.

Esercizi.

1. Verificare il teorema di Fermat per tutti i numeri primi minori di 24.
2. Verificare che si ha a) $2^{341} - 2 \overset{341}{\equiv} 0$; b) $3^{91} - 3 \overset{91}{\equiv} 0$; c) $8^9 - 8 \overset{9}{\equiv} 0$.
3. Osserviamo che 9 = 3 · 3; 99 = 9 · 11; 999 = 3^3 · 37; 999 = 99 · 101. Provare che ogni numero primo diverso da 2 e da 5, è divisore di un numero del tipo 999…9.
4. Il teorema inverso del Teorema 38 afferma: se esiste un numero *n* coprimo con *p* per cui si ha $n^{p-1} - n \overset{p}{\equiv} 0$ ma $n^h - n \overset{p}{\not\equiv} 0, \forall h \in \mathbb{N} : 1 < h < p$ allora *p* è un numero primo. Verificare che $3^m - 3$ non è divisibile per 17 per ogni *m*: 1 < *m* < 17. Verificare altresì che ciò non vale per $2^m - 2$. **[$2^9 - 2 = 17 \cdot 30$]**
5. Verificare il teorema di Eulero per *n* = 12, 15, 18, 20 e tutti i numeri minori di essi con cui sono coprimi.
6. Esistono numeri *n* che per *p* numero primo, sono tali che ($n^p - n$) è divisibile anche per p^2. Verificare che questo succede per $3^{11} - 3$. Determinare il primo *n* per cui si ha: a) ($n^5 - n$) è divisibile per 25; b) ($n^3 - n$) è divisibile per 9; a) ($n^7 - n$) è divisibile per 49. **[a) 7; b) 8; c) 18]**
7. Determinare le radici primitive di 17. **[3; 5; 6; 7; 10; 11; 12; 14]**
8. Dimostrare che se *p* e 4*p* + 1 sono entrambi primi allora 2 = *Rp*(4*p* + 1). Verificare su valori a piacere.
9. Dimostrare che se 4*p* + 1 e 8*p* + 3 sono entrambi primi allora 2 = *Rp*(8*p* + 3). Verificare su valori a piacere.

Verificare la validità delle seguenti proprietà su numeri a piacere.

10. $\prod_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} 1$, per *p* numero primo maggiore di 3.
11. Se *p* – 1 è un multiplo di un quadrato perfetto allora $\sum_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} 0$.
12. Se *p* – 1 non è un multiplo di un quadrato perfetto allora $\sum_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} \pm 1$, dove si sceglie (+) se *p* – 1 ha un numero pari di fattori primi, e (–) altrimenti..

§16. Sviluppo decimale delle frazioni.

Vogliamo prendere in considerazione i cosiddetti numeri razionali, considerati come coppie di numeri interi, ossia l'anello delle frazioni. Poiché definiamo numero razionale il risultato della divisione di due numeri naturali, è semplice capire che possiamo ottenere solo tre diversi tipi di numeri razionali. Intanto stabiliamo di continuare la divisione se dovessimo ottenere un resto inferiore al divisore, poi metteremo una virgola nel quoziente e moltiplicheremo per 10 ciascun resto che si otterrà da questo momento in poi. Così facendo la divisione di due numeri naturali m ed n può concludersi dopo un numero finito di passi, ottenendo come resto zero, oppure può entrare in un ciclo. Ciò dipende dal fatto che, dividendo per n, tutti i resti che possono ottenersi sono 0, 1, 2, ..., $n-2$, $n-1$. Quindi è evidente che o al più dopo n passi otteniamo 0, oppure dopo $n-1$ passi otteniamo un resto che avevamo già ottenuto, quindi riotterremo all'infinito la successione dei resti. In quest'ultimo caso la ripetizione dei resti può avvenire subito dopo la virgola o subito dopo un certo numero di valori decimali che non si ripetono.

Esempio 48.

- Dividendo 11 per 16 otteniamo 0,6875.
- Dividendo 31 per 13 otteniamo 1,384615384615... con il gruppo 384615 che si ripete.
- Infine dalla divisione di 73 per 14 otteniamo 5,2142857142857... con il gruppo 142857 che si ripete.

Poniamo allora la seguente definizione.

Definizione 21. Un numero razionale si indica con $a_1a_2...a_n,b_1b_2...b_mc_1c_2...c_pc_1c_2...c_p....$, in cui ciascun simbolo indica una cifra e le cifre $c_1c_2...c_p$ possono essere anche tutte uguali a zero.
All'interno della precedente definizione possono accadere i seguenti fatti.

a) tutte le cifre $b_1b_2...b_m$ e tutte le cifre $c_1c_2...c_p$ sono nulle. Diciamo che il simbolo rappresenta un **numero intero**;
b) non tutte le cifre $b_1b_2...b_m$ sono nulle e tutte le cifre $c_1c_2...c_p$ sono nulle. Diciamo che il simbolo rappresenta un **numero decimale limitato**;
c) tutte le cifre $b_1b_2...b_m$ sono nulle e almeno una delle cifre $c_1c_2...c_p$ non è nulla. Diciamo che il simbolo rappresenta un **numero periodico semplice** di periodo $c_1c_2...c_p$;
d) almeno una delle cifre $b_1b_2...b_m$ non è nulla e almeno una delle cifre $c_1c_2...c_p$ non è nulla. Diciamo che il simbolo rappresenta un **numero periodico misto** di periodo $c_1c_2...c_p$ e antiperiodo $b_1b_2...b_m$.

Data una frazione m/n, siamo curiosi di stabilire quando accade ciascuno dei quattro precedenti fatti. Per il caso 1, non vi sono problemi. Infatti, abbiamo più volte detto che se m è un multiplo di n, allora m/n è un numero intero. La frazione in questo caso viene detta apparente. Anche il caso 2 è abbastanza semplice da affrontare. Sia infatti il numero decimale limitato $A,b_1b_2...b_m$ (con A abbiamo rappresentato il numero $a_1a_2...a_n$), esso può anche essere scritto nel modo seguente: $A + 0,b_1 + 0,0b_2 + ... + 0,00..0b_m$ (gli zeri in questo caso sono in numero di m). Moltiplicando e dividendo numeratore per 10 elevato al numero di zeri presenti in ciascuna espressione abbiamo: $A+\frac{b_1}{10}+\frac{b_2}{10^2}+...+\frac{b_m}{10^m}$. Il

che può anche scriversi nel seguente modo: $\frac{10^m A + 10^{m-1} b_1 + 10^{m-2} b_2 + \ldots + b_m}{10^m}$. Quindi ogni numero decimale limitato può essere rappresentato da un'unica frazione il cui denominatore è una potenza di 10. In realtà la condizione è troppo forte, vale infatti il seguente risultato.

Teorema 42. Ogni frazione il cui denominatore contiene solo potenze di 2 o di 5, rappresenta un numero decimale limitato.

Dimostrazione. Sia $\frac{m}{2^p \cdot 5^q}$, supponiamo che sia $p \geq q$, moltiplichiamo allora numeratore e denominatore per 5^{p-q}, ottenendo così la frazione equivalente: $\frac{m \cdot 5^{p-q}}{10^p}$, che è appunto una frazione del tipo indicato. Il caso $p < q$ si risolve allo stesso modo, solo che stavolta moltiplicheremo e divideremo per 2^{q-p} ottenendo $\frac{m \cdot 2^{q-p}}{10^q}$.

Da quanto visto possiamo anche enunciare il seguente risultato di immediata dimostrazione.

Teorema 43. Una frazione il cui denominatore contiene solo potenze di 2 o di 5, rappresenta un numero decimale limitato le cui cifre decimali sono quante il massimo fra gli esponenti di 2 e 5, contenuti nel denominatore.

Esempio 49.

La frazione $\frac{7}{40}$, rappresenta un numero decimale limitato la cui parte decimale è formata da tre cifre, dato che $40 = 2^3 \cdot 5$. Infatti si ha: $\frac{7}{40} = \frac{7}{2^3 \cdot 5} = \frac{7 \cdot 5^2}{10^3} = \frac{175}{10^3} = 0{,}175$.

Questo fatto ci dovrebbe permettere anche di stabilire quali frazioni rappresentano numeri periodici semplici e quali numeri periodici misti. È evidente che in questo caso il denominatore deve contenere potenze diverse da 2 e da 5. Vediamo prima qualche esempio.

Esempio 50.

Consideriamo la frazione $\frac{1}{12}$, il cui denominatore contiene potenze di 2 e di 3. Operando come nel caso delle frazioni con denominatore contenente solo potenze di 2 o 5, possiamo trasformarla nella frazione equivalente: $\frac{25}{300} = \frac{1}{3} \cdot \frac{25}{100}$, l'abbiamo quindi scritta come prodotto fra una frazione il cui denominatore è privo di fattori 2 e 5 ed una che rappresenta un numero decimale limitato: 0,25. Questo dovrebbe suggerirci il fatto che probabilmente questo numero è periodico misto, dato che il periodo dovrebbe essere "generato" da $\frac{1}{3}$ mentre l'antiperiodo dovrebbe essere determinato da 0,25.

Quanto congetturato nell'esempio precedente deve essere provato. Intanto possiamo os-

servare che se la frazione $\frac{1}{n}$ è periodica di periodo di ampiezza *h*, anche la frazione $\frac{m}{n}$ deve essere periodica, poiché ottenuta moltiplicando il numero periodico $\frac{1}{n}$ per il numero intero *m*. Ciò può eventualmente cambiare le cifre del periodo ma non la loro periodicità. Quindi possiamo ragionare solo sulle frazioni del tipo $\frac{1}{n}$. Costruiamo l'ormai consueta tabella:

n	**3**	**6**	**7**	**9**	**11**	**12**	**13**	**14**	**15**
$\frac{1}{n}$	$0,\overline{3}$	$0,1\overline{6}$	$0,\overline{142857}$	$0,\overline{1}$	$0,\overline{09}$	$0,0\overline{83}$	$0,\overline{76925}$	$0,\overline{714285}$	$0,0\overline{6}$

Notiamo che in effetti la nostra congettura è avvalorata da tale tabella, essendo i numeri periodici misti quelli il cui denominatore contiene fattori 2 o 5. Dobbiamo però provarlo.

Teorema 44. Ogni frazione il cui denominatore non contiene alcuna potenza di 2 e di 5, rappresenta un numero periodico semplice.
Dimostrazione. Supponiamo di avere il seguente numero periodico semplice $q = A,c_1c_2...c_pc_1c_2...c_p...$, moltiplichiamo adesso q per il numero $a = 10^p q = Ac_1c_2...c_p, c_1c_2...c_p...$ questa operazione non fa altro che spostare la virgola a destra di p posti, ottenendo un numero diverso da q ma che ha lo stesso periodo. Sottraiamo i due numeri: $a - q = 10^p q - q = q \cdot (10^p - 1) = Ac_1c_2...c_p - A \Rightarrow q = \frac{Ac_1c_2...c_p - A}{10^p - 1} = \frac{Ac_1c_2...c_p - A}{\underbrace{999...9}_{p}}$. Quindi q è una frazione priva di potenze di 2 e di 5, ossia la tesi.

Nella dimostrazione precedente abbiamo anche provato la ben nota

Regola per trasformare un numero periodico semplice in frazione.

Al numeratore si scriva la differenza fra il numero formato dalla parte intera e dal periodo e il numero formato dalla parte intera, al denominatore tanti 9 quante sono le cifre del periodo.

Esempio 51.

Troviamo la frazione associata al numero 123,456456… usando la regola enunciata: $123,\overline{456} = \frac{123456 - 123}{999} = \frac{123333}{999} = \frac{41111}{333}$. Verifichiamo effettuando la divisione che il risultato è corretto.

Analogamente a quanto visto possiamo provare, con una procedura analoga o semplicemente per esclusione di casi, anche il seguente teorema.

Teorema 45. Ogni frazione il cui denominatore contiene potenze di 2 o di 5 e potenze di altri fattori primi con 2 e 5, rappresenta un numero periodico misto.

Troviamo anche la seguente regola.

Regola per trasformare un numero periodico misto in frazione.

Al numeratore si scriva la differenza fra il numero formato dalla parte intera, dall'antiperiodo e dal periodo e il numero formato dalla parte intera e dal periodo, al denominatore tanti 9 quante sono le cifre del periodo seguiti da tanti zeri quante sono le cifre dell'antiperiodo.

Esempio 52.

Troviamo la frazione associata al numero 123,45678678… usando la regola enunciata: $123,45\overline{678} = \frac{12345678-12345}{99900} = \frac{12333333}{99900} = \frac{4111111}{33300}$. Verifichiamo effettuando la divisione che il risultato è corretto.

Vogliamo adesso cercare un modo per stabilire l'ampiezza del periodo, noto che sia solo il denominatore della frazione. Vale il seguente risultato.

Teorema 46. Data la frazione *m/n*, con *n* non contenente solo potenze di 2 o 5, essa rappresenta un numero periodico il cui periodo è formato da *k* termini ed il cui antiperiodo è formato da *h* termini. Con *h* e *k* i minimi numeri naturali verificanti la congruenza $10^h \overset{n}{\equiv} 10^{h+k}$.

Esempio 53.

- Consideriamo la frazione 1/7. Ricordiamo i resti delle successive potenze di 10 modulo 7, che abbiamo già calcolato: $10^0 \overset{7}{\equiv} 1, 10 \overset{7}{\equiv} 3, 10^2 \overset{7}{\equiv} 2, 10^3 \overset{7}{\equiv} 6, 10^4 \overset{7}{\equiv} 4, 10^5 \overset{7}{\equiv} 5, 10^6 \overset{7}{\equiv} 1$. Vuol dire che 1/7 ha un periodo di ampiezza 6, come avevamo già visto. In effetti tutte le frazioni con denominatore 7 hanno un periodo di ampiezza 6.
- Sia adesso la frazione 1/12. Calcoliamo i resti delle successive potenze di 10 modulo 12: $10 \overset{12}{\equiv} -2, 10^2 \overset{12}{\equiv} 4, 10^3 \overset{12}{\equiv} 4, \ldots, 10^n \overset{12}{\equiv} 4, n > 1$. A questo punto otterremo sempre lo stesso valore, quindi $10^2 \equiv 10^3 \equiv 4$. Pertanto possiamo dire che 1/12 rappresenta un numero periodico misto di ampiezza del periodo 1, ed ampiezza dell'antiperiodo 2, fatto già verificato.

Un altro fatto curioso che notiamo è quello mostrato nella seguente tabella:

1/7	**2/7**	**3/7**	**4/7**	**5/7**	**6/7**
$0,\overline{142857}$	$0,\overline{285714}$	$0,\overline{428571}$	$0,\overline{571428}$	$0,\overline{714285}$	$0,\overline{857142}$

Cioè non solo le cifre che compongono i periodi delle sei frazioni sono sempre le stesse, ma ciascun periodo è una permutazione circolare di un altro, ossia le cifre si ripetono nello stesso ordine, a parte il valore di partenza. Ciò dipende dai risultati delle congruenze delle potenze di 10 modulo 7. Infatti, è facile capire che se moltiplichiamo un numero periodico semplice *n* per 10, non facciamo altro che spostare la virgola di un posto. Così il numero 10*n* avrà lo stesso periodo di *n* come ampiezza, ma esso sarà una permutazione ciclica di quello di *n* di un passo. Così per esempio 10/7 = $1,\overline{428571}$, analogamente moltiplicando per 100 avremo un numero periodico il cui periodo avrà ciclato di due passi, quindi 100/7 = $14,\overline{285714}$ e via di questo passo. Poiché $10 \overset{7}{\equiv} 3$, vuol di-

re che 3/7 e 10/7 hanno lo stesso periodo, allo stesso modo, poiché $10^2 \overset{7}{\equiv} 2$, 2/7 avrà lo stesso periodo di 100/7 e via di questo passo. Ma allora, dato che i resti delle successive potenze di 10 modulo 7 sono 3, 2, 6, 4, 5, 1; possiamo dire che le frazioni 3/7, 2/7, 6/7, 4/7, 5/7 si ottengono da 1/7 spostando ciascuna volta di tanti posti a destra le cifre del suo periodo, quanto la posizione che esse occupano.

Esempio 54.

Consideriamo le frazioni di denominatore 13. Abbiamo $10^0 \overset{13}{\equiv} 1, 10 \overset{13}{\equiv} 10, 10^2 \overset{13}{\equiv} 9, 10^3 \overset{13}{\equiv} 12$, $10^4 \overset{13}{\equiv} 3, 10^5 \overset{13}{\equiv} 4, 10^6 \overset{13}{\equiv} 1$. Quindi le dette frazioni rappresentano numeri periodici di periodo di ampiezza 6. Dato che $\frac{1}{13} = 0,\overline{076923}$, facilmente possiamo costruire i valori di 10/13, 9/13, 12/13, 3/13, 4/13 che sono: $0,\overline{769230}$; $0,\overline{692307}$; $0,\overline{923076}$; $0,\overline{230769}$; $0,\overline{307692}$. Notiamo che mancano i valori delle altre sei frazioni proprie, il che dipende dal fatto che non abbiamo ottenuto tali valori come resti. Consideriamo allora le seguenti congruenze:

$$2 \cdot 10^0 \overset{13}{\equiv} 2, 2 \cdot 10 \overset{13}{\equiv} 7, 2 \cdot 10^2 \overset{13}{\equiv} 5, 2 \cdot 10^3 \overset{13}{\equiv} 11, 2 \cdot 10^4 \overset{13}{\equiv} 6, 2 \cdot 10^5 \overset{13}{\equiv} 8, 2 \cdot 10^6 \overset{13}{\equiv} 2$$

Calcoliamo quindi $\frac{2}{13} = 0,\overline{153846}$ e da tale valore quello delle rimanenti frazioni: $\frac{7}{13} = 0,\overline{538461}$; $\frac{5}{13} = 0,\overline{384615}$; $\frac{11}{13} = 0,\overline{846153}$; $\frac{6}{13} = 0,\overline{461538}$; $\frac{6}{13} = 0,\overline{615384}$.

L'esempio precedente ha mostrato che i periodi delle frazioni *m/n* associate a numeri periodici, pur essendo della stessa lunghezza possono essere diversi anche nella composizione delle cifre, a seconda di *n*. questo ovviamente succede quando il periodo non ha (*n* – 1) cifre. Vale anzi il seguente risultato.

Teorema 47. Data la frazione *m/n* che rappresenta un numero periodico. Il suo periodo ha un numero *p* di cifre che è il minimo divisore di $\phi(n)$ che è soluzione di $10^p \overset{n}{\equiv} 1$. Le frazioni dell'insieme $\{k/n: 1 \le k \le n - 1$, con MCD$(n, k) = 1\}$ hanno un totale di $\phi(n)/p$ periodi che si ripetono ciclicamente.

Esempio 55.

Consideriamo le frazioni 1/63, 2/63, …, 62/63, abbiamo $\phi(63) = 36$, quindi il periodo delle 36 che rappresentano numeri periodici semplici è un divisore di 36. Dato che $10 \overset{63}{\equiv} 10, 10^2 \overset{63}{\equiv} 100 \overset{63}{\equiv} 37, 10^3 \overset{63}{\equiv} 370 \overset{63}{\equiv} -8, 10^4 \overset{63}{\equiv} -80 \overset{63}{\equiv} -17, 10^5 \overset{63}{\equiv} 19, 10^6 \overset{63}{\equiv} 190 \overset{63}{\equiv} 1$, il periodo è 6. E vi sono perciò 6 diversi periodi. Il primo è $\frac{1}{63} = 0,\overline{015873}$ e i suoi cicli che hanno le frazioni $\frac{10}{63} = 0,\overline{158730}, \frac{37}{63} = 0,\overline{587301}, \frac{55}{63} = 0,\overline{873015}, \frac{46}{63} = 0,\overline{730158}, \frac{19}{63} = 0,\overline{301587}$.

Per trovare gli altri calcoliamo a partire da $2 \cdot 10 \overset{63}{\equiv} 20$ fino $2 \cdot 10^6 \overset{63}{\equiv} 2$ che fornisce il secondo periodo 317460. E così via, sempre per multipli di 10 ovviamente con valori non ottenuti già. Così otteniamo i rimanenti 4 periodi: 063492; 079365; 126984; 206349 e 253968.

Infine possiamo anche stabilire fra le frazioni $1/p$, con p numero primo quali sono quelle che per esempio hanno un periodo fissato.

Esempio 56.

- Abbiamo $10 - 1 = 3^2$, cioè $10 \overset{9}{\equiv} 1$, significa che solo 1/3 ha periodo 1.
- Allo stesso modo $10^2 - 1 = 3^2 \cdot 11$, cioè $10^2 \overset{11}{\equiv} 1$, quindi solo 1/11 ha periodo 2, e così via.

Abbiamo visto che alcune frazioni $1/p$ con p numero primo hanno la massima lunghezza del periodo, ossia $(p - 1)$. Da quanto visto la precedente proprietà equivale a dire che $p - 1$ è la minima potenza di 10 multipla di p, ossia che $10^n \overset{p}{\not\equiv} 1, 1 \le n < p-1$, mentre per il Teorema di Fermat si ha sempre $10^{p-1} \overset{p}{\equiv} 1, p \notin \{2,5\}$. In pratica ciò accade solo quando 10 è una radice primitiva di p.

Osserviamo anche un altro fatto curioso.

Esempio 57.

- Consideriamo il periodo di 1/7: 142857. Osserviamo che se lo dividiamo in due terne: 142 e 857, la somma delle cifre che occupano la stessa posizione (1 + 8; 4 + 5 e 2 + 7) dà per somma 9, ossia 142 + 857 = 999. Lo stesso accade ovviamente con le altre frazioni di tipo $m/7$, data la ciclicità.
- Ma accade anche per il periodo di 1/17, che è 0588235294117647. Infatti si ha: 05882352 + 94117647 = 99999999

Quanto visto prima è in effetti un risultato che vale per parecchie frazioni.

Teorema 48. Ogni frazione $1/p$ con p numero primo di periodo formato da un numero pari di cifre, $2n$, ha la proprietà che il suo periodo si può dividere in modo che le prime n cifre e le ultime n sono tali che cifre che occupano la stessa posizione sommano 9.

Ovviamente la proprietà precedente vale per tutte le radici primitive di 10.

Esercizi.

1. Determinare il numero di cifre del periodo delle frazioni di denominatore un numero primo maggiore di 5 e minore di 50.
   [6; 2; 6; 16; 18; 22; 28; 15; 3; 5; 21; 46]
2. Con riferimento al precedente quesito quali delle frazioni precedenti hanno più di un periodo? **[*n*/11 ne ha 5; *n*/13:2; *n*/31: 2; *n*/37: 12; *n*/41: 8; *n*/43: 2]**
3. Con riferimento al quesito 1, osserviamo che le frazioni m/p che hanno periodo $(p - 1)$ hanno la sequenza delle congruenze delle diverse potenze di 10, in modo che le prime $(p - 1)/2$ sono uguali alle opposte delle altre in modo che si abbia $10^n \overset{p}{\equiv} a \Rightarrow 10^{n+(p-1)/2} \overset{p}{\equiv} -a$. Dimostrare tale congettura.
4. Osserva i diversi periodi di $n/11$ e spiega il motivo di tali caratteristiche.
   [Sono i multipli di 9 da 09 a 90]
5. Scrivi le cifre dei diversi periodi di $n/37$.
   [027; 054; 081; 135; 162; 189; 243; 297; 378; 459; 486; 567]
6. Provare che non possono esistere numeri di periodo 9.
7. Tenuto conto di quanto visto nell'esempio 56, stabilire quali sono i valori di p primo per cui $1/p$ ha un periodo formato da: a) 3; b) 4; c) 5; d) 6 cifre.
   [a) 37; b) 101; c) 41 e 207; d) 7 e 13]
8. Dopo aver determinato tutti i numeri primi minori di 100 a cui si può applicare il Teorema 48, verificarlo con essi.

§17. Principio di induzione.

Ricordiamo l'assioma di Peano numero 5:
Se A è un insieme di numeri tale che $0 \in A$, *e ogni volta che* $a \in A$ *anche* $a^+ \in A$, *allora A è l'insieme* $\mathbb{N}$.
Possiamo generalizzarlo per dimostrare proprietà che riguardano i cosiddetti insiemi numerabili, ossia quelli che possono essere messi in corrispondenza biunivoca con $\mathbb{N}$ e quindi possono essere indicati simbolicamente con $\{a_1, a_2, a_3, \ldots, a_n, \ldots\}$, ossia ogni elemento dell'insieme occupa una determinata posizione e mediante essa è univocamente determinato.

Esempio 58.

- L'insieme dei numeri dispari: $\{1, 3, 5, 7, \ldots, 2n - 1, \ldots\}$ è numerabile.
- L'insieme dei numeri primi: $\{2, 3, 5, 7, 11, \ldots\}$ è numerabile.
- L'insieme delle frazioni di numeratore unitario: $\{1, ½, 1/3, 1/4, \ldots, 1/n, \ldots\}$ è numerabile.
- L'insieme delle radici quadrate irrazionali: $\left\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, ...,\right\}$ è numerabile.

Come si vede consideriamo insiemi numerabili non per forza insiemi formati solo da numeri interi, ma anche da numeri razionali o irrazionali. Ciò non significa che tutti gli insiemi numerici siano numerabili. Per esempio l'insieme dei numeri reali non lo è. Ma non approfondiamo questi concetti perché non sono indispensabili per i nostri obiettivi.
È invece importante distinguere fra insiemi numerabili i cui elementi possono essere indicati con una legge generale dipendente da una variabile, come l'insieme dei numeri dispari e quelli invece per cui ciò non è possibile, come l'insieme dei numeri primi. Noi ci riferiremo solo al primo tipo di insiemi.

Esempio 59.

Consideriamo l'insieme dei numeri dispari ed osserviamo quanto mostrato:
$$1 = 1^2;\ 1 + 3 = 2^2;\ 1 + 3 + 5 = 3^2;\ 1 + 3 + 5 + 7 = 4^2.$$
Questo ci fa pensare che valga una proprietà generale, ossia che si abbia:
$$1 + 3 + 5 + \ldots + (2n - 1) = n^2$$

Per provare la precedente congettura, per gli insiemi del primo tipo enunciamo un nuovo principio.

Principio di induzione

Se $A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\}$ è un insieme numerabile e P è una proprietà, se
1. a_1 verifica P
2. comunque scegliamo un elemento a_n in A, il sapere che P è verificata da a_n implica che P è verificata anche da a_{n+1}, allora P è verificata da tutti gli elementi di A.

In pratica la precedente tecnica equivale ad effettuare infinite verifiche mediante solo due di esse. Infatti la verifica 2 ci permette di affermare che se una proprietà vale per un generico elemento vale anche per il successivo. Quindi se vale per il nono vale anche per il decimo e quindi per l'undicesimo e poi per il dodicesimo e così via. Il problema è che non sappiamo se valga per il nono. Però mediante la verifica 1 abbiamo verificato che vale per il primo elemento, quindi per la 2 varrà per il secondo e poi per il terzo, il

quarto e quindi per tutti, non importa se siano un numero finito o infinito.

Esempio 60.

Per dimostrare la proprietà enunciata nell'esempio precedente dobbiamo verificare che si abbia $1 = 1^2$ e questo è vero. Poi dobbiamo supporre che sia vero anche che sia $1 + 3 + 5 + \ldots + (2n - 1) = n^2$, che perciò è la nostra ipotesi, e mediante essa dobbiamo provare la nostra tesi, cioè che sia anche $1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1) = (n + 1)^2$. Come si vede abbiamo aggiunto un addendo a sinistra e una unità alla base di destra. La prova è immediata, dato che ai primi n addendi possiamo sostituire ciò che dice l'ipotesi, quindi la somma diventa $n^2 + (2n + 1)$, che non è altro che lo sviluppo di $(n + 1)^2$. Pertanto possiamo affermare che la nostra congettura era corretta.

Vediamo un altro esempio.

Esempio 61.

Osserviamo che si ha: $8 = 1\cdot 2 + 2\cdot 3 = \frac{2\cdot 3\cdot 4}{3}; 20 = 1\cdot 2 + 2\cdot 3 + 3\cdot 4 = \frac{3\cdot 4\cdot 5}{3}$. Pensiamo allora che sia vera la seguente formula generale:

$$1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \ldots + n\cdot(n+1) = \frac{n\cdot(n+1)\cdot(n+2)}{3}$$

Verifichiamola per $n = 1$. $1\cdot 2 = \frac{1\cdot(1+1)\cdot(1+2)}{3} = \frac{1\cdot 2\cdot \cancel{3}}{\cancel{3}} = 1\cdot 2$.

Adesso mostriamo che se $1\cdot 2 + 2\cdot 3 + \ldots + n\cdot(n+1) = \frac{n\cdot(n+1)\cdot(n+2)}{3}$, allora si ha: $1\cdot 2 + 2\cdot 3 + \ldots + (n+1)\cdot(n+2) = \frac{(n+1)\cdot(n+2)\cdot(n+3)}{3}$. Come visto in precedenza, i primi n addendi si possono riscrivere: $\frac{n\cdot(n+1)\cdot(n+2)}{3} + (n+1)\cdot(n+2)$, a questo punto basta solo semplificare per ottenere la tesi.

Un ultimo esempio sulla divisibilità.

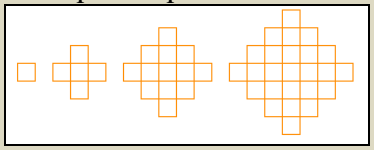
Esempio 62.

Provare per induzione che $n \cdot (n + 1) \cdot (n + 2)$ è divisibile per 6, $\forall\, n \in \mathbb{N}$.

Per $n = 1$, si ha $1 \cdot 2 \cdot 3 = 6$. Adesso proviamo che se è vero che $n \cdot (n + 1) \cdot (n + 2)$ è divisibile per 6 è anche vero che $(n + 1) \cdot (n + 2) \cdot (n + 3)$ è divisibile per 6. Dobbiamo però formalizzare che significa che un numero è divisibile per 6. Che possa scriversi come prodotto di 6 per un termine generico, cioè $n \cdot (n + 1) \cdot (n + 2) = 6 \cdot h$. Ora si ha: $(n + 1) \cdot (n + 2) \cdot (n + 3) = (n + 1) \cdot (n + 2) \cdot n + (n + 1) \cdot (n + 2) \cdot 3$. Adesso applichiamo l'ipotesi induttiva al primo addendo: $6 \cdot h + (n + 1) \cdot (n + 2) \cdot 3 = 3 \cdot [2h + (n+1) \cdot (n + 2)]$. Il prodotto di due numeri interi consecutivi è pari, quindi possiamo scrivere $3 \cdot (2h + 2 \cdot k) = 6 \cdot (h + k)$, che è quello che voleva dimostrarsi.

Esercizi.

Provare la validità delle seguenti proprietà, usando il metodo di dimostrazione per induzione

1. a) $1+2+3+\ldots+n=\frac{n\cdot(n+1)}{2}$; b) $1 + 3 + 5 + \ldots + (2n - 1) = n^2$;
2. a) $1^2+2^2+\ldots+n^2=\frac{n\cdot(n+1)\cdot(2n+1)}{6}$; b) $1^2+3^2+5^2+\ldots+(2n-1)^2=\frac{n\cdot(4n^2-1)}{3}$
3. a) $2^2 + 5^2 + 8^2 + \ldots + (3n - 1)^2 = \frac{n\cdot(6n^2+3n-1)}{2}$; b) $n \geq 10 \Rightarrow 2^n > n^3$
4. a) $1^3+2^3+3^3+\ldots+n^3=\left[\frac{n\cdot(n+1)}{2}\right]^2$; b) $\frac{1}{1\cdot5}+\frac{1}{5\cdot9}+\ldots+\frac{1}{(4n-3)\cdot(4n+1)}=\frac{n}{4n+1}$
5. a) $\frac{1}{1\cdot2}+\frac{1}{2\cdot3}+\ldots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$; b) $\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\ldots+\frac{1}{(2n-1)\cdot(2n+1)}=\frac{n}{2n+1}$
6. $\frac{1^2}{1\cdot3}+\frac{2^2}{3\cdot5}+\ldots+\frac{n^2}{(2n-1)\cdot(2n+1)}=\frac{n\cdot(n+1)}{2\cdot(2n+1)}$;
7. $\frac{1}{1\cdot4}+\frac{1}{4\cdot7}+\ldots+\frac{1}{(3n-2)\cdot(3n+1)}=\frac{n}{3n+1}$
8. $1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3 = n^2 \cdot (2n^2 - 1)$; b) $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$
9. $1^5+2^5+3^5+\ldots+n^5=\frac{n^2\cdot(n+1)^2\cdot(2n^2+2n-1)}{12}$
10. $1\cdot2\cdot3+2\cdot3\cdot4+\ldots+n\cdot(n+1)\cdot(n+2)=\frac{n\cdot(n+1)\cdot(n+2)\cdot(n+3)}{4}$
11. La somma degli angoli interni di un poligono convesso di n lati è $(n - 2)\cdot180°$, $n\geq3$.
12. $(1^5 + 2^5 + \ldots + n^5) + (1^7 + 2^7 + \ldots + n^7) = 2 \cdot (1 + 2 + \ldots + n)^4$.
13. $3 \cdot (1^2 + 2^2 + \ldots + n^2) - 3 \cdot (1 + 2 + \ldots + n) = n^3 - n$.
14. $3 \cdot (1^5 + 2^5 + \ldots + n^5) + (1^3 + 2^3 + \ldots + n^3) = 4 \cdot (1 + 2 + \ldots + n)^3$.
15. a) $n^3 + 1 > n^2 + n$, $n \geq 2$; b) $11^{n+2} + 12^{2n+1}$ è divisibile per 133.
16. Il numero di regioni in cui n rette dividono il piano è minore o uguale a 2^n.
17. a) $17^n - 12^n$ è divisibile per 5; b) $5^n + 2 \cdot 3^{n-1} + 1$ è divisibile per 8.
18. a) $7^n + 5^{2n+1}$ è divisibile per 6; b) $9^n - 8n - 1$ è divisibile per 64.
19. a) $8^n - 3^n$ è divisibile per 5; b) $3^{2n+2} - 8n - 9$ è divisibile per 64.
20. a)$13^{2n} + 6$ è divisibile per 7; b) $3^{2n} + 4^{n+1}$ è divisibile per 5.
21. $cos(\alpha) + cos(3\alpha) + \ldots + cos[(2n - 1)\cdot\alpha] = \frac{sin(2n\cdot\alpha)}{2\cdot sin(\alpha)}$
22. $sin(\alpha) + sin(3\alpha) + \ldots + sin[(2n - 1)\cdot\alpha] = \frac{1-cos(2n\cdot\alpha)}{2\cdot sin(\alpha)}$
23. Le figure seguenti costituiscono una successione di poligoni, che prosegue sempre seguendo la stessa legge. Determinare quanti quadrati formano il poligono al passo n e dimostrarla poi per induzione.  **[$2n^2 + 2n + 1$]**

Determina una legge che descriva le seguenti somme e provale per induzione.

24. a) $1^2 = 1$; $2^2 - 1^2 = 3$; $3^2 - 2^2 + 1^2 = 6$; … b) $1 = 1^3$; $3 + 5 = 2^3$; $7 + 9 + 11 = 3^3$; …

$$\left[\text{a) } \sum_{k=1}^{n}(-1)^{k+1}(n+1-k)^2 = \frac{n(n+1)}{2}\text{; b) } \sum_{k=1}^{n}\left(n^2 - n + 2k - 1\right) = n^3\right]$$

25. $2 + 3 + 4 = 1 + 8$; $5 + 6 + 7 + 8 + 9 = 8 + 27$; $10 + 11 + \ldots + 16 = 27 + 64$; …

$$\left[\sum_{k=n^2+1}^{(n+1)^2} k = n^3 + (n+1)^3\right]$$

Esercizi svolti

§1.

1. Determinare per quali valori di *n* vi sono numeri interi nei seguenti insiemi di frazioni. a) $\frac{2n+11}{2n-3}$; b) $\frac{n+12}{n+15}$; c) $\frac{n^2+n+1}{n^2+n-1}$; d) $\frac{2n+1}{3n-1}$; e) $\frac{4-3n}{n^2+1}$

a) $\frac{2n-3+14}{2n-3}=1+\frac{14}{2n-3}$, perché l'espressione rappresenti un numero intero $2n-3$ deve essere un divisore di 14, ossia 1, $n=2$; –1, $n=1$; 7, $n=5$; –7, $n=-2$; ±14, nessuna soluzione perché n non risulterebbe intero; b) $1-\frac{3}{n+15}$, $n+15$ deve essere un divisore di 3, ossia 1, $n=-14$; –1, $n=-16$; 3, $n=-12$; –3, $n=-18$; c) $1+\frac{2}{n^2+n-1}$, n^2+n-1 deve essere un divisore di 2, ossia 1, $n=-2 \vee n=1$; –1, $n=-1 \vee n=0$; ±2, nessuna soluzione perché n non risulterebbe intero; d) La frazione è impropria o apparente solo se $2n+1 \geq 3n-1 \Rightarrow 0 \leq n \leq 2$, quindi basta controllare i valori: {0, 1, 2}, vanno bene solo $n=0$ e $n=2$; e) $\frac{4-3n}{n^2+1}$, La frazione è impropria o apparente solo se $-2 \leq n \leq 0$, otteniamo valori interi solo se $n=-2$ e $n=0$

2. Dimostrare la validità delle seguenti catene di uguaglianze.

a) $9 \cdot 9 + 7 = 88$; $98 \cdot 9 + 6 = 888$; ...; $98765432 \cdot 9 + 0 = \underbrace{888...8}_{9}$

b) $1 \cdot 8 + 1 = 9$; $12 \cdot 8 + 2 = 98$; …; $123456789 \cdot 8 + 9 = 987654321$.

c) $12345679 \cdot 9 = 111111111$; $12345679 \cdot 18 = 222222222$; … $12345679 \cdot 81 = 999999999$.

a) Consideriamo solo l'ultima uguaglianza, provata questa valgono anche le precedenti. Possiamo scrivere $98765432 \cdot 9 + 0 = [9 \cdot 10^7 + 8 \cdot 10^6 + \ldots + 3 \cdot 10 + 2 \cdot 10^0] \cdot (10-1) = 9 \cdot 10^8 + 8 \cdot 10^7 + \ldots + 3 \cdot 10^2 + 2 \cdot 10^1 - [9 \cdot 10^7 + 8 \cdot 10^6 + \ldots + 3 \cdot 10^1 + 2 \cdot 10^0] = 9 \cdot 10^8 - [1 \cdot 10^7 + \ldots + 1 \cdot 10^2 + 1 \cdot 10^1] - 2$. L'espressione in parentesi quadrate si può scrivere $\frac{10^8-1}{10-1}-1$, quindi avremo: $=$

$$9\cdot 10^8-\frac{10^8-1}{10-1}-1=\frac{9\cdot 10^9-9\cdot 10^8-10^8+1-9}{9}=\frac{9\cdot 10^9-10\cdot 10^8-8}{9}=$$

$$=\frac{9\cdot 10^9-10^9-8}{9}=8\cdot\frac{10^9-1}{9}=\underbrace{888...8}_{9}$$

b) $123456789 \cdot 8 + 9 = (1 \cdot 10^8 + 2 \cdot 10^7 + \ldots + 8 \cdot 10 + 9 \cdot 10^0) \cdot (10-2) + 9 = (1 \cdot 10^9 + 2 \cdot 10^8 + \ldots + 8 \cdot 10^2 + 9 \cdot 10^1) - 2 \cdot (1 \cdot 10^8 + 2 \cdot 10^7 + \ldots + 8 \cdot 10 + 9 \cdot 10^0) + 9 = 1 \cdot 10^9 + (2-2) \cdot 10^8 + (3-4) \cdot 10^7 + (4-6) \cdot 10^6 + \ldots + (9-16) \cdot 10 - 2 \cdot 9 + 9 = 1 \cdot 10^9 - (1 \cdot 10^7 + 2 \cdot 10^6 + \ldots + 7 \cdot 10 + 9) = 1 \cdot 10^9 - 12345679 = 987654321$

c) Basta provare la prima, le altre si ottengono da questa moltiplicando per 2, 3, …, 9. Si ha: $12345679 \cdot (10-1) = 123456790 - 12345679 = 111111111$.

3. Possiamo generalizzare la 2a)? Se sì come?

La regola generale potrebbe sembrare $987\ldots (10-n) \cdot 9 + (8-n) = \underbrace{888...8}_{n+1}$, dato che la sua dimostrazione è identica a quella fatta nel caso particolare, la riportiamo.

$[9 \cdot 10^{n-1} + 8 \cdot 10^{n-2} + \ldots + (10-n+1) \cdot 10 + (10-n) \cdot 10^0] \cdot (10-1) + (8-n) = 9 \cdot 10^n + 8 \cdot 10^{n-1} + \ldots + (10-n+1) \cdot 10^2 + (10-n) \cdot 10^1 - [9 \cdot 10^{n-1} + 8 \cdot 10^{n-2} + \ldots + (10-n+1) \cdot 10 + (10-n) \cdot 10^0] + (8-n) = 9 \cdot 10^n - [1 \cdot 10^{n-1} + \ldots + 1 \cdot 10^2 + 1 \cdot 10^1 + 1] - 1 =$

$$9 \cdot 10^n - \frac{10^n - 1}{10-1} - 1 = \frac{9 \cdot 10^{n+1} - 9 \cdot 10^n - 10^n + 1 - 9}{9} = \frac{9 \cdot 10^{n+1} - 10 \cdot 10^n - 8}{9} =$$

$$= \frac{9 \cdot 10^{n+1} - 10^{n+1} - 8}{9} = 8 \cdot \frac{10^{n+1} - 1}{9} = \underbrace{888...8}_{n+1}$$

Il problema però è che ovviamente per $n = 9$ e 10 dobbiamo non aggiungere ma togliere: $987654321 \cdot 9 - 1 = \underbrace{888...8}_{10}$ e $9876543210 \cdot 9 - 2 = \underbrace{888...8}_{11}$. Per $n > 10$ non funziona perché dovremmo aggiungere cifre negative: $9876543210(-1) \cdot 9 - 3 = \underbrace{888...8}_{12}$.

§2.

1. **Osserviamo che $1^3 = T_1^2$, $1^3 + 2^3 = 9 = T_2^2$, $1^3 + 2^3 + 3^3 = 36 = T_3^2$. Senza effettuare i calcoli, quanto fa $1^3 + 2^3 + 3^3 + 4^3 + 5^3$?**
   Tenuto conto degli altri calcoli dovrebbe essere $1^3 + 2^3 + 3^3 + 4^3 + 5^3 = T_4^2 = \left(\frac{4 \cdot 5}{2}\right)^2 = 15^2 = 225$
2. **Osserviamo che $8T_1 + 1 = 9$, $8T_2 + 1 = 25$, $8T_3 + 1 = 49$. Senza effettuare i calcoli, quanto fa $8T_4 + 1$?**
   Dato che $9 = 3^3$, $25 = 5^2$, $49 = 7^2$, dovrebbe essere $8T_4 + 1 = 9^2 = 81$.
3. **Quali fra i seguenti è un numero triangolare: 91, 106, 153, 170, 190, 231?**
   Per quanto già visto lo sono quelli il cui doppio si può scrivere come prodotto di due numeri interi consecutivi.
   $2 \times 91 = 2 \times 7 \times 13 = 13 \times 14$. 91 è triangolare, precisamente è T_{13};
   $2 \times 106 = 2^2 \times 53$. 106 non è un numero triangolare;
   $2 \times 153 = 2 \times 9 \times 17 = 17 \times 19$. 153 è triangolare, precisamente è T_{17};
   $2 \times 170 = 2^2 \times 5 \times 17$. 170 non è un numero triangolare;
   $2 \times 190 = 2^2 \times 5 \times 19 = 19 \times 20$. 190 è T_{19};
   $2 \times 231 = 2 \times 3 \times 7 \times 11 = 21 \times 22$. 231 è T_{21}.
4. **Osserviamo che $T_1 + T_2 = 4$, $T_2 + T_3 = 9$, $T_3 + T_4 = 16$. Senza fare conti possiamo ipotizzare quanto fa $T_{10} + T_{11}$?**
   Dato che $4 = 2^2$, $9 = 3^2$, $16 = 4^2$, avremo $T_{10} + T_{11} = 11^2 = 121$.
5. **Determinare i primi 5 numeri esagonali, verificando che confermano il Teorema 4.**
   Per il Teorema 3:

$$P_6^{(1)} = \frac{1 \cdot \left[(1-1) \cdot 6 - 2 \cdot (1-2)\right]}{2} = 1; P_6^{(2)} = \frac{2 \cdot \left[(2-1) \cdot 6 - 2 \cdot (2-2)\right]}{2} = 6;$$

$$P_6^{(1)} = \frac{3 \cdot \left[(3-1) \cdot 6 - 2 \cdot (3-2)\right]}{2} = 15; P_6^{(4)} = \frac{4 \cdot \left[(4-1) \cdot 6 - 2 \cdot (4-2)\right]}{2} = 28; .$$

$$P_6^{(5)} = \frac{5 \cdot \left[(5-1) \cdot 6 - 2 \cdot (5-2)\right]}{2} = 45$$

Verifichiamo il Teorema 4, che diventa 32N + 4 deve essere un quadrato perfetto. $32 + 4 = 6^2$, $32\cdot6 + 4 = 14^2$, $32\cdot15 + 4 = 22^2$, $32\cdot28 + 4 = 30^2$, $32\cdot45 + 4 = 38^2$. Osserviamo che i quadrati hanno le basi appartenenti a una progressione aritmetica di ragione 8.

6. Possiamo dire che $P_5^{(6)} = P_5^{(5)} + x$. Quanto vale *x*?

Si ha:

$$x = P_5^{(6)} - P_5^{(5)} = \frac{6\cdot\left[(6-1)\cdot5-2\cdot(6-2)\right]}{2} - \frac{5\cdot\left[(5-1)\cdot5-2\cdot(5-2)\right]}{2} = 51-35 = 16\,.$$

7. Trovare altri due numeri triangolari che siano quadrati perfetti, oltre i tre da noi mostrati.

Dobbiamo cercare quindi un numero *n* per cui $\frac{n\cdot(n+1)}{2}$ è un quadrato perfetto. Il che significa che o *n* è un quadrato perfetto e l'altro è il doppio di un quadrato perfetto, o viceversa. Operando in questo modo troviamo

$$P_3^{(288)} = \frac{288\cdot289}{2} = 144\cdot289 = 12^2\cdot17^2 = 204^2;\; P_3^{(1681)} = \frac{1681\cdot1682}{2} = 41^2\cdot29^2 = 1189^2$$

Esprimere le seguenti espressioni mediante un solo numero poligonale

8. a) $P_5^{(4)} - P_3^{(3)}$; b) $P_5^{(r)} - P_3^{(r-1)}$; c) $14P_3^{(2)} + 2P_3^{(3)} + 1$; d) $6P_3^{(r)} + r + 1$

a) $P_5^{(4)} - P_3^{(3)} = \frac{4\cdot(3\cdot4-1)}{2} - \frac{3\cdot(3+1)}{2} = \frac{44-12}{2} = \frac{32}{2} = 4^2 = P_4^{(4)}$

b) $P_5^{(r)} - P_3^{(r-1)} = \frac{r\cdot(3r-1)}{2} - \frac{(r-1)\cdot r}{2} = \frac{r\cdot(3r-1-r+1)}{2} = \frac{r\cdot2r}{2} = r^2 = P_4^{(r)}$

c) $14\cdot\frac{3\cdot2}{2} + 2\cdot\frac{4\cdot3}{2} + 1 = 42+12+1 = 55 = \frac{10\cdot11}{2} = P_3^{(10)}$

d) $6\cdot\frac{r(r+1)}{2} + r + 1 = 3r(r+1) + r + 1 = (3r+1)(r+1) = P_8^{(r+1)}$

9. a) $P_3^{(r)} + P_3^{(r+1)}$; b) $8P_3^{(r)} + 1$; c) $3P_3^{(r)} + r + 1$; d) $3P_3^{(r)} + P_3^{(r+1)}$; e) $4P_3^{(r)} + r + 1$

a) $\frac{r\cdot(r+1)}{2} + \frac{(r+1)\cdot(r+2)}{2} = \frac{(r+1)\cdot(r+r+2)}{2} = \frac{(r+1)\cdot2\cdot(r+1)}{2} = (r+1)^2 = P_4^{(r+1)}$;

b) $\cancel{8}^{\,4}\cdot\frac{r\cdot(r+1)}{\cancel{2}} + 1 = 4r\cdot(r+1) + 1 = 4r^2 + 4r + 1 = (2r+1)^2 = P_4^{(2r+1)}$

c) $3\cdot\frac{r(r+1)}{2} + r + 1 = \frac{(3r+2)(r+1)}{2} = P_5^{(r+1)}$

d) $3\cdot\frac{r\cdot(r+1)}{2} + \frac{(r+1)\cdot(r+2)}{2} = \frac{(3r+r+2)\cdot(r+1)}{2} = (2r+1)\cdot(r+1) = P_3^{(2r+1)}$

e) $4\cdot\frac{r(r+1)}{2} + r + 1 = (2r+1)(r+1) = P_6^{(r+1)}$

10. Tenuto conto di alcuni degli esercizi precedenti esprimere $nP_3^{(r)} + r + 1, n \geq 2$.

$$n\cdot\frac{r(r+1)}{2} + r + 1 = \frac{(nr+2)(r+1)}{2} = P_{n+2}^{(r+1)}$$

11. Provare che $P_4^{(r)} + P_3^{(r-1)} = P_5^{(r)}$.

$$\frac{r\cdot\left[(r-1)\cdot 4-2\cdot(r-2)\right]}{2}+\frac{(r-1)\cdot r}{2}=\frac{r\cdot\left[(r-1)\cdot 4-2\cdot(r-2)+(r-1)\right]}{2}=$$

$$=\frac{r\cdot\left[(r-1)\cdot 5-2\cdot(r-2)+(r-1)\right]}{2}=P_5^{(r)}$$

12. Determinare una relazione fra $P_n^{(r)}$ e $P_n^{(r-1)}$.

$$P_n^{(r)}=\frac{r\cdot\left[(r-1)n-2(r-2)\right]}{2}=\frac{(r-1)\cdot\left[(r-1)n-2(r-2)\right]+(r-1)n-2(r-2)}{2}=$$

$$=\frac{(r-1)\cdot\left[(r-2)n-2(r-3)+n-2\right]+(r-1)n-2(r-2)}{2}=P_n^{(r-1)}+\frac{(r-1)\cdot(n-2)+(r-1)n-2(r-2)}{2}=$$

$$P_n^{(r-1)}+\frac{(r-1)\cdot(2n-2)-2(r-2)}{2}=P_n^{(r-1)}+(r-1)(n-1)-r+2$$

§3.

1. **Mediante un software di tipo CAS costruire una tabella del tipo di quella presentata nell'esempio 9.**
2. **Costruire una tabella analoga a quella da noi costruita considerando i numeri $p_1 \cdot p_2 \cdot p_3 \cdot \ ... \ \cdot p_h - 1$.**

$2 \cdot 3 - 1 = 5$	Numero primo
$2 \cdot 3 \cdot 5 - 1 = 29$	Numero primo
$2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$	Numero composto
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 - 1 = 2309$	Numero primo
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 - 1 = 30029$	Numero primo
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 - 1 = 510509 = 61 \cdot 8369$	Numero composto
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 - 1 = 9699689 = 53 \cdot 197 \cdot 929$	Numero composto

3. **Osserviamo che le due tabelle di cui all'esercizio precedente forniscono numeri con cifra delle unità sempre uguale ad 1 e a 9 rispettivamente. Possiamo dire che ciò vale sempre? Giustificare la risposta.**
   Escludendo 2 ± 1 e $2 \cdot 3 \pm 1$, tutti gli altri prodotti finiscono per 0, dato che contengono $2 \cdot 5$, quindi ovviamente i primi finiscono per $0 + 1 = 1$ e gli altri per $10 - 1 = 9$.
4. **Dimostrare il teorema di Dirichlet per la progressione di termine generale $6n - 1$**
   Supponiamo per assurdo che esistono solo un numero finito di primi, che indichiamo con $p_1, p_2, p_3, ..., p_h$, che hanno la forma $6n - 1$. Consideriamo quindi il numero $N = 6 \cdot (p_1 \cdot p_2 \cdot p_3 \cdot \ ... \cdot p_h) - 1$, che non è divisibile per nessuno dei p_i. Se N è primo abbiamo finito. Diversamente N è divisibile per un numero primo P diverso dai p_i. P può avere la forma $6n \pm 1$ $6n + 3$. Dato che $(6n + 1) \cdot (6m + 1) = 6k + 1$; $(6n + 3) \cdot (6m + 3) = 6k + 3$ e $(6n + 1) \cdot (6m + 3) = 6k + 3$, almeno uno dei fattori di P deve essere della forma $6n - 1$.
5. **Mostrare che la dimostrazione del teorema di Dirichlet utilizzata per la progressione $4n - 1$, non è utile per le progressioni $4n + 1$ e $8n - 1$.**
   Per $4n + 1$, il prodotto $4 \cdot (p_1 \cdot p_2 \cdot p_3 \cdot \ ... \cdot p_h) + 1$ potrebbe ottenersi mediante $(4n - 1) \cdot (4m - 1)$. Allo stesso modo $8 \cdot (p_1 \cdot p_2 \cdot p_3 \cdot \ ... \cdot p_h) - 1 = (8n + 3) \cdot (8m + 5) = 8k + 15 = 8(k + 2) - 1$.
6. **Costruire una tabella dei primi 10 termini delle progressioni di termine generale $4n + 1$, $4n + 3$ e $6n + 5$, evidenziando i numeri primi.**

$4n + 1$	**5**	3^2	**13**	**17**	$3 \cdot 7$	5^2	**29**	$3 \cdot 11$	**37**	**41**
$4n + 3$	**7**	**11**	$3 \cdot 5$	**19**	**23**	3^3	**31**	$5 \cdot 7$	$3 \cdot 13$	**43**
$6n + 5$	**11**	**17**	**23**	**29**	$5 \cdot 7$	**41**	**47**	**53**	**59**	$5 \cdot 13$

7. **Utilizzando un software di tipo CAS costruire la tabella dei valori $(n - 1)! + 1$ per n da 18 a 50.**
Con Derive

18	355687428096001
19	6402373705728001
20	121645100408832001
21	2432902008176640001
22	51090942171709440001
23	1124000727777607680001
24	25852016738884976640001
25	620448401733239439360001
26	15511210043330985984000001
27	403291461126605635584000001
28	10888869450418352160768000001
29	304888344611713860501504000001
30	8841761993739701954543616000001
31	265252859812191058636308480000001
32	8222838654177922817725562880000001
33	263130836933693530167218012160000001
34	8683317618811886495518194401280000001
35	295232799039604140847618609643520000001
36	10333147966386144929666651337523200000001
37	371993326789901217467999448150835200000001
38	13763753091226345046315979581580902400000001
39	523022617466601111760007224100074291200000001
40	20397882081197443358640281739902897356800000001

```
41          8159152832478977343456112695961158942720000000001
42          3345252661316380710817006205344075166515200000001
43          1405006117752879898543142606244511569936384000000001
44          6041526306337383563735513206851399750726451200000001
45          2658271574788448768043625811014615890319638528000000001
46          1196222208654801945619631614956577150643837337600000000001
47          550262215981208894985030542880025489296165175296000000001
48          258623241511168180642964355153611979969197632389120000000001
49          124139155925360726708622890473733750385214863546777600000000001
50          60828186403426756087225216332129537688755283137921024000000001
```

8. **Determinare se una proprietà analoga a quella stabilita dal teorema di Wilson vale anche per $(n-1)!-1$.**
   No, per esempio $(5-1)!-1 = 119 = 7 \cdot 17$
9. **Provare che un primo della forma $p = 4n-1$ non può esprimersi come somma di due quadrati.**
   Dato che p è dispari, se fosse somma di due quadrati essi dovrebbero avere diversa parità. Quindi dovrebbe essere $4n-1 = (2m)^2 + (2t+1)^2 = 4m^2 + 4t^2 + 4t + 1 = 4(m^2 + t^2 + t) + 1$, che è ovviamente impossibile.
10. **Verificare sui numeri primi minori di 100 della forma $p = 4n+1$ che possono esprimersi come somma di due quadrati in un solo modo. Esempio $5 = 1^2 + 2^2$.**
    I primi richiesti sono: $5 = 1^2 + 2^2$; $13 = 2^2 + 3^2$; $17 = 1^2 + 4^2$; $29 = 2^2 + 5^2$; $37 = 1^2 + 6^2$; $41 = 4^2 + 5^2$; $53 = 1^2 + 7^2$; $61 = 5^2 + 6^2$; $73 = 3^2 + 8^2$; $89 = 5^2 + 8^2$; $97 = 4^2 + 9^2$.
11. **Dato $n!$ possiamo stabilire qual è la massima potenza di un numero primo p che lo divide, provando che essa è data da $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^k} \right\rfloor$, $p^k \le n < p^{k+1}$, in cui il simbolo $\lfloor x \rfloor$ indica il cosiddetto *pavimento* del numero reale x, ossia il più grande numero intero minore o uguale a x. Provare questo fatto.**
    La dimostrazione è abbastanza ovvia, dato che dobbiamo stabilire quante volte p è contenuto nei fattori di $n!$ che sono appunto il quoziente della divisione $n!/p$. Ma ovviamente in questo modo contiamo una sola volta le potenze di p. Per esempio considerando 10!, abbiamo i fattori 3, 6 e 9 che contengono 3, solo che i primi due lo contengono una volta e il secondo 2. Per questo dobbiamo considerare anche i quozienti delle divisioni $n!/p^k$, ovviamente senza dividere per numeri maggiori di n.
12. **Stabilire la massima potenza di 7 che divide 1000!.**
    Dal risultato precedente abbiamo che $7^3 < 1000 < 7^4$, quindi 1000! Divide 7^n ma non 7^{n+1}, con $n = \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{7^2} \right\rfloor + \left\lfloor \frac{1000}{7^3} \right\rfloor = 142 + 20 + 2 = 164$

§5.

1. **Usando il crivello di Eratostene per determinare tutti i 168 numeri primi minori di 1000, qual è l'ultimo numero composto che andremo a cancellare?**
   Dato che $31 < \sqrt{1000} < 32$, ci fermiamo a $31^2 = 961$.

2. **Determinare una formula che valuti il numero di eliminazioni da operare con il crivello di Eratostene, per ottenere tutti i numeri primi minori di *n*, senza contare numeri già controllati.**
   Ci serve la funzione *floor*, ogni volta dobbiamo dividere n per i successivi numeri primi, per stabilire quanti numeri dobbiamo eliminare. Ovviamente in questo modo però non consideriamo eliminazioni già fatte. $\lfloor n/2 \rfloor + \lfloor n/3 \rfloor + \lfloor n/5 \rfloor \cdot \ldots \cdot \lfloor n/p_k \rfloor$, con p_k il k– esimo numero primo tale che $(p_k)^2 < n < (p_{k+1})^2$

§6.

1. **Utilizzare il metodo di Fermat per fattorizzare il numero *n* che lo stesso matematico francese pose ad esempio: 2027651281.**
   $45029^2 < 2027651281 < 45030^2$. $45030^2 - 2027651281 = 49619$ non è un quadrato perfetto. Continuiamo questo procedimento, finché troviamo $45041^2 - 2027651281 = 1040400 = 1020^2$. Quindi: $2027651281 = 45041^2 - 1020^2 = 44021 \cdot 46061$.
2. **Usando il metodo di Fermat determinare una fattorizzazione dei seguenti numeri: a) 24047; b) 123456789; c) 1234554321.**
   a) $155^2 < 24047 < 156^2$. $156^2 - 24047 = 289 = 17^2$. Quindi: $24047 = 156^2 - 17^2 = 139 \cdot 173$, che sono entrambi fattori primi;
   b) $11111^2 < 123456789 < 11112^2$. $11112^2 - 12345789 = 49619$ non è un quadrato perfetto. Continuiamo questo procedimento, finché troviamo $11115^2 - 123456789 = 86436 = 294^2$. Quindi: $123456789 = 11115^2 - 294^2 = 11409 \cdot 10821$. Continuando a scomporre si ottiene: $123456789 = 3^2 \cdot 3607 \cdot 3803$;
   c) $35136^2 < 1234554321 < 35137^2$. $35137^2 - 1234554321 = 54448$ ancora non è un quadrato perfetto. Continuiamo questo procedimento, finché troviamo $35185^2 - 1234554321 = 3429904 = 1852^2$. Quindi: $1234554321 = 35185^2 - 1852^2 = 33333 \cdot 37037$. La scomposizione può farsi adesso con i metodi tradizionali, ottenendo: $3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 41 \cdot 271$
3. **Utilizzando il metodo di Fermat verificare che i seguenti sono numeri primi: a) 197; b) 3121; c) 7919.**
   a) $14^2 < 197 < 15^2$. $15^2 - 197 = 28$ non è un quadrato perfetto, e $n^2 - 197$ non è un quadrato perfetto, per ogni n compreso tra 15 e $(197 - 1)/2 = 98$. Quindi il numero è primo.
   b) $55^2 < 3121 < 56^2$. $56^2 - 3121 = 15$, e $n^2 - 3121$ non è un quadrato perfetto, per ogni n compreso tra 56 e $(3121 - 1)/2 = 1560$. Quindi il numero è primo.
   c) $88^2 < 7919 < 89^2$. $89^2 - 7919 = 2$, e $n^2 - 7919$ non è un quadrato perfetto, per ogni n compreso tra 89 e $(7919 - 1)/2 = 3959$. Quindi il numero è primo.
4. **Scriviamo i numeri da 1 a 2023 uno di seguito all'altro. Dire perché l'enorme numero così ottenuto non può essere un quadrato perfetto.**
   Finisce per 3

§7.

1. **Provare che l'espressione $n^2 + n + a$, con $a \in \mathbb{N}$, $a > 1$, è divisibile per $(a - 1)$.**
   Sostituiamo $(a - 1)$ ad n: $(a - 1)^2 + (a - 1) + a = (a - 1) \cdot (a - 1 + 1) + a = (a - 1) \cdot a$
2. **Determinare una sequenza consecutiva di numeri primi per le espressioni a) $2n^2 + 29$; b) $6n^2 + 6n + 31$; c) $3n^2 + 3n + 23$.**
   a) $1 \le n \le 28$: {31, 37, 47, 61, 79, 101, 127, 157, 191, 229, 271, 317, 367, 421, 479, 541, 607, 677, 751, 829, 911, 997, 1087, 1181, 1279, 1381, 1487, 1597};

b) $1 \le n \le 28$: {43, 67, 103, 151, 211, 283, 367, 463, 571, 691, 823, 967, 1123, 1291, 1471, 1663, 1867, 2083, 2311, 2551, 2803, 3067, 3343, 3631, 3931, 4243, 4567, 4903, 5251, 5611}
c) $1 \le n \le 21$: {29, 41, 59, 83, 113, 149, 191, 239, 293, 353, 419, 491, 569, 653, 743, 839, 941, 1049, 1163, 1283, 1409, 1541}

3. **Utilizzare la dimostrazione del teorema 11 per provare che $n^2 + n + 17$ e $x^2 – 79x + 1601$ non possono generare solo numeri primi.**
Supponiamo che il polinomio $p(n) = n^2 + n + 17$ generi solo numeri primi quale che sia il valore intero assegnato alla sua variabile n. Supponiamo per esempio che $p(h) = h^2 + h + 17 = k$, con k numero primo. Consideriamo adesso il valore di p calcolato in $h + m \cdot k$: $[h + m \cdot (h^2 + h + 17)]^2 + h + m \cdot (h^2 + h + 17) + 17$, tale numero non è primo ma è divisibile per $h^2 + h + 17$. Infatti consideriamo la differenza: $[h + m \cdot (h^2 + h + 17)]^2 + h + m \cdot (h^2 + h + 17) + 17 – h^2 – h – 17 = h^2 + m^2 \cdot (h^2 + h + 17)^2 + 2hm(h^2 + h + 17) + m \cdot (h^2 + h + 17) – h^2 = m^2 \cdot (h^2 + h + 17)^2 + 2hm(h^2 + h + 17) + m \cdot (h^2 + h + 17)$ che è divisibile per $m \cdot (h^2 + h + 17)$ e dato che $p(h)$ è divisibile per k anche $p(h + m \cdot k)$ deve esserlo.
Supponiamo che il polinomio $p(x) = x^2 – 79x + 1601$ generi solo numeri primi quale che sia il valore intero assegnato alla sua variabile n. Supponiamo per esempio che $p(h) = h^2 – 79h + 1601 = k$, con k numero primo. Consideriamo adesso il valore di p calcolato in $h + m \cdot k$: $[h + m \cdot (x^2 – 79x + 1601)]^2 + h + m \cdot (x^2 – 79x + 1601) + 1601$, tale numero non è primo ma è divisibile per $x^2 – 79x + 1601$. Infatti consideriamo la differenza: $[h + m \cdot (x^2 – 79x + 1601)]^2 + h + m \cdot (x^2 – 79x + 1601) + 1601 – h^2 + 79h – 1601 = h^2 + m^2 \cdot (x^2 – 79x + 1601)^2 + 2hm(x^2 – 79x + 1601) + m \cdot (x^2 – 79x + 1601) – h^2 = m^2 \cdot (x^2 – 79x + 1601)^2 + 2hm(x^2 – 79x + 1601) + m \cdot (x^2 – 79x + 1601)$ che è divisibile per $m \cdot (x^2 – 79x + 1601)$ e dato che $p(h)$ è divisibile per k anche $p(h + m \cdot k)$ deve esserlo.

4. **Utilizzando un software di tipo CAS, tabulare per un centinaio di valori, facendo scrivere solo i valori per cui essi forniscono numeri primi. a) $n^2 + n + 41$; b) $n^2 + n + 17$; c) $n^2 – 79n + 1601$.**
a) Si ottengono numeri primi per $x \in$ {1, 2, … 39, 42, 43, 45, …, 48, 50, …, 55, 57, … 64, 66, …, 75, 77, …, 80, 83, 85, 86, 88, 90, 92, …, 95, 97, …, 100};
b) Si ottengono numeri primi per $n \in$ {1, 2, ... 15, 18, 19, 21, …, 24, 26, … 31, 35, 37, 38, 40, 42, 44, …, 47, 49, 53, 56, 57, 59, 60, 62, 63, 64, 70, 72, 73, 75, 76, 79, 81, 82, 86, 87, 91, 92, 95, 98}
c) Si ottengono numeri primi per $x \in$ {1, 2, …, 79, 82, 83, 85, …, 88, 90, …, 95, 97, …, 100}

5. **Verificare la congettura di Goldbach per tutti i numeri pari da 4 fino a 50.**
4 = 2 + 2; 6= 3 + 3; 8 = 3 + 5; 10 = 3 + 7; 12 = 5 + 7; 14 = 7 + 7; 16 = 5 + 11; 18 = 7 + 11; 20 = 3 + 17; 22 = 5 + 17; 24 = 7 + 17; 26 = 3 + 23; 28 = 5 + 23; 30 = 7 + 23; 32 = 3 + 29; 34 = 5 + 29; 36 = 7 + 29; 38 = 7 + 31; 40 = 3 + 37; 42 = 5 + 37; 44 = 7 + 37; 46 = 3 + 43; 48 = 5 + 43; 50 = 7 + 43.

6. **Tenuto conto dell'esercizio precedente osservare che se $2n = p_1 + p_2$, anche $2n + 2$ e $2n + 4$ verificano certamente la congettura di Goldbach per opportuni valori di p_1 e p_2. Quali?**
Se $2n = 3 + p_2$, allora $3 + p_2$, $5 + p_2$, e $7 + p_2$, verificano certamente la congettura.

7. **Possiamo dire che se $2n = p_1 + p_2$ verifica la congettura di Goldbach, in quale caso certamente la verifica anche $2n + 2$?**
Se almeno una coppia fra $(p_1, p_1 + 2)$ e $(p_2, p_2 + 2)$ è di primi gemelli.

8. **Notiamo che alcuni numeri sono esprimibili anche in due modi diversi come somme di due numeri primi. Trovare tutti i numeri pari minori di 50 che non verificano quest'ultima proprietà.**
   2, 4, 6, 8, 12
9. **Trovare il primo numero pari esprimibile in tre modi diversi come somma di due numeri primi.**
   $22 = 3 + 19 = 5 + 17 = 11 + 11$
10. **Trovare il primo numero pari esprimibile in quattro modi diversi come somma di due numeri primi.**
    $34 = 3 + 31 = 5 + 29 = 11 + 23 = 17 + 17$

§8.

1. **Il numero 12 si può scrivere come $2 \cdot 6$ o anche come $3 \cdot 4$, che sono fattorizzazioni distinte, anche se non formate da numeri primi. Esistono numeri che si possono esprimere in un solo modo come prodotto di due numeri nessuno dei quali è uguale a 1? Se la risposta è positiva quali sono?**
   Sì: i numeri prodotto di due numeri primi
2. **Con riferimento al quesito precedente, quali sono i numeri che hanno due sole fattorizzazioni?**
   I numeri del tipo p^2q, con p e q numeri primi
3. **Risolvere il problema degli "occhi azzurri" nella sua versione originaria, ossia con il prodotto delle età pari a 72 anni.**
   La prima informazione ci dice che i figli possono avere una delle seguenti tre terne di età: (1, 1, 72), (1, 2, 36), (1, 3, 24), (1, 4, 18), (1, 6, 12), (1, 8, 9), (2, 2, 18), (2, 3, 12), (2, 4, 9), (2, 6, 6) (3, 3, 8), (3, 4, 6); dato che esse sono le uniche terne il cui prodotto fornisce 72. Se le sommiamo otteniamo sempre risultati diversi tranne nei casi $2 + 6 + 6 = 3 + 3 + 8 = 14$. Dato che Anna ha detto di non riuscire a determinare le età dei tre ragazzi esse devono essere ferme davanti ad una abitazione posta al numero 14. La terza informazione svela l'inghippo, dato che la mamma parla di un maggiore, i due gemelli che vi sono fra i tre figli non possono comprendere il primogenito, come accadrebbe nel caso (2, 6, 6). Quindi i bambini hanno 3, 3 e 8 anni.
4. **Un quesito da Stanford 1958. Moltiplicando fra loro l'età del capitano, il numero dei suoi figli e la lunghezza della sua barca si ottiene 32118. Il capitano ha figli di entrambi i sessi, ha più anni che figli e ha meno di 100 anni. La barca è misurata in un numero intero di piedi, ed è più di 1 piede. Determinare i tre numeri.**
   $32118 = 2 \cdot 3 \cdot 53 \cdot 101$, dato che i fattori sono 4 o 5 se consideriamo anche il numero 1, dobbiamo moltiplicare fra loro due dei fattori. Dato che vogliamo avere dati realistici l'unica possibilità è che siano 53 anni, 6 figli e 101 piedi.
5. **Un quesito da Stanford 1960. Delle penne a sfera venivano vendute a 50 cents, ma non avevano molti clienti, così il prezzo fu ridotto e si vendettero tutte quelle rimaste al prezzo complessivo di \$ 31.93. Qual era il prezzo scontato?**
   Dato che $3193 = 31 \cdot 103$, abbiamo solo la possibilità 31 cents, dato che 103 cents non è un prezzo scontato.
6. **Un quesito da Stanford 1963. Provare che $n^2 \cdot (n^2 - 1) \cdot (n^2 - 4)$ è divisibile per 360 qualunque sia n numero naturale.**
   Abbiamo $n^2 \cdot (n - 1) \cdot (n + 1) \cdot (n - 2) \cdot (n + 2)$, quindi abbiamo 5 numeri naturali consecutivi in cui ci sono perciò certamente un numero divisibile per 2, uno per 3, uno per 4 e uno per 5, quindi il prodotto è divisibile almeno per 120. Inoltre se vi è un solo multiplo di 3 è n, ed è perciò multiplo di 9. Quindi il numero di partenza è multiplo di 360

7. **Provare che a) $n^2 \cdot (n^2 - 1)$ è divisibile per 12; b) $n^5 - n$ è divisibile per 30; c) $n^4 + 2n^3 + 3n^2 + 2n$ è divisibile per 8**
   a) se n è pari, cioè $n = 2h$, avremo: $n^2 \cdot (n^2 - 1) = 4h^2 \cdot (4h^2 - 1)$, che è divisibile per 4, se poi h è multiplo di 3, $h = 3m$, allora è divisibile per 12. Se invece $h = 3m \pm 1$, $4h^2 - 1 = 4 \cdot (3m \pm 1)^2 - 1 = 36m^2 \pm 24m + 4 - 1 = 36m^2 \pm 24m + 3 = 3 \cdot (12m^2 \pm 8m + 1)$, divisibile per 3, quindi va bene.
   b) $n^5 - n = n \cdot (n^4 - 1) = n \cdot (n^2 - 1) \cdot (n^2 + 1) = n \cdot (n - 1) \cdot (n + 1) \cdot (n^2 + 1)$. I primi tre fattori sono consecutivi, quindi uno almeno è pari, e uno solo è multiplo di 3. Perciò il prodotto è multiplo di $2 \cdot 3 = 6$. Se nessuno dei 3 è multiplo di 5, vuol dire che $n = 5m \pm 2$, quindi: $n^2 + 1 = (5m \pm 2)^2 + 1 = 25m^2 \pm 20m + 4 + 1 = 25m^2 \pm 20m + 5$, che è multiplo di 5. In ogni caso il numero è multiplo di $2 \cdot 3 \cdot 5 = 30$.
   c) $n^4 + 2n^3 + 3n^2 + 2n = n \cdot (n^3 + 2n^2 + 3n + 2) = n \cdot (n\ + 1) \cdot (n^2 + n + 2)$. I primi due fattori sono uno pari e l'altro dispari, quindi il numero è pari. Ora se $n = 2h$, allora $n^2 + n + 2 = 4h^2 + 2h + 2 = 2 \cdot (2h^2 + h + 1)$, quindi abbiamo un altro fattore 2. Il numero è divisibile per 4. Se anche h è pari è divisibile anche per 8. Se $h = 2t + 1$, $2h^2 + h + 1 = 2(2t + 1)^2 + 2t + 1 + 1 = 8t^2 + 8t + 2 + 2t + 2$, che è pari. Quindi il numero è divisibile per 8. Stesso ragionamento se $n = 2h + 1$.

8. **Provare che a) $n^3 + 11n$ è divisibile per 6; b) $7^n - 5^n$ è divisibile per 2; c) $n^3 + (n + 1)^3 + (n + 2)^3$ è divisibile per 9**
   a) $n^3 + 11n = n \cdot (n^2 + 11)$ se n è multiplo di 3, cioè $n = 3h$, avremo: $3h \cdot (9h^2 + 11)$, che è divisibile per 6 dato che se anche h è pari allora $3h$ è multiplo di 6, mentre se h è dispari, il secondo fattore è pari. Se $n = 3h \pm 1$, avremo: $(3h \pm 1) \cdot (9h^2 \pm 6h + 1 + 11) = (3h \pm 1) \cdot (9h^2 \pm 6h + 12) = (3h \pm 1) \cdot 3 \cdot (3h^2 \pm 2h + 6)$. Se h è dispari il primo fattore è pari, quindi ci siamo. Se h è pari lo è il terzo fattore.
   b) La potenza di un numero dispari è dispari, quindi la differenza di due numeri dispari è pari.
   c) Dato che i simboli sono del tutto arbitrari, basta scrivere la somma dei cubi di tre numeri consecutivi e quindi conviene scrivere: $(n - 1)^3 + n^3 + (n + 1)^3 = n^3 - 3n^2 + 3n - 1 + n^3 + n^3 + 3n^2 + 3n + 1 = 3n^3 + 6n = 3n \cdot (n^2 + 2)$, e ciò semplifica ma non incide sulla dimostrazione. Se n è multiplo di 3 abbiamo finito. Se $n = 3h \pm 1$: $3n \cdot (n^2 + 2) = 3 \cdot (3h \pm 1) \cdot [(3h \pm 1)^2 + 2] = 3 \cdot (3h \pm 1) \cdot (9h^2 \pm 6h + 1 + 2) = 3 \cdot (3h \pm 1) \cdot (9h^2 \pm 6h + 3) = 3 \cdot (3h \pm 1) \cdot 3 \cdot (3h^2 \pm 2h + 1)$. Dimostrato.
9. **Provare che fra i numeri $(m^2 - n^2)$, $2mn$ e $(m^2 + n^2)$, con m, n numeri naturali, a) uno almeno è divisibile per 3; b) uno almeno è divisibile per 5; c) il prodotto di almeno due di essi è divisibile per 12; d) il loro prodotto è divisibile per 60.**
   a) $(m^2 - n^2)$ e $(m^2 + n^2)$ sono entrambi pari o entrambi dispari. Quindi se $(m^2 - n^2) = 3h + 1$ è $(m^2 + n^2) = 3k + 1 \Rightarrow 2m^2 = 3t + 2$ e $2n^2 = 3a \Rightarrow (2mn)^2 = 3a(3t + 2)$, cioè $2mn$ è multiplo di 3. Stesso ragionamento negli altri casi in cui due dei tre non sono multipli di 3.
   b) Se $2mn$ non è multiplo di 5 allora non lo sono né m e né n. Se $m = 5a + 1$ e $n = 5b \pm 1 \Rightarrow (m^2 - n^2) = 25(a^2 - b^2) + 10(a \pm b)$; se $m = 5a + 1$ e $n = 5b \pm 2 \Rightarrow (m^2 + n^2) = 25(a^2 + b^2) + 10(a \pm 2b) + 5$.
   c) Se mn non è divisibile per 6, allora se m e n sono entrambi dispari, $(m^2 - n^2)$ e $(m^2 + n^2)$ sono entrambi pari e uno di essi è divisibile per 3 per il punto a).
   d) Per i punti precedenti il prodotto è divisibile per 15, anzi per 30 dato che abbiamo il fattore 2. Ora se mn è dispari, gli altri due fattori sono pari, quindi il prodotto è divisibile per 60.

§9.

1. **Con l'algoritmo euclideo determinare il *MCD* dei seguenti numeri:**
   a) (12345; 23456); b) (123321; 234432); c) (102132; 213243).
   a) 23456 = 12345 + 11111; 12345 = 11111 + 1234; 11111 = 9 · 1234 + 5; 1234 = 246 · 5 + 4; 5 = 4 · 1 + 1; 1 = 1 + 0. Quindi MCD(12345; 23456) = 1
   b) 234432 = 123321 + 111111; 123321 = 111111 + 12210; 11111 = 9 · 12210 + 1221; 12210 = 10 · 1221 + 0 $\Rightarrow$ MCD(123321; 234432) = 1221;
   c) 213243 = 102132 + 8979; 102132 = 11 · 8979 + 3363; 8979 = 2 · 3363 + 2253; 3363 = 2253 + 1110; 2253 = 2 · 1110 + 33; 1110 = 33 · 33 + 21; 33 = 21 + 12; 21 = 12 + 9; 12 = 9 + 3; 9 = 3 · 3 + 0 $\Rightarrow$ MCD (102132; 213243) = 3
2. **Dal *Sun Tsu Suan Ching* un testo cinese del IV secolo. *Tre sorelle escono di casa rispettivamente ogni* 3, 4 *e* 5 *giorni. Se un certo giorno escono tutti e tre insieme dopo quanti giorni riusciranno insieme?***
   mcm(3, 4, 5) = 60
3. **Nel gioco *Regina, reginella*, ciascuno deve arrivare dalla Regina facendo passi di animale. Sappiamo che Sharon arriva dalla regina con 10 passi da tartaruga, 2 da lepre e 1 da canguro. Sappiamo inoltre che un passo di canguro è lungo quanto 2 da lepre e quanto 6 da tartaruga. Se Stefania arriva dalla regina facendo solo passi da tartaruga, quanti passi fa?**
   10T + 2L + 1C = 10T + 2C = 10T + 12T = 22T
4. **Caterina ha invitato 8 suoi amici per il giorno di Pasqua e a ognuno vuole regalare lo stesso numero di ovetti. Non tutti però sono certi di poter venire: Giulio verrà solo se lo farà Giada, mentre Anna, Carlo e Tommaso forse andranno insieme a Parigi. Quanti ovetti deve comprare almeno perché possa darne a tutti lo stesso numero, quanti che siano gli intervenuti?**
   Ne verranno minimo 3, che potranno essere 5 oppure 8, quindi mcm(3, 5, 8) = 120
5. **Erika ha più di 50 ma meno di 120 caramelle. Si accorge che mentre è insieme ad Alice e Bob potrebbe dividerle in parti uguali con loro. Nel frattempo arrivano Tom ed Erika e così non può più dividere le caramelle in parti uguali fra tutti. Dopo qualche minuto arrivano Dalila e Mirko, perciò lo può fare di nuovo. Quante caramelle ha Erika a) minimo? b) massimo?**
   Dobbiamo trovare un numero compreso tra 50 e 90 multiplo di 3 e di 7 ma non di 5, quindi multiplo di 21 ma non di 5. I multipli di 21 tra 50 e 90 sono 63, 84, 105. Quindi minimo 63, massimo 84,
6. **Generalizzare il Teorema 15 a più di due numeri.**
   Si applica il principio di inclusione esclusione. Così per esempio per tre numeri:
   $mcm(a,b,c) = \dfrac{a \cdot b \cdot c \cdot MCD(a,b,c)}{MCD(a,b) \cdot MCD(a,c) \cdot MCD(b,c)}$. Così
   $$mcm(15,20,24) = \frac{15 \cdot 20 \cdot 24 \cdot MCD(15,20,24)}{MCD(15,20) \cdot MCD(15,24) \cdot MCD(20,24)} = \frac{\cancel{15}^{5} \cdot \cancel{20} \cdot \cancel{24} \cdot 1}{\cancel{5} \cdot \cancel{3} \cdot \cancel{4}} = 120$$
   Per *n* numeri:
   $$mcm(a_1,a_2,...,a_n) = \prod_{k=1}^{n} a_k \cdot \prod_{\substack{i,j=1 \\ i \neq j}}^{n} \left[MCD(a_i,a_j) \right]^{-1} \cdot \prod_{i,j,m=1}^{n} MCD(a_i,a_j,a_m) \cdot ... \cdot \left[MCD(a_1,a_2,...,a_n) \right]^{(-1)^{n+1}}$$

§10.

1. **Tenuto conto dei risultati del teorema 18, determinare per quali numeri ν(*n*) è un numero dispari.**
   Dato che ν(*n*) è prodotto dei successivi degli esponenti dei fattori primi, questi de-

vono avere solo esponenti pari

2. **Verificare il teorema 18 calcolando a) $\nu(124)$; b) $\nu(123456)$; c) $\nu(12345678)$.**
   a) I divisori di 24 sono: {1, 2, 4, 31, 62, 124} ed effettivamente, dato che $124 = 2^2 \cdot 31$, si ha: $\nu(124) = (2 + 1) \cdot (1 + 1) = 6$;
   b) I divisori di 123456 sono: {1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96, 192, 643, 1286, 1929, 2572, 3858, 5144, 7716, 10288, 15432, 20576, 30864, 41152, 61728, 123456} ed effettivamente, dato che $123456 = 2^6 \cdot 3 \cdot 643$, si ha: $\nu(123456) = (6 + 1) \cdot (1 + 1) \cdot (1 + 1) = 28$;
   c) I divisori di 12345678 sono: {1, 2, 3, 6, 9, 18, 47, 94, 141, 282, 423, 846, 14593, 29186, 43779, 87558, 131337, 262674, 685871, 1371742, 2057613, 4115226, 6172839, 12345678} ed effettivamente, dato che $12345678 = 2 \cdot 3^2 \cdot 47 \cdot 14593$, si ha: $\nu(12345678) = (2 + 1) \cdot (1 + 1)^3 = 24$

3. **Verificare il teorema 19 calcolando a) $\sigma(124)$; b) $\sigma(123456)$; c) $\sigma(12345678)$.**
   a) Abbiamo: $\sigma\left(2^2 \cdot 31\right) = \frac{2^3 - 1}{2 - 1} \cdot \frac{31^2 - 1}{31 - 1} = 7 \cdot 32 = 224 = 1 + 2 + 4 + 31 + 62 + 124$
   b) Abbiamo: $\sigma\left(2^6 \cdot 3 \cdot 643\right) = \frac{2^7 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{643^2 - 1}{643 - 1} = 127 \cdot 4 \cdot 644 = 327152 = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 16 + 24 + 32 + 48 + 64 + 96 + 192 + 643 + 1286 + 1929 + 2572 + 3858 + 5144 + 7716 + 10288 + 15432 + 20576 + 30864 + 41152 + 61728 + 123456327152$;
   c) Abbiamo:
   $\sigma\left(2 \cdot 3^2 \cdot 47 \cdot 14593\right) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{47^2 - 1}{47 - 1} \cdot \frac{14593^2 - 1}{14593 - 1} = 3 \cdot 13 \cdot 48 \cdot 14594 = 273319968$
   $= 1 + 2 + 3 + 6 + 9 + 18 + 47 + 94 + 141 + 282 + 423 + 846 + 14593 + 29186 + 43779 + 87558 + 131337 + 262674 + 685871 + 1371742 + 2057613 + 4115226 + 6172839 + 12345678$

4. **Osservato che $\sigma(3) = 1 + 3 = 2^2$, determinare tutti gli $n \leq 100$, per cui $\sigma(n) = m^2$.**
   Dobbiamo esprimere un quadrato come la somma di tutti i divisori di un numero. Verificando troviamo $36 = 1 + 2 + 11 + 22 \Rightarrow \sigma(22) = 6^2$; $144 = 1 + 2 + 3 + 6 + 11 + 22 + 33 + 66 \Rightarrow \sigma(66) = 12^2$; $144 = 1 + 2 + 5 + 7 + 10 + 14 + 35 + 70 \Rightarrow \sigma(70) = 12^2$; $144 = 1 + 2 + 3 + 6 + 11 + 22 + 33 + 66 \Rightarrow \sigma(66) = 12^2$; $121 = 1 + 3 + 9 + 27 + 81 \Rightarrow \sigma(81) = 11^2$; $144 = 1 + 2 + 47 + 94 \Rightarrow \sigma(94) = 12^2$

5. **Determinare tutti gli $n \leq 20$, per cui $\sigma(n^2) = m^2$.**
   Abbiamo già visto che $\sigma(1) = 1 = 1^2$ e $\sigma(9^2) = 11^2$. Verifichiamo quindi per i rimanenti n da 10 a 20 e troviamo solo $\sigma(20^2) = 1 + 2 + 4 + 5 + 8 + 10 + 16 + 20 + 25 + 40 + 50 + 80 + 100 + 200 + 400 = 961 = 31^2$.

6. **Determinare tutti gli $n \leq 50$, per cui $\sigma_0(n^2) = m^2$.**
   Ovviamente $\sigma_0(1^2) = 0^2$. Poi $\sigma_0(3^2) = 2^2$ e $\sigma_0(49^2) = 20^2$

7. **Trovare i minimi numeri naturali che hanno a) 2; b) 3; c) 4; d) 5; e) 6 divisori.**
   Tenuto conto della formula del Teorema 18 si ha: a) 2^1; b) $2^2 = 4$; c) $2^3 = 8$; d) $2^4 = 16$; e) $2^5 = 32$

8. **Tenuto conto del precedente quesito, qual è il minimo naturale che ha n divisori?**
   2^{n-1}

9. **Trovare i minimi numeri naturali, con almeno 2 fattori primi, che hanno a) 10; b) 20 divisori.**
   a) Dato che $10 = 2 \cdot 5$ un numero con 10 divisori e 2 fattori primi è del tipo $p_1 \cdot p_2^4$ e il più piccolo di essi è evidentemente $3 \cdot 2^4 = 48$.
   b) Si ha $20 = 4 \cdot 5 = 2 \cdot 2 \cdot 5$, quindi abbiamo numeri del tipo $p_1^3 \cdot p_2^4 \vee p_1 \cdot p_2 \cdot p_3^4$, il

minimo di essi è $3 \cdot 5 \cdot 2^4 = 240$.

10. **a) Quanti fattori primi può avere al massimo un numero che ha 34 divisori?**
    b) Per avere lo stesso risultato con *n* divisori, quanto vale *n*?
    a) Dato che $34 = 1 \cdot 34 = 2 \cdot 17$, il numero è del tipo $p^{33} \vee p_1 \cdot p_2^{16}$, quindi massimo due fattori primi.
    b) Quindi hanno massimo 2 fattori primi i numeri esprimibili come $p_1^{a-1} \cdot p_2^{b-1}$, ed $n = a \cdot b$ con a e b numeri primi.
11. **Quanti fattori primi distinti può avere al massimo un numero che ha 12 divisori?**
    Dato che 12 si può esprimere con il maggior numero di fattori come $2 \cdot 2 \cdot 3$, vuol dire che un numero con 12 divisori al massimo conterrà tre fattori primi distinti.
12. **Quanti divisori minimo ha un numero che ha a) 5; b) *n* fattori primi distinti?**
    a) $k = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$ ha $(1 + 1)^5 = 32$ divisori;
    b) dal precedente: 2^n divisori
13. **Trovare tutti i numeri minori o uguali a 30 (in effetti sono gli unici possibili) i cui numeri a essi inferiori con i quali sono coprimi sono tutti numeri primi.**
    2 è un caso particolare, dato che non è coprimo con 1; 3 coprimo con 2; 4 coprimo con 2 e 3; 6 coprimo con 5; 8 coprimo con 3, 5 e 7; 12 coprimo con 5, 7 e 11; 24 coprimo con 5, 7, 11, 13, 17, 19, 23; 30 coprimo con 7, 11, 13, 17, 19, 23, 29.
14. **Verificare il risultato del teorema 21 per *n* = 35, 40, 123**
    I numeri coprimi con 35 sono 34 – 6 – 4 = 23, dato che abbiamo tolto i multipli di 5 e quelli di 7. In effetti si ha: $35 = 5 \cdot 7$ e $\phi(35) = 5^0 \cdot (5 - 1) \cdot 7^0 \cdot (7 - 1) = 4 \cdot 6 = 24$. I numeri coprimi con 40 sono 39 – 19 – 7 + 3 = 16, dato che abbiamo tolto i multipli di 2 e quelli di 5 e poi abbiamo aggiunto i multipli di 10 che avevamo tolo due volte. In effetti si ha: $40 = 2^3 \cdot 5$ e $\phi(40) = 2^2 \cdot (2 - 1) \cdot 5^0 \cdot (5 - 1) = 4 \cdot 4 = 16$. I numeri coprimi con 123 sono 122 – 40 – 2 = 80 dato che abbiamo tolto i multipli di 3 e quelli di 41. In effetti si ha: $123 = 3 \cdot 41$ e $\phi(123) = 3^0 \cdot (3 - 1) \cdot 41^0 \cdot (41 - 1) = 2 \cdot 40 = 80$
15. **Determinare tutti i numeri naturali *n* per cui si ha $\phi(n) = 8$.**
    Si ha: $8 = 2^3 \cdot (2 - 1) \Rightarrow \phi(2^4) = 8$; $8 = 3^0 \cdot (3 - 1) \cdot 5^0 \cdot (5 - 1) \Rightarrow \phi(3 \cdot 5) = 8$; $8 = 2^1 \cdot (2 - 1) \cdot 5^0 \cdot (5 - 1) \Rightarrow \phi(2^2 \cdot 5) = 8$; $8 = 2^2 \cdot (2 - 1) \cdot 3^0 \cdot (3 - 1) \Rightarrow \phi(2^3 \cdot 3) = 8$; $8 = 2^0 \cdot (2 - 1) \cdot 3^0 \cdot (3 - 1) \cdot 5^0 \cdot (5 - 1) \Rightarrow \phi(2 \cdot 3 \cdot 5) = 8$
16. **Provare che non esistono numeri naturali per cui $\phi(n) = 34$.**
    $34 = 1 \cdot 34 = 2 \cdot 17$. 17 si può trovare solo in $17^1 \cdot (17 - 1) \neq 34$. Oppure potremmo trovare direttamente 34 in $35^0 \cdot (35 - 1)$, ma 35 non è numero primo.
17. **Trovare tutti i numeri $h < 100$ per cui $\phi(n) = h$ non ha soluzione.**
    Dato che $\phi\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1)$, per $h = 14 = 1 \cdot 14 = 2 \cdot 7$, dovrebbe essere $14 = 15^0 \cdot (15 - 1)$, ma 15 non è un numero primo, mentre non esiste un numero primo p per cui $14 = p^h \cdot (p - 1)$; Lo stesso accade con 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98
18. **Provare che $\phi(n^2) = n \cdot \phi(n)$, $\forall n \in \mathbb{N}$.**
    Osserviamo che per esempio $15 = 3 \cdot 5 \Rightarrow 15^2 = 3^2 \cdot 5^2$; $24 = 2^3 \cdot 3 \Rightarrow 24^2 = 2^6 \cdot 3^2$.
    Quindi in generale se $n = \prod_{i=1}^{k} p_i^{a_i} \Rightarrow n^2 = \prod_{i=1}^{k} p_i^{2a_i}$, pertanto
    $$\phi\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1) \Rightarrow \phi\left(\prod_{i=1}^{k} p_i^{2a_i}\right) = \prod_{i=1}^{k} p_i^{2a_i - 2} \cdot (p_i - 1) = \prod_{i=1}^{k} p_i^{a_i - 1} \cdot \prod_{i=1}^{k} p_i^{a_i - 1} \cdot (p_i - 1) = n \cdot \phi(n)$$
19. **Costruire una tabella per $\phi(n)$, per tutti gli *n* inferiori a 50.**

Dato che $\phi(p) = 0$ per p numero primo, riportiamo solo i valori per gli n composti

n	4	6	8	9	10	12	14	15	16	18	20	24	25	26	27
$\phi(n)$	**1**	**3**	**2**	**5**	**7**	**7**	**6**	**7**	**11**	**11**	**11**	**15**	**4**	**13**	**8**
n	28	30	32	33	34	35	36	38	39	40	42	44	45	48	49
$\phi(n)$	**15**	**21**	**15**	**12**	**17**	**10**	**23**	**19**	**14**	**23**	**29**	**23**	**20**	**31**	**6**

20. **Provare che $\sum_{i=0}^{h}\phi\left(p^i\right) = p^h$, per ogni numero primo p.**

$$\sum_{i=0}^{h}\phi\left(p^i\right) = 1+\sum_{i=1}^{h}\left[p^{i-1}\cdot(p-1)\right] = 1+(p-1)\cdot\sum_{i=1}^{h}\left(p^{i-1}\right) = 1+\cancel{(p-1)}\cdot\frac{p^h-1}{\cancel{p-1}} = p^h$$

21. **Provare che dato un numero naturale n, e indicati con d_i $1 \le i \le h$, tutti i suoi divisori allora $\sum_{i=1}^{h}\phi\left(d_i\right) = p^h$.**

Tenuto conto del precedente esercizio basta provare che la proprietà vale per $n = p_1 \cdot p_2$, con $p_1 \cdot p_2$ due numeri primi. Dobbiamo cioè provare che $1 + \phi(p_1) + \phi(p_2) + \phi(p_1 \cdot p_2) = p_1 \cdot p_2$. Abbiamo: $1 + \phi(p_1) + \phi(p_2) + \phi(p_1 \cdot p_2) = 1 + (p_1 - 1) + (p_2 - 1) + \phi(p_1) \cdot \phi(p_2) = p_1 + p_2 - 1 + (p_1 - 1)\ (p_2 - 1) = p_1 + p_2 - 1 + p_1p_2 - p_1 - p_2 + 1 = p_1p_2$.

Quesiti sulle serie di Farey

22. **Costruire quelle di ordine n: $6 \le n \le 10$.**
{1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6}; {1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 2/5, 3/7, 1/2, 4/7, 3/5, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7}; {1/8, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 3/8, 2/5, 3/7, 1/2, 4/7, 3/5, 5/8, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 7/8}; {1/9, 1/8, 1/7, 1/6, 1/5, 2/9, 1/4, 2/7, 1/3, 3/8, 2/5, 3/7, 4/9, 1/2, 5/9, 4/7, 3/5, 5/8, 2/3, 5/7, 3/4, 7/9, 4/5, 5/6, 6/7, 7/8, 8/9}; {1/10, 1/9, 1/8, 1/7, 1/6, 1/5, 2/9, 1/4, 2/7, 3/10, 1/3, 3/8, 2/5, 3/7, 4/9, 1/2, 5/9, 4/7, 3/5, 5/8, 2/3, 7/10, 5/7, 3/4, 7/9, 4/5, 5/6, 6/7, 7/8, 8/9, 9/10}

23. **Provare che i termini sono sempre in numero dispari e il termine centrale è sempre ½.**

Abbiamo visto che a parte $\phi(2)$, $\phi(n)$ è sempre pari, quindi $\sum_{h=2}^{n}\phi\left(h\right)$ è dispari e dato che la serie inizia con $1/n$ e finisce con $(n - 1)/n$, il suo termine centrale è ovviamente ½.

24. **Enunciare una congettura relativa alla somma delle frazioni di posto simmetrico rispetto al centro.**
Consideriamo quella di ordine 10: 1/10 + 9/10 = 1/9 + 8/9 = 1/8 + 7/8 = 1/7 + 6/7 = 1/6 + 5/6 = 1/5 + 4/5 = 2/9 + 7/9 = ¼ + ¾ = 2/7 + 5/7 = 3/10 + 7/10 = 1/3 + 2/3 = 3/8 + 5/8 = 2/5 + 3/5 =3/7 = + 4/7 = 4/9 + 5/9 = 1

25. **Enunciare una congettura relativa alla differenza fra due termini consecutivi.**
Sempre ordine 10: 1/9 – 1/10 = 1/90; 1/8 – 1/9 = 1/72; 1/7 – 1/8 = 1/56; 1/6 – 1/7 = 1/42; 1/5 – 1/6 = 1/30; 2/9 – 1/5 = 1/45; ….È uguale al reciproco del prodotto dei loro denominatori

§11.

1. **Provare che tutte le potenze dei numeri primi rappresentano numeri deficienti.**

$$\sigma_0(p^n) = 1 + p + p^2 + p^{n-1} = \frac{p^n - 1}{p - 1} < p^n$$

2. **Determinare tutti i numeri abbondanti minori di 100.**
   $\sigma_0(12) = 1 + 2 + 3 + 4 + 6 = 16 > 12$; $\sigma_0(18) = 1 + 2 + 3 + 6 + 9 = 21 > 18$; $\sigma_0(20) = 1 + 2 + 4 + 5 + 10 = 22 > 20$; $\sigma_0(24) = 1 + 2 + 3 + 4 + 6 + 8 + 12 = 36 > 24$; $\sigma_0(30) = 1 + 2 + 3 + 5 + 6 + 10 + 15 = 42 > 30$; $\sigma_0(36) = 1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 = 55 > 36$; $\sigma_0(40) = 1 + 2 + 4 + 5 + 8 + 10 + 20 = 50 > 40$; $\sigma_0(42) = 1 + 2 + 3 + 6 + 7 + 14 + 21 = 54 > 42$; $\sigma_0(48) = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 16 + 24 = 76 > 48$; $\sigma_0(54) = 1 + 2 + 3 + 6 + 9 + 18 + 27 = 66 > 54$; $\sigma_0(56) = 1 + 2 + 4 + 7 + 8 + 14 + 28 = 64 > 56$; $\sigma_0(60) = 1 + 2 + 3 + 4 + 5 + 6 + 10 + 12 + 15 + 20 + 30 = 108 > 60$; $\sigma_0(66) = 1 + 2 + 3 + 6 + 11 + 22 + 33 = 78 > 66$; $\sigma_0(70) = 1 + 2 + 5 + 10 + 14 + 35 = 74 > 70$; $\sigma_0(72) = 1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 18 + 24 + 36 = 123 > 72$; $\sigma_0(78) = 1 + 2 + 3 + 6 + 13 + 26 + 39 = 90 > 78$; $\sigma_0(80) = 1 + 2 + 4 + 5 + 8 + 10 + 16 + 20 + 40 = 106 > 80$; $\sigma_0(84) = 1 + 2 + 3 + 4 + 6 + 7 + 12 + 14 + 21 + 28 + 42 = 140 > 84$; $\sigma_0(88) = 1 + 2 + 4 + 8 + 11 + 22 + 44 = 92 > 88$; $\sigma_0(90) = 1 + 2 + 3 + 5 + 6 + 9 + 10 + 15 + 18 + 30 + 45 = 144 > 90$; $\sigma_0(96) = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 16 + 24 + 32 + 48 = 156 > 96$
3. **Verificare che 945 è un numero abbondante. In effetti è il più piccolo fra i dispari.**
   $\sigma_0(945) = 1 + 3 + 5 + 7 + 9 + 15 + 21 + 27 + 35 + 45 + 63 + 105 + 135 + 189 + 315 = 975 > 945$
4. **Provare che i numeri perfetti pari possono esprimersi nel modo seguente:** $\frac{M(p)+1}{2} \cdot M(p)$**, dove *M*(*p*) indica il numero di Mersenne di esponente *p*.**
   Dato che ogni numero perfetto pari è della forma $n = 2^{p-1} \cdot (2^p - 1)$, con $(2^p - 1)$ numero primo, e che $M_p = 2^p - 1$, abbiamo:
   $$2^{p-1} \cdot \left(2^p - 1\right) = \frac{2^p \cdot M(p)}{2} = \frac{\left(2^p - 1\right)+1}{2} \cdot M(p) = \frac{M(p)+1}{2} \cdot M(p)$$
5. **Utilizzando un CAS e mediante il teorema 27, trovare la coppia 9363584 e 9437056 di numeri amici, Per quale valore di *n* si trova?**
   Si ha $p_6 = 3 \cdot 2^6 - 1 = 191$, $p_7 = 3 \cdot 2^7 - 1 = 383$ e $q_7 = 9 \cdot 2^{13} - 1 = 73727$, sono tutti e tre primi. Quindi $2^7 \cdot p_6 \cdot p_7 = 9363584$ e $2^7 \cdot q_7 = 9437056$ sono amici.
6. **Verificare che le seguenti sono coppie di numeri amici, e che non si trovano con la formula di Thabit ben Korrah. a) (2620; 2924), b) (5020; 5564), c) (6232; 6368).**
   a) Si ha: $\sigma_0(2620) = 1 + 2 + 4 + 5 + 10 + 20 + 131 + 262 + 524 + 655 + 1310 = 2924$ e $\sigma_0(2924) = 1 + 2 + 4 + 17 + 34 + 43 + 68 + 86 + 172 + 731 + 1462 = 2620$;
   b) $\sigma_0(5020) = 1 + 2 + 4 + 5 + 10 + 20 + 251 + 502 + 1004 + 1255 + 2510 = 5564$ e $\sigma_0(5564) = 1 + 2 + 4 + 13 + 26 + 52 + 107 + 214 + 428 + 1391 + 2782 = 5020$;
   c) $\sigma_0(6232) = 1 + 2 + 4 + 8 + 19 + 38 + 41 + 76 + 82 + 152 + 164 + 328 + 779 + 1558 + 3116 = 6368$ e $\sigma_0(6368) = 1 + 2 + 4 + 8 + 16 + 32 + 199 + 398 + 796 + 1592 + 3184 = 6232$.
7. **Provare che ogni numero perfetto $n = 2^{p-1} \cdot (2^p - 1)$, con $p > 2$, è somma dei cubi dei primi $2^{(p-1)/2}$ numeri dispari, per esempio $28 = 2^2 \cdot (2^3 - 1) = 1^3 + 3^3$.**
   Sappiamo che $\sum_{k=1}^{n} k^3 = \left[\frac{n \cdot (n+1)}{2}\right]^2$ quindi

$$1^3+3^3+\ldots+(2n-1)^3=\sum_{k=1}^{2n}k^3-\sum_{k=1}^{n}(2k)^3=\left[\frac{n\cdot(n+1)}{2}\right]^2-8\cdot\sum_{k=1}^{n}k^3=$$

$$=\left[\frac{2n\cdot(2n+1)}{2}\right]^2-8\cdot\left[\frac{n\cdot(n+1)}{2}\right]^2=n^2\cdot(2n+1)^2-2n^2\cdot(n+1)^2=$$

$$=n^2\cdot(4n^2+4n+1-2n^2-4n-2)=n^2\cdot(2n^2-1)$$

Quindi: $1^3+3^3+\ldots+\left(2\cdot2^{\frac{p-1}{2}}-1\right)^3=\left(2^{\frac{p-1}{2}}\right)^3\cdot\left[2\cdot\left(2^{\frac{p-1}{2}}\right)^3-1\right]=2^{p-1}\cdot(2^p-1)$

8. **Il numero 120 si dice molteplicemente perfetto perché la somma dei suoi divisori, esso compreso, è multipla di 120 (1 + 2 + … + 120 = 3 · 120). Trovare tutti i numeri molteplicemente perfetti minori di 1000.**
   Usando un CAS troviamo $\sigma(120) = 1 + 2 + 3 + 4 + 5 + 6 + 8 + 10 + 12 + 15 + 20 + 24 + 30 + 40 + 60 + 120 = 3 \cdot 120$; $\sigma_0(672) = 1 + 2 + 3 + 4 + 6 + 7 + 8 + 12 + 14 + 16 + 21 + 24 + 28 + 32 + 42 + 48 + 56 + 84 + 96 + 112 + 168 + 224 + 336 + 672 = 3 \cdot 672$.
9. **Il numero 12 ha la proprietà che il prodotto dei suoi divisori propri è uguale al suo quadrato, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 = 144 = 12^2$. Trovare tutti i numeri minori di 50 che verificano questa proprietà.**
   12; $1 \cdot 2 \cdot 3 \cdot 6 \cdot 9 = 324 = 18^2$; $1 \cdot 2 \cdot 4 \cdot 5 \cdot 10 = 400 = 20^2$; $1 \cdot 2 \cdot 4 \cdot 7 \cdot 14 = 784 = 28^2$; $1 \cdot 2 \cdot 4 \cdot 8 \cdot 16 = 1024 = 32^2$; $1 \cdot 2 \cdot 4 \cdot 11 \cdot 22 = 1936 = 44^2$; $1 \cdot 3 \cdot 5 \cdot 9 \cdot 15 = 2025 = 45^2$.

§12.

1. **Se il 55% degli agnelli nati in un gregge sono maschi ed il 90% sopravvive il primo anno, qual è il minimo numero di agnelli maschi nati affinché alla fine del primo anno ve ne siano 100 vivi?**
   Siano x gli agnelli nati, $0{,}55x$ sono maschi, di cui ne sopravvivono $0{,}55 \cdot 0.9\ x = 0{,}495x$. Deve essere $0{,}495x = 100 \Rightarrow x = 100/0{,}495 > 202$, quindi almeno 203.
2. **Da un manoscritto arabo del 1200: Un'oca costa 5 dracme, una gallina 1 dracma e 20 pulcini 1 dracma. Avendo 100 dracme e volendo comprare 100 animali, quanti dovrai prenderne di ciascun tipo?**
   Indichiamo con x le oche, con g le galline e con p i pulcini. Si deve avere: $\begin{cases} x+g+p=100 \\ 5x+g+p/20=100 \end{cases}$, sottraiamo termine a termine ottenendo: $19p/20 - 4x = 0$ $\Rightarrow p = 80x/19$. Dato che p deve essere intero x deve essere multiplo di 19. Il minimo valore è appunto $x = 19$, in questo modo avremo: 19 oche, 1 gallina e 80 pulcini. Se consideriamo il successivo multiplo di 19, $x= 38$ avremo $p = 160 > 100$ che ovviamente non è accettabile.
3. **Da un manuale tedesco del 1526: In una taverna, 20 persone pagano un conto di 20 dobloni. Vi sono uomini, donne e bambini. Sapendo che gli uomini pagano 3 dobloni, le donne 2 ed i bambini ½ doblone, determinare quanti erano gli uomini, quante le donne e quanti i bambini.**
   Abbiamo: $\begin{cases} u+d+b=20 \\ 3u+2d+b/2=20 \end{cases} \Rightarrow \begin{cases} u+d+b=20 \\ 6u+4d+b=40 \end{cases}$, sottraendo termine a termine: $5u + 3d = 20 \Rightarrow 5u = 20 - 3d \Rightarrow u = 4 - 3/5d$, quindi le donne devono essere multiple di 5. Una soluzione è $u = 1$, $d = 5$, $b = 14$. La successiva, $d = 10$ non va

bene perché $u < 0$. Lo stesso per qualsiasi altro multiplo di 5.

4. **Dal *Lilavati* di Bhaskara: O matematico, rispondi rapidamente. Qual è il minimo numero naturale che moltiplicato per 221 ed aumentato di 65 diviene un multiplo di 195?**

   Deve essere $221n + 65 = 195m \Rightarrow m = \frac{221n+65}{195} = n + \frac{26n+65}{3\cdot 5\cdot 13} = n + \frac{2n+5}{3\cdot 5}$, si vede facilmente che per $n = 5$ la frazione sparisce.

5. **Un anno fa Alex aveva un età il cui valore numerico era reversale (per esempio 27 e 72) di quella di sua madre Xela. Quest'anno invece la sua età è reversale di quella di suo padre Eric. Se la somma delle età dei suoi genitori, oggi, è di 93, determinare l'età attuale di Alex.**

   L'anno scorso Alex aveva xy anni, ossia 10x + y e sua madre 10y + x. Quest'anno ha 10x + y + 1 e suo padre ne ha 10(y +1) + x. Si ha 10y + x + 1 + 10y + 10 + x = 93 $\Rightarrow$ 20y + 2x + 11 = 93 $\Rightarrow$ 10y + x = 41 $\Rightarrow$ y = 4, x = 1. Quindi l'anno scorso Alex aveva 14 anni e quest'anno ne ha 15

6. **Un teatro ha 100 posti. Il proprietario vuole incassare 100 euro facendo pagare 5 euro il prezzo intero, 2 euro il ridotto militari e per ogni 10 ragazzi al di sotto dei 12 anni farà pagare 1 euro. Quanti adulti, militari e ragazzi devono entrare?**

   $\begin{cases} i+m+r=100 \\ 5i+2m+r/10=100 \end{cases} \Rightarrow \begin{cases} i+m+r=100 \\ 50i+20m+r=1000 \end{cases} \Rightarrow 49i + 19m = 900 \Rightarrow$

   $m = \frac{900-49i}{19} = 47 - 2i + \frac{7-11i}{19}$, $7 - 11i$ deve essere multiplo di 19, il più piccolo valore è $i = -6$, per cui si ha $m = 19$ e $r = 70$

7. **Dall'Algebra di Eulero. Dividi 100 in due addendi, uno divisibile per 7 e l'altro per 11.**

   Deve aversi $7x + 11y = 100 \Rightarrow x = \frac{100-11y}{7} = 13 - y + \frac{9-4y}{7}$, $9 - 4y$ deve essere un multiplo negativo di 7, il minimo valore è $-7 \Rightarrow y = 4$, $x = 8$, quindi 100 = 44 + 56.

8. **Da Mahaviracarya. Furono raccolte delle mele, che furono sistemate in 37 cassette, ciascuna contenente lo stesso numero di frutti. Ogni cassetta conteneva più di 100 e meno di 200 mele. Sapendo che i raccoglitori erano 79 e che quando si divisero le mele in parti uguali ne avanzarono 17, si vuol sapere quante mele ebbe ciascun raccoglitore e quante ne conteneva ciascuna cassetta.**

   $\begin{cases} 100 < x < 200 \\ 37x = 79y + 17 \end{cases} \Rightarrow \begin{cases} 100 < x < 200 \\ x = \frac{79y+17}{37} \end{cases} \Rightarrow \begin{cases} 100 < x < 200 \\ x = 2y + \frac{5y+17}{37} \end{cases} \Rightarrow 100 < \frac{79y+17}{37} < 200 \Rightarrow 46 < y < 94$

   $5y + 17$ deve essere multiplo di 37, per i valori consentiti ciò succede solo per $y = 78$, per cui si ha: $x = 167$

9. **Risolvere le seguenti equazioni diofantee, determinando la minima soluzione positiva, se esiste. a) $37x - 41y = 11$; b) $23x + 15y = 24$; c) $123x + 35y = 15$; d) $43x - 71y = 2$; e) $132x + 61y = -4$.**

   a) $x = \frac{41y+11}{37} = y + \frac{4y+11}{37}$, il primo valore positivo di y che rende x intero positivo è $y = 25$, con $x = 28$;

   b) Non ha soluzioni positive perché per $y = x = 1$, il membro sinistro vale 38 > 24.

c) Come la precedente, per $y = x = 1$, il membro sinistro vale 158 > 15;

d) $x = \dfrac{71y+2}{43} = y + \dfrac{28y+2}{43}$, il primo valore positivo di y che rende x intero positivo è $y = 3$, con $x = 5$;

e) La somma di numeri positivi non può dare numeri negativi.

10. Un quesito da Stanford 1957. Bob tiene i suoi francobolli in tre album. Due decimi sono nel primo album, alcuni settimi nel secondo e 303 nel terzo. Quanti francobolli ha Bob?

I francobolli sono $x/5 + yx/7 + 303 = x \Rightarrow 7x + 5xy + 10605 = 35x \Rightarrow (7 + 5y - 35)x + 10605 = 0 \Rightarrow x = \dfrac{10605}{28-5y} = \dfrac{3\cdot 5\cdot 7\cdot 101}{28-5y}$. Il denominatore deve essere positivo e quindi $1 \le y \le 5$, ma deve anche essere dispari dato che deve essere un divisore del numeratore che contiene solo fattori dispari. Quindi abbiamo solo tre possibilità, l'unica che funziona è $y = 5$ che fornisce $x = 3535$

§13.

1. **Provare che la relazione di congruenza è una relazione di equivalenza.**

Ovviamente $a \overset{n}{\equiv} a$, inoltre $a \overset{n}{\equiv} b \Rightarrow a - b = kn \Rightarrow b - a = -kn \Rightarrow b \overset{n}{\equiv} a$, per la proprietà transitiva: $a \overset{n}{\equiv} b \Leftrightarrow a - b = kn \;\; b \overset{n}{\equiv} c \Leftrightarrow b - c = hn$. Ora: $a - c = (a - b) - (b - c) = kn - hn = (k - h)n \Leftrightarrow a \overset{n}{\equiv} c$

2. **Risolvere le seguenti equazioni: a)** $2^{27} \overset{23}{\equiv} n$ **; b)** $3^{41} \overset{37}{\equiv} n$ **; c)** $11^{125} \overset{41}{\equiv} n$ **; d)** $5^{217} \overset{13}{\equiv} n$ **; e)** $7^{276} \overset{29}{\equiv} n$ **.**

a) $2^4 \overset{23}{\equiv} 16 \overset{23}{\equiv} -7 \Rightarrow 2^8 \overset{23}{\equiv} 49 \overset{23}{\equiv} 3 \Rightarrow 2^{16} \overset{23}{\equiv} 9; 2^{11} \overset{23}{\equiv} 24 \overset{23}{\equiv} 1 \Rightarrow 2^{27} \overset{23}{\equiv} 9$;

b) $3^2 \overset{37}{\equiv} 9 \Rightarrow 3^4 \overset{37}{\equiv} 81 \overset{37}{\equiv} 7 \Rightarrow 3^5 \overset{37}{\equiv} 21 \overset{37}{\equiv} -16; 3^{10} \overset{37}{\equiv} 256 \overset{37}{\equiv} -3 \Rightarrow 3^{20} \overset{37}{\equiv} 9 \Rightarrow 3^{40} \overset{37}{\equiv} 7 \Rightarrow 3^{41} \overset{37}{\equiv} 21$;

c) $11^2 \overset{41}{\equiv} 39 \overset{41}{\equiv} -2 \Rightarrow 11^4 \overset{41}{\equiv} 4 \Rightarrow 11^5 \overset{41}{\equiv} 44 \overset{41}{\equiv} 3 \Rightarrow 11^{25} \overset{41}{\equiv} 243 \overset{41}{\equiv} -3 \Rightarrow 11^{125} \overset{41}{\equiv} -243 \overset{41}{\equiv} 3$;

d) $5^2 \overset{13}{\equiv} 25 \overset{13}{\equiv} 12 \Rightarrow 5^4 \overset{13}{\equiv} 144 \overset{13}{\equiv} 1 \Rightarrow \left(5^{2^n} \overset{13}{\equiv} 1\right) \Rightarrow 5^{128} \overset{13}{\equiv} 1; 5^{80} \overset{13}{\equiv} 1 \Rightarrow 5^9 \overset{13}{\equiv} 5 \Rightarrow 5^{89} \overset{13}{\equiv} 5 \Rightarrow 5^{217} \overset{13}{\equiv} 5$;

e) $7^2 \overset{29}{\equiv} 20 \Rightarrow 7^4 \overset{29}{\equiv} -6 \Rightarrow 7^8 \overset{29}{\equiv} 7 \Rightarrow 7^{256} \overset{29}{\equiv} -6; 7^{20} \overset{29}{\equiv} -120 \overset{29}{\equiv} -4 \Rightarrow 7^{276} \overset{29}{\equiv} 24 \overset{29}{\equiv} -5$

3. **Risolvere le seguenti congruenze: a)** $x^2 \overset{13}{\equiv} 1$ **; b)** $x^2 - x + 2 \overset{7}{\equiv} -1$ **; c)** $2x^2 - x + 1 \overset{5}{\equiv} 0$ **; d)** $x^3 - x - 2 \overset{12}{\equiv} 4$ **.**

a) Consideriamo i possibili resti nella divisione per 13: 0, 1, 2, …12. Dei loro quadrati abbiamo facilmente le soluzioni $x = 1$, $x = 12 = -1$;

b) Otteniamo: $0^2 - 0 + 2 = 2$; $1^2 - 1 + 2 = 2$; $2^2 - 2 + 2 = 4$; $3^2 - 3 + 2 = 8 \overset{7}{\equiv} 1$; $4^2 - 4 + 2 = 14 \overset{7}{\equiv} 0$; $5^2 - 5 + 2 = 22 \overset{7}{\equiv} 1$; $6^2 - 6 + 2 = 32 \overset{7}{\equiv} -3$. Pertanto l'equazione non ha soluzioni.

c) $2 \cdot 0^2 - 0 + 1 = 1$; $2 \cdot 1^2 - 1 + 1 = 2$; $2 \cdot 2^2 - 2 + 1 = 7 \overset{5}{\equiv} 2$; $2 \cdot 3^2 - 3 + 1 = 16 \overset{5}{\equiv} 1$; $2 \cdot 4^2 - 4 + 1 = 29 \overset{5}{\equiv} 4$. Pertanto l'equazione non ha soluzioni.

d) $0^3 - 0 - 2 = -2$; $1^3 - 1 - 2 = -2$; $2^3 - 2 - 2 = 4$; $3^3 - 3 - 2 = 22 \overset{12}{\equiv} -2$; $4^3 - 4 - 2 \overset{12}{\equiv} -2$; $5^3 - 5 - 2 \overset{12}{\equiv} -2$; $6^3 - 6 - 2 \overset{12}{\equiv} 4$; $7^3 - 7 - 2 \overset{12}{\equiv} -2$; $8^3 - 8 - 2 \overset{12}{\equiv} -2$; $9^3 - 9 - 2 \overset{12}{\equiv} -2$; $10^3 - 10 - 2 \overset{12}{\equiv} 4$; $11^3 - 11 - 2 \overset{12}{\equiv} -2$. Soluzioni: $x = \pm 2, 6$.

4. **Trovare gli inversi aritmetici di 15 moduli a) 7; b) 10; c) 11.**

a) $\bar{x}\cdot 15 \overset{7}{\equiv} 1 \Rightarrow 1\cdot 15 \overset{7}{\equiv} 1$; b) $(2n)\cdot 15 \overset{10}{\equiv} 0, (2n+1)\cdot 15 \overset{10}{\equiv} 5$, quindi non esiste l'inverso aritmetico di 15 modulo 10; c) $\bar{x}\cdot 15 \overset{11}{\equiv} 1 \Rightarrow 3\cdot 15 \overset{11}{\equiv} 1$

5. **Risolvere le congruenze lineari:**

a) $3x \overset{11}{\equiv} 7$ **; b)** $13x \overset{123}{\equiv} 17$ **; c)** $144x \overset{36}{\equiv} 60$ **; d)** $1234x \overset{12}{\equiv} 5678$.

a) MCD(3, 11) = 1 che divide 7, quindi vi è una soluzione. Si ha: $3x - 11y = 7 \Rightarrow x = \dfrac{11y+7}{3} = 4y + 2 - \dfrac{y-1}{3}$, cioè $y \overset{3}{\equiv} 1$ e quindi $x = 4(3t + 1) + 2 + t = 13t + 6$. La minima soluzione è perciò 6, le altre sono $x \overset{13}{\equiv} 6$.

b) MCD(13, 123) = 1 che divide 17, quindi vi è una soluzione. Si ha: $13x - 123y = 17 \Rightarrow x = \dfrac{123y+17}{13} = 9y + 1 + \dfrac{6y+4}{13}$, cioè $6y \overset{13}{\equiv} -4 \Rightarrow y = 8$ e quindi $x = 73 + 4 = 77$.

c) MCD(144, 36) = 36 che non divide 60, quindi non vi sono soluzioni.

d) MCD(1234, 12) = 2 che divide 5678, quindi vi sono 2 soluzioni. $1234x \overset{12}{\equiv} 5678 \Rightarrow (12\cdot 102 + 10)x \overset{12}{\equiv} (12\cdot 473 + 2) \Rightarrow 10x \overset{12}{\equiv} 2 \Rightarrow -10 \overset{12}{\equiv} 2 \vee 10\cdot 5 \overset{12}{\equiv} 2$

$1234\cdot(-1) \overset{12}{\equiv} 5678, 1234\cdot 5 \overset{12}{\equiv} 5678$

6. **Risolvere il problema delle uova con la modifica seguente: raggruppando le uova a *n* a *n* (2 ≤ *n* ≤ 5) ne rimangono *n* – 1, mentre a 7 a 7 non vi sono rimanenze. Suggerimento: cercare di scrivere le congruenze in modo da potere applicare il Teorema 35.**

Dobbiamo risolvere il sistema di 6 congruenze lineari

$$\begin{cases} x \overset{2}{\equiv} 1 \\ x \overset{3}{\equiv} 2 \\ x \overset{4}{\equiv} 3 \\ x \overset{5}{\equiv} 4 \\ x \overset{6}{\equiv} 5 \\ x \overset{7}{\equiv} 0 \end{cases} \Rightarrow \begin{cases} x \overset{2}{\equiv} -1 \\ x \overset{3}{\equiv} -1 \\ x \overset{4}{\equiv} -1 \\ x \overset{5}{\equiv} -1 \\ x \overset{6}{\equiv} -1 \\ x \overset{7}{\equiv} 0 \end{cases} \Rightarrow \begin{cases} x \overset{mcm(2,3,4,5,6)}{\equiv} -1 \\ x \overset{7}{\equiv} 0 \end{cases} \Rightarrow \begin{cases} x \overset{60}{\equiv} -1 \\ x \overset{7}{\equiv} 0 \end{cases} \Rightarrow x = 60t - 1 \overset{7}{\equiv} 0 \Rightarrow \quad .$$

$$\Rightarrow 60t \overset{7}{\equiv} 1 \Rightarrow 4t \overset{7}{\equiv} 1 \Rightarrow 20t \overset{7}{\equiv} 5 \Rightarrow -t \overset{7}{\equiv} -2 \Rightarrow t \overset{7}{\equiv} 2 \Rightarrow t = 7h + 2 \Rightarrow x = 420h + 119$$

Le uova minimo erano 119

7. **Un quesito da Stanford 1949. Provare che nessun numero della successione {11, 11, 1111, …} è un quadrato perfetto.**

$11 + 100n = 4(25n + 2) + 3 \Rightarrow 11 + 100n \overset{4}{\equiv} 3$, ogni quadrato è della forma $(2n)^2 = 4n^2 \overset{4}{\equiv} 0$ o $(2n + 1)^2 = 4n^2 + 4n + 1 \overset{4}{\equiv} 1$

8. **Un problema di Regiomontano. Risolvere** $\begin{cases} x \overset{10}{\equiv} 3 \\ x \overset{13}{\equiv} 11 \\ x \overset{17}{\equiv} 15 \end{cases}$**.**

$$\begin{cases} x \overset{10}{\equiv} 3 \\ x \overset{13}{\equiv} -2 \\ x \overset{17}{\equiv} -2 \end{cases} \Rightarrow \begin{cases} x \overset{10}{\equiv} 3 \\ x \overset{221}{\equiv} -2 \end{cases} \Rightarrow x = 221t - 2 \overset{10}{\equiv} 3 \Rightarrow 221t \overset{10}{\equiv} 5 \Rightarrow t \overset{10}{\equiv} 5 \Rightarrow t = 10h + 5 \Rightarrow x = 2210h + 1103 \Rightarrow x \overset{2210}{\equiv} 1103$$

9. **Un problema di Eulero. Risolvere** $\begin{cases} x \overset{11}{\equiv} 3 \\ x \overset{19}{\equiv} 5 \\ x \overset{29}{\equiv} 10 \end{cases}$ **.**

$$\begin{cases} x \overset{11}{\equiv} 3 \\ x \overset{19}{\equiv} 5 \\ x \overset{29}{\equiv} 10 \end{cases} \Rightarrow x = 29h + 10 \overset{19}{\equiv} 5 \Rightarrow 29h \overset{19}{\equiv} -5 \Rightarrow 10h \overset{19}{\equiv} -5 \Rightarrow 20h \overset{19}{\equiv} -10 \Rightarrow h \overset{19}{\equiv} -10 \Rightarrow h$$

$= 19t - 10 \Rightarrow x = 551t - 280 \overset{11}{\equiv} 3 \Rightarrow (50 \cdot 11 + 1)t \overset{11}{\equiv} (25 \cdot 11 + 8) \Rightarrow t \overset{11}{\equiv} 8 \Rightarrow t =$ $11n + 8 \Rightarrow x = 551(11n + 8) - 280 = 6061n + 4128 \Rightarrow x \overset{6061}{\equiv} -1993$

10. **Dal *Sun Tsu Suan Ching*. *Un numero minore di* 100 *è tale che se lo dividiamo per* 3 *il resto è* 2; *dividendolo per* 5 *il resto è* 3; *dividendolo per* 7 *il resto è* 2. *Qual è questo numero*?**

$$\begin{cases} x \overset{3}{\equiv} 2 \\ x \overset{5}{\equiv} 3 \\ x \overset{7}{\equiv} 2 \end{cases} \Rightarrow x = 7h + 2 \overset{5}{\equiv} 3 \Rightarrow 7h \overset{5}{\equiv} 1 \Rightarrow 21h \overset{5}{\equiv} 3 \Rightarrow h \overset{5}{\equiv} 3 \Rightarrow h = 5t + 3 \Rightarrow x = 35t +$$

$23 \overset{3}{\equiv} 2 \Rightarrow (12 \cdot 3 - 1)t \overset{3}{\equiv} -21 \Rightarrow t \overset{3}{\equiv} 0 \Rightarrow t = 3n \Rightarrow x = 105n + 23$. Quindi la minima soluzione positiva e minore di 100 è 23

11. **Usando le congruenze provare che $2^{32} + 1$ è divisibile per 641.**

$2^9 \overset{641}{\equiv} 512 \overset{641}{\equiv} -129 \Rightarrow 2^{18} \overset{641}{\equiv} 16641 \overset{641}{\equiv} -25$; $2^7 \overset{641}{\equiv} 128 \Rightarrow 2^{14} \overset{641}{\equiv} 16384 \overset{641}{\equiv} -282 \Rightarrow 2^{32}$ $\overset{641}{\equiv} 7050 \overset{641}{\equiv} -1$

12. **Provare che $x + y + z$ è multiplo di 6 solo se lo è $x^3 + y^3 + z^3$.**

Si ha:

$$x \overset{6}{\equiv} 1 \Leftrightarrow x^3 \overset{6}{\equiv} 1; x \overset{6}{\equiv} 2 \Leftrightarrow x^3 \overset{6}{\equiv} 2; x \overset{6}{\equiv} 3 \Leftrightarrow x^3 \overset{6}{\equiv} 3; x \overset{6}{\equiv} 4 \overset{6}{\equiv} -2 \Leftrightarrow x^3 \overset{6}{\equiv} -2; x \overset{6}{\equiv} 5 \overset{6}{\equiv} -1 \Leftrightarrow x^3 \overset{6}{\equiv} -1$$

Quindi ovviamente $x + y + z \overset{6}{\equiv} x^3 + y^3 + z^3$, perciò più in generale le due espressioni divise per 6 danno sempre lo stesso resto, in particolare se una è multipla di 6 lo è anche l'altra. Esempio: $7 + 11 + 12 = 30 = 6 \cdot 5$ e $7^3 + 11^3 + 12^3 = 3402 = 6 \cdot 567$. Anche $5 + 6 + 10 = 21 = 6 \cdot 3 + 3$ e $5^3 + 6^3 + 10^3 = 3402 = 6 \cdot 223 + 3$.

13. **Provare che $3^{2n+1} + 2^{n+2}$ è multiplo di 7, $\forall n \in \mathbb{N}$.**

Si ha: $3 \overset{7}{\equiv} 3 \Rightarrow 3^2 \overset{7}{\equiv} 2 \Rightarrow 3^{2n} \overset{7}{\equiv} 2^n \Rightarrow 3^{2n+1} \overset{7}{\equiv} 3 \cdot 2^n; 3^{2n+1} + 2^{n+2} \overset{7}{\equiv} 3 \cdot 2^n + 2^2 \cdot 2^n \overset{7}{\equiv} 7 \cdot 2^n \overset{7}{\equiv} 0$

§14.

1. **Provare che un criterio di divisibilità per *n* coinvolge un'espressione che ha al**

massimo (n – 1) termini.
Dobbiamo considerare le congruenze modulo da 0 a n – 1 finché non otteniamo un valore ripetuto, che capiterà certamente prima di n – 1.

2. **Determinare un criterio di divisibilità per 25.**
Basta osservare che ogni potenza di 25 finisce per 25
3. **Determinare un criterio di divisibilità per 5^n.**
Basta osservare che ogni potenza di 5^n finisce per 5^n
4. **Determinare un criterio di divisibilità per 13. Verificarlo sul numero 3195258885.**
Si ha: $10^0 \overset{13}{\equiv} 1 \Rightarrow 10 \overset{13}{\equiv} -3 \Rightarrow 10^2 \overset{13}{\equiv} -4 \Rightarrow 10^3 \overset{13}{\equiv} -1; 10^4 \overset{13}{\equiv} 3; 10^5 \overset{13}{\equiv} 4; 10^6 \overset{13}{\equiv} 1$, quindi la regola è $(a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5) + \ldots$ Verifichiamo: $(5 - 24 - 32 - 8 + 15 + 8) + (5 - 27 - 4 - 3) = -65 = -5 \cdot 13$
5. **Determinare un criterio di divisibilità per 17. Verificarlo con 421361401347108.**
$10^0 \overset{17}{\equiv} 1 \Rightarrow 10 \overset{17}{\equiv} -7 \Rightarrow 10^2 \overset{17}{\equiv} -2 \Rightarrow 10^3 \overset{17}{\equiv} -3; 10^4 \overset{17}{\equiv} 4; 10^5 \overset{17}{\equiv} 6; 10^6 \overset{17}{\equiv} -8; 10^7 \overset{17}{\equiv} 5; 10^8 \overset{17}{\equiv} -1;$
$10^9 \overset{17}{\equiv} 7 \Rightarrow 10^{10} \overset{17}{\equiv} 2 \Rightarrow 10^{11} \overset{17}{\equiv} 3 \Rightarrow 10^{12} \overset{17}{\equiv} -4; 10^{13} \overset{17}{\equiv} -6; 10^{14} \overset{17}{\equiv} 8; 10^{15} \overset{17}{\equiv} -5; 10^{16} \overset{17}{\equiv} 1$
Quindi: $(a_0 - 7a_1 - 2a_2 - 3a_3 + 4a_4 + 6a_5 - 8a_6 + 5a_7 - a_8 + 7a_9 + 2a_{10} + 3a_{11} - 4a_{12} - 6a_{13} + 8a_{14} - 5a_{15}) + \ldots$Verifichiamo: $8 - 0 - 2 - 21 + 16 + 18 - 8 + 0 - 4 + 7 + 12 + 9 - 4 - 12 + 32 = 51 = 3 \cdot 17$.
6. **Determinare un criterio di divisibilità per 27. Verificarlo sul numero 39363192.**
$10^0 \overset{27}{\equiv} 1 \Rightarrow 10 \overset{27}{\equiv} 10 \Rightarrow 10^2 \overset{27}{\equiv} -8 \Rightarrow 10^3 \overset{27}{\equiv} 1$ La regola è $(a_0 + 10a_1 - 8a_2) + (a_3 + 10a_4 - 8a_5) + \ldots$ divisibile per 27. Verifichiamo: $2 + 90 - 8 + 3 + 60 - 24 + 9 + 30 = 162 = 2 + 60 - 8 = 54 = 2 \cdot 27$
7. **Per numeri "grandi" conviene considerare prove con numeri superiori a 9, per esempio 99. Determinare una prova del 99 e verificarla per stabilire se può essere corretta la moltiplicazione 245678 · 1357931 = 333613772218.**
$10^0 \overset{99}{\equiv} 1 \Rightarrow 10 \overset{99}{\equiv} 10 \Rightarrow 10^2 \overset{99}{\equiv} 1$, quindi $(a_0 + 10a_1) + (a_2 + 10a_3) + \ldots$ deve essere divisibile per 99. Ora $245678 \rightarrow 8 + 70 + 6 + 50 + 4 + 20 = 158 \rightarrow 8 + 50 + 1 = 59$; $1357931 \rightarrow 1 + 30 + 9 + 70 + 5 + 30 + 1 = 146 \rightarrow 47$. Moltiplichiamo: $59 \cdot 47 = 2773 \rightarrow 3 + 70 + 7 + 20 = 100 \rightarrow 1$. Mentre $333613772218 \rightarrow 8 + 10 + 2 + 20 + 7 + 70 + 3 + 10 + 6 + 30 + 3 + 30 = 199 \rightarrow 1$. La moltiplicazione può essere corretta e in effetti lo è.
8. **Determinare i valori dell'incognita x in modo che siano veri gli enunciati seguenti: a) 123x456 è divisibile per 3; b) 23456x78 è divisibile per 8; c) 81y1058294x è divisibile per 33.**
a) Eliminiamo tutte le cifre che sommano un multiplo di 3, ottenendo x, che deve essere multiplo di 3, quindi $x \in \{0, 3, 6, 9\}$; b) $x78$ deve essere multiplo di 8, ma nessun numero da 78 a 978 lo è, quindi nessun valore; c) Deve essere multiplo di 3, quindi: $x + y + 2 \overset{3}{\equiv} 0$ e multiplo di 11 $\Rightarrow 8 - 1 + y - 1 + 0 - 5 + 8 - 2 + 9 - 4 + x \overset{11}{\equiv} 0$
$$\Rightarrow \begin{cases} x + y \overset{3}{\equiv} -2 \\ x + y \overset{11}{\equiv} -1 \end{cases} \Rightarrow \begin{cases} x + y \in \{1, 4, 7, 10, 13, 16\} \\ x + y = 10 \end{cases} \Rightarrow x + y = 10$$
9. **Enunciare una prova del 9 per le altre operazioni aritmetiche elementari.**
Valgono regole identiche. Per esempio 147 + 231 = 378, si ha: $1 + 4 + 7 = 12 \overset{9}{\equiv} 3$;

$2 + 3 + 1 = 6 \overset{9}{\equiv} 6$ e $3 + 7 + 8 = 18 \overset{9}{\equiv} 0$, Ed effettivamente $6 + 3 \overset{9}{\equiv} 0$.
La divisione la possiamo sempre considerare come una moltiplicazione.

10. **Provare che se alla somma delle cifre di un numero, applichiamo la procedura della prova del 9, e non otteniamo uno dei numeri dell'insieme {0, 1, 4, 7}, il numero non è un quadrato. Esempio 123456 → 21 → 3.**

    Ogni numero naturale si può scrivere nella forma $n = 9a \pm b$, $0 \le b \le 4$. Si ha: $n \overset{9}{\equiv} b$ quindi $n^2 \overset{9}{\equiv} b^2 \in \{0, 1, 4, 9, 16\} \overset{9}{\equiv} \{0, 1, 4, 7\}$

11. **Un quesito di Stanford 1947. Fra le carte del nonno ne è stata trovata una con la scritta 72 tacchini $ _67.9_, in cui la prima e l'ultima cifra del prezzo sono incomprensibili. Qual era il prezzo di un tacchino?**

    Dobbiamo avere $x679y$ multiplo di 72, ossia di 8 e di 9. Quindi $x + 6 + 7 + 9 + y \overset{9}{\equiv} 0$ $\Rightarrow x + y \overset{9}{\equiv} 5$ e $79y$ multiplo di 8, che succede solo per $y = 2$. Perciò $x + 2 \overset{9}{\equiv} 5 \Rightarrow x \overset{9}{\equiv} 3 \Rightarrow x = 3$. Perciò il totale era $ 367.92 che diviso 72 è $ 5.11

§15.

1. **Verificare il teorema di Fermat per tutti i numeri primi minori di 24.**

p	n	$n^{p-1} - 1$
2	$2h + 1$	$(2h + 1)^{2-1} - 1 = 2h$
3	$3h \pm 1$	$(3h \pm 1)^{3-1} - 1 = 9h^2 \pm 6h$
5	$5h \pm 1, 5h \pm 2$	$(5h \pm 1)^{5-1} - 1 \overset{5}{\equiv} 0$; $(5h \pm 2)^{5-1} - 1 \overset{5}{\equiv} 15 \overset{5}{\equiv} 0$
7	$7h \pm k, 1 \le k \le 3$	$(7h \pm 1)^6 - 1 \overset{7}{\equiv} 0$; $(7h \pm 2)^6 - 1 \overset{7}{\equiv} 0$; $(7h \pm 3)^6 - 1 \overset{7}{\equiv} 728 \overset{7}{\equiv} 0$
11	$11h \pm k, 1 \le k \le 5$	$(11h \pm k)^{10} - 1 \overset{11}{\equiv} k^{10} - 1 \overset{11}{\equiv} 0$
13	$13h \pm k, 1 \le k \le 6$	$(13h \pm k)^{12} - 1 \overset{13}{\equiv} k^{12} - 1 \overset{13}{\equiv} 0$
17	$17h \pm k, 1 \le k \le 9$	$(17h \pm k)^{16} - 1 \overset{17}{\equiv} k^{16} - 1 \overset{17}{\equiv} 0$
19	$19h \pm k, 1 \le k \le 10$	$(19h \pm k)^{18} - 1 \overset{19}{\equiv} k^{18} - 1 \overset{19}{\equiv} 0$
23	$23h \pm k, 1 \le k \le 12$	$(23h \pm k)^{22} - 1 \overset{23}{\equiv} k^{22} - 1 \overset{23}{\equiv} 0$

2. **Verificare che si ha a)** $2^{341} - 2 \overset{341}{\equiv} 0$ **; b)** $3^{91} - 3 \overset{91}{\equiv} 0$ **; c)** $8^9 - 8 \overset{9}{\equiv} 0$ **.**
   a) $2^{10} \overset{341}{\equiv} 1 \Rightarrow 2^{340} \overset{341}{\equiv} 1 \Rightarrow 2^{341} \overset{341}{\equiv} 2$; b) $3^4 \overset{91}{\equiv} -10; 3^6 \overset{91}{\equiv} -90 \equiv 1; 3^7 \overset{91}{\equiv} 3; 3^{13} \overset{91}{\equiv} 3; \Rightarrow 3^{91} \overset{91}{\equiv} 3^{13} \overset{91}{\equiv} 3$;
   c) $8 \overset{9}{\equiv} -1 \Rightarrow 8^8 \overset{9}{\equiv} 1 \Rightarrow 8^9 \overset{9}{\equiv} 8$.

3. **Osserviamo che $9 = 3 \cdot 3$; $99 = 9 \cdot 11$; $999 = 3^3 \cdot 37$; $999 = 99 \cdot 101$. Provare che ogni numero primo diverso da 2 e da 5, è divisore di un numero del tipo 999…9.**
   Per il teorema di Fermat, per p primo coprimo con 10, si ha $10^{p-1} \overset{p}{\equiv} 1 \Rightarrow 10^{p-1} - 1 = h \cdot p \Rightarrow \underbrace{999...9}_{p-1} = h \cdot p$

4. **Il teorema inverso del Teorema 38 afferma: se esiste un numero n coprimo con p per cui si ha** $n^{p-1} - n \overset{p}{\equiv} 0$ **ma** $n^h - n \overset{p}{\not\equiv} 0, \forall h \in \mathbb{N} : 1 < h < p$ **allora p è un numero primo. Verificare che $3^m - 3$ non è divisibile per 17 per ogni m: $1 < m < 17$. Verificare altresì che ciò non vale per $2^m - 2$.**

$3^2 \overset{17}{\equiv} -8; 3^3 \overset{17}{\equiv} -7; 3^4 \overset{17}{\equiv} -4; 3^5 \overset{17}{\equiv} 5; 3^6 \overset{17}{\equiv} -2; 3^7 \overset{17}{\equiv} -6; 3^8 \overset{17}{\equiv} -1;$

$3^9 \overset{17}{\equiv} -3; 3^{10} \overset{17}{\equiv} 8; 3^{11} \overset{17}{\equiv} 7; 3^{12} \overset{17}{\equiv} 4; 3^{13} \overset{17}{\equiv} -5; 3^{14} \overset{17}{\equiv} 2; 3^{15} \overset{17}{\equiv} 6; 3^{16} \overset{17}{\equiv} 1$, quindi 17 è primo.

La proprietà non deve valere per tutti i numeri coprimi con 17, ma ne basta solo 1, del resto si ha: $2^9 - 2 = 17 \cdot 30$.

5. **Verificare il teorema di Eulero per n = 12, 15, 18, 20 e tutti i numeri minori di essi con cui sono coprimi.**

n	m	$\phi(m)$	$n^{\phi(m)} - 1$
12	5	4	$12^4 \overset{5}{\equiv} 2^4 \overset{5}{\equiv} 1$
12	7	6	$12^6 \overset{7}{\equiv} (-1)^6 \overset{7}{\equiv} 1$
12	11	10	$12^{10} \overset{11}{\equiv} 1^{10} \overset{11}{\equiv} 1$
15	2	1	$15^1 \overset{2}{\equiv} 1$
15	4	2	$15^2 \overset{4}{\equiv} (-1)^2 = 1$
15	7	6	$15^6 \overset{7}{\equiv} 1^6 = 1$
15	8	4	$15^4 \overset{8}{\equiv} (-1)^4 = 1$
15	11	10	$15^{10} \overset{11}{\equiv} (4^2)^5 = (16^2)^2 \cdot 16 \overset{11}{\equiv} 3^2 \cdot 5 \overset{11}{\equiv} 45 \overset{11}{\equiv} 1$
15	13	12	$15^{12} \overset{13}{\equiv} (2^6)^2 = (64)^2 \overset{13}{\equiv} (-1)^2 = 1$
15	14	6	$15^6 \overset{14}{\equiv} 1^6 = 1$
18	5	4	$18^4 \overset{5}{\equiv} 3^4 \overset{5}{\equiv} 1$
18	7	6	$18^6 \overset{7}{\equiv} (-4)^6 = (4^2)^3 \overset{7}{\equiv} 2^3 \overset{7}{\equiv} 1$
18	11	10	$18^{10} \overset{11}{\equiv} (-4)^{10} = (4^2)^5 \overset{11}{\equiv} 5^5 = 5^4 \cdot 5 \overset{11}{\equiv} (-2) \cdot 5 \overset{11}{\equiv} 1$
18	13	12	$18^{12} \overset{13}{\equiv} 5^{12} = (5^2)^6 \overset{13}{\equiv} (-1)^6 = 1$
18	17	16	$18^{16} \overset{17}{\equiv} 1^{16} = 1$
20	3	2	$20^2 \overset{3}{\equiv} (-1)^2 = 1$
20	7	6	$20^6 \overset{7}{\equiv} (-1)^6 = 1$
20	9	6	$20^6 \overset{9}{\equiv} 2^6 = 64 \overset{9}{\equiv} 1$
20	11	10	$20^{10} \overset{11}{\equiv} (-2)^{10} = (-2^5)^2 \overset{11}{\equiv} (-1)^2 = 1$
20	13	12	$20^{12} \overset{13}{\equiv} (-6)^{12} = (6^2)^6 \overset{13}{\equiv} (-3)^6 = (3^3)^2 \overset{13}{\equiv} 1^2 = 1$
20	17	16	$20^{16} \overset{17}{\equiv} (3)^{16} = (3^4)^4 \overset{17}{\equiv} (-4)^4 = (4^2)^2 \overset{17}{\equiv} (-1)^2 = 1$
20	19	18	$20^{18} \overset{19}{\equiv} 1^{18} = 1$

6. **Esistono numeri n che per p numero primo, sono tali che ($n^p - n$) è divisibile anche per p^2. Verificare che questo succede per $3^{11} - 3$. Determinare il primo n per cui si ha: a) ($n^5 - n$) è divisibile per 25; b) ($n^3 - n$) è divisibile per 9; a) ($n^7 - n$) è divisibile per 49.**

$3^{11} = (3^2)^5 \cdot 3 \overset{9}{\equiv} 3$

a) $(n^5 - n) = n(n^4 - 1) = n(n - 1)(n + 1)(n^2 + 1)$, uno solo fra i primi 3 fattori può essere multiplo di 5, quindi deve esserlo anche $(n^2 + 1)$, il minimo valore si ha per $n = 2$, ma in questo caso nessuno dei precedenti è multiplo di 5. Lo stesso accade per $n = 3$. Dobbiamo arrivare a $n = 7$ per ottenere $7^2 + 1 = 50$.

b) $(n^3 - n) = n(n^2 - 1) = n(n - 1)(n + 1)$. Uno solo dei 3 fattori è multiplo di 3, quindi dobbiamo considerare il minimo n per cui uno dei fattori è 9, Si ha per $n = 8$.

c) $(n^7 - n) = n(n^6 - 1) = n(n - 1)(n + 1)(n^2 + n + 1)(n^2 - n + 1)$. Consideriamo il fatto che uno solo dei primi 3 fattori sia multiplo di 7. Se $n = 7h$, gli ultimi due fattori ovviamente non sono multipli di 7; se $n = 7h + 1 \Leftrightarrow n \overset{7}{\equiv} -1$, abbiamo $n^2 + n + 1 \overset{7}{\equiv} 1 - 1 + 1 = 1$ e $n^2 - n + 1 \overset{7}{\equiv} 1 + 1 + 1 = 3$; se $n = 7h - 1 \Leftrightarrow n \overset{7}{\equiv} 1, \Rightarrow n^2 + n + 1 \overset{7}{\equiv} = 3$ e $n^2 - n + 1 \overset{7}{\equiv} 1$. Quindi deve essere multiplo di 7 uno degli ultimi due fattori, ma se lo è uno non lo è l'altro, quindi uno dei due deve essere multiplo di 49. Si ha $18^2 + 18 + 1 = 343 = 7 \cdot 49$.

7. **Determinare le radici primitive di 17.**
Intanto basta verificare solo per gli esponenti {2, 4, 8} cioè per i divisori non banali di $17 - 1 = 16$. Si ha: $2^8 \overset{17}{\equiv} 4^4 \overset{17}{\equiv} 8^8 \overset{17}{\equiv} 9^8 \overset{17}{\equiv} 13^8 \overset{17}{\equiv} 15^8 \overset{17}{\equiv} 16^2 \overset{17}{\equiv} 1$, che perciò non sono radici primitive, la verifica che {3; 5; 6; 7; 10; 11; 12; 14} lo sono è lasciata per esercizio,

8. **Dimostrare che se p e $4p + 1$ sono entrambi primi allora $2 = Rp(4p + 1)$. Verificare su valori a piacere.**

Se $4p + 1$ è primo allora $2^{4p} \overset{4p+1}{\equiv} 1$, le uniche possibilità perché una potenza di 2 sia congrua a 1 è nei divisori non banali di $4p$, ossia 2, 4, $2p$, dato che p è primo. Ma $2^2 \overset{4p+1}{\equiv} 4, 2^4 \overset{4p+1}{\equiv} 16$, mentre $2^{2p} \overset{4p+1}{\equiv} \left(2^2\right)^p \overset{4p+1}{\equiv} 4^p \overset{4p+1}{\equiv} -1$, quindi effettivamente $2 = Rp(4p + 1)$. Verifichiamo: $p = 3$ abbiamo che $2 = Rp(13)$, infatti i resti di $2^n/13$, per $1 \le n \le 12$ sono: {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}

9. **Dimostrare che se $4p + 1$ e $8p + 3$ sono entrambi primi allora $2 = Rp(8p + 3)$. Verificare su valori a piacere.**

Se $8p + 3$ è primo allora $2^{8p+2} \overset{8p+3}{\equiv} 1$, le uniche possibilità perché una potenza di 2 sia congrua a 1 è nei divisori non banali di $8p + 2 = 2(4p + 1)$, ossia 2, e $4p + 1$, che è primo. Ma $2^2 \overset{8p+3}{\equiv} 4$, mentre se $2^{4p+1} \overset{8p+3}{\equiv} 1$ allora $2^{8p+2} \overset{8p+3}{\equiv} 2^2 \cdot 2^{4p+1} \overset{8p+3}{\equiv} 4$, quindi effettivamente $2 = Rp(8p + 3)$.
Verifichiamo: $p = 1$ abbiamo che $2 = Rp(11)$, infatti i resti di $2^n/11$, per $1 \le n \le 10$ sono: [2, 4, 8, 5, 10, 9, 7, 3, 6, 1]

Verificare la validità delle seguenti proprietà su numeri a piacere.

10. $\prod_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} 1$**, per p numero primo maggiore di 3.**

Conviene usare $p = 17$, dato che abbiamo già calcolato le radici primitive. Abbiamo:
$(3 \cdot 5) \cdot (6 \cdot 7) \cdot 10 \cdot 11 \cdot 12 \cdot 14 \overset{17}{\equiv} (-2) \cdot 8 \cdot [(-7) \cdot (-6)] \cdot [(-5) \cdot (-3)] \overset{17}{\equiv} (-2) \cdot 8 \cdot 8 \cdot (-2) \overset{17}{\equiv} 16^2 \overset{17}{\equiv} 1$

11. **Se $p - 1$ è un multiplo di un quadrato perfetto allora** $\sum_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} 0$**.**

Sempre $p = 17 \Rightarrow 3 + 5 + 6 + 7 + 10 + 11 + 12 + 14 = 5 \cdot 17$.

12. **Se $p-1$ non è un multiplo di un quadrato perfetto allora $\sum_{i=1}^{\phi(p-1)} Rp_i(p) \overset{p}{\equiv} \pm 1$, dove si sceglie (+) se $p-1$ ha un numero pari di fattori primi, e (–) altrimenti.**
Proviamo prima con $p = 11$ e $p - 1 = 2 \cdot 5$. Si trovano facilmente le $\phi(10) = 4$ radici primitive di 11: {2, 6, 7, 8}. Si ha: $2 + 6 + 7 + 8 = 23 \overset{11}{\equiv} 1$.
Poi $p = 31$, $p - 1 = 2 \cdot 3 \cdot 5$. Le radici primitive di 31 sono in numero di $\phi(30) = 8$ e sono: {3; 11; 12; 13; 17; 21; 22; 24}. Si ha: $(3 + 11 + 12) + (13 + 17) + (21 + 22 + 24) \overset{31}{\equiv} -5 - 1 + 5 \overset{31}{\equiv} -1$.

§16.

1. **Determinare il numero di cifre del periodo delle frazioni di denominatore un numero primo maggiore di 5 e minore di 50.**
Il numero di cifre del periodo della frazione m/n, con n primo, è dato dal minimo h tale che si abbia $10^h \overset{n}{\equiv} 1$

m/n	$10^h \overset{n}{\equiv}$	**Periodo**
$m/7$	$10 \overset{7}{\equiv} 3; 10^2 \overset{7}{\equiv} 2; 10^3 \overset{7}{\equiv} -1; 10^4 \overset{7}{\equiv} -3; 10^5 \overset{7}{\equiv} -2; 10^6 \overset{7}{\equiv} 1$	6
$m/11$	$10 \overset{11}{\equiv} -1; 10^2 \overset{11}{\equiv} 1$	2
$m/13$	$10 \overset{13}{\equiv} -3; 10^2 \overset{13}{\equiv} -4; 10^3 \overset{13}{\equiv} -1; 10^4 \overset{13}{\equiv} 3; 10^5 \overset{13}{\equiv} 4; 10^6 \overset{13}{\equiv} 1$	6
$m/17$	$10 \overset{17}{\equiv} -7; 10^2 \overset{17}{\equiv} -2; 10^3 \overset{17}{\equiv} -3; 10^4 \overset{17}{\equiv} 4; 10^5 \overset{17}{\equiv} 6; 10^6 \overset{17}{\equiv} -8; 10^7 \overset{17}{\equiv} 5; 10^8 \overset{17}{\equiv} -1;$ $10^9 \overset{17}{\equiv} 7; 10^{10} \overset{17}{\equiv} 2; 10^{11} \overset{17}{\equiv} 3; 10^{12} \overset{17}{\equiv} -4; 10^{13} \overset{17}{\equiv} -6; 10^{14} \overset{17}{\equiv} 8; 10^{15} \overset{17}{\equiv} -5; 10^{16} \overset{17}{\equiv} -1;$	16
$m/19$	$10 \overset{19}{\equiv} -9; 10^2 \overset{19}{\equiv} 5; 10^3 \overset{19}{\equiv} -7; 10^4 \overset{19}{\equiv} 6; 10^5 \overset{19}{\equiv} 3; 10^6 \overset{19}{\equiv} -8; 10^7 \overset{19}{\equiv} -4; 10^8 \overset{19}{\equiv} -2; 10^9 \overset{19}{\equiv} -1;$ $10^{10} \overset{19}{\equiv} 9; 10^{11} \overset{19}{\equiv} -5; 10^{12} \overset{19}{\equiv} 7; 10^{13} \overset{19}{\equiv} -6; 10^{14} \overset{19}{\equiv} -3; 10^{15} \overset{19}{\equiv} 8; 10^{16} \overset{19}{\equiv} 4; 10^{17} \overset{19}{\equiv} 2; 10^{18} \overset{19}{\equiv} 1$	18
$m/23$	$10 \overset{23}{\equiv} -13; 10^2 \overset{23}{\equiv} 8; 10^3 \overset{23}{\equiv} 11; 10^4 \overset{23}{\equiv} -5; 10^5 \overset{23}{\equiv} -4; 10^6 \overset{23}{\equiv} 6; 10^7 \overset{23}{\equiv} -9; 10^8 \overset{23}{\equiv} 2; 10^9 \overset{23}{\equiv} -3;$ $10^{10} \overset{23}{\equiv} -7; 10^{11} \overset{22}{\equiv} -1; 10^{12} \overset{23}{\equiv} 13; 10^{13} \overset{23}{\equiv} -8; \ldots; 10^{20} \overset{23}{\equiv} 3; 10^{21} \overset{23}{\equiv} 7; 10^{22} \overset{22}{\equiv} 1$	22
$m/29$	$10 \overset{29}{\equiv} 10; 10^2 \overset{29}{\equiv} 13; 10^3 \overset{29}{\equiv} 14; \ldots; 10^{14} \overset{29}{\equiv} -1; 10^{15} \overset{29}{\equiv} -10; 10^{16} \overset{29}{\equiv} -13; 10^{17} \overset{29}{\equiv} -11; \ldots; 10^{28} \overset{29}{\equiv} 1$	28
$m/31$	$10 \overset{31}{\equiv} 10; 10^2 \overset{31}{\equiv} 7; 10^3 \overset{31}{\equiv} 8; 10^4 \overset{31}{\equiv} -13; 10^5 \overset{31}{\equiv} -6; 10^6 \overset{31}{\equiv} 2; 10^7 \overset{31}{\equiv} -11; 10^8 \overset{31}{\equiv} 14;$ $10^9 \overset{31}{\equiv} -15; 10^{10} \overset{31}{\equiv} 5; 10^{11} \overset{31}{\equiv} 19; 10^{12} \overset{31}{\equiv} 4; 10^{13} \overset{31}{\equiv} 9; 10^{14} \overset{31}{\equiv} -3; 10^{15} \overset{31}{\equiv} 1$	15
$m/37$	$10 \overset{37}{\equiv} 10; 10^2 \overset{37}{\equiv} -11; 10^3 \overset{37}{\equiv} 1$	3
$m/41$	$10 \overset{41}{\equiv} 10; 10^2 \overset{41}{\equiv} 18; 10^3 \overset{41}{\equiv} 16; 10^4 \overset{41}{\equiv} -4; 10^5 \overset{41}{\equiv} 1$	5
$m/43$	$10 \overset{43}{\equiv} 10; 10^2 \overset{43}{\equiv} 14; 10^3 \overset{43}{\equiv} 11; 10^4 \overset{43}{\equiv} -19; 10^5 \overset{43}{\equiv} -18; 10^6 \overset{43}{\equiv} -8; 10^7 \overset{43}{\equiv} 6; 10^8 \overset{43}{\equiv} 17;$ $10^9 \overset{43}{\equiv} -2; 10^{10} \overset{43}{\equiv} -20; 10^{11} \overset{43}{\equiv} 15; 10^{12} \overset{43}{\equiv} 21; 10^{13} \overset{43}{\equiv} -5; 10^{14} \overset{43}{\equiv} -7; 10^{15} \overset{43}{\equiv} 16;$ $10^{16} \overset{43}{\equiv} -12; 10^{17} \overset{43}{\equiv} 9; 10^{18} \overset{43}{\equiv} 4; 10^{19} \overset{43}{\equiv} -3; 10^{20} \overset{43}{\equiv} 13; 10^{21} \overset{43}{\equiv} 1$	21
$m/47$	$10 \overset{47}{\equiv} 10; 10^2 \overset{47}{\equiv} 6; 10^3 \overset{47}{\equiv} 13; \ldots; 10^{23} \overset{47}{\equiv} -1; \ldots; 10^{45} \overset{47}{\equiv} -14; 10^{46} \overset{47}{\equiv} 1$	46

2. **Con riferimento al precedente quesito quali delle frazioni precedenti hanno più di un periodo?**

I periodi si ottengono dividendo $p-1$ per il periodo, quindi $n/11$ ne ha 10/2 = 5; $n/13$ ne ha 12/6 =2; $n/31$: 30/15 = 2; $n/37$: 36/3 = 12; $n/41$: 40/5 = 8; $n/43$: 42/21 = 2

3. **Con riferimento al quesito 1, osserviamo che le frazioni m/p che hanno periodo $(p-1)$ hanno la sequenza delle congruenze delle diverse potenze di 10, in modo che le prime $(p-1)/2$ sono uguali alle opposte delle altre in modo che si abbia $10^n \overset{p}{\equiv} a \Rightarrow 10^{n+(p-1)/2} \overset{p}{\equiv} -a$. Dimostrare tale congettura.**
Dato che il periodo è $p-1$, vuol dire che nella catena delle congruenze otteniamo tutti i numeri da 1 a $p-1$, e dato che questo è un numero pari, $(p-1)/2$ è intero, quindi tutti i numeri da $-(p-1)/2$ a $(p-1)/2$. Ora evidentemente $10^{p-1} \overset{p}{\equiv} \left[10^{(p-1)/2}\right]^2 \overset{p}{\equiv} 1 \Rightarrow 10^{(p-1)/2} \overset{p}{\equiv} -1$, in modo analogo $10^n \overset{p}{\equiv} a \Rightarrow 10^{n+(p-1)/2} \overset{p}{\equiv} 10^n \cdot 10^{(p-1)/2} \overset{p}{\equiv} a \cdot (-1) = -a$

4. **Osserva i diversi periodi di $n/11$ e spiega il motivo di tali caratteristiche.**
Abbiamo: $\frac{1}{11} = 0,\overline{09}; \frac{2}{11} = 0,\overline{18}; \frac{3}{11} = 0,\overline{27}; ...; \frac{10}{11} = 0,\overline{90}$ **.** Sono i multipli di 9 da 09 a 90, ciò dipende dal fatto che $\frac{m}{11} = m \cdot \frac{1}{11} = m \cdot 0,\overline{09} = 0,\overline{(9m)}$

5. **Scrivi le cifre dei diversi periodi di $n/37$.**
Da $10 \overset{37}{\equiv} 10; 10^2 \overset{37}{\equiv} -11; 10^3 \overset{37}{\equiv} 1$, troviamo il primo periodo: $\frac{1}{37} = 0,\overline{027}$ le cui cifre ciclano in $\frac{10}{37} = 0,\overline{270}; \frac{26}{37} = 0,\overline{702}$; Da $2 \cdot 10 \overset{37}{\equiv} 20; 2 \cdot 10^2 \overset{37}{\equiv} 15; 2 \cdot 10^3 \overset{37}{\equiv} 2$, troviamo il secondo periodo: $\frac{2}{37} = 0,\overline{054}$ le cui cifre ciclano in $\frac{15}{37} = 0,\overline{405}; \frac{20}{37} = 0,\overline{540}$ 054; 081; continuando otteniamo gli altri. Si tenga conto che non dobbiamo considerare tutte le congruenze del tipo $m \cdot 10^n$, dato che per esempio $3 \cdot 10^n$ e $4 \cdot 10^n$ modulo 37 forniscono gli stessi valori, anche se in diverso ordine. E ciò perché $3 \cdot 10^2 \overset{37}{\equiv} 4$.

$3 \cdot 10 \overset{37}{\equiv} 30; 3 \cdot 10^2 \overset{37}{\equiv} 4; 3 \cdot 10^3 \overset{37}{\equiv} 3 \Rightarrow \frac{3}{37} = 0,\overline{081}; \frac{4}{37} = 0,\overline{108}; \frac{30}{37} = 0,\overline{810}$

$5 \cdot 10 \overset{37}{\equiv} 13; 5 \cdot 10^2 \overset{37}{\equiv} 19; 5 \cdot 10^3 \overset{37}{\equiv} \Rightarrow \frac{5}{37} = 0,\overline{135}; \frac{13}{37} = 0,\overline{351}; \frac{19}{37} = 0,\overline{513}$

$6 \cdot 10 \overset{37}{\equiv} 23; 6 \cdot 10^2 \overset{37}{\equiv} 8; 6 \cdot 10^3 \overset{37}{\equiv} 6 \Rightarrow \frac{6}{37} = 0,\overline{162}; \frac{8}{37} = 0,\overline{216}; \frac{23}{37} = 0,\overline{621}$

$7 \cdot 10 \overset{37}{\equiv} 33; 7 \cdot 10^2 \overset{37}{\equiv} 34; 7 \cdot 10^3 \overset{37}{\equiv} 7 \Rightarrow \frac{7}{37} = 0,\overline{189}; \frac{33}{37} = 0,\overline{891}; \frac{34}{37} = 0,\overline{918}$

$9 \cdot 10 \overset{37}{\equiv} 16; 9 \cdot 10^2 \overset{37}{\equiv} 12; 9 \cdot 10^3 \overset{37}{\equiv} 9 \Rightarrow \frac{9}{37} = 0,\overline{243}; \frac{12}{37} = 0,\overline{324}; \frac{16}{37} = 0,\overline{432}$

$11 \cdot 10 \overset{37}{\equiv} 36; 11 \cdot 10^2 \overset{37}{\equiv} 27; 11 \cdot 10^3 \overset{37}{\equiv} 11 \Rightarrow \frac{11}{37} = 0,\overline{297}; \frac{27}{37} = 0,\overline{729}; \frac{36}{37} = 0,\overline{972}$

$14 \cdot 10 \overset{37}{\equiv} 29; 14 \cdot 10^2 \overset{37}{\equiv} 31; 14 \cdot 10^3 \overset{37}{\equiv} 14 \Rightarrow \frac{14}{37} = 0,\overline{378}; \frac{29}{37} = 0,\overline{783}; \frac{31}{37} = 0,\overline{837}$

$17 \cdot 10 \overset{37}{\equiv} 22; 17 \cdot 10^2 \overset{37}{\equiv} 35; 17 \cdot 10^3 \overset{37}{\equiv} 17 \Rightarrow \frac{17}{37} = 0,\overline{459}; \frac{22}{37} = 0,\overline{594}; \frac{35}{37} = 0,\overline{945}$

$18 \overset{37}{\equiv} 32; 18 \cdot 10^2 \overset{37}{\equiv} 24; 1 \cdot 10^3 \overset{37}{\equiv} 18 \Rightarrow \frac{18}{37} = 0,\overline{486}; \frac{24}{37} = 0,\overline{648}; \frac{32}{37} = 0,\overline{864}$

$21\cdot 10 \overset{37}{\equiv} 25; 21\cdot 10^2 \overset{37}{\equiv} 28; 21\cdot 10^3 \overset{37}{\equiv} 21 \Rightarrow \frac{21}{37} = 0,\overline{567}; \frac{25}{37} = 0,\overline{675}; \frac{28}{37} = 0,\overline{756}$

6. **Provare che non possono esistere numeri di periodo 9.**

   Se esistesse per esempio $1,\bar{9}$ si avrebbe: $1,\bar{9} = \frac{19-1}{9} = 2$

7. **Tenuto conto di quanto visto nell'esempio 56, stabilire quali sono i valori di *p* primo per cui 1/*p* ha un periodo formato da: a) 3; b) 4; c) 5; d) 6 cifre.**

   a) $10^3 - 1 = 3^3 \cdot 37$, cioè $10^3 \overset{37}{\equiv} 1$, quindi solo 1/37 ha periodo 3, dato che 1/3 ha periodo 1; b) $10^4 - 1 = 3^2 \cdot 11 \cdot 101$, cioè $10^4 \overset{101}{\equiv} 1$, quindi solo 1/101 ha periodo 4, dato che 1/11 ha periodo 2; c) $10^5 - 1 = 3^2 \cdot 41 \cdot 207$, cioè $10^5 \overset{41}{\equiv} 1, 10^5 \overset{207}{\equiv} 1$, quindi sia 1/41 che 1/207 hanno periodo 5; d) $10^6 - 1 = 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 37$, cioè $10^6 \overset{7}{\equiv} 1; 10^6 \overset{13}{\equiv} 1; 10^6 \overset{37}{\equiv} 1$, quindi solo 1/7 e 1/13 sono le uniche ad avere periodo 6.

8. **Dopo aver determinato tutti i numeri primi minori di 100 a cui si può applicare il Teorema 48, verificarlo con essi.**

1/*p*	Somma periodo dimezzato
1/7	142 + 857 = 999
1/11	0 + 9 = 9
1/13	076 + 923 = 999
1/17	05882352 + 94117647 = 99999999
1/19	052631578 + 947368421 = 999999999
1/23	04347826086 + 95652173913 = 99999999999
1/29	03448275862068 + 96551724137931 = 99999999999999
1/47	021276595744680851063 82 + 97872340425531914893617 = $\underbrace{999...9}_{23}$
1/59	0169491525423728813559322 0338 + 9830508474576271186440677 9661 = $\underbrace{999...9}_{29}$
1/61	0163934426229508196721311475 40+9836065573770491803278688524 59= $\underbrace{999...9}_{30}$
1/73	0136 + 9869 = 9999
1/89	01123595505617977528 08 + 98876404494382022471 91= $\underbrace{999...9}_{44}$

§17.

1. a) $1+2+3+...+n = \frac{n\cdot(n+1)}{2}$**; b) 1 + 3 + 5 + … + (2*n* – 1) = *n*^{2};**

a) Si ha $1 = \frac{1\cdot(1+1)}{2}$. Ora supponiamo vero che $1+2+3+...+n = \frac{n\cdot(n+1)}{2}$ e proviamo che $1+2+3+...+(n+1) = \frac{(n+1)\cdot(n+2)}{2}$. Come già visto sotituiamo ai primi addendi e riscriviamo: $\frac{n\cdot(n+1)}{2} + (n+1)$. Adesso mettiamo in evidenza a fattor comune: $(n+1)\cdot\left(\frac{n}{2}+1\right) = (n+1)\cdot\left(\frac{n+2}{2}\right) = \frac{(n+1)\cdot(n+2)}{2}$ e abbiamo ottenuto proprio ciò che volevamo provare. Quindi la formula è dimostrata.

b) $n = 1$: $1 = 1^2$; verificato. Hp: $1 + 3 + 5 + \ldots + (2n - 1) = n^2$, Ts: $1 + 3 + 5 + \ldots +$

$(2n-1)+(2n+1)=(n+1)^2$. Dim. $[1+3+5+\ldots+(2n-1)+(2n+1)]=n^2+2n+1=(n+1)^2$.

2. **a)** $1^2+2^2+\ldots+n^2=\dfrac{n\cdot(n+1)\cdot(2n+1)}{6}$; **b)** $1^2+3^2+5^2+\ldots+(2n-1)^2=\dfrac{n\cdot(4n^2-1)}{3}$

a) $n=1$: $1^2=\dfrac{1\cdot(1+1)\cdot(2+1)}{6}=\dfrac{1\cdot2\cdot3}{6}=1$; verificato.

Hp: $1^2+2^2+3^2+\ldots+n^2=\dfrac{n\cdot(n+1)\cdot(2n+1)}{6}$,

Ts: $1^2+2^2+3^2+\ldots+(n+1)^2=\dfrac{(n+1)\cdot(n+2)\cdot(2n+3)}{6}$.

Dim.

$$\left[1^2+2^2+3^2+\ldots+n^2\right]+(n+1)^2=\frac{n\cdot(n+1)\cdot(2n+1)}{6}+(n+1)^2=\frac{n\cdot(n+1)\cdot(2n+1)+6(n+1)^2}{6}=$$
$$=\frac{(n+1)\cdot\left[2n^2+n+6n+6\right]}{6}=\frac{(n+1)\cdot\left[2n^2+7n+6\right]}{6}=\frac{(n+1)\cdot(n+2)\cdot(2n+3)}{6}$$

b) $n=1$: $1^2=\dfrac{1\cdot(4-1)}{3}=\dfrac{1\cdot3}{3}=1$; verificato.

Hp: $1^2+3^2+5^2+\ldots+(2n-1)^2=\dfrac{n\cdot(4n^2-1)}{3}$,

Ts: $1^2+3^2+5^2+\ldots+(2n-1)^2+(2n+1)^2=\dfrac{(n+1)\cdot\left[4\cdot(n+1)^2-1\right]}{3}=$
$=\dfrac{(n+1)\cdot\left[4n^2+8n+3\right]}{3}=\dfrac{(n+1)\cdot(2n+1)\cdot(2n+3)}{3}$.

Dim.

$$\left[1^2+3^2+5^2+\ldots+(2n-1)^2\right]+(2n+1)^2=\frac{n\cdot(4n^2-1)}{3}+(2n+1)^2=\frac{n\cdot(2n-1)\cdot(2n+1)}{3}+(2n+1)^2=$$
$$=\frac{n\cdot(2n-1)\cdot(2n+1)+3\cdot(2n+1)^2}{3}=\frac{(2n+1)\cdot(2n^2-n+6n+3)}{3}=\frac{(2n+1)\cdot(2n^2+5n+3)}{3}=$$
$$=\frac{(2n+1)\cdot(n+1)\cdot(2n+3)}{3}$$

3. **a)** $\mathbf{2^2+5^2+8^2+\ldots+(3n-1)^2=\dfrac{n\cdot(6n^2+3n-1)}{2}}$; **b)** $\boldsymbol{n\geq10\Rightarrow2^n>n^3}$

a) $n=1$: $2^2=\dfrac{1\cdot(6+3-1)}{2}=\dfrac{8}{2}=4$; verificato. Hp: $2^2+5^2+8^2+\ldots+(3n-1)^2=\dfrac{n\cdot(6n^2+3n-1)}{2}$ Ts: $2^2+5^2+8^2+\ldots+(3n-1)^2+(3n+2)^2=\dfrac{(n+1)\cdot(6(n+1)^2+3n+3-1)}{2}=\dfrac{(n+1)\cdot(6n^2+12n+6+3n+2)}{2}=$
$=\dfrac{(n+1)\cdot(6n^2+15n+8)}{2}=\dfrac{(n+1)\cdot(6n^2+15n+8)}{2}$.

Dim. $[2^2+5^2+8^2+\ldots+(3n-1)^2]+(3n+2)^2=$

$$\frac{n\cdot\left(6n^2+3n-1\right)}{2}+\left(3n+2\right)^2=\frac{n\cdot\left(6n^2+3n-1\right)+2\cdot\left(3n+2\right)^2}{2}=$$

$$=\frac{6n^3+3n^2-n+18n^2+24n+8}{2}=\frac{6n^3+21n^2+23n+8}{2}=\frac{\left(n+1\right)\cdot\left(6n^2+15n+8\right)}{2}.$$

b) $2^{10} > 10^3$, ok. $2^n > n^3 \Rightarrow 2^{n+1} > (n+1)^3$. $2\cdot 2^n > 2\cdot n^3 > (1+1/10)\cdot n^3 > (1+1/n)^3\cdot n^3 > 0$ per $n > 10$, quindi $2^{n+1} > (n+1)^3$

4. **a)** $1^3+2^3+3^3+\ldots+n^3=\left[\frac{n\cdot\left(n+1\right)}{2}\right]^2$ **; b)** $\frac{1}{1\cdot 5}+\frac{1}{5\cdot 9}+\ldots+\frac{1}{\left(4n-3\right)\cdot\left(4n+1\right)}=\frac{n}{4n+1}$

a) $n = 1$: $1^3=\left[\frac{1\cdot\left(1+1\right)}{2}\right]^2=1$; verificato. Hp: $1^3+2^3+3^3+\ldots+n^3=\left[\frac{n\cdot\left(n+1\right)}{2}\right]^2$,

Ts: $1^3+2^3+3^3+\ldots+\left(n+1\right)^3=\left[\frac{\left(n+1\right)\cdot\left(n+2\right)}{2}\right]^2$. Dim.

$$\left[1^3+2^3+3^3+\ldots+n^3\right]+\left(n+1\right)^3=\left[\frac{n\cdot\left(n+1\right)}{2}\right]^2+\left(n+1\right)^3=\left(n+1\right)^2\cdot\left(\frac{n^2}{4}+n+1\right)=$$

$$=\left(n+1\right)^2\cdot\left(\frac{n^2+4n+4}{4}\right)=\left[\frac{\left(n+1\right)\cdot\left(n+2\right)}{2}\right]^2$$

.

b) $\frac{1}{1\cdot 5}+\frac{1}{5\cdot 9}+\ldots+\frac{1}{\left(4n-3\right)\cdot\left(4n+1\right)}+\frac{1}{\left(4n+1\right)\cdot\left(4n+5\right)}=\frac{n+1}{4n+5}$. Dim.

$$\left[\frac{1}{1\cdot 5}+\frac{1}{5\cdot 9}+\ldots+\frac{1}{\left(4n-3\right)\cdot\left(4n+1\right)}\right]+\frac{1}{\left(4n+1\right)\cdot\left(4n+5\right)}=\frac{n}{4n+1}+\frac{1}{\left(4n+1\right)\cdot\left(4n+5\right)}=$$

$$=\frac{4n^2+5n+1}{\left(4n+1\right)\cdot\left(4n+5\right)}=\frac{\cancel{\left(4n+1\right)}\cdot\left(n+1\right)}{\cancel{\left(4n+1\right)}\cdot\left(4n+5\right)}=\frac{n+1}{4n+5}$$

5. **a)** $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots+\frac{1}{n\cdot\left(n+1\right)}=\frac{n}{n+1}$ **; b)** $\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{\left(2n-1\right)\cdot\left(2n+1\right)}=\frac{n}{2n+1}$

a) $n = 1$: $\frac{1}{1\cdot 2}=\frac{1}{1+1}$; verificato. Hp: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots+\frac{1}{n\cdot\left(n+1\right)}=\frac{n}{n+1}$,

Ts: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots+\frac{1}{n\cdot\left(n+1\right)}+\frac{1}{\left(n+1\right)\cdot\left(n+2\right)}=\frac{n+1}{n+2}$.

Dim. $\left[\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots+\frac{1}{n\cdot\left(n+1\right)}\right]+\frac{1}{\left(n+1\right)\cdot\left(n+2\right)}=\frac{n}{n+1}+\frac{1}{\left(n+1\right)\cdot\left(n+2\right)}=$

$$=\frac{n^2+2n+1}{\left(n+1\right)\cdot\left(n+2\right)}=\frac{\left(n+1\right)\cancel{^2}}{\cancel{\left(n+1\right)}\cdot\left(n+2\right)}=\frac{n+1}{n+2}$$

.

b) $n = 1$: $\frac{1}{1\cdot 3}=\frac{1}{2+1}$; verificato. Hp: $\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{\left(2n-1\right)\cdot\left(2n+1\right)}=\frac{n}{2n+1}$,

Ts: $\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)\cdot(2n+1)}+\frac{1}{(2n+1)\cdot(2n+3)}=\frac{n+1}{2n+3}$.

Dim.

$$\left[\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)\cdot(2n+1)}\right]+\frac{1}{(2n+1)\cdot(2n+3)}=\frac{n}{2n+1}+\frac{1}{(2n+1)\cdot(2n+3)}=$$

$$=\frac{2n^2+3n+1}{(2n+1)\cdot(2n+3)}=\frac{\cancel{(2n+1)}\cdot(n+1)}{\cancel{(2n+1)}\cdot(2n+3)}=\frac{n+1}{2n+3}$$

6. $\frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\ldots+\frac{n^2}{(2n-1)\cdot(2n+1)}=\frac{n\cdot(n+1)}{2\cdot(2n+1)}$**;**

$n = 1$: $\frac{1^2}{1\cdot 3}=\frac{1\cdot(1+1)}{2\cdot(2+1)}=\frac{2}{2\cdot 3}$; verificato.

Hp: $\frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\ldots+\frac{n^2}{(2n-1)\cdot(2n+1)}=\frac{n\cdot(n+1)}{2\cdot(2n+1)}$,

Ts: $\frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\ldots+\frac{n^2}{(2n-1)\cdot(2n+1)}+\frac{(n+1)^2}{(2n+1)\cdot(2n+3)}=\frac{(n+1)\cdot(n+2)}{2\cdot(2n+3)}$.

Dim.

$$\left[\frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\ldots+\frac{n^2}{(2n-1)\cdot(2n+1)}\right]+\frac{(n+1)^2}{(2n+1)\cdot(2n+3)}=\frac{n\cdot(n+1)}{2\cdot(2n+1)}+\frac{(n+1)^2}{(2n+1)\cdot(2n+3)}=$$

$$=\frac{n\cdot(n+1)\cdot(2n+3)+2\cdot(n+1)^2}{2\cdot(2n+1)\cdot(2n+3)}=\frac{(n+1)\left(2n^2+3n+2n+2\right)}{2\cdot(2n+1)\cdot(2n+3)}=\frac{(n+1)\left(2n^2+5n+2\right)}{2\cdot(2n+1)\cdot(2n+3)}=$$

$$=\frac{(n+1)(n+2)\cdot\cancel{(2n+1)}}{2\cdot\cancel{(2n+1)}\cdot(2n+3)}=\frac{(n+1)\cdot(n+2)}{2\cdot(2n+3)}$$

7. $\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\ldots+\frac{1}{(3n-2)\cdot(3n+1)}=\frac{n}{3n+1}$

$n = 1$: $\frac{1}{1\cdot 4}=\frac{1}{3+1}$; verificato. Hp: $\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\ldots+\frac{1}{(3n-2)\cdot(3n+1)}=\frac{n}{3n+1}$,

Ts: $\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\ldots+\frac{1}{(3n-2)\cdot(3n+1)}+\frac{1}{(3n+1)\cdot(3n+4)}=\frac{n+1}{3n+4}$.

Dim.

$$\left[\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\ldots+\frac{1}{(3n-2)\cdot(3n+1)}\right]+\frac{1}{(3n+1)\cdot(3n+4)}=\frac{n}{3n+1}+\frac{1}{(3n+1)\cdot(3n+4)}=$$

$$=\frac{3n^2+4n+1}{(3n+1)\cdot(3n+4)}=\frac{(n+1)\cdot\cancel{(3n+1)}}{\cancel{(3n+1)}\cdot(3n+4)}=\frac{n+1}{3n+4}$$

8. a) $1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3 = n^2 \cdot (2n^2 - 1)$; b) $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$

a) $n = 1$: $1^3 = 1^2 \cdot (2 - 1)$; verificato. Hp: $1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3 = n^2 \cdot (2n^2 - 1)$, Ts: $1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3 + (2n + 1)^3 = (n + 1)^2 \cdot (2n^2 + 4n + 1)$. Dim. $[1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3] + (2n + 1)^3 = n^2 \cdot (2n^2 - 1) + (2n + 1)^3 = 2n^4 + 8n^3 + 11n^2 + 6n + 1 = (n + 1)^2 \cdot (2n^2 + 4n + 1)$

b) $n = 0$: $1 = 2^{0+1} - 1 = 1$; verificato. Hp: $1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$, Ts: $1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 11 + 2 + 2^2 + 2^3 + \ldots + 2^n + 2^{n+1} = 2^{n+2} - 1$. Dim.

$[1 + 2 + 2^2 + 2^3 + ... + 2^n] + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$

9. $\mathbf{1^5 + 2^5 + 3^5 + \ldots + n^5 = n^2 \cdot (n+1)^2 \cdot (2n^2 + 2n - 1)/12}$

$n = 1$: $1^5 = 1^2 \cdot (1+1)^2 \cdot (2 + 2 - 1)/12 = 12/12$; verificato. Hp: $1^5 + 2^5 + 3^5 + \ldots + n^5 = n^2 \cdot (n+1)^2 \cdot (2n^2 + 2n - 1)/12$, Ts: $1^5 + 2^5 + 3^5 + \ldots + (n+1)^5 = (n+1)^2 \cdot (n+2)^2 \cdot [2(n+1)^2 + 2(n+1) - 1)/12 = (n+1)^2 \cdot (n+2)^2 \cdot (2n^2 + 6n + 3)/12$. Dim. $[1^5 + 2^5 + 3^5 + \ldots + n^5] + (n+1)^5 = n^2 \cdot (n+1)^2 \cdot (2n^2 + 2n - 1)/12 + (n+1)^5 = (n+1)^2 \cdot [n^2 \cdot (2n^2 + 2n - 1) + 12 \cdot (n+1)^3]/12 = (n+1)^2 \cdot (n+2)^2 \cdot (2n^2 + 6n + 3)/12$

10. $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + n \cdot (n+1) \cdot (n+2) = \dfrac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4}$

$n = 1$: $1 \cdot 2 \cdot 3 = \dfrac{1 \cdot (1+1) \cdot (1+2) \cdot (1+3)}{4} = \dfrac{1 \cdot 2 \cdot 3 \cdot \cancel{4}}{\cancel{4}}$; verificato.

Hp: $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + n \cdot (n+1) \cdot (n+2) = \dfrac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4}$,

Ts:

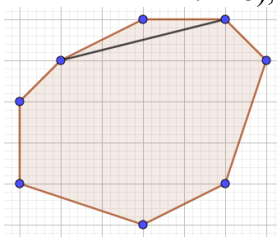
$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + n \cdot (n+1) \cdot (n+2) + (n+1) \cdot (n+2) \cdot (n+3) = \dfrac{(n+1) \cdot (n+2) \cdot (n+3) \cdot (n+4)}{4}$ Dim.

$\left[1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + ... + n \cdot (n+1) \cdot (n+2)\right] + (n+1) \cdot (n+2) \cdot (n+3) = \dfrac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4} +$

$+ (n+1) \cdot (n+2) \cdot (n+3) = (n+1) \cdot (n+2) \cdot (n+3) \cdot \dfrac{n+4}{4} = \dfrac{(n+1) \cdot (n+2) \cdot (n+3) \cdot (n+4)}{4}$

11. La somma degli angoli interni di un poligono convesso di *n* lati è $(n-2) \cdot 180°$, $n \geq 3$.

$n = 3$, vera perché nel triangolo si ha: $(3 - 2) \cdot 180°$. Hp: $(n - 2) \cdot 180°$; Ts: $(n - 1) \cdot 180°$. Dim. Tiriamo una diagonale nel poligono di n lati in modo da unire i due vertici non comuni di due lati consecutivi, (in figura consideriamo il caso di $n = 8$), in



questo modo abbiamo un poligono di n lati e uno di 3 lati, la somma degli angoli interni del poligono di $n + 1$ lati è uguale a quella delle somme dei due poligoni cioè $(n - 2) \cdot 180° + 180° = (n - 1) \cdot 180°$.

12. $\mathbf{(1^5 + 2^5 + \ldots + n^5) + (1^7 + 2^7 + \ldots + n^7) = 2 \cdot (1 + 2 + \ldots + n)^4}$

$n = 1$: $1^5 + 1^7 = 2 \cdot 1^4$; verificato.

Osserviamo che. $1 + 2 + ... + n = \dfrac{n \cdot (n+1)}{2}; 1 + 2 + ... + n + (n+1) = \dfrac{(n+1) \cdot (n+2)}{2}$,

quindi Hp: $(1^5 + 2^5 + \ldots + n^5) + (1^7 + 2^7 + \ldots + n^7) = 2 \cdot \left[\dfrac{n \cdot (n+1)}{2}\right]^4$, Ts: $[1^5 + 2^5 + \ldots + (n+1)^5] + [1^7 + 2^7 + \ldots + (n+1)^7] = 2 \cdot \left[\dfrac{(n+1) \cdot (n+2)}{2}\right]^4$ Dim. $[1^5 + 2^5 + \ldots + n^5 + (n+1)^5] + [1^7 + 2^7 + \ldots + n^7 + (n+1)^7] = 2 \cdot \left[\dfrac{n \cdot (n+1)}{2}\right]^4 + (n+1)^5 + (n+1)^7 = (n+1)^4 \cdot \left[\dfrac{n^4}{8} + (n+1) + (n+1)^3\right] =$

$(n+1)^4 \cdot \dfrac{n^4 + 8n + 8 + 8n^3 + 24n^2 + 24n + 8}{8} = (n+1)^4 \cdot \dfrac{n^4 + 8n^3 + 24n^2 + 32n + 16}{8} = 2 \cdot \left[\dfrac{(n+1) \cdot (n+2)}{2}\right]^4$

13. $\mathbf{3 \cdot (1^2 + 2^2 + \ldots + n^2) - 3 \cdot (1 + 2 + \ldots + n) = n^3 - n}$

$n = 1$: $3 \cdot 1^2 - 3 \cdot 1 = 1^3 - 1 \Rightarrow 0 = 0$; verificato. Hp: $3 \cdot (1^2 + 2^2 + \ldots + n^2) - 3 \cdot (1 + 2 + \ldots + n) = n^3 - n$, Ts: $3 \cdot [1^2 + 2^2 + \ldots + (n + 1)^2] - 3 \cdot [1 + 2 + \ldots + (n + 1)] = (n + 1)^3 - (n + 1)$. Dim. $3 \cdot [1^2 + 2^2 + \ldots + (n + 1)^2] - 3 \cdot [1 + 2 + \ldots + (n + 1)] = n^3 - n + 3 \cdot [(n + 1)^2 - (n + 1)] = n^3 - n + 3 \cdot (n^2 + 2n + 1 - n - 1) = (n^3 + 3n^2 + 3n + 1) - (n + 1) = (n + 1)^3 - (n + 1)$

14. $\mathbf{3 \cdot (1^5 + 2^5 + \ldots + n^5) + (1^3 + 2^3 + \ldots + n^3) = 4 \cdot (1 + 2 + \ldots + n)^3}$

$n = 1$: $3 \cdot 1^5 + 1^3 = 4 \cdot (1)^3 \Rightarrow 4 = 4$; verificato. Scriviamo meglio il secondo membro : $4n^3 \cdot (n + 1)^3/8 = n^3 \cdot (n + 1)^3/2$, tenuto conto di quel che sappiamo sulla somma dei primi n naturali. Quindi: Hp: $3 \cdot (1^5 + 2^5 + \ldots + n^5) + (1^3 + 2^3 + \ldots + n^3) = n^3 \cdot (n + 1)^3/2$, Ts: $3 \cdot [1^5 + 2^5 + \ldots + (n + 1)^5] + [1^3 + 2^3 + \ldots + (n + 1)^3] = (n + 1)^3 \cdot (n + 2)^3/2$. Dim. $3 \cdot [1^5 + 2^5 + \ldots + (n + 1)^5] + [1^3 + 2^3 + \ldots + (n + 1)^3] = n^3 \cdot (n + 1)^3/2 + 3 \cdot (n + 1)^5 + (n + 1)^3 = (n + 1)^3 \cdot [n^3 + 6 \cdot (n + 1)^2 + 2]/2 = (n + 1)^3 \cdot (n^3 + 6n^2 + 12n + 6 + 2)/2 = (n + 1)^3 \cdot (n + 2)^3/2$.

15. a) $\mathbf{n^3 + 1 > n^2 + n}$**,** $\mathbf{n \geq 2}$**; b)** $\mathbf{11^{n+2} + 12^{2n+1}}$ **è divisibile per 133**

a) $n = 2$, $2^3 + 1 > 2^2 + 2 \Rightarrow 9 > 6$; ok. Hp: $n^3 + 1 > n^2 + n$, $n \geq 2$, Ts: $(n + 1)^3 + 1 > (n + 1)^2 + n + 1$, $n \geq 2$. Dim. $(n + 1)^3 + 1 = n^3 + 3n^2 + 3n + 1 + 1 > n^2 + n + 3n^2 + 3n + 1 = n^2 + 2n + 1 + 3n^2 + n = (n + 1)^2 + 3n^2 + n > (n + 1)^2 + n + 1$

b) $n = 1$: $11^3 + 12^3 = 1331 + 1728 = 3059 = 133 \cdot 23$; verificato. Hp: $11^{n+2} + 12^{2n+1} = 6h$, Ts: $11^{n+3} + 12^{2n+3} = 6k$ Dim. $11^{n+3} + 12^{2n+3} = 11 \cdot 11^{n+2} + 144 \cdot 12^{2n+1} = 11 \cdot 11^{n+2} + (11 + 133) \cdot 12^{2n+1} = 11 \cdot (11^{n+2} + 12^{2n+1}) + 133 \cdot 12^{2n+1} = 11 \cdot 133h + 133 \cdot 12^{2n+1} = 133 \cdot (11h + 12^{2n+1})$.

16. Il numero di regioni in cui $\boldsymbol{n}$ **rette dividono il piano è minore o uguale a** $\mathbf{2^n}$**.**

$n = 1$. Una retta divide il piano in $p = 2^1$ parti. Hp: $p \leq 2^n$. Ts: $p \leq 2^{n+1}$. Dim. Consideriamo 2 rette, queste possono essere incidenti, nel qual caso raddoppiamo p, o parallele, nel qual caso p aumenta di 1. Quindi nell'ipotesi in cui la $(n + 1)$ – esima retta incontra tutte le precedenti p raddoppia e quindi se prima era $p \leq 2^n$, adesso sarà $p \leq 2 \cdot 2^n = 2^{n+1}$, in tutti gli altri casi sarà minore di questo valore.

17. a) $\mathbf{17^n - 12^n}$ **è divisibile per 5; b)** $\mathbf{5^n + 2 \cdot 3^{n-1} + 1}$ **è divisibile per 8**

a) $n = 1$: $17 - 12 = 5$; verificato. Hp: $17^n - 12^n = 5h$, Ts: $17^{n+1} - 12^{n+1} = 5k$ Dim. $17^{n+1} - 12^{n+1} = 17 \cdot 17^n - 12 \cdot 12^n = (12 + 5) \cdot 17^n - 12 \cdot 12^n = 12 \cdot (17^n - 12^n) + 5 \cdot 17^n = 5h + 5 \cdot 17^n = 5 \cdot (h + 17^n)$.

b) $n = 1$: $5 + 2 \cdot 1 + 1 = 8$; verificato. Hp: $5^n + 2 \cdot 3^{n-1} + 1 = 8h$, Ts: $5^{n+1} + 2 \cdot 3^n + 1 = 8k$ Dim. $5^{n+1} + 2 \cdot 3^n + 1 = 5 \cdot 5^n + 2 \cdot 3 \cdot 3^{n-1} + 1 = 5 \cdot 5^n + 2 \cdot 3^{n-1} + 4 \cdot 3^{n-1} + 5 - 4 = 5 \cdot (5^n + 3^{n-1} + 1) + 4 \cdot 3^{n-1} - 4 = 5 \cdot 8h + 4 \cdot (3^{n-1} - 1)$. Dobbiamo provare che $3^{n-1} - 1$ è pari per qualsiasi n. Questo è ovvio perché 3^{n-1} è sempre dispari. Quindi abbiamo finito.

18. a) $\mathbf{7^n + 5^{2n+1}}$ **è divisibile per 6; b)** $\mathbf{9^n - 8n - 1}$ **è divisibile per 64**

a) $n = 1$: $7 + 125 = 132 = 6 \cdot 22$; verificato. Hp: $7^n + 5^{2n+1} = 6h$, Ts: $7^{n+1} + 5^{2n+3} = 6k$ Dim. $7^{n+1} + 5^{2n+3} = 7 \cdot 7^n + 25 \cdot 5^{2n+1} = 7 \cdot 7^n + (7 + 18) \cdot 5^{2n+1} = 7 \cdot (7^n + 5^{2n+1}) + 18 \cdot 5^{2n+1} = 7 \cdot 6h + 6 \cdot 3 \cdot 5^{2n+1} = 6 \cdot (7h + 3 \cdot 5^{2n+1})$.

b) $n = 1$: $9 - 8 - 1 = 0 = 64 \cdot 0$; verificato. Hp: $9^n - 8n - 1 = 64h$, Ts: $9^{n+1} - 8n - 9 = 64k$ Dim. $9^{n+1} - 8n - 9 = 9 \cdot 9^n - 9 \cdot 8n - 9 + 8 \cdot 8^n = 9 \cdot (9^n - 8n - 1) + 64 \cdot 8^{n-1} = 9 \cdot 64h + 64 \cdot 8^{n-1} = 64 \cdot (9h + 8^{n-1})$

19. a) $\mathbf{8^n - 3^n}$ **è divisibile per 5; b)** $\mathbf{3^{2n+2} - 8n - 9}$ **è divisibile per 64**

a) $n = 1$: $8 - 3 = 5$; verificato. Hp: $8^n - 3^n = 5h$, Ts: $8^{n+1} - 3^{n+1} = 5k$ Dim. $8^{n+1} - 3^{n+1} = 8 \cdot 8^n - 3 \cdot 3^n = (3 + 5) \cdot 8^n - 3 \cdot 3^n = 3 \cdot (8^n - 5^n) + 5 \cdot 8^n = 5h + 5 \cdot 8^n = 5 \cdot (h + 8^n)$.

b) $n = 1$: $3^{2+2} - 8 - 9 = 64$; verificato. Hp: $3^{2n+2} - 8n - 9 = 64h$, Ts: $3^{2n+4} - 8n -$

$17 = 64k$ Dim. $3^{2n+4} - 8n - 17 = 9 \cdot 3^{2n+4} - 9 \cdot 8n - 9 \cdot 9 + (8 \cdot 8n + 64) = 9 \cdot (3^{2n+2} - 8n - 9) + 64 \cdot (n + 1) = 9 \cdot 64h + 64 \cdot (n + 1) = 64 \cdot (9h + n + 1)$

20. a) $13^{2n} + 6$ è divisibile per 7; b) $3^{2n} + 4^{n+1}$ è divisibile per 5;

a) $n = 1$: $13^2 + 6 = 169 + 6 = 175 = 7 \cdot 25$; verificato. Hp: $13^{2n} + 6 = 7h$, Ts: $13^{2n+2} + 6 = 7k$ Dim. $13^{2n+2} + 6 = 169 \cdot 13^{2n} + 6 = 168 \cdot 13^{2n} + 13^{2n} + 6 = 168 \cdot 13^{2n} + 7h = 7 \cdot 24 \cdot 13^{2n} + 7h = 7 \cdot (24 \cdot 13^{2n} + h)$.

b) $n = 1$: $3^2 + 4^2 = 9 + 16 = 25$; verificato. Hp: $3^{2n} + 4^{n+1} = 5h$, Ts: $3^{2n+2} + 4^{n+2} = 5k$ Dim. $3^{2n+2} + 4^{n+2} = 9 \cdot 3^{2n} + 4 \cdot 4^{n+1} = (5 + 4) \cdot 3^{2n} + 4 \cdot 4^{n+1} = 5 \cdot 3^{2n} + 4 \cdot (3^{2n} + 4^{n+1}) = 5 \cdot 3^{2n} + 4 \cdot 5h = 5 \cdot (3^{2n} + 4h)$.

21. $\boldsymbol{cos(\alpha) + cos(3\alpha) + ... + cos[(2n-1)\cdot\alpha] = \dfrac{sin(2n\cdot\alpha)}{2\cdot sin(\alpha)}}$

$n = 1$: $cos(\alpha) = \dfrac{sin(2\alpha)}{2\cdot sin(\alpha)} = \dfrac{2sin(\alpha)cos(\alpha)}{2\,sin(\alpha)} = cos(\alpha)$; verificato. Hp: $cos(\alpha) + cos(3\alpha) + ... + cos[(2n-1)\cdot\alpha] = \dfrac{sin(2n\cdot\alpha)}{2\cdot sin(\alpha)}$, Ts: $cos(\alpha) + cos(3\alpha) + ... + cos[(2n+1)\cdot\alpha] = \dfrac{sin[2(n+1)\alpha]}{2\cdot sin(\alpha)} = \dfrac{sin[(2n+2)\alpha]}{2\cdot sin(\alpha)}$ Dim. Osserviamo intanto che $sin[(2n+2)\cdot\alpha] = sin(2n\alpha + 2\alpha) = sin(2n\alpha)cos(2\alpha) + cos(2n\alpha)sin(2\alpha)$ e $cos[(2n+1)\cdot\alpha] = cos(2n\alpha)cos(\alpha) - sin(2n\alpha)sin(\alpha)$. Adesso abbiamo: $cos(\alpha) + cos(3\alpha) + ... + cos[(2n-1)\cdot\alpha] + cos[(2n+1)\cdot\alpha] =$

$$\frac{sin(2n\alpha)}{2\cdot sin(\alpha)} + cos[(2n+1)\alpha] = \frac{sin(2n\alpha) + 2sin(\alpha)cos[(2n+1)\alpha]}{2\cdot sin(\alpha)} =$$

$$= \frac{sin(2n\alpha) + 2sin(\alpha)[cos(2n\alpha)cos(\alpha) - sin(2n\alpha)sin(\alpha)]}{2\cdot sin(\alpha)} =$$

$$= \frac{sin(2n\alpha) + cos(2n\alpha)sin(2\alpha) - 2sin(2n\alpha)sin^2(\alpha)}{2\cdot sin(\alpha)} =$$

$$= \frac{sin(2n\alpha)\cdot[1 - 2sin^2(\alpha)] + cos(2n\alpha)sin(2\alpha)}{2\cdot sin(\alpha)} =$$

$$= \frac{sin(2n\alpha)\cdot cos(2\alpha) + cos(2n\alpha)sin(2\alpha)}{2\cdot sin(\alpha)}$$

22. $\boldsymbol{sin(\alpha) + sin(3\alpha) + ... + sin[(2n-1)\cdot\alpha] = \dfrac{1 - cos(2n\cdot\alpha)}{2\cdot sin(\alpha)}}$

$n = 1$: $sin(\alpha) = \dfrac{1 - cos(2\alpha)}{2\cdot sin(\alpha)} = \dfrac{1 - 1 + 2sin^2(\alpha)}{2sin(\alpha)} = \dfrac{2sin^2(\alpha)}{2sin(\alpha)} = sin(\alpha)$; verificato. Hp: $sin(\alpha) + sin(3\alpha) + ... + sin[(2n-1)\cdot\alpha] = \dfrac{1 - cos(2n\cdot\alpha)}{2\cdot sin(\alpha)}$, Ts: $sin(\alpha) + sin(3\alpha) + ... + sin[(2n+1)\cdot\alpha] = \dfrac{1 - cos(2n\cdot\alpha + 2\alpha)}{2\cdot sin(\alpha)} = \dfrac{1 - cos(2n\cdot\alpha)cos(2\alpha) + sin(2n\alpha)sin(2\alpha)}{2\cdot sin(\alpha)}$

Dim. $sin(\alpha) + sin(3\alpha) + ... + sin[(2n-1)\cdot\alpha] + sin[(2n+1)\cdot\alpha] =$

$$\frac{1-cos(2n\cdot\alpha)}{2\cdot sin(\alpha)} + sin\left[(2n+1)\alpha\right] = \frac{1-cos(2n\cdot\alpha)+2sin(\alpha)sin\left[(2n+1)\alpha\right]}{2\cdot sin(\alpha)} =$$

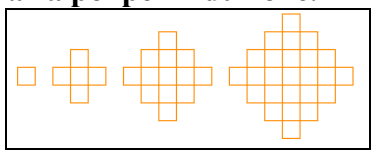
$$= \frac{1-cos(2n\cdot\alpha)+2sin(\alpha)\left[sin(2n\alpha)cos(\alpha)+cos(2n\alpha)sin(\alpha)\right]}{2\cdot sin(\alpha)} =$$

$$= \frac{1-cos(2n\cdot\alpha)+sin(2n\alpha)sin(2\alpha)+2cos(2n\alpha)sin^2(\alpha)}{2\cdot sin(\alpha)} =$$

$$= \frac{1-cos(2n\cdot\alpha)\cdot\left[1-2sin^2(\alpha)\right]+sin(2n\alpha)sin(2\alpha)}{2\cdot sin(\alpha)} =$$

$$= \frac{1-cos(2n\cdot\alpha)\cdot cos(2\alpha)+sin(2n\alpha)sin(2\alpha)}{2\cdot sin(\alpha)}$$

23. Le figure seguenti costituiscono una successione di poligoni, che prosegue sempre seguendo la stessa legge. Determinare quanti quadrati formano il poligono al passo *n* e dimostrarla poi per induzione.



[$2n^2 + 2n + 1$]

Nei primi passi abbiamo 1, 5, 13, 25. Osserviamo che a partire dal secondo passo, $n = 2$, i quadratini sono in numero di $1 + 1 + 3 = 2 \cdot 1 + 3 = 2 \cdot 1 + (2 \cdot 2 - 1) = 5$; $n = 3$: $2 \cdot (1 + 3) + 5 = 2 \cdot (1 + 3) + (2 \cdot 3 - 1) = 13$; $n = 4$: $2 \cdot (1 + 3 + 5) + 7 = 2 \cdot (1 + 3 + 5) + (2 \cdot 4 - 1) = 25$. Quindi in generale al passo n saranno $2 \cdot [1 + 3 + 5 + ... + (2n - 3)] + (2n - 1)$. Abbiamo $1 + 3 + 5 + ... + (2n - 3) = (n - 1)^2$ (lo proveremo per induzione). Quindi deve essere: $2(n - 1)^2 + 2n - 1 = 2n^2 - 4n + 2 + 2n - 1 = 2n^2 - 2n + 1$. Proviamo che $1 + 3 + 5 + ... + (2n - 1) = n^2$, che equivale a quello che vogliamo provare, ma ha più senso perché in quel caso per $n = 1$ $2n - 3 = -1 : 1 = 1^2$. Hp: $1 + 3 + 5 + ... + (2n - 1) = n^2$; Ts: $1 + 3 + 5 + ... + (2n + 1) = (n + 1)^2$. Infatti $1 + 3 + 5 + ... + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$.

Determina una legge che descriva le seguenti somme e provale per induzione

24. a) $1^2 = 1$; $2^2 - 1^2 = 3$; $3^2 - 2^2 + 1^2 = 6$; … b) $1 = 1^3$; $3 + 5 = 2^3$; $7 + 9 + 11 = 3^3$; …

a) $\sum_{k=1}^{n}(-1)^{k+1}(n+1-k)^2 = \frac{n(n+1)}{2}$. $n = 1 \Rightarrow 1^2 = 1$. Osserviamo che, indicando con $s(n)$ la somma di n addendi si ha: $s(n + 1) = (n + 1)^2 - s(n)$, quindi: $s(n + 1) = (n + 1)^2 - \frac{n(n+1)}{2} = (n+1)\cdot\frac{2n+2-n}{2} = \frac{(n+1)\cdot(n+2)}{2}$, ossia la tesi.

b) Ogni somma ha un addendo in più della precedente, così la seconda somma è $(2 \cdot 1 + 1) + (2 \cdot 2 + 1)$, la terza è $(2 \cdot 3 + 1) + (2 \cdot 4 + 1) + (2 \cdot 5 + 1)$; la quarta $(2 \cdot 6 + 1) + (2 \cdot 7 + 1) + (2 \cdot 8 + 1) + (2 \cdot 9 + 1)$. Quindi il primo addendo è $(2 \cdot T_{n-1} + 1)$ e l'ultimo $[2 \cdot (T_n - 1) + 1]$, in cui $T_n = \frac{n\cdot(n+1)}{2}$ è l'n-esimo numero triangolare. Pertanto il termine generale è

c) $\left(2\cdot\frac{(n-1)\cdot n}{2}+1\right)+\left[2\cdot\left(\frac{(n-1)\cdot n}{2}+1\right)+1\right]+\ldots+\left[2\cdot\left(\frac{n\cdot(n+1)}{2}-1\right)+1\right]=$

$=\left[(n-1)\cdot n+1\right]+\left[(n-1)\cdot n+3\right]+\ldots+\left[(n-1)\cdot n+2n-1\right]=$. Passiamo alla

$=\sum_{k=1}^{n}\left[(n-1)\cdot n+2k-1\right]=\sum_{k=1}^{n}\left[n^2-n+2k-1\right]$

dimostrazione per induzione: $n = 1 \Rightarrow 1 = 1^3$;

$\sum_{k=1}^{n+1}\left[n\cdot(n+1)+2k-1\right]-\sum_{k=1}^{n}\left[n^2-n+2k-1\right]=\sum_{k=1}^{n+1}\left[n\cdot(n+1)\right]+\sum_{k=1}^{n+1}\left[2k-1\right]-n^3=$

$=n\cdot(n+1)^2+(n+1)^2-n^3=\cancel{n^3}+2n^2+n+n^2+2n+1\cancel{-n^3}=3n^2+3n+1$

Ciò equivale a dire che la prima somma è $(n + 1)^3$, dato che $(n + 1)^3 – n^3 = 3n^2 + 3n + 1$.

25. 2 + 3 + 4 = 1 + 8; 5 + 6 + 7 + 8 + 9 = 8 + 27; 10 + 11 + … + 16 = 27 + 64; …

Gli addendi del primo membro vanno dal successivo di un quadrato al quadrato successivo, quindi da $n^2 + 1$ a $(n + 1)^2$; quelli del secondo membro invece sono somme di due cubi successivi cioè $n^3 + (n + 1)^3$, quindi: $\sum_{k=n^2+1}^{(n+1)^2} k=n^3+(n+1)^3$. Proviamola. 2 + 3 + 4 = 1 + 8.

$\sum_{k=(n+1)^2+1}^{(n+2)^2} k-\sum_{k=n^2+1}^{(n+1)^2} k=\left[(n+1)^2+1\right]+\left[(n+1)^2+2\right]+\ldots+\left[(n+1)^2+2n+3\right]-\left[n^3+(n+1)^3\right]=$

$=(n+1)^2\cdot(2n+3)+\frac{(2n+3)\cdot(2n+4)}{2}-n^3-n^3-3n^2-3n-1=$

$= (2n + 3)\,[(n + 1)^2 + n + 2) – 2n^3 – 3n^2 – 3n – 1 = (2n + 3)(n^2 + 3n + 3) – 2n^3 – 3n^2 – 3n – 1 = 2n^3 + 9n^2 + 15n + 9 – 2n^3 – 3n^2 – 3n – 1 = 6n^2 + 12n + 8$. Ed effettivamente $(n + 2)^3 – n^3 = 6n^2 + 12n + 8$

Bibliografia

Beiler A. H., *Recreations in the theory of numbers*, Dove, New York, 1964

Courant R. Robbins H. *Che cos'è la matematica?*, Boringhieri, Torino 1971.

Di Stefano C., *Zero*, Nuova Secondaria, nn. 8 – 9, Aprile – Maggio 1999.

Ore O., *Number theory and its history*, Dover, New *Y*ork, 1988

Polya G., *La scoperta matematica*, in due volumi, Feltrinelli, Milano 1971.

Polya G., *Come risolvere i problemi di matematica*, Feltrinelli, Milano 1969.

Polya G., *Induction and analogy in mathematics,* 2 vol., Princeton University Press, 1954