ARITMETICA

Un importante ramo della matematica è l'*aritmetica*, o *teoria dei numeri*, qui intesi come numeri interi. Ci si pone il problema di stabilire se certe relazioni possano essere soddisfatte da numeri interi, e in quanti modi ciò sia possibile.
Uno strumento essenziale per questa materia è il *principio di induzione.* Questo fa parte degli Assiomi di Peano per l'introduzione dei numeri naturali; può essere enunciato in varie forme equivalenti. La più adeguata alle applicazioni dimostrative di teoremi sui numeri interi è la seguente:

Sia $P(n)$ *una proposizione riguardante il numero intero n. Se avviene che:*

- *Esiste un numero intero* n_0 *tale che* $P(n_0)$ *è vera.*
- •• $P(n) \Rightarrow P(n+1)$*, cioè dalla supposizione della verità di* $P(n)$ *per un determinato n si può dedurre la verità di* $P(n+1)$

allora $P(n)$ *è vera per ogni numero intero* $n \geq n_0$.

Qualche volta è utile una forma leggermente diversa del principio di induzione, che appare più debole di quella classica sopra ricordata, ma in effetti è ad essa equivalente. Si tratta di sostituire la seconda richiesta (••) con

••• $\left(\forall k \left(n_0 \leq k \leq n \Rightarrow P(k)\right)\right) \Rightarrow P(n+1)$.

Rispetto a (•••) la differenza consiste nel fatto che l'*ipotesi induttiva* appare rafforzata: per dedurre $P(n+1)$ non si suppone più soltanto la verità di $P(n)$ ma, di più, si vuole che sia vera $P(k)$ per ogni *k* compreso tra n_0 e *n.* Sono abbastanza rare le occasioni in cui è necessario ricorrere a questa forma particolare del principio di induzione, che viene ricordata come "induzione completa".

Vediamo alcuni esempi.

Problema 1 (la disuguaglianza di Bernoulli). *Se* x *è un numero reale* ≥ -1*, allora per ogni numero naturale* $n \geq 1$ *risulta* $(1+x)^n \geq 1+nx$.

Dimostrazione. Qui $P(n)$ è l'affermazione «$(1+x)^n \geq 1+nx$». Solo *n* ha il ruolo di effettiva variabile, in quanto *x* viene pensato come un valore fissato. Seguiamo i due passi indicati per la dimostrazione per induzione.

1) $P(1)$ dice: $(1+x)^1 \geq 1+1\cdot x$. Questa è vera, perché i due membri sono uguali.

2) Supponiamo verificata $P(n)$ per un *n*, e cerchiamo di dedurre che è vera $P(n+1)$, la quale dice: $(1+x)^{n+1} \geq 1+(n+1)x$. Ebbene, si ha

$$(1+x)^{n+1} = (1+x)^n \cdot (1+x) \geq (1+nx)\cdot(1+x)$$

perché $P(n)$, che stiamo assumendo per ipotesi, dice che $(1+x)^n \geq 1+nx$, e $1+x \geq 0$ perché $x \geq -1$. Svolgiamo i calcoli all'ultimo membro, e otteniamo

$$(1+x)^{n+1} \geq 1+nx+x+nx^2 = 1+(n+1)x+nx^2 \geq 1+(n+1)x$$

perché $nx^2 \geq 0$.

Problema 2. *Dimostrare che per ogni numero naturale* n *abbastanza grande, è* $2^n > n^{100}$

Soluzione. È possibile dimostrare l'affermazione applicando la disuguaglianza di Bernoulli. La disuguaglianza in oggetto equivale a: $\left(2^{\frac{1}{200}}\right)^n > n$. Ora osserviamo che $2^{\frac{1}{200}} > 1$; possiamo quindi scrivere $2^{\frac{1}{200}} = 1+x$ con $x = 2^{\frac{1}{200}} - 1 > 0$. Abbiamo allora

$$\left(2^{\frac{1}{200}}\right)^n = (1+x)^n \geq 1+nx \left(\text{disuguaglianza di Bernoulli}\right) > nx .$$

Allora:

$$2^n > n^{200} x^{200} = \left(nx^2\right)^{100} \cdot n^{100} .$$

Per realizzare la disuguaglianza desiderata è sufficiente che sia $nx^2 > 1$, cioè $n \geq \frac{1}{x^2} = \frac{1}{\left(2^{\frac{1}{200}} - 1\right)^2}$.

Il procedimento esposto si può generalizzare per dimostrare che, se *a* è un numero reale ≥ 1 e *p* un numero naturale qualunque, allora $a^n > n^p$ per tutti gli *n* abbastanza grandi; cioè qualunque funzione esponenziale con base maggiore di 1 supera, prima o poi, qualunque funzione potenza.

Il principale difetto operativo del principio di induzione consiste nel fatto che esso dà uno strumento per dimostrare teoremi, ma non è di alcun aiuto per *scoprire* questi teoremi: occorre avere già formulato una congettura, e per induzione si potrà cercare di provarla.

Qualche volta è possibile giungere a una congettura "per tentativi"; poi si dovrà procedere alla dimostrazione. Per esempio:

Problema 3. *Determinare per ogni numero naturale* $n \geq 1$ *il valore dell'espressione* $S_n = \sum_{k=1}^{n} k! \cdot k$.

Soluzione. Calcoliamo materialmente i valori di S_n per alcuni valori di *n*, nella speranza di riconoscere qualche regolarità nei risultati, e cercare poi di dimostrare la validità generale delle regola scoperta.

Ecco che cosa si ottiene; la terza riga della tabella contiene l'«interpretazione» del risultato, da cui la formula che poi dimostreremo.

n	1	2	3	4	5	6
S_n	1	5	23	119	719	5039
$S_n =$	2!–1	3!–1	4!–1	5!–1	6!–1	7!–1

Per tutti gli *n* compresi tra 1 e 6 risulta dunque $S_n = \sum_{k=1}^{n} k! \cdot k = (n+1)! - 1$. Cerchiamo di dimostrare per induzione che tale formula è valida per ogni $n \in \mathbf{N}$. Il primo passo ($P(1)$ è vera) è già stato svolto; vediamo se risulta $P(n) \Rightarrow P(n+1)$. $P(n+1)$ dice:

$$S_{n+1} = \sum_{k=1}^{n+1} k! \cdot k = (n+2)! - 1.$$

Supponiamo di sapere che $S_n = \sum_{k=1}^{n} k! \cdot k = (n+1)! - 1$; allora avremo

$$S_{n+1} = \sum_{k=1}^{n+1} k! \cdot k = \underbrace{\sum_{k=1}^{n} k! \cdot k}_{=(n+1)!-1} + (n+1)! \cdot (n+1) = (n+1)! - 1 + (n+1)! \cdot (n+1)$$

$$= (n+1)! - 1 + (n+1)! \cdot (n+1) = (n+1)!(n+2) - 1 = (n+2)! - 1$$

come volevamo dimostrare.

Naturalmente, non sempre è facile intuire la formula corretta dai tentativi fatti su pochi valori di *n*; e non sempre la regola che si crede di intuire dai tentativi su alcuni valori di *n* è corretta; in questo caso naturalmente la dimostrazione per induzione non potrà avere successo. È piuttosto noto l'esempio dei

cosiddetti *numeri primi di Fermat.* Fermat era convinto che fossero primi tutti i numeri interi della forma $2^{2^n}-1$, con *n* intero non negativo. In effetti è così per $n=0,1,2,3,4$; invece $2^{2^5}-1$ non è primo; fu Leonhard Euler nel 1732 a trovare una fattorizzazione di questo numero: $2^{32}-1=641\cdot 6700417$.

La tecnica mostrata nel precedente problema 3 si applica tutte le volte in cui si vuole dimostrare per induzione una formula che esprime in forma chiusa il valore di una sommatoria. Ecco alcune formule relative a somme di qualche importanza in certe applicazioni; ciascuna di esse può facilmente essere provata per induzione:

$$\sum_{k=1}^{n}(2k-1)^2=\frac{4n^3-n}{3};\quad \sum_{k=1}^{n}k=\frac{n(n+1)}{2};\quad \sum_{k=1}^{n}k^2=\frac{2n^3+3n^2+n}{6};\quad \sum_{k=1}^{n}k^3=\frac{\left(n^2+n\right)^2}{4}.$$

Problema 4. *Dimostrare che la successione definita da:* $a_1=1$; $a_{n+1}=\sqrt{2+a_n}$ *è crescente e superiormente limitata;determinare infine il suo limite.*

L'affermazione "(a_n) è crescente" significa che, per ogni *n*, $a_{n+1}\ge a_n$. Quest'ultima disuguaglianza è la proposizione $P(n)$ che si vuole dimostrare vera per ogni *n.*

$P(1)$ dice: $a_2\ge a_1$, cioè $\sqrt{3}\ge 1$: vero.

Supponiamo $P(n)$ vera per un *n.* $P(n+1)$ dice: $a_{n+2}\ge a_{n+1}$. Tenendo presente la definizione ricorsiva della successione, questa disuguaglianza equivale a $\sqrt{2+a_{n+1}}\ge\sqrt{2+a_n}$, la quale è vera perché stiamo supponendo vera $P(n)$, ossia $a_{n+1}\ge a_n$. È così provato che (a_n) è una successione crescente.

Per quanto riguarda una limitazione superiore, dobbiamo "indovinare" un valore idoneo *M*, e poi cercare di dimostrare la maggiorazione $a_n\le M$ per ogni *n.* Il calcolo diretto dei primi valori di a_n mostra che tutti sono <2. Proviamo a dimostrare che $a_n<2$ per ogni *n.* Ciò è vero per $n=1$; supponendo $a_n<2$ per un *n*, segue che $a_{n+1}=\sqrt{2+a_n}<\sqrt{2+2}=2$, e quindi è provato per induzione che $a_n<2$ per ogni *n.*

Infine, il limite di a_n è un numero ℓ tale che $\ell=\sqrt{2+\ell}$, quindi $\ell^2-\ell-2=0$; questa relazione è soddisfatta da $\ell=-1$ oppure $\ell=2$; ma poiché (a_n) è crescente e $a_1=1$, si conclude che $\ell=2$.

Divisione euclidea. Siano *a*, *b* numeri interi, $a\ne 0$. Allora esistono e sono unici due numeri interi *q*, *r* tali che:

(1) $b=a\cdot q+r$

(2) $0\le r<|a|$

q e *r* si chiamano *quoziente* e *resto* della divisione intera di *b* per *a.*

Divisibilità. Si dice che *a* è un *divisore* di *b* (scriveremo $a|b$) se vale (1) con $r=0$.

Ogni numero intero diverso da zero ha qualche divisore: ±1, ±*b* sono divisori di *b.* Ce ne possono essere altri, oppure no.

Numeri primi. Un numero intero $p\ge 2$ si dice *primo* se gli unici divisori positivi di *p* sono 1 e *p.*

Ci sono infiniti numeri primi. Questo fatto è già noto a Euclide, che ne dà una elegante dimostrazione per assurdo.

I numeri primi, oltre che nel modo su indicato, possono essere caratterizzati diversamente, mediante una proprietà che risulta spesso utile nelle applicazioni:

Se *p* è un numero primo, e *a*, *b* sono numeri interi diversi da 0, allora

(*) $$p|(a\cdot b)\ \Rightarrow\ p|a \text{ oppure } p|b.$$

Questa proprietà *caratterizza* i numeri primi, ossia vale anche viceversa: se per ogni coppia di numeri interi *a*, *b* diversi da 0 vale (*), allora *p* è primo.

Se *p* non è primo, (*) non è vera: per esempio $6|(15\cdot 4)$, ma 6 non è divisore di 15 né di 4.

Ecco un esempio di un facile problema sulla divisibilità, che può essere risolto applicando il principio di induzione.

Problema 5. *Dimostrare che, per ogni numero naturale n, il numero* 4^n-1 *è divisibile per 3.*

Più in generale: se a è un numero naturale qualunque (≥ 1) *allora* a^n-1 *è divisibile per* $a-1$.

Soluzione. La risoluzione più rapida si ottiene applicando le congruenze modulo *m*; qui vogliamo esporre una risoluzione che non utilizza questo strumento.

Osserviamo che il problema "generale" appare, circostanza inconsueta, più facile da risolvere del caso particolare che lo precede; infatti, osservando *a* come indeterminata il polinomio a^n-1 è divisibile per $a-1$ per il Teorema di Ruffini, e il polinomio quoziente ha coefficienti interi; se ora *a* assume il valore di un numero intero, la fattorizzazione $a^n-1=(a-1)\cdot q(a)$ mostra a^n-1 come prodotto di $a-1$ per un altro numero intero.

Altrimenti possiamo applicare il principio di induzione. Ci riferiamo al caso $a=4$; il caso generale si tratta nella stessa maniera. La proposizione

$$P(n):\ \text{“}4^n-1 \text{ è divisibile per 3”}$$

è vera per $n=1$ perché $4^1-1=3$. Supponiamo vera $P(n)$ per un *n*, e mostriamo che allora è vera $P(n+1)$, cioè $4^{n+1}-1$ è divisibile per 3. Risulta

$$4^{n+1}-1 \;=\; 4^{n+1}-4+3 \;=\; \underbrace{4\left(4^n-1\right)}_{\text{multiplo di } 3}+3$$

da cui risulta evidente che l'espressione ottenuta rappresenta un multiplo di 3. L'informazione che abbiamo utilizzato, che 4^n-1 sia multiplo di 3, è l'ipotesi di induzione.

Problema 6. *Sia* $x_0=2$ *e, per ogni* $n\in\mathbf{N}$, $x_{n+1}=5+x_n^2$. *Mostrare che nessun termine della successione è un numero primo, ad eccezione di* $x_0=2$.

Soluzione. La formula di ricorrenza mostra che i termini della successione sono numeri interi alternativamente pari e dispari. Siccome $x_0=2$ è pari, tutti i termini di posto pari sono numeri pari, ed essendo maggiori di 2, non sono primi. Andiamo a vedere come sono i termini di posto dispari. È utile ricavare una formula di ricorrenza che esprima ciascun termine della successione non in funzione del precedente, bensì di quello che o precede di due posti. Risulta

$$x_{n+2} \;=\; 5+x_{n+1}^2 \;=\; 5+\left(5+x_n^2\right)^2 \;=\; 30+10\,x_n^2+x_n^4$$

Ora è facile provare per induzione che tutti i termini x_n con *n* dispari sono multipli di 3 e maggiori di 3, quindi non primi. Intanto, direttamente si calcola $x_1=5+2^2=9$, che soddisfa la proprietà; poi, se supponiamo che x_n sia multiplo di 3, dalla formula $x_{n+2}=30+10\,x_n^2+x_n^4$ segue che anche x_{n+2} è multiplo di 3, perché tali sono tutti e tre gli addendi che formano il valore di x_{n+2}.

Fattorizzazione. Ogni numero intero $n\geq 2$ si può fattorizzare in uno e un solo modo, a meno dell'ordine, in prodotto di potenze di numeri primi:

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$$

con $p_1,\ldots,p_k$ numeri primi distinti e $\alpha_1,\ldots,\alpha_n$ interi ≥ 1, gli uni e gli altri univocamente determinati.

Ecco un esempio in cui utilizziamo questi fatti

Problema 7. *Quante sono le terne di numeri interi positivi* (x,y,z) *che soddisfano la relazione:*

(#) $$2x+17y+34z=2006\ ?$$

Soluzione. È utile fattorizzare il numero 2006 in prodotto di potenze di numeri primi. La fattorizzazione si realizza controllando la divisibilità di 2006 per i numeri primi, fino al raggiungimento di $\sqrt{2006}$, il cui valore è minore di 45; infatti $45^2=2025$. I fattori primi di 2006, escluso al più uno, sono tutti non superiori a 43. Si trova che $2006=2\cdot17\cdot59$ cosicché (#) si può scrivere

$$2x+17y+34z=2\cdot17\cdot59\,.$$

Tre fattori su quattro contengono il fattore 17; può essere utile metterlo in evidenza, scrivendo quest'ultima relazione nella forma

(##) $$2x\ =\ 17\left(2\cdot59-y-2z\right).$$

La (##) dice che $17\left|(2x)\right.$, e siccome 17 è primo, ciò comporta $17\left|2\right.$ oppure $17\left|x\right.$. Poiché non è vero che $17\left|2\right.$, deve essere $17\left|x\right.$, cioè esiste un numero intero positivo x' tale che $x=17x'$. Sostituiamo x con $17x'$ in (##), e semplifichiamo il fattore 17. Otteniamo la relazione:

$$2x'\ =\ 2\cdot59-y-2z$$

dalla quale si ricava

$$y\ =-2x'+2\cdot59-2z\,.$$

Questa manifesta il fatto che y deve essere pari; indichiamo quindi $y=2y'$. In questo modo la relazione scritta sopra si può esprimere nel modo seguente:

(§) $$x'+y'+z\ =\ 59$$

nella quale $x',\ y',\ z$ indicano numero interi positivi. Non resta che contare in quanti modi si possono scegliere $x',\ y',\ z$. Se $x'=1$ il valore di y' si può scegliere in 57 modi (da 1 a 57); infine z risulta univocamente determinato come $59-x'-y'$; se $x'=2$ ci sono 56 modi possibili per scegliere y' e z; e così via fino a quando $x'=57$, che lascia per y' e z l'unica scelta $y'=z=1$. Il numero di terne $x',\ y',\ z$ di numeri interi positivi, soddisfacenti (§) è pertanto

$$57+56+55+\ldots+3+2+1\ =\ \frac{57\cdot58}{2}\ =\ 1653\,.$$

Problema 8. *Dimostrare che, comunque si prendano 18 numeri interi positivi consecutivi minori o uguali a 2005, ce n'è almeno uno divisibile per la somma delle sue cifre.* (Cesenatico, 6 maggio 2005).

Soluzione. Il problema non chiede di trovare *tutti* i numeri minori o uguali a 2005 aventi questa proprietà, ma soltanto di mostrare che se ne trova almeno uno ogni 18 consecutivi. Tra 18 numeri interi consecutivi ci sono sempre due consecutivi multipli di 9. La somma delle cifre di ciascuno di essi è a sua volta un multiplo di 9, per il noto criterio di divisibilità. La somma delle cifre di un numero intero ≤ 2005 è al massimo 28 (somma delle cifre di 1999); quindi la somma delle cifre di un multiplo di 9 non superiore a 2005 può essere 9, 18 o 27.

Se tra i due multipli di 9 compresi nell'intervallo considerato ce n'è uno per il quale la somma delle cifre è 9, questo è divisibile per la somma delle sue cifre, essendo multiplo di 9.

Se per entrambi la somma delle cifre è 18, basta osservare che tra due consecutivi multipli di 9 uno è pari, quindi è divisibile per 18.

Se la somma delle cifre è 27, il numero è uno tra 999, 1899, 1989, 1998. Ebbene, 999 e 1998 sono divisibili per 27. 1899 non è divisibile per 27, ma 1890 è divisibile per $1+8+9=18$ come pure 1908; un intervallo di 18 interi contenente 1899 contiene anche uno dei due numeri 1890 e 1908. 1989 non è divisibile per 27, ma 1980 è divisibile per 18, somma delle sue cifre, e 1998 è divisibile per 27, somma delle sue cifre.

Problema 9. *Dimostrare che, per ogni numero naturale n, la frazione $\frac{21n+4}{14n+3}$ è irriducibile.*

Soluzione. Indichiamo con q un divisore comune di $21n+4$ e $14n+3$; cerchiamo di dimostrare che deve essere $q=1$.

Ogni combinazione lineare con coefficienti interi di $21n+4$ e $14n+3$ è un multiplo di q; informazioni decisive su q si ottengono trovando combinazioni lineari che non contengono n. Ebbene, si osserva che

$$3(14n+3)-2(21n+4)=1$$

quindi $q|1$, e di conseguenza $q=1$, come volevamo dimostrare.

L'argomento utilizzato per risolvere questo problema ricorda da vicino il *Teorema di Bezout* sul massimo comune divisore:

Teorema di Bezout. *Se a, b sono due numeri interi diversi da zero, e d è il massimo comune divisore tra a e b, allora esistono (non unici) due numeri interi m, n tali che*

(°) $$d = ma+nb$$

La determinazione di m, n soddisfacenti (°) si può realizzare con il metodo delle *divisioni euclidee iterate.* Questo, oltre a determinare d, permette di risolvere anche il problema della determinazione di m, n. Vediamo un esempio in un caso numerico: $a=44$, $b=34$. Scriviamo la relazione corrispondente alla divisione euclidea, $a=b\cdot q+r$, in cui q e r sono il quoziente e il resto della divisione di a per b:

$$\underline{44} = \underline{34}\cdot 1+\underline{10}$$

Abbiamo sottolineato dividendo, divisore e resto.

Adesso calcoliamo nuovamente una divisione intera, assumendo come dividendo il quoziente ottenuto sopra e come divisore il resto:

$$\underline{34} = \underline{10}\cdot 3+\underline{4}$$
$$\underline{10} = \underline{4}\cdot 2+\underline{2}$$

Il procedimento della determinazione del massimo comune divisore ha termine quando il quoziente ottenuto è multiplo del resto, come accade nell'ultima riga che abbiamo scritto. L'ultimo resto, qui 2, è il massimo comune divisore tra a e b.

Utilizzando opportunamente i calcoli svolti sopra è possibile ricavare m, n come desiderati. Da ciascuna uguaglianza ricaviamo il *resto:*

$$\underline{44} = \underline{34}\cdot 1+\underline{10} \;\Rightarrow\; \underline{10}=\underline{44}-\underline{34}\cdot 1$$
$$\underline{34} = \underline{10}\cdot 3+\underline{4} \;\Rightarrow\; \underline{4}=\underline{34}-\underline{10}\cdot 3$$
$$\underline{10} = \underline{4}\cdot 2+\underline{2} \;\Rightarrow\; \underline{2}=\underline{10}-\underline{4}\cdot 2$$

Adesso prendiamo l'ultima uguaglianza ottenuta; nell'ultimo addendo del secondo membro figura il resto della divisione precedente; lo sostituiamo con la sua espressione tratta dalla riga superiore, e così via:

$$\underline{2}=\underline{10}-\underline{4}\cdot 2 = \underline{10}-(\underline{34}-\underline{10}\cdot 3)\cdot 2 = \underline{10}\cdot 7-\underline{34}\cdot 2;\ \text{ora } \underline{10}=\underline{44}-\underline{34}\cdot 1 \text{ e quindi:}$$
$$=(\underline{44}-\underline{34}\cdot 1)\cdot 7-\underline{34}\cdot 2 = \underline{44}\cdot 7-\underline{34}\cdot 9.$$

Abbiamo così scritto 2, che è il massimo comune divisore tra 44 e 34, come combinazione lineare di questi due numeri con coefficienti interi, come desideravamo.

Questa rappresentazione del M.C.D. di due numeri serve per risolvere problemi abbastanza classici di aritmetica, riguardanti misurazioni di pesi o volumi con strumenti che apparentemente non sembrano idonei allo scopo. Ecco un paio di esempi.

Problema 10. *Disponendo di due recipienti non graduati, di capacità rispettivamente 44 e 34 litri, e di una fontana che fornisce tanta acqua quanta se ne vuole, si desidera ottenere, in uno dei due recipienti, esattamente 2 litri d'acqua. Come si può fare?*

Soluzione. Indichiamo con a il recipiente da 44 litri, con b quello da 34. Abbiamo visto sopra che $2=44\cdot 7-34\cdot 9$. Allora procediamo così: riempiamo interamente a e subito versiamo da a fino a riempire b; quando b è pieno, buttiamo via l'acqua che contiene e poi versiamo in b l'acqua che ancora resta in a (10 litri), senza buttarla via. Riempiamo ancora a, e versiamo da a in b fino a colmare b. Quando b è pieno, lo svuotiamo buttando via il contenuto, poi versiamo in b l'acqua che era rimasta in a. Continuiamo in questo modo: riempiamo a ogni volta che è vuoto; versiamo in b l'acqua di a fino al

completo riempimento di *b*; buttiamo via l'acqua di *b* ogni volta che *b* è pieno. Quando *a* sarà stato riempito per la settima volta, con parte dei 44 litri d'acqua contenuti colmeremo prima *b* per la ottava volta, poi, dopo averlo svuotato, riempiremo *b* per la nona volta. A questo punto in *a* saranno rimasti due litri d'acqua.

Problema 11. *Avendo a disposizione soltanto una bilancia a due piatti, due pesi da 8 e 5 Kg e tanta farina quanta se ne desidera, pesare 1 Kg di farina.*

Soluzione. Il problema si può risolvere perché $\text{M.C.D.}(8,5)=1$. Serve scrivere 1 come combinazione lineare di 8 e 5 con coefficienti interi. Quando i numeri in gioco sono piccoli come nel caso attuale, questa si può trovare abbastanza facilmente "per tentativi", senza ricorrere al metodo algoritmico descritto sopra. Per esempio, $1=8\times 2-5\times 3$. Allora possiamo pesare 8 Kg di farina e metterli da parte; altri 8 Kg di farina, e metterli insieme ai precedenti 8, per avere una misura di 16 Kg di farina. Da questi 16 Kg preleviamo ora per tre volte 5 Kg; la rimanenza sarà di 1 Kg.
L'espressione $\text{M.C.D}(a,b)=na+mb$, come abbiamo già osservato, non è unica, nel senso che non sono unici *m* e *n* che soddisfano la relazione. Per esempio, nel caso di 8 e 5 risulta anche $1=5\times 5-3\times 8$; questa relazione suggerisce un'altra possibile risoluzione del problema considerato: cinque pesate da 5 Kg ciascuna, per accumulare 25 Kg di farina, e poi otto pesate da 3 Kg ciascuna per togliere 24 Kg; il metodo è meno efficiente di quello descritto sopra perché richiede un maggiore numero di pesate e una maggiore quantità di farina da movimentare (25 Kg anziché 16).

Il numero dei divisori di un numero intero.

Se *n* è un numero intero maggiore di 1, indichiamo con $d(n)$ il numero dei divisori di *n* (inclusi 1 e *n*).
Per esempio, $d(12)=6$; infatti i divisori di 12 sono 1, 2, 3, 4, 6, 12, in tutto sei.
Come si calcola $d(n)$? Vediamo. Un numero naturale $n\geq 2$ è prodotto di potenze di numeri primi:

$$n = 2^{r_2}\cdot 3^{r_3}\cdot 5^{r_5}\cdot 7^{r_7}\cdot\ldots$$

dove in effetti figurano soltanto i fattori p^{r_p} in cui l'esponente r_p è maggiore di zero; sarà quindi

$$n = p_1^{r_{p1}}\cdot p_2^{r_{p2}}\cdot p_3^{r_{p3}}\cdot\ldots\cdot p_r^{r_{ph}} \tag{1}$$

per certi numeri primi $p_1,\ldots,p_h$ ed altrettanti esponenti positivi $r_{p_1},\ldots,r_{p_h}$.
Un numero *m* è divisore di *n* se si può fattorizzare *m* con gli stessi fattori primi di *n* o soltanto alcuni di essi, ma nessun altro, con esponenti minori o uguali di quelli che appaiono nella fattorizzazione di *n*; vale a dire che un divisore di *n* è

$$m = p_1^{s_{p1}}\cdot p_2^{s_{p2}}\cdot p_3^{s_{p3}}\cdot\ldots\cdot p_h^{s_{ph}} \tag{2}$$

in cui, per $0\leq i\leq h$, s_{p_i} è un numero intero tale che $0\leq s_{p_i}\leq r_{p_i}$. Per ciascun fattore primo p_i ci sono dunque $r_{p_i}+1$ modi di scegliere il corrispondente esponente per ottenere un divisore di *n*. Segue dunque che

$$d(n) = \left(r_{p_1}+1\right)\cdot\left(r_{p_2}+1\right)\cdot\ldots\cdot\left(r_{p_h}+1\right). \tag{3}$$

La (3) manifesta alcune proprietà interessanti di $d(n)$:

1) $d(n)$ non dipende da *quali* sono i fattori primi di *n*, ma soltanto da *quanti* sono, e con quali esponenti figurano nella fattorizzazione di *n*.

2) $d(n)$ è dispari se e solo se tutti gli esponenti r_{p_i} che figurano nella (1) sono pari, cioè se *n* è un quadrato.

Inoltre può essere utile osservare che

3) $d(2)=2$; $d(n)<n$ per ogni $n\geq 3$**.**

Infatti i divisori di *n* appartengono all'insieme $\{1,2,\ldots,n\}$, e in generale non sono tutti questi numeri; anzi, sono tutti solo se $n=2$, perché se $n\geq 3$ allora $n-1$ non è divisore di *n*.

4) Per ogni coppia di numeri naturali $m,n\geq 2$ risulta $d(m\cdot n)\leq d(m)\cdot d(n)$; vale l'uguaglianza se e solo se *m* e *n* sono primi tra loro o *coprimi*, ossia non hanno alcun divisore comune tranne 1.

Infatti, consideriamo i due casi:

I) *m* e *n* sono primi tra loro. Allora la fattorizzazione (1) di *n* e l'analoga fattorizzazione di *m* sono non hanno alcun fattore primo comune; in tal caso la fattorizzazione di $m\cdot n$ contiene tutti i fattori primi di *n* e tutti i fattori primi di *n*, ciascuno con lo stesso esponente che aveva nella fattorizzazione di *m* o di *n*. $d(m\cdot n)$ è dato allora dal prodotto di tutti i fattori $\left(r_{p_i}+1\right)$ che costituiscono $d(n)$ e di tutti i fattori analoghi che costituiscono $d(m)$; dunque $d(m\cdot n)=d(m)\cdot d(n)$.

II) *m* e *n* hanno qualche divisore comune maggiore di 1. Allora almeno uno dei fattori primi di *n* è anche fattore di *m*; sia *p* questo primo. Nella fattorizzazione (1) di *n* figura una potenza p^r, in quella di *m* la potenza p^s, con *r*, *s* interi positivi. Tra i fattori costituenti $d(n)$ di (3) c'è $r+1$; tra gli analoghi fattori che producono $d(m)$ c'è $s+1$. Nella fattorizzazione di $m\cdot n$ il fattore primo *p* appare con esponente $r+s$, cosicché nello sviluppo analogo a (3) di $d(m\cdot n)$ appare il fattore $(r+s+1)$, il quale prende il posto dei fattori $(r+1)$, $(s+1)$ che appaiono nella formazione di $d(n)$, $d(m)$ rispettivamente. Ebbene, $(r+1)(s+1)=rs+r+s+1>r+s+1$, e quindi $d(n)\cdot d(m)>d(m\cdot n)$.

La funzione $d(n)$ può essere oggetto di problemi vari, o può essere strumento utile per risolverne altri; ecco un paio di esempi.

Problema 12. Sia n_0 un numero naturale ≥ 4. Poniamo $a_1=d(n_0)$ e per ogni $k\geq 1$, $a_{k+1}=d(a_k)$. Mostrare che la successione (a_k) contiene almeno un quadrato.

Soluzione. Poiché per ogni $n\geq 3$ è $d(n)<n$, la successione (a_k) è strettamente decrescente fino a quando non raggiunge il valore 2, dopo di che rimane costante. Sia a_m il primo termine della successione che vale 2; allora a_{m-1} è un numero primo dispari, e quindi è dispari il numero di divisori di a_{m-2}; questo, come abbiamo osservato in precedenza, equivale a dire che a_{m-2} è un quadrato.

Problema 13. Stabilire se esistono, e in caso affermativo, quali sono, il più piccolo e il più grande numero intero positivo aventi esattamente 10 divisori.

Soluzione. Certamente non esiste il *massimo* dell'insieme dei numeri che hanno 10 divisori: se *p* è un numero primo, p^9 ha 10 divisori; poiché i numeri primi sono infiniti, *p* si può prendere grande a piacere. Il minimo invece esiste certamente, perché ogni sottoinsieme non vuoto di **N** ha minimo. Cerchiamo di calcolare questo minimo. Sia *n* un numero naturale con esattamente 10 divisori, cioè $d(n)=10$. Ciò significa che *n* si può scomporre in fattori primi nella forma

$$n=p_1^{r_{p_1}}\cdot p_2^{r_{p_2}}\cdot p_3^{r_{p_3}}\cdot\ldots\cdot p_r^{r_{p_h}}$$

e che

(*) $$10=d(n)=\left(r_{p_1}+1\right)\cdot\left(r_{p_2}+1\right)\cdot\ldots\cdot\left(r_{p_h}+1\right).$$

Poiché $10=2\cdot 5$, la (*) si può realizzare in due soli modi:

- Con un solo fattore: $10=(9+1)$. Ciò significa che $n=p^9$ con *p* numero primo. Il più piccolo valore di *n* esprimibile in questo modo è $n=2^9=512$.
- •• Con due fattori: $10=(1+1)(4+1)$. Ciò significa che $n=p^1\cdot q^4$ con *p*, *q* numeri primi distinti. Il più piccolo valore di *n* esprimibile in questo modo è $n=3^1\cdot 2^4=48$, il quale è anche la soluzione del nostro problema.

Il problema può naturalmente essere proposto con un altro valore *k* al posto di 10, e la risoluzione si svolge analogamente a come abbiamo proceduto sopra. I casi da considerare dipendono non tanto da come è grande *k*, quanto da come *k* si fattorizza.

Il principio della discesa infinita. L'osservazione contenuta nella risoluzione del precedente problema, che ogni sottoinsieme non vuoto di **N** ha minimo, equivale in sostanza al cosiddetto *principio della discesa infinita:*

Se $(k_n)_{n\in\mathbf{N}}$ *è una successione non crescente di numeri naturali allora, da un certo* n *in poi,* k_n *è costante.*

Infatti l'insieme $\{k_n\,;\, n\in\mathbf{N}\}$ ha minimo, sia *m* il minimo; sia n_0 il primo valore di *n* per cui $k_n = m$. Allora per ogni $n \ge n_0$ deve essere $k_n \ge m$ perché *m* è il minimo valore assunto dalla successione; ma anche $k_n \le k_{n_0} = m$ perché la successione è non decrescente; dunque $k_n = m\ \forall n \ge n_0$.

Questa osservazione apparentemente banale riesce talvolta utile per provare la *falsità* di proposizioni riguardanti i numeri naturali; una specie di "principio di induzione in negativo". Precisamente: sia $P(n)$ una proposizione riguardante il numero naturale *n*, di cui si vuole provare la *falsità per qualunque valore di n.* Si può allora supporre "per assurdo" che esista un valore di *n* per il quale $P(n)$ sia vera, e cercare di dimostrare che se $P(n)$ è vera per un *n*, allora esiste $n_1 < n$ tale che è vera anche $P(n_1)$. Iterando il ragionamento si concluderebbe l'esistenza di infiniti numeri naturali $n_j < n$ per i quali $P(n_j)$ è vera, e questo è impossibile perché non ci sono infiniti numeri naturali minori di *n.* Ecco un semplice esempio:

Problema 14. *Mostrare che non esistono quattro numeri naturali x, y, z, w (non tutti uguali a zero) tali che*

$$x^2+y^2 = 3(z^2+w^2). \tag{\#}$$

Soluzione. Supponiamo, contrariamente alla tesi, che quattro numeri siffatti esistano. In particolare, risulta che x^2+y^2 è multiplo di 3. Ora, questa proprietà può valere se e solo se *x* e *y* sono entrambi multipli di 3. Infatti, se *k* è un numero naturale risulta

$$(3k+1)^2 = 9k^2+6k+1\,; \qquad (3k+2)^2 = 9k^2+12k+4\,.$$

Si nota che la somma dei quadrati di due numeri non multipli di 3 dà in ogni caso resto 2, nella divisione per 3 (questa verifica riesce ancora più semplicemente applicando l'aritmetica "modulo 3", di cui parleremo tra poco).

Dunque *x* e *y* sono multipli di 3; siano $x = 3x',\ y = 3y'$. La relazione (#) si scrive allora

$$9x'^2+9y'^2 = 3(z^2+w^2) \qquad \text{ossia} \qquad z^2+w^2 = 3(x'^2+y'^2)\,.$$

I quattro numeri z, w, x', y' soddisfano quindi a loro volta la relazione (#), e $z^2+w^2 < x^2+y^2$. Chiamiamo $n_1 = x^2+y^2,\ n_2 = z^2+w^2$. È $n_2 < n_1$. Il ragionamento può proseguire nello stesso modo, deducendo che $z = 3z',\ w = 3w'$, quindi $z^2+w^2 = 9(z'^2+w'^2)$; così $x'^2+y'^2 = 3(z'^2+w'^2)$. Sia $n_3 = x'^2+y'^2$; è $n_3 < n_2$. Si genera in questo modo una successione strettamente decrescente di numeri naturali; ciò non è possibile, quindi non è possibile trovare *x*, *y*, *z*, *w* soddisfacenti (#).

CONGRUENZE MODULO ***m.***

Sia *m* un numero intero ≥ 2. Si dice che due numeri interi sono *congrui modulo m* se $m\,|\,(b-a)$; si scrive

$$a \equiv b \pmod m \qquad \text{oppure} \qquad a \equiv b\ (m). \tag{1}$$

Se *m* può essere sottinteso scriveremo semplicemente $a \equiv b$.

La congruenza modulo *m* di *a* e *b* significa che *a* e *b* danno lo stesso resto nella divisione intera per *m.*

La relazione *congruenza modulo m* è una *relazione di equivalenza* in **Z**, cioè essa è

- *riflessiva*: per ogni *a*, è $a \equiv a$
- *simmetrica*: per ogni *a*, *b* è $a \equiv b \Leftrightarrow b \equiv a$
- *transitiva*: per ogni *a*, *b*, *c* è $(a \equiv b \text{ e } b \equiv c) \Rightarrow a \equiv c$.

Essendo una relazione di equivalenza, la congruenza modulo *m* ripartisce **Z** in classi di equivalenza, dette *classi di resto modulo m.* Le classi sono in numero di *m*, e ciascuna contiene uno e uno solo dei numeri 0, 1, …, $m-1$, che sono i possibili resti della divisione per *m* di un numero intero. Questi numeri sono "rappresentanti privilegiati" per le classi di resto modulo *m.* Indicheremo la classe di equivalenza che contiene *k* con $[k]_m$, o semplicemente con $[k]$, se non ci sono dubbi su chi sia *m.*

Oltre alle proprietà ricordate sopra, la cui verifica è semplicissima, la congruenza modulo *m* è "stabile" rispetto a addizione (e sottrazione) e moltiplicazione, cioè per ogni *a*, *b*, a', b' si ha che:

$$a \equiv a' \text{ e } b \equiv b' \Rightarrow (a+b \equiv a'+b',\ a-b \equiv a'-b',\ a \cdot b \equiv a' \cdot b').$$

Ciò consente di definire le operazioni di addizione e moltiplicazione *tra le classi* operando tra i rappresentanti, con la certezza che il risultato è indipendente dalla scelta del rappresentante. Per esempio, sia $m = 5$; consideriamo le classi $[2]$ e $[4]$ costituite rispettivamente dai numeri congrui a 2 e a 4, modulo 5, cioè

$$[2] = \{2, 7, 12, 17, \ldots, -3, -8, -13, \ldots\} = \{2+5k;\ k \in \mathbf{Z}\};$$
$$[4] = \{4, 9, 14, 19, \ldots, -1, -6, -11, \ldots\} = \{4+5k;\ k \in \mathbf{Z}\}.$$

Il *prodotto modulo 5* delle due classi è per definizione la classe contenente il prodotto di due qualunque rappresentanti di $[2]$ e $[4]$; quindi per esempio

$$[2] \cdot [4] \overset{def}{=} [2 \cdot 4] = [8] = [3].$$

L'ultima uguaglianza dipende dal fatto che $8 \equiv 3 \pmod 5$. Scegliendo altri rappresentanti per le classi $[2]$ e $[4]$ il risultato non sarebbe cambiato; per esempio, 17 è un rappresentante per $[2]$, 9 un rappresentante per $[4]$; risulta $17 \cdot 9 = 153$, e $153 \equiv 3 \pmod 5$, quindi otteniamo ancora $[2] \cdot [4] = [3]$.

Qui sotto mostriamo le tavole dell'addizione e della moltiplicazione modulo 5, utilizzando i rappresentanti privilegiati 0, 1, 2, 3, 4, e omettendo le parentesi quadre che denotano le classi, come d'uso. Nasce la struttura algebrica costituita dall'insieme quoziente $\mathbf{Z}_m = \mathbf{Z}/\equiv_m$, munita delle operazioni di addizione e moltiplicazione; essa è un *anello commutativo con unità*; e in certi casi, come vedremo tra poco, è un *campo*.

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Equazioni lineari modulo *m*.

Fissato *m*, e altri due numeri interi *a*, *b*, con $a \not\equiv 0 \pmod m$, cerchiamo soluzioni dell'equazione

(1) $$a\,x = b \quad \textbf{\textit{nell'aritmetica modulo m.}}$$

Nell'aritmetica di **Z** la (1) ha soluzione (unica) se e solo se *b* è multiplo di *a*; in $\mathbf{Z}_m$ le cose vanno in modo piuttosto diverso. Risolvere (1) "modulo *m*" significa trovare numeri interi *x* tali che: per un *k* intero, si abbia

(2) $$a\,x = b + k\,m \qquad \text{cioè} \qquad x \cdot a - k \cdot m = b$$

L'equazione (1) in una sola incognita, variabile in $\mathbf{Z}_m$, equivale dunque all'equazione (2) in due incognite *x*, *k*, variabili in **Z**. Questa, specialmente nella seconda forma in cui l'abbiamo scritta, ricorda

da vicino il Teorema di Bezout: x e k sono i coefficienti interi di una combinazione lineare di a e m che dà come risultato b. Se $b \neq 0$ una siffatta combinazione lineare esiste se e solo se b è multiplo del $\text{M.C.D.}(a,m)$.

Nel caso particolare di $b = 1$, la relazione (1) può essere interpretata come ricerca dell'inverso moltiplicativo di a in Z_m. Per quanto visto, l'inverso esiste se e solo se $\text{M.C.D.}(a,m) = 1$, cioè se a è primo con m. Se m è un numero primo, e solo in questo caso, allora tutti gli elementi non nulli di $\mathbf{Z}_m$ possiedono l'inverso moltiplicativo, cosicché $\mathbf{Z}_m$ è un *campo*. È questo il caso, per esempio, di $\mathbf{Z}_5$; nella tavola della moltiplicazione in $\mathbf{Z}_5$ infatti ogni riga (e ogni colonna) mostra il valore 1.

Invece, se m non è primo, ci sono in $\mathbf{Z}_m$ dei *divisori dello zero*, ossia elementi non nulli che soddisfano la relazione

$$a\,x = 0 \text{ in } \mathbf{Z}_m \qquad \text{cioè} \qquad a\,x \equiv 0 \pmod{m}.$$

Per esempio, sia $m = 6,\ a = 4$; l'equazione $4\,x \equiv 0 \pmod{6}$ ha come soluzione non nulla $x = 3$, e ogni altro valore di x multiplo di 3. In $\mathbf{Z}_6$ le soluzioni di $4\,x = 0$ sono due: quella ovvia, $x = 0$ (che è rappresentante della classe nulla, avente per elementi i multipli di 6), e l'altra, $x = 3$, che rappresenta la classe dei multipli dispari di 3. Quest'ultima è una soluzione non nulla (in questo caso unica) di $4\,x = 0$ in $\mathbf{Z}_6$.

In generale, se m non è primo e a, m non sono coprimi, indicato $d = \text{M.C.D.}(a,m)$, le soluzioni non banali (ossia non congrue a 0 modulo m) di $a\,x = 0$ in $\mathbf{Z}_m$ sono i multipli positivi di d, *minori di* m; invece, se a, m sono coprimi, la relazione $a\,x \equiv 0 \pmod{m}$ ha soltanto le soluzioni banali, cioè i multipli di m.

L'algebra "modulo m" consente di trattare alcuni problemi di aritmetica assai più agevolmente che con l'ordinaria algebra degli interi. Si ricavano facilmente i "criteri di divisibilità" per 2, 4, 5, 9, 11; vediamo un paio di esempi di altro tipo.

Problema 15. *Una pulce si trova sul numero 12 del quadrante di un orologio. Sceglie un numero naturale n compreso tra 1 e 12, estremi inclusi, e comincia a fare salti di n numeri sul quadrante, in senso orario (se ad esempio n = 3, dopo il primo salto è sul 3,dopo il secondo è sul 6 e così via). Dopo 12 salti, per la prima volta si ritrova sul numero 12 del quadrante. In quanti modi distinti può aver scelto n?* (da *Giochi di Archimede,* novembre 2009)

Soluzione. L'evento descritto dal testo si può descrivere dicendo che:

$$12n \equiv 0 \pmod{12} \quad \text{e} \quad k\,n \not\equiv 0 \pmod{12} \quad \text{per } 1 \le k \le 11.$$

La prima relazione è verificata da qualunque n, quindi non serve per risolvere il problema. La seconda dice che l'equazione $k\,n \equiv 0 \pmod{12}$ (nell'incognita k) ha soltanto le soluzioni banali, cioè i k multipli di 12. Come abbiamo visto, ciò accade se e solo se n e 12 sono coprimi. Poiché il testo assegna anche il vincolo $1 \le n \le 12$, le soluzioni sono i numeri 1, 5, 7, 11.

Problema 16. *Il direttore di un ristorante con capienza di 600 posti non ricorda quante persone ha servito in occasione di un pranzo collettivo. Egli però ricorda che ha dovuto apparecchiare i tavoli con 7 coperti ciascuno, perché apparecchiando i tavoli per 3, 4, 5 o 6 coperti ciascuno, e occupando completamente ogni tavolo fino ad esaurimento dei convitati, avrebbe dovuto lasciare da sola una persona. Invece i tavoli da 7 coperti sono stati tutti riempiti. In quanti erano a tavola?*

Soluzione. Sia N il numero dei commensali. Le informazioni del testo dicono che $N \equiv 1 \pmod{m}$ per $m = 3, 4, 5, 6$, mentre $N \equiv 0 \pmod{7}$. La prima equivale a $N - 1 \equiv 0 \pmod{m}$ per $m = 3, 4, 5, 6$. Ciò significa che $N - 1$ è multiplo di 3, 4, 5, 6, e quindi è multiplo del m.c.m. di questi numeri, che è 60. La seconda informazione si può scrivere $N - 1 \equiv -1 \pmod{7}$, oppure anche $N - 1 \equiv 6 \pmod{7}$, perché –1 e 6 sono congrui modulo 7. Cerchiamo allora $N - 1$ tra i multipli di 60, in modo che sia congruo a 6 modulo 7. I calcoli sono semplificati se operiamo secondo l'aritmetica di $\mathbf{Z}_7$. L'equazione da risolvere è

$$60k \equiv 6 \pmod{7} \qquad \text{cioè} \qquad [60]_7 \cdot [k]_7 = [6]_7$$

($[\bullet]_7$ indica la classe modulo 7 di $\bullet$). Ma $[60]_7 = [4]_7$ cosicché la relazione scritta sopra si può scrivere

$$[4]_7 \cdot [k]_7 = [6]_7 \qquad \text{cioè} \qquad [4k]_7 = [6]_7 .$$

Non resta che cercare tra i multipli di 4 un numero che sia congruo a 6 modulo 7. La seguente tabella indica la classe modulo 7 di $4k$ per k da 1 a 7 (da lì in avanti il ciclo si riproduce identico).

k	1	2	3	4	5	6	7
$[4k]_7$	4	1	5	2	6	3	0

Si ottiene un risultato di classe 6 quando $k = 5$; infatti $4 \cdot 5 = 20 \equiv 6 \pmod{7}$, mentre ciò non accade per i valori precedenti di k. Allora $N - 1 = 60k = 300$, e infine, $N = 301$. Questo è il numero dei commensali. Non ci sono altre soluzioni possibili, perché la relazione $[4k]_7 = [6]_7$ ritorna ad essere soddisfatta per la seconda volta solo quando $k = 5 + 7 = 12$, che darebbe $N = 1 + 60 \cdot 12 = 721$, non accettabile perché superiore a 600.

Problema 17. *Dimostrare che, se n è un numero naturale non multiplo di 3, allora il numero* $3^{2n} + 3^n + 1$ *è multiplo di 13. Determinare inoltre il resto della divisione per 13 di tale numero, se n è multiplo di 3.*

Soluzione. Dobbiamo stabilire, per ogni n, la classe modulo 13 di $3^{2n} + 3^n + 1$. Il testo del problema annuncia che questa è 0 se n non è multiplo di 3; andiamo a vedere. Compiliamo una tabella con i valori delle classi di resto modulo 13 degli addendi che formano il nostro numero. È utile notare che nel gruppo moltiplicativo $\mathbf{Z}_{13} - \{0\}$ l'elemento (classe) 3 ha periodo 3; infatti $3^3 = 27 \equiv 1 \pmod{13}$; quindi la tabella si ripete ciclicamente ad ogni tre passi; basterebbe quindi compilare soltanto le prime tre colonne. Ecco i risultati:

n	1	2	3	4	5	6	7	8	…
$\left[3^n\right]_{13}$	3	9	1	3	9	1	3	9	…
$\left[3^{2n}\right]_{13}$	9	3	1	9	3	1	9	3	…
$\left[3^{2n} + 3^n + 1\right]_{13}$	0	0	3	0	0	3	0	0	…

Non serve aggiungere altro: i risultati sono evidenti dalla tabella. Il numero $3^{2n} + 3^n + 1$ è multiplo di 13 quando n non è multiplo di 3; quando n è multiplo di 3, la divisione di $3^{2n} + 3^n + 1$ per 13 dà resto 2.

Problema 18. *Trovare tutti i numeri naturali* n *di tre cifre* $(100 \le n \le 999)$ *che sono uguali al numero formato dalle ultime tre cifre di* n^2. (Cesenatico, 9 maggio 2003, problema 1)

Soluzione. La proprietà di n descritta dal testo equivale a dire che $n^2 - n$ è divisibile per $1000 = 2^3 \cdot 5^3$. D'altra parte è anche $n^2 - n = n(n-1)$. Poiché $n - 1$ e n sono primi fra loro, uno solo dei due è divisibile per 5; inoltre uno solo dei due è pari, quindi anche il fattore 2^3 appartiene interamente a uno solo fra n e $n - 1$. Possiamo allora considerare i seguenti casi (in tutto quattro)

1) Sia 2^3, sia 5^3 sono fattori di n;

2) Sia 2^3, sia 5^3 sono fattori di $n - 1$;

3) ; $5^3 \mid n$, $2^3 \mid (n-1)$

4) . $2^3 \mid n$, $5^3 \mid (n-1)$

I casi 1) e 2) sono da escludere, perché incompatibili con l'ipotesi $n \geq 999$. Consideriamo il caso 3. Tra i numeri multipli di 125, cerchiamo quelli tali che il loro precedente sia multiplo di 8. Compiliamo dunque una tabella nella quale indichiamo quale sia la classe modulo 8 dei multipli di 125, ossia dei numeri $n = 125k$, $1 \leq k \leq 7$, perché si vuole $100 \leq n \leq 999$. Il calcolo delle classi modulo 8 è facilitato se si nota che $125 \equiv 5 \pmod{8}$, quindi $[125]_8 = [5]_8$. Allora $[125 \cdot 2]_8 = [5 \cdot 2]_8 = [2]_8$; i valori successivi di $[125k]_8$ si ottengono ciascuno addizionando 5 "modulo 8" al risultato precedente. Ecco i risultati.

k	1	2	3	4	5	6	7
$[125k]_8$	5	2	7	4	1	6	3

Il numero naturale che precede $n = 125k$ è multiplo di 8 se e solo se la classe modulo 8 di $125k$ è $[1]_8$; ciò avviene se $k = 5$. Dunque $n = 125 \cdot 5 = 625$ soddisfa i requisiti del problema.

In effetti si calcola $625^2 = 390625$.

Passiamo al caso 4). Questa volta cerchiamo un multiplo di 8 il cui precedente sia multiplo di 125. Conviene però continuare la ricerca tra i multipli di 125, che sono meno numerosi. Tra essi ne cerchiamo uno tale che sia multiplo di 8 il suo successivo, in quanto adesso $125k$ rappresenta $n-1$. Il successivo di un numero è multiplo di 8 se la sua classe modulo 8 è $[7]_8$. La tabella che abbiamo compilato sopra mostra questo risultato per $k = 3$; dunque un altro valore di *n* (l'unico altro valore) che soddisfa quanto richiesto è quello per cui $n - 1 = 125 \cdot 3 = 375$, ossia $n = 376$. In effetti $376^2 = 141376$.

Il Teorema di Wilson e il "Piccolo Teorema di Fermat".

Si tratta di due teoremi riguardanti le congruenze modulo *p*, con *p* primo. Vi sono versioni più sofisticate di questi teoremi per congruenze modulo *m*, con *m* non primo, di cui non parliamo.

Teorema di Wilson. *Se p è un numero primo, allora* $(p-1)! \equiv -1 \pmod{p}$.

Dimostrazione. Se $p = 2$, la proprietà è banale. Supponiamo $p \geq 3$. Quando *p* è un numero primo, la struttura moltiplicativa $(\mathbf{Z}_m - \{0\}, \times)$, in cui $\times$ indica la moltiplicazione modulo *p*, è n *gruppo*, in cui è 1 l'elemento neutro. Ogni elemento ha inverso moltiplicativo; in particolare 1 è inverso di sé stesso, e anche $p-1$. Infatti $p - 1 \equiv -1 \pmod{p}$, quindi $(p-1) \cdot (p-1) \equiv (-1) \cdot (-1) = 1 \pmod{p}$. Gli altri numeri compresi tra 2 e $p-2$ si possono accoppiare a due a due in modo che il prodotto di ciascuna coppia sia 1 $\pmod{p}$. Così, se sviluppiamo $(p-1)!$ abbiamo il fattore 1, il fattore $p - 1 \equiv -1 \pmod{p}$, e altri $p-3$ fattori il cui prodotto modulo p dà 1. Ne segue che $1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv -1 \pmod{p}$, come volevamo dimostrare. Per esempio, con $n = 11$ si ha

$$(11-1)! = 10! = 1 \cdot \underbrace{(2 \cdot 6)}_{\equiv 1 \pmod{11}} \cdot \underbrace{(3 \cdot 4)}_{\equiv 1 \pmod{11}} \cdot \underbrace{(5 \cdot 9)}_{\equiv 1 \pmod{11}} \cdot \underbrace{(7 \cdot 8)}_{\equiv 1 \pmod{11}} \cdot \underbrace{10}_{\equiv -1 \pmod{11}} \equiv -1 \pmod{11}$$

Osserviamo che la relazione $(p-1)! \equiv -1 \pmod{p}$ vale soltanto se *p* è primo; se non è così, tra 2 e $p-1$ ci sono due numeri il cui prodotto è multiplo di *p*; quindi se *p* non è primo, $(p-1)! \equiv 0 \pmod{p}$.

Piccolo Teorema di Fermat. Così detto per distinguerlo dall'"Ultimo Teorema di Fermat", si può enunciare in due forme equivalenti:

(1) *Se p è un numero primo, a è un numero intero positivo, e i numeri a, p sono primi tra loro, allora* $a^{p-1} \equiv 1 \pmod{p}$.

(2) *Se p è un numero primo, e a un intero qualunque, allora* $a^p \equiv a \pmod{p}$.

Dimostrazione. Mostriamo prima di tutto che (1) e (2) sono equivalenti. Supponiamo dimostrato (1). Se a e p sono primi tra loro, per (1) è $a^{p-1} \equiv 1 \pmod{p}$; moltiplicando entrambi i membri per a si ottiene $a^p \equiv a \pmod{p}$. Siano a e p non primi tra loro; poiché p è primo, ciò vuole dire che $p \mid a$. Allora sia a, sia a^p sono congrui a zero modulo p, quindi è ancora $a^p \equiv a \pmod{p}$.

Viceversa: supponiamo provata (2), e sia a primo con p. Allora la classe $[a]_p$ è invertibile in $\mathbf{Z}_p$, cioè esiste un numero intero b tale che $a \cdot b \equiv 1 \pmod{p}$. Moltiplicando per b entrambi i membri della relazione $a^p \equiv a \pmod{p}$ si ottiene $a^{p-1} \equiv 1 \pmod{p}$, come si voleva.

Adesso dimostriamo il teorema, nella forma (2), per induzione su $a \geq 0$ (dopo ci occuperemo di $a < 0$).

Se $a = 0$ la relazione $0^p \equiv 0 \pmod{p}$ è ovvia.

Supponiamo che per un intero $a \geq 0$ risulti $a^p \equiv a \pmod{p}$; cerchiamo di dimostrare che $(a+1)^p \equiv a+1 \pmod{p}$.

La formula dello sviluppo della potenza di un binomio (cosiddetta "di Newton") dà

(°) $$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + a^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k .$$

I coefficienti binomiali che figurano nell'ultima sommatoria sono tutti multipli di p. Infatti il denominatore della frazione $\frac{p!}{k!(p-k)!}$ è il prodotto di numeri interi tutti $< p$, quindi non divisori di p, perché p è primo; il numeratore della frazione invece contiene il fattore p: quindi $\frac{p!}{k!(p-k)!}$ (che in ogni caso è un numero intero), dà un numero multiplo di p, ossia congruo a 0 modulo p. Perciò

$$\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k \equiv 0 \pmod{p}$$

e allora da (°) segue

$$(a+1)^p \equiv 1 + a^p \pmod{p}.$$

L'ipotesi induttiva dice che $a^p \equiv a \pmod{p}$; perciò la relazione scritta sopra dà

$$(a+1)^p \equiv 1 + a \pmod{p}$$

come si voleva dimostrare.

Se $a < 0$, quanto appena mostrato dice che $(-a)^p \equiv -a \pmod{p}$. Poiché a è un numero primo, se $p \neq 2$ allora p è dispari; in tal caso $(-a)^p \equiv -a^p$, e si ha la tesi. Se $p = 2$ la relazione $(-a)^p \equiv -a \pmod{p}$ diventa $a^2 \equiv -a \pmod{2}$, cioè $a(a+1) \equiv 0 \pmod{2}$ che è vera perché il prodotto di due numeri interi consecutivi è sempre pari.

Rappresentazioni in base b**.** Fissato un numero intero $b \geq 2$, ogni numero intero positivo N si può scrivere in uno e un solo modo nella forma

(1) $$N = \sum_{k \geq 0} x_k \cdot b^k$$

in cui x_k, per ogni k, indica un numero intero tra 0 e $b-1$. Soltanto un numero finito di addendi è diverso da zero; se n è il più grande k per cui $x_k \neq 0$, la (1) si scrive

(2) $$N = x_n x_{n-1} \ldots x_2 x_1 x_0 \quad (\text{in base } b).$$

Normalmente il contesto permette di evitare l'ambiguità interpretativa di questa scrittura con il prodotto di $x_n, x_{n-1}, \ldots$.

Anche la rappresentazione di numeri in base *b* può essere spunto per interessanti problemi; ecco un paio di esempi.

Problema 19. *Si ritiene che la scelta consueta della base 10 per rappresentare i numeri sia dovuta al fatto che abbiamo 10 dita. Un marziano in visita sulla Terra, dopo avere visto scritta l'equazione di secondo grado* $x^2 - 16x + 41 = 0$*, scrive: "la differenza delle soluzioni è 10". Quante dita ha il marziano? (si precisa che le cifre da 0 a 6 hanno per il marziano ed per noi lo stesso significato).*

Soluzione. Il problema chiede in modo pittoresco quale sia la base di numerazione rispetto alla quale risulta corretta la valutazione data della differenza delle soluzioni dell'equazione.

È necessario ricordare che, se x_1, x_2 sono le soluzioni di un'equazione di secondo grado, questa si può scrivere:

$$x^2 - (x_1 + x_2) \cdot x + x_1 \cdot x_2 = 0 .$$

Dunque, qualunque sia la basa usata, si ha

$$x_1 + x_2 = 16 ; \quad x_1 \cdot x_2 = 41$$

il cui significato dipende però da quale base si adotta. Se la base è *b*, allora

(*) $$x_1 + x_2 = b + 6 ; \quad x_1 \cdot x_2 = 4b + 1 .$$

La valutazione della differenza delle soluzioni fatta dal marziano significa, se x_2 indica la soluzione maggiore, che $x_2 - x_1 = b$, cioè $x_2 = x_1 + b$. Sostituiamo questa espressione di x_2 in (*), e svolgiamo i calcoli necessari per determinare *b*.

$$\begin{cases} 2x_1 + b = b + 6 \\ x_1 \cdot (x_1 + b) = 4b + 1 \end{cases} ; \quad \begin{cases} x_1 = 3 \\ 9 + 3b = 4b + 1 \end{cases} \quad \text{da cui } b = 8 .$$

In effetti il marziano interpreta l'equazione $x^2 - 16x + 41 = 0$ come quella che, in base 10, verrebbe scritta $x^2 - 14x + 33 = 0$; le sue soluzioni, in base 10, sono 3 e 11, la cui differenza è 8, che in base 8 si scrive appunto 10.

Problema 20. *Determinare tutti i numeri interi positivi* N *tali che: la rappresentazione in base 2 di* N *coincide con la rappresentazione in base 3 di* $2N$. (Gara di febbraio 2009).

Soluzione. Sia $x_n x_{n-1} \ldots x_2 x_1 x_0$ la rappresentazione di *N* in base 2, e in virtù dell'ipotesi, la rappresentazione in base 3 di $2N$. $x_0, x_1, \ldots, x_n$ possono valere soltanto 0 oppure 1, essendo le cifre di una rappresentazione in base 2.

La rappresentazione in base 2 di $2N$ è: $x_n x_{n-1} \ldots x_2 x_1 x_0 0$; questa stringa rappresenta in base 2 lo stesso numero che $x_n x_{n-1} \ldots x_2 x_1 x_0$ rappresenta in base 3. Si ha quindi

$$\sum_{k=0}^{n} x_k \cdot 2^{k+1} = \sum_{k=0}^{n} x_k \cdot 3^k \quad \text{cioè} \quad \sum_{k=0}^{n} x_k \cdot \left(2^{k+1} - 3^k\right) = 0 .$$

Scriviamo esplicitamente i primi addendi:

$$x_0 + x_1 - x_2 - 11x_3 - \ldots = 0 .$$

I coefficienti $2^{k+1} - 3^k$, negativi per $k \geq 2$, aumentano in valore assoluto al crescere di *k*. Poiché $x_0, x_1, \ldots, x_n$ sono uguali a 0 o 1, se qualche x_k con $k \geq 3$ è diverso da zero, la somma considerata è negativa anziché uguale a zero. Bisogna quindi che sia $x_k = 0$ per $k \geq 3$. Rimane così la relazione

$$x_0 + x_1 - x_2 = 0$$

la quale è soddisfatta nei due casi: $x_0 = 1, x_1 = 0, x_3 = 1$ e $x_0 = 0, x_1 = 1, x_3 = 1$. I numeri *N* soddisfacenti i requisiti del testo sono due; essi si rappresentano in base 2 come segue:

$$N = 101; \qquad N' = 110.$$

Passando dalla base 2 alla base 10 si ottiene $N = 5$ e $N' = 6$; invece le stringhe 101 e 110 rappresentano in base 3 rispettivamente i numeri (scritti in base 10) $9 + 1 = 10$ e $9 + 3 = 12$.

Il principio dei cassetti (o dei piccioni). *Se $n+1$ oggetti [piccioni] sono sistemati in n cassetti [gabbie], allora almeno un cassetto [gabbia] contiene almeno due oggetti [piccioni].*

Il teorema afferma una proprietà ovvia; tuttavia la sua applicazione consente a volte di risolvere problemi non altrettanto ovvi; ecco un esempio.

Problema 21 (Gara nazionale 1989). *In un grande tavolo di forma circolare sono uniformemente distribuiti 60 commensali: 30 uomini e le rispettive 30 mogli (non necessariamente ciascuna moglie è seduta accanto al marito). Dimostrare che ci sono almeno due signore che siedono alla stessa distanza dai rispettivi mariti.*

Soluzione. Le 60 persone occupano i vertici di un poligono regolare di 60 lati inscritto nella circonferenza; siano $A_1, \ldots, A_{30}$ i vertici occupati dagli uomini, $B_1, \ldots, B_{30}$ i vertici occupati dalle mogli, conveniamo che in B_k sieda la consorte di chi si trova in A_k. La distanza tra ciascun marito e la propria moglie è la misura della diagonale A_kB_k del poligono. Le diagonali di un poligono di 60 lati possono avere soltanto 29 diverse misure: fissato un vertice V, la misura massima delle diagonali è $\overline{VW}$, dove W è il vertice diametralmente opposto a V; VW è asse di simmetria del poligono, e ciascuna delle due parti in cui VW divide il poligono contiene altri 28 vertici, ciascuno a una diversa distanza da V. Ogni altra diagonale misura quanto una delle 29 uscenti da V e situate in una delle due metà del poligono. Ora consideriamo le 30 diagonali A_kB_k, e raggruppiamole in classi di lunghezza. Poiché, come abbiamo visto, ci sono soltanto 29 possibili misure delle diagonali, almeno due delle diagonali A_kB_k debbono essere di uguale lunghezza; ciò è quanto si doveva dimostrare.

Problema 22 (Gara di febbraio 2004). *Determinare il più piccolo numero naturale n tale che: dati n numeri interi distinti, ce ne sono sicuramente due tali che la loro somma o la loro differenza è divisibile per 9.*

Soluzione. La richiesta è di trovare fra gli n numeri dati due numeri a, b tali che $a \equiv b \pmod 9$ oppure $a \equiv -b \pmod 9$. È sufficiente ragionare sui resti modulo 9; raggruppiamo i numeri interi da 0 a 9 in modo da mettere insieme quelli legati dalla relazione $a \equiv -b \pmod 9$. I "cassetti" che si formano sono:

$$\{0\},\ \{1, 8\},\ \{2, 7\},\ \{3, 6\},\ \{4, 5\}.$$

Ogni numero intero è congruo modulo 9 a uno dei numeri su elencati. Poiché i gruppi ("cassetti") sono 5, dati sei o più numeri ce ne saranno almeno due che appartengono (modulo 9) allo stesso cassetto. Questi due numeri o sono congrui modulo 9, o è tale la loro somma. 6 è la quantità minima da richiedere per avere la certezza di soddisfare quanto richiesto: tra i cinque numeri 0, 1, 2, 3, 4 non si forma alcuna coppia con le caratteristiche desiderate. Pertanto $n = 6$.