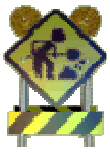
"Come si fa" a svolgere vari tipi di esercizi



1 – numeri e congruenze

(algoritmi – avvertenze – casi speciali – esempi) Attenzione… gli argomenti non sono in ordine…

Alcuni degli esercizi presentati erano parte di temi d'esame, e le lettere che compaiono hanno i seguenti significati:
Matricola(**N**) data di nascita (**G**/**M**/**A**)
n:= N mod 1000; g:= (G mod 5) + 4; m:= (M mod 6) + 2; a:= A mod 100

Numeri primi, MCD ecc.

algoritmo euclideo per il calcolo del MCD:

se $b = 0$ allora MCD$(a,b) = a$,
se $b > 0$, si divide a per b ottenendo come resto r;
poi si divide b per r, ottenendo un resto r_1 ,
quindi si divide r per r_1 ottenendo un resto r_2,
...
finché $r_k = 0$. ⇨ r_{k-1} = MCD(a,b).

$$\text{mcm}(a,b) = \frac{ab}{\text{MCD}(a,b)}.$$

- Se $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ allora il numero $\tau(n)$ dei divisori di n è $\tau(n) = (e_1 + 1)(e_2 + 1) \dots (e_k + 1)$.
- Si indica con $\varphi(n)$, chiamato **numero di Eulero** di n, il numero dei numeri naturali minori di n e primi con n.

Esempio 1 Scrivere i numeri minori di 15 e primi con 15; calcolare $\varphi(15)$,
Poiché 15 ha come fattori primi 3 e 5, i numeri richiesti sono 1, 2, 4, 7, 8, 11, 13, 14, quindi $\varphi(15) = 6$.

Esempio 2 Calcolare, mediante l'algoritmo euclideo, MCD (387, 144).
$387 = 144 \times 2 + 99$
$144 = 99 + 45$
$99 = 45 \times 2 + 9$
$45 = 9 \times 5 + 0$ ⇨ MCD (387, 144) = 9

Esempio 3 Mostrare che MCD$(x, y) \mid x - y$ o MCD$(x, y) \mid y - x$
La differenza tra le due richieste, è perché, in N, solo una delle due differenze è definita, supponiamo che sia $x > y$ e quindi sia definita $x - y$.
Se MCD$(x, y) = k$, significa che $x = kq$, e $y = kp$, con $q > p$. Allora $x - y = kq - kp = k(q - p)$, che è un numero naturale per l'ipotesi fatta, quindi MCD$(x, y) \mid x - y$.

Esercizi:

1. Calcolare, mediante l'algoritmo euclideo, MCD(n,a), MCD(N,a).
2. Calcolare, mediante l'algoritmo euclideo, MCD(m,n,a).

3. Calcolare MCD(33,168) sia con l'algoritmo euclideo, sia per mezzo della fattorizzazione.
4. Usare la proprietà precedente per calcolare MCD(1492, 1776)
5. Dimostrare che h MCD(x, y) = MCD(hx, hy)
6. Calcolare MCD e identità di Bezout per 222 e 1870; 135 e 216
7. Mostrare che MCD(x, y)|mcm(x, y), comunque scelti x e y.
8. Scrivere i numeri minori di 16 e primi con 16. (lo stesso con 24, 32, 22)

Cambio di base

Cambio base per numeri interi, da base 10 a base b.

L'algoritmo è semplice e funziona con qualsiasi base b >1,
Si divide il numero per la base e si considera il resto della divisione.
Si itera il passaggio fino ad avere quoziente 0.
La sequenza dei resti, presa nel senso inverso rispetto all'ordine con cui sono stati determinati dà la soluzione. **Attenzione**. Se la base è maggiore di 10, usare un segno di interpunzione per esempio ":" per dividere le "cifre", che possono non essere numeri tra 0 e 9, come nell'esempio 1.

Esempio 1: Scrivere 646727 in base x=12.

646727	
53893	11
4491	1
374	3
31	2
2	7
0	2

646727_{10}= 2:7:2:3:1:11_{12}

Esempio 2: Dati due numeri v=12012 e w=2120 in base 3, senza passare alla base 10, esprimere v+w o v×w in base 3.

```
12012+
 2120=
-----
21202
```

```
   12012
    2120
-------
   00000
  101101-
  12012--
 101101---
---------
 111020210
```

×

Cambio base per numeri razionali da base 10 a base b.

L'algoritmo è diverso per la parte intera e la parte decimale, che quindi vanno trattate separatamente.
Per la parte intera si agisce come nel caso precedente.
Per la parte decimale, la si moltiplica per la base.
Si toglie la parte intera, che è la prima cifra dopo la virgola.
Si moltiplica il nuovo numero per la base, si toglie la parte intera, che è la seconda cifra dopo la virgola.

Si itera il procedimento finché:

- Si ottiene 0. Allora il numero ha una rappresentazione decimale finita nella base assegnata.
- Si ottiene un numero già trovato.
  - Se il numero già trovato è il primo (quello di partenza) si ha un numero decimale periodico, senza antiperiodo.
  - Se invece il numero che si ripete è ad un posto k >1, le prime k −1 cifre sono cifre di antiperiodo e le successive formano il periodo

Esempio 1: Scrivere p=7,2 in base 6.
La parte intera è 7 e $7_{10}=11_{6.}$
La parte decimale è 0,2.
0,2 ×6 = 1,2 – 1 = 0,2 ⇨ $0,3_{10} = 0,1\ldots$
0,2
0,2 è già stato trovato, in posizione 1, quindi non c'è antiperiodo ⇨ $7,2_{10} = 11,(1)_6$

Esempio 2: Scrivere p=7,3 in base 8 indicandone eventuali periodo e antiperiodo.
La parte intera è 7 e $7_{10}=7_{8.}$
La parte decimale è 0,3.
0,3 ×8 = 2,4 – 2 = 0,4 ⇨ $0,3_{10} = 0,2\ldots$
0,4 ×8 = 3,2 – 3 = 0,2 ⇨ $0,3_{10} = 0,23$
0,2 ×8 = 1,6 – 1 = 0,6 ⇨ $0,3_{10} = 0,231\ldots$
0,6 ×8 = 4,8 – 4 = 0,8 ⇨ $0,3_{10} = 0,2314\ldots$
0,8 ×8 = 6,4 – 6 = 0,4 ⇨ $0,3_{10} = 0,23146\ldots$
0,4
0,4 è già stato trovato, in posizione 2, quindi si ha 1 cifra di antiperiodo, le altre di periodo.
⇨ $7,3_{10} = 7,2(3146)_8$

Esempio 3: Scrivere p = 9,4 in base 5.
La parte intera è 9 e $9_{10}=14_{5.}$
La parte decimale è 0,4.
0,4 ×5 = 2,0 – 2 = 0 ⇨ $0,4_{10} = 0,2_5$ e non si prosegue, poiché il numero risulta finito.
⇨ $9,4_{10} = 14,2_5$

Cambio base per numeri razionali, da base b a base 10.

Si usa la scrittura polinomiale del numero: per esempio il numero $x{:}y{:}w,v{:}z_b$ si può scrivere come:

$$x{:}y{:}w,v{:}z_b = x\times b^2 + y\times b^1 + w\times b^0 + v\times b^{-1} + z\times b^{-2} = x\times b^2 + y\times b + w + v\times\frac{1}{b} + z\times\frac{1}{b^2}$$

e adesso basta fare i conti…

Esempio: scrivere in base 10 il numero $2341,143_5$.

$$2341,143_5 = 2\times5^3 + 3\times5^2 + 4\times5 + 1 + 1\times\frac{1}{5} + 4\times\frac{1}{5^2} + 3\times\frac{1}{5^3} =$$

$$= 2\times125 + 3\times25 + 4\times5 + 1 + \frac{1}{5} + 4\times\frac{1}{25} + 3\times\frac{1}{125} = 346 + \frac{148}{125}$$

e trasformando tutto in modo da avere denominatore 1000 (e quindi una facile rappresentazione in base

10) $\frac{148}{125}=\frac{1184}{1000}$ per cui $2341{,}143_5 = 347{,}184_{10}$

Passaggio da base b a base b^2 o b^3 e viceversa

Se si ha un numero in base b e si vuol ricavare, senza passare attraverso la base 10, alla rappresentazione in una base che sia una potenza del numero stesso, bisogna osservare la scrittura polinomiale del numero, e raccogliere opportunamente le potenze della base.
Per esempio volendolo esprimere in base b^2 il numero $u{:}x{:}y{:}w{,}v{:}z_b$ si può scriverlo come:
$u{:}x{:}y{:}w{,}v{:}z_b = u\times b^3 + x\times b^2 + y\times b + w + v\times b^{-1} + z\times b^{-2} = (u\times b + x)\, b^2+(y\times b + w)+(v\times b + z)b^{-2}$, quindi le sue cifre saranno $(u\times b + x)$ $(y\times b + w)$ prima della virgola e $(v\times b + z)$ dopo la virgola.
Quindi, per passare da base b a base b^2 ogni coppia di cifre dà luogo a una cifra sola, viceversa se vogliamo passare da base b^2 a base b, ogni cifra dà luogo a una coppia di cifre, sia a sinistra che a destra della virgola, partendo dalla virgola stessa. Se si passa da base b a base b^3, le cifre andranno raccolte a 3 a 3, ecc.
Si faccia attenzione al periodo…

Esempio 1: considerare il numero $101201121{,}2(1021)_3$ e dedurne l'espressione in base 9 e in base 27.

Per passare alla base $9 = 3^2$ suddividiamo mentalmente le cifre a coppie, partendo dalla virgola. Poiché c'è un periodo, questo andrà ripetuto tante volte quante serve per "osservare" ancora un periodo.
1 01 20 11 21 , 21 02 11 ~~02 11 02 1~~….
Le ultime coppie sono state eliminate perché si ripetono. Allora:
1 0×3+1 2×3+1 1×3+1 2×3+1 , 2×3+1 0×3+2 1×3+1 e quindi
1 1 7 4 7 , 7 (2 4)
$101201121, 2(1021)_3 = 11747{,}7(24)_9$
Per passare alla base $27 = 3^3$ suddividiamo mentalmente le cifre a terne, partendo dalla virgola, con la stessa osservazione sul periodo.

Esercizi:

1. Applicare a 1789 l'algoritmo per ottenere la rappresentazione posizionale in base 8 e ricavarne quella in base 2 e 16 ($1789_{10} = 3375_8 = 11011111101_2 = 6FD_{16}$)
2. Applicare a 2315_{10} l'algoritmo per ottenere la rappresentazione posizionale in base 4 e ricavarne quella in base 2, 8 e 16 ($2315_{10}=210023_4 = 100100001011_2=99B_{16}=4413_8$)
3. Scrivere N in base 2, 4, 16.
4. Pensati n e a come numeri in base 11, eseguirne la somma senza passare alla rappresentazione in base 10.
5. Scrivere la tavola pitagorica della somma in base g.
6. Scrivere la tavola pitagorica del prodotto in base m.
7. Disporre i seguenti numeri in ordine crescente: x = 110011_2, y = 2201_3, z = $B4_{16}$.
8. Sia n′ il numero ottenuto invertendo l'ordine delle cifre di n (es. 346 ⇨ 643). Scrivere n *e* n′ in base 3 e ricavarne l'espressione in base 9. Senza passare alla base 10, esprimere n+n′ in base 3.
9. Sia n′ il numero ottenuto invertendo l'ordine delle cifre di n (es. 346 ⇨ 643). Scrivere n e n′ in base 16 e ricavarne l'espressione in base $256=16^2$ e in base $4=\sqrt{16}$
10. Sia x il numero decimale N,g. Scrivere l'espressione di x in base 23.

11. Sia p il numero decimale 1983,6 Scrivere l'espressione di p in base 12.
($1983{,}6_{10} = 1{:}1{:}9{:}3{,}(7{:}2{:}4{:}9)_{12}$)

Sui numeri razionali

I due tipi di esercizio prevedono il passaggio da frazione a numero decimale (e quindi rappresentazione finita o illimitata con periodo e eventuale antiperiodo) o quella inversa: trasformare un numero decimale periodico in frazione (per questa vedi dispense: il metodo pratico coincide esattamente con la teoria).
Per determinare che tipo di rappresentazione decimale ha una data frazione bisogna ricordare che:

Sia $\frac{a}{b}$ un numero razionale, con MCD(a,b) = 1, e sia $b = 2^h \cdot 3^k \cdot 5^r \cdot 7^s \cdot 11^t \cdot \ldots$ la scomposizione in fattori primi di b (con esponenti eventualmente nulli).

- Se **tutti** gli esponenti diversi da h e da r sono **nulli** allora la rappresentazione decimale è **limitata**.
- Se **almeno un** esponente diverso da h e da r è maggiore di 0 allora la rappresentazione decimale è **illimitata e periodica**.
- **L'antiperiodo** è costituito da m= max(h, r) cifre.
- Il periodo è costituito, al più, da b–1 cifre.

Si chiama **gaussiano** di b e si indica con $g(b)$ il numero di cifre del periodo di qualunque frazione $\frac{a}{b}$ tale che MCD(a, b) = 1.
Per ogni p primo, $g(p)$ è un divisore di p – 1.

Esempio 1: Esprimere q = 17,6(92) come frazione. Abbiamo una cifra di antiperiodo e due di periodo.
$10q$ = 176,(92)
$1000q$ = 17692,(92)

$1000q - 10q = 17692{,}(92) - 176{,}(92) = 17692 - 176 = 17516 = 990q \quad q = \frac{17516}{990}$ da semplificare…

Esempio 2: Stabilire quante cifre di periodo e quante di antiperiodo ha la frazione $\frac{45}{210}$.

Bisogna innanzitutto ridurre la frazione ai minimi termini: $\frac{45}{210} = \frac{3}{14}$.

Ora il denominatore è 2 · 7 e il gaussiano di 7 è 6, quindi la frazione ha 1 cifra di antiperiodo (l'esponente del fattore 2) e 6 di periodo: $g(7)$.

Esercizi:

1. Sia q=a.g(m) (cioè con parte intera a, antiperiodo g e periodo m). Esprimere q come frazione.
2. Se n non è divisibile per 11, dare la rappresentazione decimale periodica di $\frac{n}{11}$, altrimenti dare quella di $\frac{n+1}{11}$, scrivendo l'algoritmo usato.
3. Determinare tre numeri razionali compresi tra $\frac{1}{g}$ e $\frac{1}{g+1}$.

4. Le frazioni $\frac{m}{g}$ e $\frac{g}{m}$ sono limitate o illimitate? Se illimitate hanno antiperiodo?

5. Calcolare quante cifre di antiperiodo ha $\frac{N}{a}$, se non è limitata.

Congruenze

Proprietà delle congruenze lineari

1. $a\,x \equiv b \pmod{n}$ $\Leftrightarrow$ $(a \bmod n)\,x \equiv (b \bmod n) \pmod{n}$.
   esempio: $155x \equiv 85 \bmod 6 \Rightarrow 5x \equiv 1 \bmod 6$
2. $a\,x \equiv b \bmod n$ $\Rightarrow$ $k\,a\,x \equiv k\,b \bmod n$
   esempio: $5x \equiv 2 \bmod 7 \Rightarrow 3\cdot 5x \equiv 3\cdot 2 \bmod 7 \Rightarrow x \equiv 1 \bmod 7$
3. $k\,a\,x \equiv k\,b \bmod kn$ $\Rightarrow$ $a\,x \equiv b \bmod n$
   esempio: $3x \equiv 3 \bmod 6 \Rightarrow x \equiv 1 \bmod 2$
4. $k\,a\,x \equiv k\,b \bmod n$ e $MCD(k,n)=1$ $\Rightarrow$ $a\,x \equiv b \bmod n$
   esempio: $3x \equiv 3 \bmod 7 \Rightarrow x \equiv 1 \bmod 7$
5. $k\,a\,x \equiv k\,b \bmod n$ $(k\neq 0)$ $\Rightarrow$ $a\,x \equiv b \bmod \frac{n}{MCD(k,n)}$
   esempio: $6x \equiv 6 \bmod 21 \Rightarrow x \equiv 1 \bmod 7$
6. $a\,x \equiv b \bmod n$ e $d \mid n$ $\Rightarrow$ $a\,x \equiv b \bmod d$
   esempio: $3x \equiv 4 \bmod 10 \Rightarrow 3x \equiv 4 \bmod 2$ ($\Rightarrow x \equiv 0 \bmod 2$) e $3x \equiv 4 \bmod 5$
7. $a\,x \equiv b \bmod r$ e $a\,x \equiv b \bmod s$ $\Rightarrow$ $a\,x \equiv b \bmod (\text{mcm}(r,s))$
   esempio: $5x \equiv 4 \bmod 9$ e $5x \equiv 4 \bmod 6 \Rightarrow 5x \equiv 4 \bmod 18$

Esempio 1: Si dimostri che risulta $7x \equiv x \bmod 4$ se e solo se x è pari.

se x è pari $\Rightarrow$ $3x \equiv x \bmod 4$ infatti se $x = 2k$ è $2x \equiv 0 \bmod 4$ perché $2x = 4k \equiv 0 \bmod 4$

se $3x \equiv x \bmod 4$ $\Rightarrow$ x è pari infatti se $2x \equiv 0 \bmod 4$ allora $2x=4k \Rightarrow x=2k$

Esempio 2: Determinare tutte le possibili soluzioni del sistema di congruenze $\begin{cases} 86x \equiv 124 \mod 3 \\ 312 \equiv 82 \mod 11 \end{cases}$ illustrando le proprietà usate per la soluzione.

Poiché $a\,x \equiv b \pmod{n} \Leftrightarrow (a \bmod n)\,x \equiv (b \bmod n) \pmod{n}$, il sistema è $\begin{cases} 2x \equiv 1 \mod 3 \\ 4 \equiv 5 \mod 11 \end{cases}$.

L'inverso di 2 in Z_3 è 2, l'inverso di 4 in Z_{11} è 3, quindi poiché $a\,x \equiv b \bmod n \Rightarrow k\,a\,x \equiv k\,b \bmod n$ il sistema diventa $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 11 \end{cases}$.

Se $x \equiv 4 \bmod 11$, $x = 4 + 11k$. Cerchiamo k perché sia soddisfatta la prima congruenza.
$k = 0 \Rightarrow x = 4 \equiv 1 \bmod 3$, $k = 1 \Rightarrow x = 15 \equiv 0 \bmod 3$, $k = 2 \Rightarrow x = 26 \equiv 2 \bmod 3$, quindi la soluzione è $x = 26 + 33h$.

Esercizi:

1. Risolvere le congruenze lineari $3x \equiv 1 \pmod{25}$ e $2142x \equiv 442 \pmod{238}$.
2. Risolvere la congruenza lineare $3^9 x \equiv 2^8 \pmod 5$.
3. Stabilire quali e quante sono, in funzione di h, le soluzioni intere (tra 0 e 8) della congruenza $hx \equiv 1$ (mod. 9).
4. In Z_{11} determinare l'inverso rispetto al prodotto di n e a e risolvere l'equazione $5x = g$.
5. Quali e quante sono le soluzioni intere della congruenza $12x \equiv 18$ (mod. 33) con $0 \le x < 33$?
6. Calcolare l'inverso di g e di m in Z_{13}.
7. Scrivere quali elementi di Z_m sono invertibili rispetto al prodotto. Determinare l'inverso dei due elementi più grandi.
8. Determinare l'inverso rispetto al prodotto in Z_{11} di n e a.

Sulle congruenze del tipo $x^y \equiv w^z$

Qualche osservazione generale.
In un anello Z_p (con p primo) per il teorema di Fermat ogni elemento elevato alla $p-1$ è il neutro (del prodotto, quindi 1), per cui se m =2, 3, 5 o 7 è possibile non solo ridurre le basi a e 11 mod m, ma anche i due esponenti, (questi mod $m-1$, però)e poi i calcoli sono abbastanza semplici.
Se invece il modulo non è primo (e quindi se m =4, 6, 8 o 9), dopo aver ridotto le due basi, si può osservare che per basi prime con m vale una proprietà analoga. (teorema di Eulero–Fermat) La proprietà è la seguente: Z^*_m è un gruppo di ordine $k = \varphi(m)$ (k = numero di Eulero di m, che in particolare vale $p-1$ nel caso in cui sia $m = p$ primo). Allora ogni elemento di Z^*_m, cioè ogni elemento x primo con m ha un periodo che è un divisore di k, per cui sicuramente $x^k \equiv 1$. Allora si può ridurre l'esponente modulo k.
Per i restanti valori basta calcolare le prime potenze per capire l'andamento delle potenze e di conseguenza ottenere il risultato.

Esempio 1: Calcolare se risulta $17 \equiv 92^{129} \pmod 6$.
$17 \equiv 92^{129} \pmod 6 \Rightarrow 5 \equiv 2^{129} \mod 6 \Rightarrow$ poiché 6 non è primo e non è primo con 2 $\Rightarrow 2^3 \equiv 2 \mod 6 \Rightarrow 2^{129} = (2^3)^{43} \equiv 2^{43} = 2(2^{42}) \equiv 2(2^3)^{14} \equiv 2^{15} \equiv 2^5 \equiv 2^2 = 4 \Rightarrow$ falso: 5 non è congruo a 4

Esempio 2: Calcolare se risulta $14 \equiv 78^{129} \mod 10$
$14 \equiv 78^{129} \mod 10 \Rightarrow 4 \equiv 8^{129} \mod 10 \Rightarrow$ poiché 10 non è primo e non è primo con 8 $\Rightarrow 8^2 \equiv 4 \mod 10 \Rightarrow$ allora $8^{129} = 8\,(8^2)^{64} \equiv 8\,(4)^{64} \equiv 8\,(6)^{32} \equiv 48 \equiv 8$ quindi NO

Esempio 3: Calcolare se risulta $3 \equiv 77^{79} \mod 10$
10 non è primo, ma MCD(7,10)=1, Z^*_{10} ha ordine 4 $7^4 \equiv 1$ $7^{79} \equiv 7^3 \times 7^{76} \equiv 7^3 \equiv 3$ quindi sì

Esempio 4: Calcolare se risulta $19 \equiv 83^{67} \mod 8$
$3 \equiv 3^{67} \mod 8$ 8 non è primo, ma MCD(3,8)=1 Z^*_8 ha ordine 4, $3^{67} = 3^3 \times 3^{64} \equiv 3^3 = 27 \equiv 3$ quindi sì

Esempio 5: Calcolare se risulta $19 \equiv 88^{67} \mod 7$. 7 è primo, vale il teorema di Fermat:

$5 \equiv 4^{67} \bmod 7 \quad 4^6 \equiv 1 \quad 4^{67} \equiv 4$ dunque no

Esempio 5: Sia $z \in Z$ e sia MCD(z,47)=1. Stabilire quanto vale $z^{95} \bmod 47$.
47 è primo $z^{46} \equiv 1 \bmod 47$ per il teo di Fermat. $z^{95} = z^{46} \cdot z^{46} \cdot z^3 \equiv z^3$

Esercizi:

1. Che ore sono n ore dopo le g?
2. Calcolare se risulta $n \equiv a^{12} \pmod m$ o $n \equiv a^{12} \pmod g$
3. Calcolare se risulta $n \equiv a^{66} \pmod m$.
4. Calcolare se risulta $n^{123} \equiv a^{32} \pmod 7$ oppure mod 11, o mod 5, o mod 9.

Divisibilità

- Se si cerca la divisibilità **per un numero composto**, bisogna controllare la divisibilità per **tutti** i fattori primi, con l'avvertenza che se uno dei fattori primi ha esponente maggiore di 1, il criterio di divisibilità cambia (per esempio un numero non è divisibile per 12 se lo è per 2 e per 3, che sono i fattori primi di 12, ma se lo è per 4 e per 3, perché il criterio di divisibilità per 4 è diverso da quello per 3).
- Nel caso dei numeri primi, a parte i semplici criteri di divisibilità per 3 e 9, per 2 e 5, 4 e 25, 11, ci sono due metodi fondamentali per controllare la divisibilità, uno basato sulla scrittura polinomiale del numero e uno basato sulla "vicinanza" di una decina ad un multiplo del numero (metodo delle congruenze).
  - **scrittura polinomiale** Si può cercare un criterio di divisibilità per qualsiasi numero d: siano $r_0, r_1, r_2, \ldots$ i resti della divisione di $10^0, 10^1, 10^2, \ldots$ per d.
    Dette $a_0, a_1, a_2, \ldots, a_n$ le cifre di x, risulta $x \equiv r_0a_0 + r_1a_1 + r_2a_2 + \ldots + r_na_n$.
    Allora x è divisibile per d se $r_0a_0 + r_1a_1 + r_2a_2 + \ldots + r_na_n \equiv 0 \pmod d$.
    La successione dei resti è **sicuramente periodica**, dato che i resti non nulli della divisione per d possono essere al più $d - 1$
  - **congruenze.** Questo metodo ha senso se si trova un multiplo del numero d che interessa che disti 1 (in più o in meno) da una decina, altrimenti è più scomodo che fare la divisione... Il metodo si può usare se il numero k per cui bisogna moltiplicare 10 per avere la decina in questione è primo con d.
    Per esempio
    $13 \times 3 = 39$, dunque $40 \equiv 1 \bmod 39$, e quindi anche mod 13 e MCD(4,13)=1;
    $17 \times 3 = 51$ e quindi $50 \equiv -1 \bmod 17$ e MCD(5, 17)=1
    $20 \equiv 1 \bmod 19$ e MCD(2,19)=1 ecc.
    L'algoritmo è semplice: si scrive il numero nella forma $x \times 10 + u$ (dove u è la cifra delle unità, poi si moltiplica per k ottenendo (per la proprietà distributiva) $x \times (k \times 10) + ku$. Ma $k \times 10 \equiv 1$ (o $k \times 10 \equiv -1$ a seconda dei casi), quindi $x \times (k \times 10) + ku \equiv x + ku$ (o a $-x + ku$).
    Si itera poi fino ad avere un numero piccolo (due o 3 cifre…) e a quel punto si fa il calcolo a mano.
- La fondamentale differenza tra i due metodi (a parte che il secondo non sempre è conveniente) è che il primo dà come ultimo risultato il resto della divisione del numero per d, mentre il secondo no.

Esempio 1: Utilizzando la relazione 17×3=51, stabilire se 646727 è divisibile 17.
È richiesto il secondo dei due metodi. Risulta $50 \equiv -1 \mod 51$ (e quindi anche mod 17, dal momento che MCD(5,17)=1)

646727	64672×10+ 7	64672×50+ 35 ≡ - 64672 + 35=- 64637
64637	6463×10+7	6463×50+35 ≡ - 6463 + 35= -
6428	642×10+ 8	642×50+40 ≡ - 642+40 =-
602	60×10+2	60×50+10 ≡ -60+10= -50 non congruo a 0

Esempio 2: Stabilire se 646727 *N* è divisibile per 31
Non è assegnato il metodo, ma visto che risulta $30 \equiv -1 \mod 31$ conviene il secondo metodo.

646727	64672×10+7	64672×30+21≡ -64672+21= -64651
64651	6465×10+1	6465×30+3≡ -6465+3=-6462
6462	646×10+2	646×30+6≡ -646+6=-640
640	64×10+0	64×30≡ -64 non divisibile per 31

Esempio 3: lo stesso problema con l'altro metodo
$6\times10^5 + 4\times10^4 + 6\times10^3 + 7\times10^2 + 2\times10 + 7$ scrittura polinomiale
Calcolo i resti delle potenze di 10:
$1 \equiv 1 \mod 31$ $10 \equiv 10 \mod 31$ $10^2 \equiv 7 \mod 31$ $10^3 \equiv 8 \mod 31$ $10^4 \equiv 18 \mod 31$ $10^5 \equiv 25 \mod 31$
(non serve proseguire perché 10^5 è la potenza maggiore che compare nel numero)
Il numero è divisibile per 31 se lo è il numero a cui si perviene sostituendo alle potenze di 10 i loro resti:
$6\times25+4\times18+6\times8+7\times7+2\times10+7 \equiv -6\times6+4\times18+6\times8+7\times7+2\times10+7 \equiv -5+10+17+18+20+7 \equiv 67$ che non è divisibile per 31

Esempio 4: Trovare se 7438927 è divisibile per 39.
39 in realtà è 3×13, quindi si può prima di tutto vedere se il numero è divisibile per 3, e se non lo è è inutile proseguire, ma il numero dato non lo è, quindi il discorso ha senso.
$40 \equiv 1 \mod 39$ MCD(4, 39)=1 quindi posso usare il metodo (⇨: moltiplico per 4)

743892×10+7	⇨ 743892×40+28	≡ 743892+28 = 743920
74392×10+ 0	⇨ 74392×40	≡ 74392
7439×10+2	⇨ 7439×40+8	≡ 7439+8 = 7447
744×10+7	⇨ 744×40+28	≡ 744+28 = 772
77×10+2	⇨ 77×40+8	≡ 85
8×10+5	⇨ 8×40+20	≡ 28

28 non è divisibile per 39, quindi non lo è neppure 7438927

Esempio 5: Osservando che $50 \equiv 1 \pmod 7$, stabilire un diverso criterio di divisibilità per 7.
7438927 MCD(5,7)=1 posso usare il metodo (⇨: moltiplico per 5)

743892×10+7	⇨ 743892×50+35	≡ 743892+35 = 743927
74392×10+7	⇨ 74392×50+35	≡ 74392+35 = 74427
7442×10+7	⇨ 7442×50+35	≡ 7442+35 = 7477
747×10+7	⇨ 747×50+35	≡ 747+35 = 782
78×10+2	⇨ 78×50+10	≡ 88 non è divisibile per 7

Esempio 6: Stabilire se N è divisibile per 660 e determinare tutti i divisori di 660 per cui è divisibile
$660 = 11 \times 5 \times 3 \times 2^2$ allora N è divisibile per 660 se lo è per 11, per 5, per 3, per 4
N= 646727 non per 4 (dispari), non per 5 (finisce per 7), non per 3 (somma delle cifre $32 \equiv 2$), non per 11 (somma cifre a segni alterni $14-18=-4 \equiv 7$), quindi per nessuno dei divisori di 660, ma solo per 1.
N= 715924 sì per 4 ($24 \equiv 0 \bmod 4$), non per 5 (finisce per 4), non per 3 (somma delle cifre $28 \equiv 1$), sì per 11 (somma cifre a segni alterni $14-14=0$). Quindi è divisibile per 1, 2, 4, 22, 44.

Esempio 7: Stabilire quanti e quali sono i divisori di $10000 \cdot m$.

m=4 $40000 = 2^6 5^4$ i divisori sono 35 $=(6+1)\times(4+1)$

1	2	2^2	2^3	2^4	2^5	2^6
5	5×2	5×2^2	5×2^3	5×2^4	5×2^5	5×2^6
5^2	25×2	25×2^2	25×2^3	25×2^4	25×2^5	25×2^6
5^3	125×2	125×2^2	125×2^3	125×2^4	125×2^5	125×2^6
5^4	625×2	625×2^2	625×2^3	625×2^4	625×2^5	625×2^6

Esempio 7: Ricordando i criteri di divisibilità, mostrare che un numero le cui cifre in ordine crescente sono 1, 1, 2, 4, 4 più un numero sconosciuto di zeri non può mai essere un quadrato perfetto.

Quali criteri di divisibilità dipendono dalle cifre, ma non dal loro ordine e non tengono conto degli zeri né della loro posizione nel numero? Di quelli noti solo quello per 3 e 9, che usa la somma delle cifre. La somma delle cifre date vale 12, che è divisibile per 3, ma non per 9. Se il numero dato fosse un quadrato perfetto, avendo il fattore primo 3 sarebbe divisibile per 9, mentre non lo è.

Esercizi:

1. Calcolare il numero dei divisori di 280, 315, 1260, 440, 756 e indicarli tutti.
2. Stabilire se N è divisibile per 3, 4, 6, 9, 11. Ricordando che 19 = 20–1, costruire un algoritmo di divisibilità per 19 e stabilire se N è divisibile per 19.
3. Stabilire se N è divisibile per 3, 4, 6, 9, 11. Ricordando che $13\times3=39$, costruire un algoritmo di divisibilità per 13 e stabilire se N è divisibile per 13.
4. Stabilire se N è divisibile per 4, 6, 12, 24. Ricordando che $23\times3=69$, costruire un algoritmo di divisibilità per 23 e stabilire se *n* è divisibile per 23.
5. Utilizzando la relazione $7\times3=21$, stabilire se N è divisibile 7. (si osservi che $21=20+1=2\cdot10+1$) Illustrare i passi del procedimento usato. Lo stesso procedimento indica anche se N è divisibile per 3? Perché?
6. Utilizzando la relazione $17\times3=51$, stabilire se N è divisibile 17.
7. Stabilire se il numero 52341 è divisibile per 29, tenendo presente che $30 \equiv 1 \bmod 29$.

Equazioni diofantee

equazione diofantea = equazione algebrica a coefficienti interi, della quale si ricerchino soltanto le soluzioni intere (dunque se negli esercizi si trova un numero non intero, è **sbagliato**).
L'equazione $Ax + By = C$ (con $A, B, C \in \mathbb{Z}$) ammette soluzioni intere se e solo se C è un multiplo di MCD(A, B). In particolare, se A e B sono primi tra loro, esistono soluzioni intere.
Se una equazione diofantea lineare ammette soluzioni, queste sono infinite.

- La prima operazione da fare, se MCD(A, B) = k >1 e divide C è dividere per k tutta l'equazione. Supponiamo di aver fatto questa operazione e sia $ax + by = c$ il risultato.
- L'equazione $ax + by = c$ è equivalente ad una delle due seguenti congruenze:
$$ax \equiv c \bmod b \quad \text{oppure} \quad yb \equiv c \bmod a$$
- Non servono entrambe, ne basta una, ma:
  - il modulo **NON** può essere 1, quindi se $a = 1$ le soluzioni sono $y = k, x = c - bk$, se $b = 1$, le soluzioni sono $x = h, y = c - ah$.
  - **Conviene**, per la semplicità dei conti, scegliere delle due congruenze quella con modulo minore.
- Se la congruenza rimasta è $ax \equiv c \bmod b$, si usano le proprietà delle congruenze, moltiplicando ambo i membri per l'inverso di a in $\mathbb{Z}_b$, ottenendo $x \equiv c' \bmod b \Rightarrow x = c' + hb$.
- Si sostituisce il valore di x così trovato nell'equazione $ax + by = c$ (cioè quella ridotta) e si ricava y, che, se i conti sono esatti, deve essere un intero, funzione di h.

Esempio 1: Risolvere l'equazione diofantea $2x+3y=12$
$2x-12=-3y$ $\quad 2x\equiv 12 \bmod 3$ $\quad 2x\equiv 0 \bmod 3$ $\quad x\equiv 0 \bmod 3$ $\quad 3y+2(3k)=12$ $\quad y=4-2k, x=3k$
$x=0, y=4$ $\quad x=3, y=2$ $\quad x=6, y=0$ $\quad x=-3, y=6$ ……

Esempio 2: Risolvere l'equazione diofantea $3x + 7y = 23$.
Ricaviamo la congruenza $3x \equiv 23 \pmod 7$, cioè $3x \equiv 2 \pmod 7$.
In $\mathbb{Z}_7$ l'inverso di [3] è [5], dunque moltiplicando ambo i membri per 5 si ottiene $15x \equiv 3 \pmod 7$ cioè $x \equiv 3 \pmod 7$.
Le soluzioni per l'incognita x sono tutti e soli i numeri interi della forma $x = 3 + 7k$; sostituendo x nell'equazione $3x + 7y = 23 \Rightarrow 3(3 + 7k) + 7y = 23 \Rightarrow 7y=14-21k$ otteniamo $y = 2 - 3k$.
Concludendo: per ogni $k \in \mathbb{Z}$ dalle equazioni $x = 3 + 7k$ e $y = 2 - 3k$
si ottengono le infinite soluzioni ..., (–4, 5), (3,2) , (10,–1), …
Ricaviamo la congruenza $7y \equiv 23 \pmod 3$ cioè $y \equiv 2 \pmod 3$
Le soluzioni per l'incognita y sono tutti e soli i numeri interi della forma $y = 2 + 3k$
sostituendo y nell'equazione $3x + 7y = 23 \Rightarrow 3x + 14+21k = 23 \Rightarrow 3x = 9-21k \Rightarrow x=3-7k$

Esercizi:

1. Risolvere l'equazione diofantea $5x + 6y = 3$ $\quad (x= -3-6k\ ,\ y= 3+5k\ )$
2. Calcolare l'inverso di [6] in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{13}$; risolvere quindi le equazioni diofantee
$$6x+13y=11 \quad \text{e} \quad 6x+11y=11$$
3. Determinare il più piccolo $p > 2$ per cui l'equazione diofantea $gx + my = p$ ammette soluzioni.
4. Determinare il più piccolo numero $a' \geq a$ per cui l'equazione diofantea $gx + my = a'$ ammette

soluzioni e determinarle.

5. Determinare il più piccolo $p > 2$ per cui l'equazione diofantea $6x + 8y = p$ ammette soluzioni. Per tale valore determinare tali soluzioni.
6. Determinare il più grande $p <$ a per cui l'equazione diofantea $18x + 8y = p$ ammette soluzioni. Per tale valore determinare tali soluzioni.
7.