Aritmetica Modulare

Def Siano a, b interi e sia m un intero positivo.
Si dice che a e b sono congruenti modulo m se m divide $a-b$.

se a e b sono congruenti modulo m scriviamo $a \equiv b \pmod m$
(a è congruo a b modulo m)
se a e b non sono congruenti modulo m scriviamo $a \not\equiv b \pmod m$
(a non è congruo a b modulo m)

Esempi: $17 \equiv 5 \pmod 6$ $\quad 24 \equiv 0 \pmod 6$ $\quad 24 \not\equiv 14 \pmod 6$

OSS Essere congruenti modulo m è una relazione di equivalenza su $\mathbb{Z}$. cioè
(1) per ogni $a \in \mathbb{Z}$ $\quad a \equiv a \pmod m$
(2) per ogni $a, b \in \mathbb{Z}$ $\quad$ se $a \equiv b \pmod m$ allora $b \equiv a \pmod m$.
(3) per ogni $a, b, c \in \mathbb{Z}$ $\quad$ se $a \equiv b \pmod m$ e $b \equiv c \pmod m$ allora $a \equiv c \pmod m$

Dim: (1) $m \mid a-a$
(2) se $m \mid a-b$ allora $m \mid -(a-b)$, cioè $m \mid b-a$
(3) se $m \mid a-b$ e $m \mid b-c$ allora $m \mid a-b+b-c$, cioè $m \mid a-c$.

se due numeri sono congruenti modulo m vogliamo "identificarli".
Dobbiamo studiare $[a] = \{ b \in \mathbb{Z} \mid a \equiv b \pmod m \}$ (la classe di equivalenza di a).

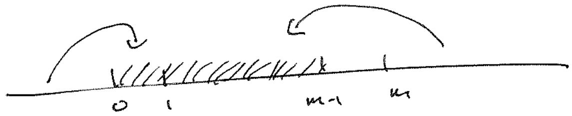
OSS Sia $a \in \mathbb{Z}$ e m un intero positivo. Allora $a \equiv r \pmod m$, dove r è il resto dopo la divisione di a per m.

Dim: $a = qm + r$. Quindi $m \mid a-r$, perciò $a \equiv r \pmod m$.

OSS Siano $a, b \in \mathbb{Z}$ e m un intero positivo. Siano $a = q_1 m + r_1$ con $0 \le r_1 < m$ e $b = q_2 m + r_2$ con $0 \le r_2 < m$. Allora $a \equiv b \pmod m$ se e solo se $r_1 = r_2$.

Dim: $(a-b) = (q_1 - q_2) m + r_1 - r_2$. Allora $-m < r_1 - r_2 < m$, quindi $m \mid (a-b)$ se e solo se $r_1 - r_2 = 0$.

i resti dopo la divisione di m sono $0, 1, \dots, m-1$. Questi numeri non sono congruenti modulo m fra di loro



ogni numero è congruente modulo m a uno di questi

<u>Notazione</u> denotiamo con $a \pmod m$ il resto della divisione di a per m cioè il numero tra 0 e $< m$ che è congruo ad a modulo m.

OSS Siano $a, b \in \mathbb{Z}$ e m un intero positivo
Allora $a \equiv b \pmod m$ se e solo se esiste un $k \in \mathbb{Z}$ con $a = b + km$

Dim. Se $a \equiv b \pmod m$ allora $m \mid a-b$. Quindi esiste un $k \in \mathbb{Z}$ con $a - b = km$, Quindi $a = b + km$.
Se $a = b + km$ per certo $k \in \mathbb{Z}$. allora $m \mid a-b$. Quindi $a \equiv b \pmod m$.

Esempio modulo 6 $\quad [a] = \{ b \in \mathbb{Z} \mid a \equiv b \pmod 6 \}$.

$[0] = \{ \cdots -12, -6, 0, 6, 12, \cdots \}$
$[1] = \{ \cdots -11, -5, 1, 7, 13, \cdots \}$
$[2] = \{ \cdots -10, -4, 2, 8, 14, \cdots \}$
$[3] = \{ \cdots -9, -3, 3, 9, 15, \cdots \}$
$[4] = \{ \cdots -8, -2, 4, 10, 16, \cdots \}$
$[5] = \{ \cdots -7, -1, 5, 11, 17, \cdots \}$

Teorema. Sia m un intero positivo, e siano $a, b, c, d \in \mathbb{Z}$ con
$a \equiv b \pmod m$ e $c \equiv d \pmod m$
Allora
$$a + c \equiv b + d \pmod m$$
$$a - c \equiv b - d \pmod m$$
$$a \cdot c \equiv b \cdot d \pmod m$$
"(mod m) si comporta bene rispetto a $+, -, \cdot$"

Dim: $a = b + km$ per certo $k \in \mathbb{Z}$
$c = d + lm$ per certo $l \in \mathbb{Z}$.
Quindi:
$$a + c = b + d + (k + l)m$$
$$a - c = b - d + (k - l)m$$
$$a \cdot c = (b + km)(d + lm) = bd + blm + dkm + klm^2$$
$$= bd + (bl + dk + klm)m.$$

Esempi

International standard book number
ISBN-10 $\quad$ 10 cifre $\quad x_1 x_2 \cdots x_{10}$ dove $x_1, \ldots, x_9 \in \{0, \ldots, 9\}$ e $x_{10} \in \{0, \ldots, 9, X\}$ $X = 10$
il numero x_{10} si dice numero di controllo.

$\underbrace{\text{Lingua} \quad \text{editore} \quad \text{titolo}}_{\text{9 cifre}} \quad \underbrace{\text{numero di controllo}}_{\text{1 cifra}}$ $\qquad$ Italiano: 88

vale $\displaystyle\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

osservazione: si vede l'errore di scambio di due numeri adiacenti

$x_1 x_2 \cdots x_{10}$ $\qquad x_1 + 2x_2 + \cdots + 10x_{10} \equiv 0 \pmod{11}$
$x_2 x_1 \cdots x_{10}$ $\qquad x_2 + 2x_1 + \cdots + 10x_{10} \equiv 0 \pmod{11}$

$x_1 - x_2 + 2x_2 - 2x_1 \equiv 0 \pmod{11}$

cioè $x_2 - x_1 \equiv 0 \bmod (11)$ $\quad$ cioè $x_1 \equiv x_2 \pmod{11}$ quindi $x_1 = x_2$.

European Article Number

EAN - 13   13 cifre $x_1, \dots, x_{13}$ dove $x_1, \dots, x_{13} \in \{0, \dots, 9\}$

il numero x_{13} si dice numero di controllo.

$$\underbrace{\underbrace{}_{\text{Paese dove il produttore è registrato}} \underbrace{}_{\text{produttore}} \underbrace{}_{\text{prodotto}}}_{12 \text{ cifre}} \underbrace{\underbrace{}_{\text{numero di controllo}}}_{1 \text{ cifra}}$$

Italia : 80 - 83

vale $x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} \equiv 0 \pmod{10}$.

ISBN - 13   13 cifre   978 e poi i primi 9 cifre del ISBN
979 e poi i primi 9 cifre del ISBN
977 per ISSN

vale la stessa regola come del EAN-13.

Esempio   calcolare potenze modulo m

Trovare il resto di 12^4 dopo la divisione per 17

$12^2 \equiv 144 \equiv 8 \pmod{17}$
$12^3 \equiv 8 \cdot 12 = 96 \equiv 11 \pmod{17}$
$12^4 \equiv 12 \cdot 11 = 132 \equiv 13 \pmod{17}$

Alternativa:
$12 \equiv -5 \pmod{17}$
$12^2 \equiv 25 \equiv 8 \pmod{17}$
$12^4 \equiv 64 \equiv 13 \pmod{17}$

Esempio : Trucci della scuola.

Sia $a \in \mathbb{N}$ $a = a_k a_{k-1} \dots a_1 a_0$ $a_0, \dots a_k \in \{0, \dots, 9\}$

$= a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$

a è divisibile per 9?

$1 \equiv 1 \pmod 9$
$10 \equiv 1 \pmod 9$
$10^i \equiv 1^i \equiv 1 \pmod 9$ quindi $a \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod 9$ cioè

$9 | a$ se e solo se $a \equiv 0 \pmod 9$
se e solo se $a_k + a_{k-1} + \dots + a_1 + a_0 \equiv 0 \pmod 9$
se e solo se la somma delle cifre è divisibile per 9.

simile per divisibilità per 3.

a è divisibile per 5?

$1 \equiv 1 \pmod 5$
$10 \equiv 0 \pmod 5$
$10^i \equiv 0 \pmod 5$ se $i \geq 1$.   Quindi $a \equiv a_0 \pmod 5$ cioè

$5 | a$ se e solo se $a \equiv 0 \pmod 5$ se e solo se $a_0 = 0$ o 5.

a è divisibile per 11?

$1 \equiv 1 \pmod{11}$
$10 \equiv -1 \pmod{11}$
$10^i \equiv (-1)^i \pmod{11}$ Quindi $a \equiv (-1)^k a_k + \dots + a_2 - a_1 + a_0 \pmod{11}$

$11 | a$ se e solo se $(-1)^k a_k + \dots + a_2 - a_1 + a_0 \equiv 0 \pmod{11}$.

<u>Teorema</u> Sia b un intero, $b \geq 2$. Ogni intero $a \geq 0$ può essere scritto in un e solo un modo nella forma

$$a = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 \quad \text{con} \quad 0 \leq a_i < b, \quad \text{per} \quad 1 \leq i \leq k, \quad \text{e} \quad a_k \neq 0$$

Scriviamo $a = (a_k a_{k-1} \dots a_1 a_0)_b$ (diciamo a in base b).

Dim. Esistenza

Sia $k \in \mathbb{Z}$ tale che $b^k \leq a < b^{k+1}$. Definiamo $q_0, \dots, q_k, a_0, \dots, a_k$ nel modo seguente:

$$\begin{aligned} a &= q_0 b + a_0 & 0 \leq a_0 < b \\ q_0 &= q_1 b + a_1 & 0 \leq a_1 < b \\ q_1 &= q_2 b + a_2 & 0 \leq a_2 < b \\ &\vdots \\ q_{k-1} &= q_k b + a_k & 0 \leq a_k < b \end{aligned}$$

Allora

$$\begin{aligned} a &= q_0 b + a_0 \\ &= q_1 b^2 + a_1 b + a_0 \\ &= q_2 b^3 + a_2 b^2 + a_1 b + a_0 \\ &\vdots \\ &= q_k b^{k+1} + a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 \end{aligned}$$

Ma $a < b^{k+1}$ quindi $q_k = 0$

inoltre se $a_k = 0$ $\quad a = a_{k-1} b^{k-1} + \dots + a_1 b + a_0 \leq (b-1)(b^{k-1} + \dots + 1) = b^k - 1 < a$, in contraddizione con $b^k \leq a$. Quindi $a_k \neq 0$.

unicità: più tardi.

Esempi

in base 2: $\quad 351 = 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2 + 1 \quad$ quindi $351 = (101011111)_2$

$$\begin{aligned} 135 &= 2 \cdot 67 + 1 \\ 67 &= 2 \cdot 33 + 1 \\ 33 &= 2 \cdot 16 + 1 \\ 16 &= 2 \cdot 8 + 0 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

$351 = (10000111)_2$

in base 8

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

$12345 = (30071)_8$

in base 16 usiamo $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, $F = 15$

Quindi $(DAF)_{16} = 13 \cdot 16^2 + 10 \cdot 16 + 15 = 3503$

Esempi in base 2 / calcolare modulo 2

$0+0 \equiv 0 \pmod 2$
$0+1 \equiv 1+0 \equiv 1 \pmod 2$
$1+1 \equiv 0 \pmod 2$

$a\,2^k + b\,2^k = (a+b)\,2^k$
$2^k + 2^k = 2^{k+1}$
$2 \cdot 2^k = 2^{k+1}$ ogni multiplicazione è un shift.

esempi: $(1110)_2 + (1011)_2$ $\qquad$ $(111)_2 + (111)_2 + (11)_2$

$$\begin{array}{r} 1110 \\ 1011 \\ \hline 11001 \end{array} \qquad \begin{array}{r} 111 \\ 111 \\ 011 \\ \hline 10001 \end{array}$$

$(1011)_2 \cdot (1110)_2$ $\qquad$ $(1101)_2 \cdot (11)_2$ $\qquad$ $(1111)_2 \cdot (1111)_2$

$$\begin{array}{r} 1110 \\ 1110\cdot \\ 0000\cdot\cdot \\ 1110\cdot\cdot\cdot \\ \hline 10011010 \end{array} \qquad \begin{array}{r} 11 \\ 00\cdot \\ 11\cdot\cdot \\ 11\cdot\cdot\cdot \\ \hline 100111 \end{array} \quad \begin{array}{r} 1101 \\ 1101\cdot \\ \hline 100111 \end{array} \qquad \begin{array}{r} 1111 \\ 1111\cdot \\ 1111\cdot\cdot \\ 1111\cdot\cdot\cdot \\ \hline 11100001 \end{array}$$

Torniamo alle congruenze

Esempio $\quad 10 \cdot 10 \equiv 100 \equiv 1 \pmod{11}$
$2 \cdot 5 \equiv 10 \equiv 0 \pmod{10}$ però $2 \not\equiv 0 \pmod{10}$ e $5 \not\equiv 0 \pmod{10}$.

Def Sia $a \in \mathbb{Z}$.
a si dice invertibile modulo m se esiste un $b \in \mathbb{Z}$ tale che $a \cdot b \equiv 1 \pmod m$
In tal caso b si dice un inverse di a modulo m.

Esempio $\quad 3 \cdot 5 \equiv 1 \pmod 7$ $\qquad$ $10 \cdot 5 \equiv 1 \pmod 7$
3 è un inverse di 5 $\pmod 7$ $\qquad$ 10 è un inverse di 5 $\pmod 7$
5 è un inverse di 3 $\pmod 7$

Oss se b esiste allora b è unico modulo m
Dim: se $a \cdot b \equiv 1 \pmod m$ e $a \cdot b' \equiv 1 \pmod m$ allora
$b \equiv b \cdot 1 \equiv b \cdot a b' \equiv 1 \cdot b' \equiv b' \pmod m$

Oss Sia $a \in \mathbb{Z}$, $a \neq 0$, e m un intero positivo.
a è invertibile modulo m se e solo se $\mathrm{mcd}(a,m) = 1$.

Dim "$\Rightarrow$" Sia $a \in \mathbb{Z}$. supponiamo che a è invertibile modulo m. Allora esiste un $b \in \mathbb{Z}$ tale che $a \cdot b \equiv 1 \pmod m$. Cioè $ab = 1 + km$ per certo $k \in \mathbb{Z}$.
Allora $ab - km = 1$. Quindi l'equazione diofantea lineare $ax + my = 1$ ha soluzioni (prendo $x = b$ e $y = -k$). Quindi $\mathrm{mcd}(a,m) = 1$
"$\Leftarrow$" se $\mathrm{mcd}(a,m) = 1$ esistono $x, y \in \mathbb{Z}$ tale che $1 = ax + my$.
Cioè $1 \equiv ax \pmod m$. Quindi x è un inverse di a modulo m.

Con l'inverso intendiamo quello tra 0 e $m-1$

Esempio: le inverse di 3 mod 13

$\operatorname{mcd}(3,13)$ $\quad 13 = 3.4+1$ $\quad\quad 1 = 13 - 3.4$

$3 = 1.3+0$ $\quad\quad 1 = 13.1 + 3.(-4)$

$\operatorname{mcd}(3,13)=1$ inverso esiste $\quad 1 \equiv 3.(-4) \pmod{13}$

un inverso di 3 è -4. $\quad -4 \equiv 9 \pmod{13}$

Quindi le inverse di 3 sono $\{\dots,-4,9,22,\dots\}$. L'inverso è 9.

OSS. Siano $a,b,c,m,x \in \mathbb{Z}$, $m>0$, con a invertibile modulo m e c una sua inversa. Allora $ax \equiv b \pmod{m}$ se e solo se $x \equiv bc \pmod{m}$.

Dim: Esiste un $l \in \mathbb{Z}$ con $ac = 1 + lm$.

"$\Rightarrow$" Se $ax \equiv b \pmod{m}$ allora $ax = b + km$ per certo $k \in \mathbb{Z}$. Quindi $acx = bc + kcm$. Cioè $(1+lm)x = bc + kcm$. Quindi $x = bc + (kc - lx)m$. Quindi $x \equiv bc \pmod{m}$.

"$\Leftarrow$" se $x \equiv bc \pmod{m}$ allora $x = bc + km$ per certo $k \in \mathbb{Z}$. Quindi $ax = abc + akm$. Cioè $ax = b(1+lm) + akm$. Quindi $ax = b + (bl + ak)m$. Quindi $ax \equiv b \pmod{m}$.

Esempio: risolvere il sistema $5x \equiv 3 \pmod{7}$.

$\operatorname{mcd}(5,7)$ $\quad 7 = 5.1+2$ $\quad\quad 1 = 5 - 2.2$

$5 = 2.2+1$ $\quad\quad = 5 - (7 - 5.1).2 = 5.3 - 7.2$

$2 = 1.2 + 0$ $\quad\quad 1 = 5.3 + 7.(-2)$

$\operatorname{mcd}(5,7) = 1$ $\quad\quad 1 \equiv 5.3 \pmod{7}$

un inverso di $5 \pmod{7}$ è 3

$$5x \equiv 3 \pmod{7}$$
$$3.5x \equiv 3.3 \pmod{7}$$
$$x \equiv 9 \pmod{7}$$
$$x \equiv 2 \pmod{7}.$$

OSS Se m è un numero primo ogni intero a, con $1 \le a \le m-1$ è invertibile. (perché se m è primo $\operatorname{mcd}(a,m)=1$ per ogni $1 \le a \le m-1$.)

Ma non sempre si può trovare un inverso:

Esempio risolvere $5x \equiv 5 \pmod{10}$ $\quad \operatorname{mcd}(5,10)=5$ 5 non è invertibile

però 1, 3, 5, 7, 9 sono soluzioni

risolvere $5x \equiv 1 \pmod{10}$ non ha soluzioni perché 5 non è invertibile.

OSS Siano $a, b \in \mathbb{Z}$ e m un intero positivo.

Consideriamo l'equazione $ax \equiv b \pmod m$.

Allora (1) l'equazione ha soluzioni se e solo se $\mathrm{mcd}(a,m) \mid b$

(2) Se l'equazione ha soluzioni ne ha $\mathrm{mcd}(a,m)$ modulo m

Dim (1) "$\Rightarrow$" Supponiamo che x_0 è una soluzione di $ax \equiv b \pmod m$.

Allora esiste un $k \in \mathbb{Z}$ con $ax_0 = b + km$, cioè $ax_0 - km = b$.

Quindi l'equazione diofantea lineare $ax + my = b$ ha soluzioni

Quindi dobbiamo avere $\mathrm{mcd}(a,m) \mid b$.

"$\Leftarrow$" Se $\mathrm{mcd}(a,m) \mid b$ allora l'equazione $ax + my = b$ ha soluzioni

sia (x_0, y_0) una soluzione. Allora $ax_0 + my_0 = b$, quindi $ax_0 \equiv b \pmod m$

Quindi x_0 è una soluzione di $ax \equiv b \pmod m$.

osservazione: le soluzioni di $ax \equiv b \pmod m$ sono quelli di $ax + my = b$ dove si guarda solo al valore di x.

(2) Sia $d = \mathrm{mcd}(a,m)$. Supponiamo che $d \mid b$

Le soluzioni di $ax + my = b$ sono $x = \frac{x'b + mk}{d}$, $y = \frac{y'b - ak}{d}$

dove (x', y') è una soluzione di $ax + my = d$ e $k \in \mathbb{Z}$. Allora $x = \frac{x'b}{d} + k\frac{m}{d}$

Sia $x_0 = \frac{x'b}{d}$. Allora le soluzioni sono $x = x_0 + k\frac{m}{d}$, $k \in \mathbb{Z}$.

modulo m ci sono d soluzioni diversi.

Esempio

Trovare le soluzioni di $6x \equiv 8 \pmod{14}$.

- calcoliamo $\mathrm{mcd}(6, 14)$ $\quad 14 = 6 \cdot 2 + 2$
  $6 = 2 \cdot 3 + 0 \quad \mathrm{mcd}(6,14) = 2$

- $2 \mid 8$ quindi ci sono soluzioni e modulo 14 ci sono 2.

- consideriamo $6x + 14y = 8$ $\quad \mathrm{mcd}(6,14) = 2$, $2 \mid 8$ ci sono soluzioni

  - omogeneo $6x + 14y = 0$
    $3x + 7y = 0$ $\quad$ soluzioni omogeneo $\begin{cases} \tilde{x} = -7k \\ \tilde{y} = 3k \end{cases}$ $k \in \mathbb{Z}$.

  - sol. particolare $2 = 14 - 6 \cdot 2$
    $2 = 6 \cdot (-2) + 14 \cdot (1)$
    $8 = 6 \cdot (-8) + 14(4)$ $\quad$ una sol. particolare: $\begin{cases} x_0 = -8 \\ y_0 = 4 \end{cases}$

  Le soluzioni di $6x + 14y = 8$ sono $\begin{cases} x = -8 - 7k \\ y = 4 + 3k \end{cases}$ $k \in \mathbb{Z}$.

- Le soluzioni di $6x \equiv 8 \pmod{14}$ sono $x = -8 - 7k$ $\quad k \in \mathbb{Z}$

  però vogliamo la risposta modulo 14. $-8 \equiv 6 \pmod{14}$ $\quad 6 + 7 = 13$

  soluzioni: $x \equiv 6 \pmod{14}$ o $x \equiv 13 \pmod{14}$.

Vogliamo anche studiare sistemi di equazioni del tipo

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 3 \pmod 5 \end{cases}$$

<u>Teorema cinese dei resti</u>

Siano $m_1, m_2, \ldots, m_n$ interi positivi, due a due relativamente primi, e siano $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Sia $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$. Allora

il sistema $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$ ha un unico soluzione modulo m.

Cioè c'è un unico soluzione x con $0 \leq x < m$ e tutti gli altri soluzioni sono congruente modulo m ad x.

Dim: Sia $M_k = m_1 \cdot m_2 \cdots m_{k-1} \, m_{k+1} \cdots m_n = \frac{m}{m_k}$, $k \in \{1, \ldots, n\}$.

m_k è relativamente primo con $m_1, m_2, \ldots, m_{k-1}, m_{k+1}, \ldots, m_n$. Quindi

$\mathrm{mcd}(m_k, M_k) = 1$. Cioè M_k è invertibile modulo m_k.

per ogni $1 \leq k \leq n$ esiste un $y_k \in \mathbb{Z}$ con $M_k y_k \equiv 1 \pmod{m_k}$

Sia $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$. Sia $1 \leq j \leq n$,

Se $j \neq k$ allora $m_k \mid M_j$ quindi $M_j \equiv 0 \pmod{m_k}$

Quindi $x \equiv a_k M_k y_k \pmod{m_k}$. Ma $M_k y_k \equiv 1 \pmod{m_k}$

Quindi $x \equiv a_k \pmod{m_k}$

Quindi per ogni k, $1 \leq k \leq n$, $x \equiv a_k \pmod{m_k}$.

Segue che x è una soluzione.

Sia y una soluzione. Allora $\begin{cases} x - y \equiv 0 \pmod{m_1} \\ x - y \equiv 0 \pmod{m_2} \\ \vdots \\ x - y \equiv 0 \pmod{m_n} \end{cases}$

Quindi $x - y$ è divisibile per $m_1, m_2, \ldots, m_n$. Segue che $x - y$ è divisibile per m perché $m_1, m_2, \ldots, m_n$ sono due a due relativamente primi.

Quindi $x - y \equiv 0 \pmod m$. Cioè $x \equiv y \pmod m$.

Sia $z \in \mathbb{Z}$ con $x \equiv z \pmod m$. Allora $z = x + l \cdot m$ per certo $l \in \mathbb{Z}$

Allora $\begin{cases} z \equiv x \pmod{m_1} \\ \vdots \\ z \equiv x \pmod{m_n} \end{cases}$ cioè $\begin{cases} z \equiv a_1 \pmod{m_1} \\ \vdots \\ z \equiv a_n \pmod{m_n} \end{cases}$. Quindi z è una soluzione.

Esempio risolvere $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 7 \pmod{31} \end{cases}$

$m = 3 \cdot 7 \cdot 31 = 651$

modulo 3: $M_1 = 7 \cdot 31 = 217$ $\quad 217 \equiv 1 \pmod 3$ $\quad M_1 y_1 \equiv 1 \pmod 3$ $\quad 1 \cdot y_1 \equiv 1 \pmod 3$ $\quad y_1 = 1$.

modulo 7: $M_2 = 3 \cdot 31 = 93$ $\quad 93 \equiv 2 \pmod 7$ $\quad M_2 y_2 \equiv 1 \pmod 7$ $\quad 2 y_2 \equiv 1 \pmod 7$ $\quad y_2 = 4$

modulo 31: $M_3 = 3 \cdot 7 = 21$ $\quad 21 \equiv 21 \pmod{31}$ $\quad M_3 y_3 \equiv 1 \pmod{31}$ $\quad 21 y_3 \equiv 1 \pmod{31}$

$31 = 21 \cdot 1 + 10$ $\qquad 1 = 21 - 10 \cdot 2$

$21 = 10 \cdot 2 + 1$ $\qquad = 21 - (31 - 21 \cdot 1) \cdot 2 = 3 \cdot 21 - 31 \cdot 2$

$10 = 1 \cdot 10 + 0$ $\qquad 1 = 3 \cdot 21 + 31(-2)$ quindi $1 \equiv 3 \cdot 21 \pmod{31}$ $\qquad y_3 = 3$

$x = 1 \cdot 217 \cdot 1 + 2 \cdot 93 \cdot 4 + 7 \cdot 21 \cdot 3$

$= 217 + 744 + 441 = 1402$ $\qquad 1402 \equiv 100 \pmod{651}$

Quindi $x \equiv 100 \pmod{651}$.

(controllo: $100 \equiv 1 \pmod 3$ ok!
$100 \equiv 2 \pmod 7$ ok!
$100 \equiv 7 \pmod{31}$ ok!).

Esempio risolvere $\begin{cases} 2x \equiv 5 \pmod 3 \\ 9x \equiv -2 \pmod{10} \end{cases}$ $\qquad 3 \cdot 10 = 30$

1° equazione: $2x \equiv 5 \pmod 3$ $\quad \mathrm{mcd}(2,3) = 1$ quindi 2 è invertibile modulo 3. l'inverso è 2. Quindi $4x \equiv 10 \pmod 3$ cioè $x \equiv 1 \pmod 3$.

2° equazione: $9x \equiv -2 \pmod{10}$ $\quad \mathrm{mcd}(9,10) = 1$, quindi 9 è invertibile modulo 10 un inverso è -1. Quindi $-9x \equiv 2 \pmod{10}$ cioè $x \equiv 2 \pmod{10}$

Dobbiamo risolvere $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod{10} \end{cases}$

modulo 3 $\quad M_1 = 10$ $\quad M_1 y_1 \equiv 1 \pmod 3$
$10 y_1 \equiv 1 \pmod 3$
$y_1 \equiv 1 \pmod 3$
$y_1 = 1$

modulo 10 $\quad M_2 = 3$ $\quad M_2 y_2 \equiv 1 \pmod{10}$
$3 y_2 \equiv 1 \pmod{10}$
$y_2 = -3$

$x = 1 \cdot 10 \cdot 1 + 2 \cdot 3 \cdot (-3) = 10 - 18 = -8$ è una soluzione. $\qquad -8 \equiv 22 \pmod{30}$

soluzioni: $x \equiv 22 \pmod{30}$. (Fai i controlli).

Esempio risolvere $\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 3 \pmod 8 \end{cases}$ $\qquad 15 \cdot 8 = 120$

modulo 15 $\quad M_1 = 8$ $\quad 8 y_1 \equiv 1 \pmod{15}$

$15 = 8 \cdot 1 + 7$ $\qquad 1 = 8 - 7 \cdot 1 = 8 - (15 - 8 \cdot 1) \cdot 1$
$8 = 7 \cdot 1 + 1$ $\qquad = 8 \cdot 2 - 15 \cdot 1$
$7 = 1 \cdot 7 + 0$ $\qquad 1 = 8 \cdot 2 + 15 \cdot (-1)$ $\qquad y_2 = 2$

modulo 8 $\quad M_2 = 15$ $\quad 15 y_2 \equiv 1 \pmod 8$
$-y_2 \equiv 1 \pmod 8$ $\qquad y_2 = -1$

una soluzione $x = 2 \cdot 8 \cdot 2 + 3 \cdot 15 \cdot (-1) = -13$ $\qquad -13 \equiv 107 \pmod{120}$

soluzione $x \equiv 107 \pmod{120}$ $\qquad$ (controllo $107 \equiv 2 \pmod{15}$ $\quad 107 \equiv 3 \pmod 8$)

Esempio prendiamo $m_1 = 3$ $m_2 = 7$ $m_3 = 31$ $m = 3 \cdot 7 \cdot 31 = 651$.

Sia $a \in \mathbb{Z}$ con $0 \leq a < 651$

consideriamo $a \longmapsto (a \pmod 3, \ a \pmod 7, \ a \pmod{31})$

cioè
$$100 \longmapsto (1, 2, 7)$$
$$3 \longmapsto (0, 3, 3)$$
$$17 \longmapsto (2, 3, 17)$$

$117 = 100 + 17$ $\qquad 107 \longmapsto (0, 5, 24) = (1, 2, 7) + (2, 3, 17)$

$117 \equiv 1 + 2 \pmod 3$ $\qquad$ "componente per componente"

$\equiv 2 + 3 \pmod 7$

$\equiv 7 + 17 \pmod{31}$

$51 = 3 \cdot 17$ $\qquad 51 \longmapsto (0, 2, 20) = (0, 3, 3) \cdot (2, 3, 17)$

$51 \equiv 0 \cdot 2 \pmod 3 = 0 \pmod 3$ $\qquad$ "componente per componente"

$\equiv 3 \cdot 3 \pmod 7 \equiv 2 \pmod 7$

$= 3 \cdot 17 \pmod{31} \equiv 20 \pmod{31}$

c'è una biezione tra i numeri a, $0 \leq a < 651$ è i tripli $(-,-,-)$

il calcolo si riduce modulo 3, modulo 7, modulo 31.

Alla fine si deve usare il teorema cinesi dei resti per convertire il numero $(-,-,-)$ in un numero tra 0 e 651.

Applicazione: Calcolo veloce sul compute con numeri grandi

osservazione (falso) fatto dei cinesi

n è primo se e solo se $2^{n-1} \equiv 1 \pmod n$.

Non è vero!! prendo $n = 341 = 11 \cdot 31$ però $2^{340} \equiv 1 \pmod{341}$

perche: $2^{10} = 1024 = 3 \cdot 341 + 1$ quindi $2^{10} \equiv 1 \pmod{341}$

$2^{340} \equiv (2^{10})^{34} \equiv (1)^{34} \equiv 1 \pmod{341}$.

che è vero:

<u>Teorema</u> (il piccolo teorema di Fermat)

Sia p un primo e a un intero. Allora

(1) $a^p \equiv a \pmod p$

(2) se $p \nmid a$ allora $a^{p-1} \equiv 1 \pmod p$

Dim (2) segue da (1) perche se $p \nmid a$ allora $\text{mcd}(a, p) = 1$.

Quindi a è invertibile modulo p. Sia b una sua inverse

Allora $a^p \equiv a \pmod p$

$a \cdot a^{p-1} \equiv a \pmod p$

$b\,a\,a^{p-1} \equiv b\,a \pmod p$

$a^{p-1} \equiv 1 \pmod p.$

Basta dimostrare che vale (1).

se $a \equiv 0 \pmod p$ allora $a^p \equiv 0^p \pmod p$

$\equiv 0 \pmod p$

$\equiv a \pmod p$ quindi $a^p \equiv a \pmod p$.

se $a \not\equiv 0 \pmod p$ allora $\mathrm{mcd}(a,p)=1$ (perché p è un primo)

Quindi a è invertibile modulo p.

Sia $h : \{1,2,\dots,p-1\} \longrightarrow \{1,2,\dots,p-1\}$

$x \longmapsto a\,x \pmod p$

allora h è un applicazione invertibile. Perciò

$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv h(1) \cdot h(2) \cdot \ldots \cdot h(p-1) \pmod p$

$\equiv a^{p-1}\, 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p$

Ma $1 \cdot 2 \cdot \ldots (p-1) \not\equiv 0 \pmod p$ quindi è invertibile modulo p.

segue che $a^{p-1} \equiv 1 \pmod p$.

Più tardi facciamo un altra dimostrazione.

Il teorema implica:

siano $a, n \in \mathbb{Z}$, $n > 1$ con $\mathrm{mcd}(a,n)=1$

se $a^{n-1} \not\equiv 1 \pmod n$ allora n non è primo

Esempio

$n = 51$ $\quad 2^{50} \equiv 4 \pmod{51}$. Quindi 51 non è primo

sta attento, se $a^{n-1} \equiv 1 \pmod n$ allora non è detto che n è primo:

$n = 341$ allora $2^{340} \equiv 1 \pmod{341}$, ma 341 non è primo $341 = 11 \cdot 31$

Quindi si può usare il piccolo teorema di Fermat per far vedere che un numero non è primo <u>senza</u> trovare un fattorizzazione in primi del numero.