Lezione di martedì 26 marzo 2019 (0)

(Scaricatela e portatela in aula F8: vi può essere d'aiuto).

Il teorema cinese del resto

Consideriamo le due congruenze $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 4 \end{cases}$: evidentemente il sistema non ha soluzione, anche se le due congruenze, separatamente, hanno soluzione. Si tratta di due congruenze incompatibili. Il seguente importante teorema ci dice che k congruenze sono sempre compatibili (cioè il sistema ha soluzione) se i moduli sono relativamente primi a due a due. Vale infatti il seguente

Teorema cinese del resto

Siano $m_1, m_2, \dots, m_k$ moduli a due a due relativamente primi, cioè $(m_i, m_j) = 1$ se $i \neq j$, $1 \leq i, j \leq k$. Allora il sistema di congruenze

$$1) \quad \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad - \qquad - \\ \quad - \qquad - \\ x \equiv b_k \pmod{m_k} \end{cases}$$

ha soluzione unica modulo $M = m_1 m_2 \cdots m_k$.

Dimostrazione

La dimostrazione è costruttiva: poniamo

$M = m_1 m_2 \cdots m_k$ e $M_i = \frac{M}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j$.

Si ha $(M_i, m_i) = 1$ e quindi esiste M_i' tale che

$$2) \quad M_i M_i' \equiv 1 \pmod{m_i}$$

per ogni $i = 1, 2, \ldots, k$.

Dico che

$$x_0 \equiv M_1 M_1' b_1 + M_2 M_2' b_2 + \cdots + M_k M_k' b_k \pmod{M}$$

è soluzione del sistema 1).

Infatti si ha

$$4) \quad x_0 \equiv M_i M_i' b_i \pmod{m_i}$$

per ogni $i = 1, 2, \ldots, k$ (questo perché gli M_h con $h \neq i$ sono $\equiv 0 \pmod{m_i}$).

Inoltre, per la 2), si ha

$$5) \quad M_i M_i' b_i \equiv b_i \pmod{m_i}$$

per ogni i. Da 4) e 5) segue

$$6) \quad x_0 \equiv b_i \pmod{m_i}$$

per ogni $i = 1, 2, \ldots, k$.

Ciò prova che x_0 è soluzione del sistema.

Dimostriamo ora che tale soluzione è unica

$\mod M$, dove $M = m_1 m_2 \cdots m_k$. Infatti, se x_1 ed x_2 sono due soluzioni del sistema 1), si ha

$$x_1 \equiv b_i \pmod{m_i}, \quad \forall i = 1, 2, \ldots, k$$

e

$$x_2 \equiv b_i \pmod{m_i}, \quad \forall i = 1, 2, \ldots, k$$

da cui segue

$$7) \quad x_1 \equiv x_2 \pmod{m_i}, \quad \forall i = 1, 2, \ldots, k$$

Dato che i moduli m_i sono relativamente primi a due a due, dalla 7) segue

$$8) \quad x_1 \equiv x_2 \pmod{M}$$

dove, appunto, $M = m_1 m_2 \cdots m_k$.

Ciò prova completamente il teorema.

Ovviamente, se x_0 è soluzione del sistema 1), ogni $x \equiv x_0 \pmod{M}$ è pure soluzione.

Esempio

Risolvere il sistema

$$9) \begin{cases} x \equiv b_1 \pmod 7 \\ x \equiv b_2 \pmod{11} \\ x \equiv b_3 \pmod{13} \end{cases}$$

In questo caso $m_1 = 7$, $m_2 = 11$ e $m_3 = 13$, quindi i moduli sono relativamente primi a due a due. Ne segue, per il teorema cinese del resto, che

il sistema 9) ha soluzione unica mod M, dove

10) $M = m_1 m_2 m_3 = 7 \cdot 11 \cdot 13 = 1001$

Procedendo come indicato nella dimostrazione del teorema, poniamo

11) $M_1 = \frac{M}{m_1} = 11 \cdot 13 = 143$

$M_2 = \frac{M}{m_2} = 7 \cdot 13 = 91$

$M_3 = \frac{M}{m_3} = 7 \cdot 11 = 77$

Dobbiamo ora calcolare M_1', M_2', M_3', dove

$M_1 M_1' \equiv 1 \pmod{m_1}$

12) $M_2 M_2' \equiv 1 \pmod{m_2}$

$M_3 M_3' \equiv 1 \pmod{m_3}$

cioè

13) $143 M_1' \equiv 1 \pmod 7$

$91 M_2' \equiv 1 \pmod{11}$

$77 M_3' \equiv 1 \pmod{13}$

Ma $143 \equiv 3 \pmod 7$ e quindi la prima di 13) equivale a $3 M_1' \equiv 1 \pmod 7$: siccome $7 = 3 \cdot 2 + 1$ si ha $3(-2) \equiv 1 \pmod 7$, quindi

14) $M_1' \equiv -2 \equiv 5 \pmod 7$

Per la seconda di 13) si ha, dato che $91 \equiv 3 \pmod{11}$, che $3M_2' \equiv 1 \pmod{11}$: poiché

$$\begin{cases} 11 = 3 \cdot 3 + 2 \\ 3 = 2 \cdot 1 + 1 \\ 2 = 1 \cdot 2 + 0 \end{cases}$$

si ha $1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11$, da cui

15) $M_2' \equiv 4 \pmod{11}$

Infine, siccome $77 \equiv 12 \pmod{13}$, la terza congruenza di 13) equivale a

16) $12 M_3' \equiv 1 \pmod{13}$

Ma $13 = 12 \cdot 1 + 1$ e quindi $12(-1) \equiv 1 \pmod{13}$, perciò

17) $M_3' \equiv -1 \equiv 12 \pmod{13}$

Da 14), 15) e 17) segue, ricordando le 11),

18) $M_1 M_1' = (143) \cdot (5) = 715$

$M_2 M_2' = (91)(4) = 364$

$M_3 M_3' = (77)(12) = 924$

Ne segue che la soluzione del sistema 9) è data da

19) $x_0 \equiv M_1 M_1' b_1 + M_2 M_2' b_2 + M_3 M_3' b_3 \equiv$

$\equiv (715) b_1 + (364) b_2 + (924) b_3 \pmod{1001}$

Qualunque sia le terne assegnate b_1, b_2, b_3.

Ad esempio, per $b_1 = 5$, $b_2 = 3$, $b_3 = 10$ il sistema

20) $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 3 \pmod{11} \\ x \equiv 10 \pmod{13} \end{cases}$

ha come soluzione

21) $x_0 \equiv (715)(5) + (364)(3) + (924)(10) \equiv$

$\equiv (-286)(5) + (364)(3) + (-77)(10) \equiv$

$\equiv (-1430) + (1092) - (770)$

$\equiv (-338) - (770) \equiv$

$\equiv -1108 \equiv -107 \equiv$

$\equiv 894 \pmod{1001}$

Osservazione

La dimostrazione del teorema cinese ci dice che l'algoritmo per la soluzione del sistema 1) di congruenze lineari simultanee è molto "veloce". In effetti si tratta di calcolare degli inversi moltiplicativi (vedi formula 2), quindi l'algoritmo euclideo

Un'importante conseguenza del teorema cinese del resto è la moltiplicatività della funzione φ di Eulero. Ricordiamo che una funzione f definita sui naturali, $f: \mathbb{N} \to \mathbb{R}$, si dice moltiplicativa, se vale l'implicazione

22) $(m_1, m_2) = 1 \implies f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$

Dimostriamo ora il seguente

Teorema

La funzione φ di Eulero è moltiplicativa.

Dimostrazione

Ci rifacciamo al precedente simbolismo: siano $m_1, m_2, \dots, m_k$ moduli relativamente primi a due a due, cioè $(m_i, m_j) = 1$ se $i \neq j$, e sia $M = m_1 m_2 \cdots m_k$. Dimostreremo, ricordando il teorema cinese del resto, che la funzione

23) $$\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \cdots \mathbb{Z}^*_{m_k} \longrightarrow \mathbb{Z}^*_M$$

$$(b_1, b_2, \dots, b_k) \longrightarrow x \equiv M_1 \pi'_1 b_1 + \cdots + M_k \pi'_k b_k \pmod{M}$$

è

i) iniettiva

ii) suriettiva

(Qui $\mathbb{Z}^*_{m_i}$ indica un sistema ridotto di resti mod m_i, $\mathbb{Z}^*_M$ indica un sistema ridotto di resti mod $M = m_1 m_2 \cdots m_k$)

Come prima cosa osserviamo che la funzione è ben definita, cioè che $x \in \mathbb{Z}_M^*$. Infatti si ha $x \equiv M_i M_i' b_i \equiv b_i \pmod{m_i}$, per ogni i, e dato che $(b_i, m_i) = 1$, si ha anche $(x, m_i) = 1$ per ogni $i = 1, 2 \dots, k$, da cui segue $(x, M) = 1$.
Inoltre l'applicazione è iniettiva: infatti, se

$$24) \quad x' \equiv M_1 M_1' b_1' + \dots + M_k M_k' b_k' \pmod{M}$$

da $x \equiv x' \pmod{M}$ segue $b_i \equiv b_i' \pmod{m_i}$, per ogni i.
Ciò si dimostra osservando che

$$25) \quad x \equiv x' \pmod{M} \iff x \equiv x' \pmod{m_i}, \ i = 1, 2, \dots, k$$

ma

$$26) \quad \begin{aligned} x &\equiv M_i M_i' b_i \equiv b_i \pmod{m_i} \\ x' &\equiv M_i M_i' b_i' \equiv b_i' \pmod{m_i} \end{aligned} \quad \text{e, } i = 1, \dots, k$$

Da 25) e 26) segue appunto

$$27) \quad x \equiv x' \pmod{M} \Rightarrow b_i \equiv b_i' \pmod{m_i}$$
per ogni $i = 1, \dots, k$.

Ciò prova l'iniettività.
Infine l'applicazione è suriettiva, infatti da $(x, M) = 1$ segue $(x, m_i) = 1$ per ogni i, e quindi

$$28) \quad \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_k \pmod{m_k} \end{cases} \quad \text{con } (b_i, m_i) = 1 \ \forall i = 1, \dots, k$$

da cui segue, per il teorema cinese,

29) $x \equiv M_1 M_1' b_1 + \dots + M_k M_k' b_k \pmod M$

che è la rappresentazione 23). Ciò prova la suriettività.

Quanto dimostrato implica che i due insiemi

$\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \dots \times \mathbb{Z}^*_{m_k}$ e $\mathbb{Z}^*_{M = m_1 m_2 \dots m_k}$

abbiano la stessa cardinalità (infatti l'applicazione 23) è biiettiva): ma il primo ha

30) $\varphi(m_1)\varphi(m_2)\dots\varphi(m_k)$

elementi ed il secondo ne ha

31) $\varphi(M) = \varphi(m_1 m_2 \dots m_k)$

Da 30) e 31) segue

32) $\varphi(m_1 m_2 \dots m_k) = \varphi(m_1)\varphi(m_2)\dots\varphi(m_k)$

se $(m_i, m_j) = 1$ per $i \neq j$.

Ciò prova che la funzione φ è moltiplicativa.

Osservazione

La moltiplicatività della funzione φ di Eulero equivale a dire che (con riferimento alla formula 23)) quando b_1 descrive un sistema ridotto di resti mod m_1, b_2 un sistema ridotto di resti mod m_2, $\dots$ e b_k un sistema ridotto di resti mod m_k il numero $x \equiv M_1 M_1' b_1 + \dots + M_k M_k' b_k$ descrive un sistema ridotto di resti mod $M = m_1 m_2 \dots m_k$. Lo stesso si

può dimostrare per i sistemi completi di resti. (10)

Ulteriore esempio di applicazione del teorema cinese del resto: costruire un messaggio fisso per un crittosistema R.S.A.

Consideriamo il problema seguente: esistono messaggi il cui cifrato coincide con il messaggio stesso? Ci sono due casi banali, cioè $M=1$ e $M=n-1$ (dove n è il modulo dell'R.S.A.) Ne esistono anche altri? La risposta è positiva, studieremo meglio questo problema), comunque con il teorema cinese potete sempre costruire un messaggio fisso non banale nel modo seguente. Supponiamo che A. sia titolare del crittosistema R.S.A. con

n, e chiave pubblica
ed chiave privata $\quad (n=pq,\ p,q$ primi$)$.

Per costruire un messaggio fisso si procede nel modo seguente: si risolve (con il teorema cinese) il sistema

$$33)\quad \begin{cases} x \equiv 1 \pmod p \\ x \equiv -1 \pmod q \end{cases}$$

Dato che $(p,q)=1$ il sistema 33) ammette soluzione unica $\bmod(pq)$ cioè $\bmod n$.

Se x è soluzione del sistema 33) si ha necessariamente

$$34)\quad \begin{cases} x^2 \equiv 1 \pmod p \\ x^2 \equiv 1 \pmod q \end{cases} \Longrightarrow x^2 \equiv 1 \pmod{pq} \equiv 1 \pmod n$$

A questo punto osserviamo che l'encryption_key e è dispari (infatti deve essere $(e, \varphi(n)) = 1$), e quindi $e-1$ è pari. Dalla 34) segue quindi

$$35)\quad (x^2)^{(e-1)/2} \equiv x^{e-1} \equiv 1 \pmod n$$

da cui segue

$$36)\quad x^e \equiv x \pmod n$$

e quindi x è un messaggio fisso.

Esercizio

Considerate l'R.S.A. con $p = 29$, $q = 53$, $e = 17$. Calcolate la decryption_key. Calcolate anche un messaggio fisso per questo crittosistema risolvendo il sistema

$$37)\quad \begin{cases} x \equiv 1 \pmod{29} \\ x \equiv -1 \pmod{53} \end{cases}$$