ARITMETICA 23 OTT 2017

Note Title 10/23/2017

Piccolo teorema di Fermat:

Se p è primo e $(x, p) = 1$

allora $x^{p-1} \equiv 1 \pmod{p}$.

Generalizzazione di Eulero

$n \in \mathbb{N}$ $n \geq 1$. $(x, n) = 1$

Allora $x^{\phi(n)} \equiv 1 \pmod{n}$

$$S = \left\{ \bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\phi(n)} \;\middle|\; a \in \mathbb{Z}/n\mathbb{Z},\ (a, n) = 1 \right\}$$

Oss. Se $(x, n) = 1$

allora $(x a_i, n) = 1$.

Posso scrivere $x s + n t = 1$ $a_i u + n v = 1$

$x a_i s u + n(\dots) = 1$

$$f : S \to S$$
$$a_i \mapsto x a_i$$

f è iniettiva, cioè $x a_i = x a_j \Rightarrow a_i = a_j$

$x(a_i - a_j) = 0$

Passando ai numeri interi

$n \mid x(a_i - a_j)$ $(n, x) = 1$

$\Rightarrow n \mid a_i - a_j$ $a_i \equiv a_j \pmod{n}$

Le classi sono le stesse. $\bar{a}_i = \bar{a}_j$.

$$A = \prod_{i=1}^{\phi(n)} a_i = \prod_{i=1}^{\phi(n)} a_i x = \bar{x}^{\phi(n)} A$$

↑ prodotto di tutti gli elementi di S

$$A = \bar{x}^{\phi(n)} A \qquad A(\bar{x}^{\phi(n)} - \bar{1}) = \bar{0}$$

$$n \mid A(x^{\phi(n)} - 1) \qquad (n, A) = 1.$$

$$\Rightarrow n \mid x^{\phi(n)} - 1.$$

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

$$x, x^2, x^3, \dots, \underline{x^d \equiv 1} \pmod{n}$$

Il più piccolo $d > 0$ per cui
$x^d \equiv 1 \pmod{n}$
è un DIVISORE di $\phi(n)$?

Infatti $x^i \equiv x^j \pmod{n} \iff$
i e j hanno lo stesso resto nella divisione per d.

Supponiamo $i = qd + r \quad j = q'd + r$
(stesso resto)

$$x^i = x^{qd+r} = x^{qd} \cdot x^r = (x^d)^q \cdot x^r = 1^q \cdot x^r = x^r$$
$$x^j = x^{q'd+r} = \dots = x^r.$$

Viceversa, supponiamo che $x^i = x^j$

$i = qd + r \qquad j = q'd + r'$

Con il calcolo di sopra, ottengo

$x^i = x^r \qquad x^j = x^{r'}$

Posso supporre $r \geq r' \qquad x^{r-r'} = 1$

$0 \leq r - r' < d$

$\Rightarrow \quad r - r' = 0 \qquad r = r'$ ∎

Esempio Voglio calcolare d nel caso $x = 5 \qquad n = 17$

$\phi(n) = 16 \qquad d \in \{1, 2, 4, 8, 16\}$

$5^1 \equiv 5 \not\equiv 1 \qquad 5^2 \equiv 25 \equiv 8 \not\equiv 1$

$5^4 = (5^2)^2 \equiv 8^2 \equiv 64 \equiv -4 \not\equiv 1$

$5^8 = (5^4)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \not\equiv 1.$

$\Rightarrow d = 16.$

Esercizio $11^x \equiv 1 \pmod{36}$

$$\begin{cases} 11^x \equiv 1 \pmod 4 \\ 11^x \equiv 1 \pmod 9 \end{cases} \qquad \begin{cases} 3^x \equiv 1 \pmod 4 \\ 2^x \equiv 1 \pmod 9 \end{cases}$$

$3^x \equiv (-1)^x \pmod 4$: Sol. $\boxed{x \equiv 0 \pmod 2}$

$2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 8 \equiv -1 \qquad \boxed{d = 6}$

$\varphi(9) = 6$

$$\boxed{x \equiv 0 \pmod 6}$$

$$\begin{cases} X \equiv 0 \pmod 2 \\ X \equiv 0 \pmod 7 \\ X \equiv 0 \pmod 3 \end{cases} \iff x \equiv 0 \pmod 6$$

Primi della forma

- $2^n - 1$ (primi di Mersenne)
- $2^n + 1$ (primi di Fermat)

① Se $2^n - 1 = p$ primo, allora a sua volta $n = q$ è primo.

Assurdo: se $n = ab \quad 1 < a, b < n$

$$2^n - 1 = 2^{ab} - 1$$

$$x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \dots + x + 1)$$

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)$$

$$\neq 1 \qquad \neq 1$$

$2^n + 1 = p \quad \Rightarrow \quad n = 2^k$.

Assurdo: supponiamo $n \neq 2^k$.

Allora esiste q dispari primo tale che $q \mid n$.

$n = mq$

Uso l'identità

$$x^q + 1 = (x+1)(x^{q-1} - x^{q-2} \dots - x + 1)$$

$x = 2^m$

$$2^n + 1 = 2^{mq} + 1 = (2^m + 1)(\underbrace{2^{m(q-1)} - 2^{m(q-2)}}_{\neq 1} \dots \underbrace{- 2^m + 1}_{\neq 1})$$

3 5 17 257 65537 ...

$2^{2^4} + 1$

$2^{2^n} + 1 \equiv 0 \pmod p$

$2^{2^n} \equiv -1 \pmod p$

$2^{2^{n+1}} \equiv 1 \pmod p$

$2^{n+1} \mid p - 1$

$64 = 2^{5+1} \mid p-1 \qquad p \equiv 1 \pmod{64}$

$p = 641$ è un DIVISORE.

MAZZO DI CARTE 52

26 + 26

MESCOLARE

oooo.... o x x.... x

x o x o x o x o x.... o

123 .... 27 28 29

27 1 28 2 29 3

Quanti passi dovremo fare per tornare alla posizione iniziale?

$x^p \equiv x \pmod{p} \qquad p = 1 + (p-1)$

$x^m \equiv x \pmod{p} \qquad m = 1 + 2(p-1)$

$m = 1 + k(p-1)$

RSA: Rivest - Shamir - Adleman 1978

$N = pq$ $\quad p, q$ primi distinti

$x^m \equiv x \pmod{pq}$

$$\begin{cases} x^m \equiv x \pmod{p} & m \equiv 1 + k(p-1) \\ x^m \equiv x \pmod{q} & m \equiv 1 + h(q-1) \end{cases}$$

$m \equiv 1 \quad ((p-1)(q-1))$

Utente $X_1, X_2, \ldots, X_k$

$X_i \leftrightarrow (A_i, B_i)$

A_i = indirizzo pubblico NOTO A TUTTI
B_i = chiave segreta NOTO SOLO A X_i

CODIFICAZIONE

$x \to x^{A_i} \pmod{N}$

DECODIFICAZIONE

$(x^{A_i}) \to x^{A_i B_i} = x$

se $A_i B_i \equiv 1 \pmod{(p-1)(q-1)}$

Bisogna risolvere la congruenza

$A_i B_j + t(p-1)(q-1) = 1$

$N = pq$ NOTI

$A_1, \dots, A_k$

CHIAVI

$N = pq$ mod $(p-1)(q-1)$

$= pq - (p+q) + 1$

$= N - (p+q) + 1$

FIRMA DIGITALE

Messaggio da X_1 a X_2

(A_1, B_1) (A_2, B_2)

$X \to X^{A_2}$

$f \to f^{A_2 B_1}$

$f^{A_2 B_1} \to f^{(A_2 B_1)(A_1 B_2)}$

$= f^{(A_1 B_1)(A_2 B_2)}$

$= f^{(A_2 B_2)} = f$.

$$x \to x^A$$

$$A = 2^{n_1} + 2^{n_2} + \cdots + 2^{n_k}$$

$$x = \underbrace{x^{2^{n_1}} \cdot x^{2^{n_2}} \cdots x^{2^{n_k}}}$$

$y \to y^2$ ripetute