Teoria dei Numeri IV

Titolo nota 06/09/2007

$ak + bh = 1$ [1]

(k_1, h_1) verificano

$ak + bh = c$ $c \neq 0$ non con

$ak + bh = 0$

$a(k_2 - k_1) + b(h_2 - h_1) = 0$

$ak = -bh$

$ak_2 + bh_2 = 1$

$a \equiv \quad (m)$ inverso

b : $ab \equiv 1 \ (m)$

$x \cdot 3 \equiv 1 \ (6)$

$(a, m) = 1$

$xa \equiv 1 \ (m)$

$xa - km = 1$

$$ax \equiv b \pmod{m}$$

$$x \equiv \frac{b}{a} \pmod{m} \equiv ba^{-1}$$

TEOREMA CINESE

$$a \equiv b_1 \pmod{x \cdot y}$$

$$a \equiv b_2 \pmod{x}$$

$$a \equiv b_3 \pmod{y}$$

$a \equiv 5 \ (6)$

$\Downarrow$

$\begin{cases} a \equiv 5 \ (2) \\ a \equiv 5 \ (3) \end{cases}$ $\Uparrow$?

$m_1, m_2 \dots m_n$ modul.

a due a due primi

allora

$$\begin{cases} x_1 \equiv a_1 \ (m_1) \\ x_2 \equiv a_2 \ (m_2) \\ \vdots \\ x_1 \equiv a_n \ (m_n) \end{cases}$$

HA SOLUZIONE MOD $m_1 m_2 \cdots m_n$

$$\begin{cases} x \equiv a_1 \ (m_1) \leftarrow \\ x \equiv a_2 \ (m_2) \end{cases}$$

$$x - a_1 = k m_1$$

$$x \equiv k m_1 + a_1 \ (m_2)$$

$(m_1, m_2) = 1$

$k \in \{1 \dots m_2\}$

$\exists\, k_{m_2} : \quad k m_1 + a_2 \equiv a_2 \pmod{m_2}$

Esistono 2007 interi consecutivi ciascuno multiplo di un quadrato (> 1)

$$\begin{cases} x \equiv 0 \pmod{2^2} \\ x+1 \equiv 0 \pmod{3^2} \\ x+2 \equiv 0 \pmod{5^2} \\ \vdots \end{cases}$$

$x + 2006 \equiv 0 \pmod{p_{2\cdots n}^{2}}$

$x \equiv 1 \pmod{p_1}$ ⊨

$x \equiv 0 \pmod{p_2}$

$\vdots$

$x \equiv 0 \pmod{p_n}$

$\Rightarrow x \equiv a_1 \pmod{p_1}$

$x \equiv 0 \pmod{p_2 \cdots p_n}$

$x \equiv a_2$ ⊨

$x \equiv a_1$

$\vdots$

$x \equiv a_n$

$x \equiv 0$, ⇐

$x \equiv a_2$ ⇐

⋮

$x \equiv a_1 \ (p_1)$

$x \equiv 0 \ (p_2 \cdots p_n)$

$x \equiv a_2 \ (p_2)$

$x \equiv 0 \ (p_1 p_3 \cdots)$

$(m_1, m_2) \neq 1$

$x \equiv 1 \ (2)$ ⇐

$x \equiv 2 \ (6)$ ⇐

$x \equiv 3 \ (12)$ $2^2 \cdot 3$

$x \equiv 6 \ (28)$ $2^2 \cdot 7$

$x \equiv 3 \ (4)$

$x \equiv 0 \ (3)$

$x \equiv 6 \ (4)$

$x \equiv 2 \ (4)$

$x \equiv 6 \ (7)$

$x \vdots 6 \ (4^5)$

Se 7, allora è definita mod mcm (m_i)

Dimostrare che $\forall n$ $\exists 7$ n interi consecut.. nessuno di loro una potenza perfetta

$\rightarrow x \equiv p_1 \ (p_1^7)$

$x+1 \equiv p_2 \ (p_2^2)$

$x+2 \equiv p_3 \ (p_3^2)$

$x+y-1 \equiv p_n \quad (p_n^2)$

$a \quad a^2 \quad a^3 \ldots \ldots$

$a^{p-1} \equiv 1 \ (p) \qquad (a, p) = 1$

$ord_p(a)$: il più piccolo esponente k_a:

$a^{k_a} \equiv 1 \ (p)$

$\exists$ generatori. $\qquad x^0 \equiv 1 \ (p)$

$ord_p(a) \mid p-1$

n2 : quels sont les générateurs

$g \quad g^2 \quad g^3 \quad \dots \quad g^{p-1}$

$g^k \quad : (k, p-1) = 1$

$(k, p-1) = d \qquad g^{\frac{k}{d}(p-1)}$

$g^{k \cdot h} \equiv 1 (p)$

$(p-1) \mid k h$

ϕ di eulero

$\phi(n)$: il numero di numeri ≥ 1 e $\leq n$ relativamente primi con n

$n_1 \quad n_2$

$\phi(n_1 n_2) = \phi(n_1)\,\phi(n_2)$ ϕ è moltiplicat.

COMPLETAM. MOLT. $f(ab) = f(a) f(b)$

$\phi(6) \quad \phi(4) \stackrel{?}{=} \phi(24)$

$x \equiv r_1 \pmod{p_1}$

$x \equiv r_2 \pmod{p_2}$

(r_1, r_2)

$m_1 = 6$

$m_2 = 35$

p^k

$1 \dots p^k$

$\varphi(p^k) = p^k - p^{k-1}$

$x \equiv (?) \pmod{p_1 p_2}$

$(e, p^k) = 1$

$$a^{p-1} \equiv 1 \ (p)$$

$$a^{\square} \equiv 1 \ (m)$$

$$a^{\phi(m)} \equiv 1 \ (m)$$

FERMAT GRAFNALI ZAP

$$\{1, 2, \dots n_1, \quad n_2\}$$

$$a^{k_1} \quad a^{k_2} \quad \dots \quad a^{k_{p-1}}$$

$$a^{\phi(m)} \equiv 1 \ (m)$$

TEOREMA DI WILSON

$$(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv -1 \ (p)$$

$\rightarrow$ $g, g^2 \dots g^{p-1}$

$$g^{\frac{(p-1)\cdot p}{2}} = g^{\frac{p-1}{2} \cdot p} \ (p)$$

$$g^{\frac{p-1}{2}} = \pm 1 \ (p) \qquad g^{\frac{p-1}{2}} \equiv -1 \ (p)$$

$$x^2 \equiv 1 \ (p) \qquad x \equiv 1 \ \vee \ x \equiv -1 \ (p)$$

$$(x-1)(x+1) \equiv 0 \ (p)$$

$$(-1)^p \equiv -1 \pmod{p}$$

Esistenza di un generatore

- p primo ($\neq 2$)
- p^n primo dispari ($\neq 2$)
- $2, 4$
- $2p^n$

$6 \pmod{16}$ $\rightarrow$ $2 \pmod{16}$ $\rightarrow$ $2 \pmod{16}$

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$

$\left(\begin{array}{l} x^{\alpha_1} \equiv 1 \ (p_1^{\alpha_1}) \\ x^{\alpha_2} \equiv 1 \ (p_2^{\alpha_2}) \end{array} \right.$

$\phi(p)$ por.

$g^{a_1 = \phi(p_1^{\alpha_1})} \equiv 1$

$ord_p(a) \mid p-1$

$ord_m(a) \mid \phi(m)$

$p \mid x^2 + y^2$ $\qquad$ $p \mid x^2 + y^2$ $\qquad$ $p = 4k+1$

$x^2 + y^2 \equiv 0 \ (p)$

$(xy^{-1})^2 + 1 \equiv 0 \ (p)$

$$a^2 + 1 \equiv 0 \pmod p$$

$$\rightarrow \quad a^2 \equiv -1 \pmod p$$

$$a^4 \equiv 1 \pmod p \quad \leftarrow$$

$\operatorname{ord}_p(a) \mid 4 \leq 2 \cdot 2$

$4 \mid p-1$

$4k = p-1 \qquad p = 4k+1$

$p^p - 1$ ha un fattore della forma $kp+1$

$\Rightarrow \boxed{p^p \equiv 1 \ (q)}$

$p^{\mathrm{ord}_q(p)} \equiv 1 \ (q)$

$\mathrm{ord}_q(p) \mid p \begin{cases} 1 \\ p \end{cases} \Rightarrow p \equiv 1 \ (q)$

$p^{q-1} \equiv 1 \ (q)$

$\mathrm{ord}_q(p) \mid q-1$

$p \mid q-1$ ou $\Leftrightarrow$ $kp = q-1$ $q = kp+1$

$p \equiv 1 \ (q)$

$p^p - 1 = (p-1)\left(1 + p + p^2 + \cdots + p^{p-1}\right)$

Π

$p \mid x^2 + y^2$ $\qquad$ $p = 4k+1$

1) $x^2 + y^2 = cp$ $\qquad$ $(c, p) = 1$

$\exists\, a, b : a^2 + b^2 = p \in \mathbb{Z}$

$3 \mid 6 + 9i$

$\frac{6+9i}{3}$

$\exists [i]$

$a + bi \qquad a, b \in \mathbb{Z}$

$p \mid ab \Rightarrow p \mid a \vee p \mid b$

$cp = x^2 + y^2 = (x + yi)(x - yi)$

$p \qquad p$

$p \mid x+yi$ $\qquad x = up$, $y = vp$

$$x-yi = p(u-vi)$$

$$cp = p(u+vi)\cdot p(u-vi)$$

$$p = (a+bi)(c+di)$$

$a^2+b^2 = 1$

$a+bi$

INVERTIBILI $\qquad a = e^{-1} \in \mathbb{Z}$

$$p = (a-bi)(c-di)$$

1

-1

2 $\quad$ 1

2

$$p^2 = (a^2+b^2)(c^2+d^2)$$

$a^2+b^2 \neq 1$

$a^2+d^2 \neq 1$

$a^2+b^2 = p$

→ p primo è un numero della forma $4n+1$

$p = a^2+b^2$

LEMMA

$p = 4n+1$

$x^2 \equiv -1 \ (p)$ ha soluzione

$$x = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$$

$$x = (-1)(-2) \cdot \ldots \cdot -\left(\frac{p-1}{2}\right)$$

$$p - k \equiv -k \ (p)$$

$$x^2 \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (-1)(-2) \cdots -\left(\frac{p-1}{2}\right) \equiv$$

$$\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot p-1 \equiv (p-1)! \equiv -1 \ (p)$$

Se p è un numero primo, $p = 4n+1$, allora

$\exists a, b : \quad a^2 + b^2 = p$

$x^2 \equiv -1 \pmod p$

$x \in [0 \dots p-1]$

$|x| < p/2$

$p \mid x^2+1$ $\qquad |x| < \frac{p}{2}$

$cp = x^2 + 1$

$cp < \frac{p^2}{4} + 1$

$c < \frac{p}{4} + \frac{1}{p^2} < 1$

$p = a^2 + b^2$

nessuno

$p = 4n + 3$

$a^2 + b^2 \ (4) \equiv 0 \ (2$

$p \equiv 3 \ (4)$

$(p-1)! \equiv -1 \ (p)$

$\prod_{(i,m)=1} i \overset{?}{\equiv} -1 \ (m)$

$\exists \ g$ allora $\equiv -1$

$\nexists \ g$ allora $\equiv 1$

$T_a(m) = a^{a^{a^{\cdots^{a}}}}$ (m a)

Dimostrare che $T_a(m)$ è costante (n)

da un certo punto in poi

$$T(m) = a^{T(m-1)} \qquad T(1) = a$$

$$a^{T(m-1)} \equiv a^{a^{T(m-2)}} \pmod{n}$$

$$T(m-1) \equiv a^{T(m-2)} \pmod{\phi(n)}$$

$$a^k \equiv a^h \pmod{n}$$

$$a^{k-h} \equiv 1 \pmod{n}$$

$k-h$ è multiplo $ord_a(n)$