Senior 2006 – Teoria dei Numeri 2 (N.C.)

Titolo nota 13/09/2006

$$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 0 \pmod 4 \end{cases} \iff x \equiv 0 \pmod{12}$$

Th: $(m, n) = 1 \qquad 0 \leq r < m, \quad 0 \leq s < n$

$$\begin{cases} x \equiv r \pmod m \\ x \equiv s \pmod n \end{cases}$$

$\{0, 1, 2 \dots mn-1\}$

$y \to (r_y, s_y)$

$z \to (r_z, s_z)$

$r_y = r_z \qquad s_y = s_z$

$$\begin{cases} z \equiv y \pmod m \\ z \equiv y \pmod n \end{cases} \implies z \equiv y \pmod{mn}$$

(r, s)

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \\ \vdots \\ x \equiv r_k \pmod{m_k} \end{cases} \quad x \equiv \bigcirc \pmod{m_1, m_2} \quad m_1 m_2 m_3$$

$$\boxed{x \equiv r \pmod{m}}$$

$$\begin{cases} x \equiv r \pmod{p_1^{a_1}} \\ \vdots \\ x \equiv r \pmod{p_m^{a_m}} \end{cases}$$

$$m = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

$$\begin{cases} x \equiv 16 \pmod{24} \\ x \equiv 4 \pmod{15} \\ x \equiv 4 \pmod{44} \end{cases} \Longrightarrow \begin{cases} x \equiv 16 \equiv 1 \pmod 3 \checkmark \\ x \equiv 16 \equiv 0 \pmod 8 \checkmark \\ x \equiv 4 \equiv 1 \pmod 3 \checkmark \\ x \equiv 4 \pmod 5 \checkmark \\ x \equiv 0 \pmod 4 \checkmark \\ x \equiv 4 \pmod{11} \checkmark \end{cases} \Longrightarrow \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 4 \pmod{11} \\ x \equiv 0 \pmod 8 \end{cases}$$

$$\begin{cases} x \equiv r \pmod m \\ x \equiv s \pmod n \end{cases}$$

$$x \equiv m\bar{\bar{m}}\, s + m\bar{m}\, r$$

$\bar{m}$: inverso di $m \bmod n$

$$\begin{cases} x \equiv r \pmod m \\ x \equiv s \pmod n \\ x \equiv t \pmod o \end{cases}$$

$$x = mn\bar{o}\bar{m}\bar{a}s + mn\bar{m}\bar{n}\bar{m}t + me\bar{n}\bar{o}r$$

Es: dimostrare che esistono n interi consecutivi che contengono esattamente una potenza perfetta.

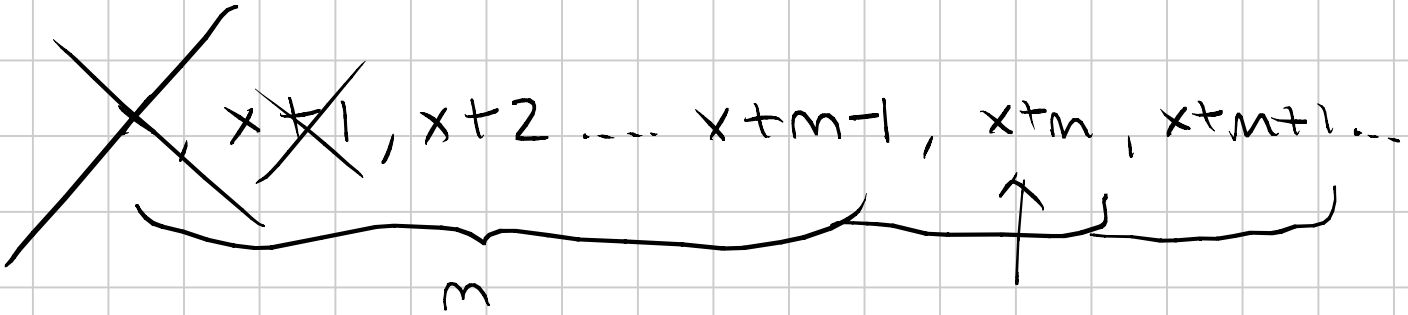
① dimostrare la tesi con 0 potenze perfette

② esattamente una potenza perfetta.

$$x \equiv p \pmod{p^2}$$

$$\begin{cases} x \equiv p_1 & (p_1^2) \\ x+1 \equiv p_2 & (p_2^2) \\ \vdots \\ x+m-1 \equiv p_{m-1} & (p_{m-1}^2) \end{cases}$$

$x,\ x+1,\ \dots\ x+m-1$



$(x, p) = 1$

$x,\ x^2,\ x^3 \dots\ x^n \dots$

$\{0, 1 \dots p-1\}$

$x^a \equiv x^b \quad (p)$

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

$x^m \equiv 1 \quad (p)$

k_0 il più piccolo esponente tale che $x^{k_0} \equiv 1 \ (p)$

*Th.: i numeri m tali che $x^m \equiv 1 \ (p)$ sono hk_0

DIM:

$$x^{hk_0} \equiv (x^{k_0})^h \equiv 1^h \equiv 1$$

$$x^m \equiv 1 \overset{?}{\Longrightarrow} m = hk_0$$

$m = hk_0 + r \qquad x^m \equiv x^{hk_0+r} \equiv (x^{k_0})^h \cdot x^r \equiv 1 \cdot x^r \equiv x^r$

$0 \le r < k_0 \qquad r = 0$

k_0 = ordine di x mod p = $\mathrm{ord}_p(x)$.

$x \quad x^2 \quad x^3 \quad \dots \quad x^{\mathrm{ord}_p(x)} \quad x^{\mathrm{ord}_p(x)+1}$

$\| \qquad\qquad\qquad\qquad\quad \| \qquad\quad \|$

$x \quad x^2 \quad x^3 \quad \dots \quad 1 \qquad 1 \cdot x \quad x^2 \quad x^3 \quad \dots$

$x^a \equiv x^b \qquad x^{a-b} \equiv 1$

Th $x^{p-1} \equiv 1 \quad (p)$

DIM:

$\{1, \dots, p-1\}$

$\{x, 2x, 3x, \dots (p-1)x\}$

$ax \equiv bx \quad a-b \equiv 0 \quad (p)$

$1 \cdot 2 \cdots p-1 \equiv x \cdot 2x \cdot 3x \cdots (p-1)x$

$(p-1)! \equiv (p-1)! \, x^{p-1} \quad (p)$

$1 \equiv x^{p-1} \quad (p)$

$x^{\phi_m} \equiv 1 \quad (m)$

$x^m \equiv 1 \qquad m = h \, ord_p(x)$

$p-1 = k \, ord_p(x)$

Th: $ord_p(x) \mid p-1$

$ord_{\phi_m}(x) \mid \phi_m$

$p=7$ $x=2$

2	2^2	2^3	2^4	2^5	2^6
$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$
2	4	1	2	4	1

$ord_7(2)=3$

$x=3$

3	3^2	3^3	3^4	3^5	3^6
$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$	$\|\|\|$
3	2	$-1\equiv 6$	4	5	1

$ord_7(3)=6$ $\quad 6 \mid 6=7-1$

$53 \nmid 2^{27}-1$ $\qquad 2^{27}\equiv 1 \pmod{53}$

$ord_{53}(2) \mid 53-1=52$

$ord_{53}(2) \mid 27$

$ord_{53}(2) \mid (52,27)=1$ $\qquad ord_{53}(2)=1$ $\quad 2^1 \not\equiv 1 \pmod{53}$

Es: Dimostrare che $p^p - 1$ ha almeno un divisore primo della forma $kp+1$.

$p^p \equiv 1 \ (q)$

$\text{ord}_q(p) \mid p$

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

$\Rightarrow$

1. $\text{ord}_q(p) = 1$
2. $\text{ord}_q(p) = p$

$p \mid q-1$

$q = kp+1$

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

$q \mid$

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

$p^p \equiv 1 \ (q)$ $\qquad \text{ord}_q(p) = 1$

$p \equiv 1 \ (q)$

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

$x^m \equiv -1 \quad (p)$

TR: m esiste sse $ord_p(x)$ è pari e un tale caso

$$m = (2k+1)\frac{ord_p(x)}{2}$$

1. se m esiste $\Rightarrow$ l'ordine è pari

$$x^m \equiv 1 \ (p) \Rightarrow x^{2m} \equiv 1 \ (p)$$

$m < ord_p(x)$ $\qquad$ $2m = ord_p(x)$

$ord_p(x) \mid 2m$ $\qquad$ $2m = h\, ord_p(x) > h\, m$ $\quad h = 1$

2. se l'ordine è pari $\Rightarrow$ m esiste $\qquad 2m = ord_p(x)$

$$x^{ord_p(x)} \equiv 1$$

$$x^{ord_p(x)} - 1 \equiv 0 \qquad \left(x^{\frac{ord_p(x)}{2}} - 1\right)\left(x^{\frac{ord_p(x)}{2}} + 1\right) \equiv 0 \quad (p)$$

$$x^{\frac{ord_p(x)}{2}} \equiv 1 \quad (p)$$

$$x^{\frac{ord_p(x)}{2}} \equiv -1 \qquad m = \frac{ord_p(x)}{2} + \frac{2k}{2} ord_p(x) +$$

$$= \frac{ord_p(x)}{2}(2k+1)$$

g $\quad ord_p(g) = p-1$ $\qquad ord_m(g) = \phi m$

$g \quad g^2 \quad g^3 \ldots$

$2, 4, p^k, 2p^k$

Th: esiste un generatore modulo p

Es. Dato k, $\sum_{i=0}^{p-1} i^k \equiv 0 \quad (p)$, $p-1 \nmid k$

$1^k + 2^k + 3^k + \ldots + (p-1)^k \overset{?}{\equiv} 0 \quad (p)$

$g^i \quad i = 0 \dots p-2$

$$\sum i^k \equiv \sum_{i=0}^{p-2} (g^i)^k \equiv \sum (g^k)^i \equiv \frac{g^{k(p-1)} - 1}{g^k - 1} \equiv \frac{0}{\dots} \equiv 0 \ (p)$$

$1 + a + a^2 + \dots a^n = \frac{a^{n+1} - 1}{a - 1}$

$g^k - 1 \not\equiv 0 \qquad g^k \not\equiv 1 \qquad p-1 \nmid k$

$$x^2 \equiv r \ (p)$$

Th: il numero di residui quadratici è $\frac{p+1}{2}$.

- $r = 0 \qquad 1$

  1

- $\{1, 2 \dots p-1\}$

  $(1, p-1) \ | \ (2, p-2) \dots$

  $x^2 \equiv (p-x)^2 \ (p)$

  $x^2 \equiv x^2$

  $\frac{p-1}{2}$

$a^2 \equiv b^2 \equiv c^2 \pmod p$

$a^2 \equiv b^2 \pmod p \Rightarrow a^2 - b^2 \equiv 0 \pmod p$

$(a-b)(a+b) \equiv 0 \pmod p$

$p \mid a-b \quad a \equiv b$

$a+b \equiv 0 \pmod p$

$a \equiv -b \pmod p$

$a^2 \equiv c^2 \quad a \equiv -c \quad b \equiv c \pmod p$

Es: $\frac{p+1}{2}$ residui g-esimi $\frac{p-1}{gcd(p-1,g)} + 1$

Es: $x^3 + 9 = 5y^4$

$\frac{p-1}{gcd(p-1,3)} + 1$

$3 \cdot 4 \mid p-1 \quad p \neq 3$

$x^3 \equiv 0, 1, 8, 5, -1$

$y^4 \equiv 0, 1, 3, 9$

$\rightarrow 9, 10, 4, 1, 8$

$0, 5, 2, 6$

1
8 16
1 3

$\phi(m) = |\{x \in \{0,1,\dots m-1\} \mid (x,m)=1\}|$

$\phi(p) = p-1$ $\quad \phi(6)=2$ $\quad \phi(15)=8$

1 2 3 4 5 6

0 1 2 3 4 5 6 7 8 9 10

11 12 13 14

$f: N \to N \quad f(ab) = f(a) \cdot f(b) \quad (a,b)=1$

ϕ è moltiplicativa

Th: ϕ n è moltiplicativa

$\phi(ab) = \phi a \, \phi b$ se $(a,b)=1$

(r_a, r_b)

$x \equiv r_a \ (a)$ $\quad (r_a, a) = 1 = (r_b, b)$

$x \equiv r_b \ (b)$

$\phi \, p^k$ $\qquad n = p_1^{a_1} \cdots p_m^{a_m}$

$\phi(n) = \phi p_1^{a_1} \cdot \phi p_2^{a_2} \cdots \phi p_m^{a_m}$

$\phi \, p = p - 1$

$\phi \, p^2 = p^2 - p$ $\qquad p \cdot k$ $\qquad k = 0 \ldots p-1$

$\vdots$

$\phi p^k = p^k - p^{k-1}$ $\qquad p h$ $\qquad h = 0 \ldots p^{k-1} - 1$

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_m^{a_m} - p_m^{a_m-1})$$

$$= \prod p_i^{a_i}\left(1 - \frac{1}{p_i}\right) = n \prod \left(1 - \frac{1}{p_i}\right)$$

Es.: $\sum_{d|n} \phi d = n$ $\quad \left(\phi * 1 = n\right)$

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

$m = 1$

$n = p_1^{a_1}$ $\quad \sum \phi d = \phi 1 + \phi p + \phi p^2 \cdots + \phi p^a =$

$= \cancel{1} + \cancel{p} - \cancel{1} + \cancel{p^2} - \cancel{p} + \cancel{p^3} - \cancel{p^2} + \cdots p^a - p^{a-1} =$

$= p^a.$

$n = p_1^{a_1} \boxed{\cdots p_{m+1}^{a_{m+1}}} = p_1^{a_1} \cdot h$ $\quad \sum_{d|h} \phi d = h$

$$\sum_{d \mid m} \phi d = \sum_{d \mid h} \phi d + \sum_{d \mid h} \phi(pd) + \sum \phi(p^2 d) + \ldots + \sum \phi(p^a d) =$$

$$= \sum_{d \mid h} \phi d + \sum_{d \mid h} \phi_p \cdot \phi d + \sum \phi p^2 \cdot \phi d + \ldots + \sum \phi_p^a \cdot \phi d =$$

$$= \sum_{d \mid h} \phi d + \phi_p \sum \phi d + \phi p^2 \sum \phi d + \ldots + \phi p^a \sum \phi d =$$

$$= \left(\sum \phi d\right)\left(1 + p - 1 + p^2 - p + \ldots + p^a - p^{a-1}\right) =$$

$$= \left(\sum (\phi d)\right)(p^a) = p^a \cdot h = m$$

Th: nessun numero della forma $4K+3$ divide a^2+b^2. $(a,b)=1$

Nessun primo della forma $4K+3 \mid a^2+b^2$

$a^2+b^2 \equiv 0 \quad (p)$

~~$p \mid a, p \nmid b$~~

$\overline{b}$ = inv $(a\overline{b})^2 + 1 \equiv 0 \quad (p) \qquad a\overline{b} = x$

$x^2 \equiv -1 \quad (p)$

$x^4 \equiv 1 \quad (p)$

$ord_p(x) \mid 4 \qquad ord_p(x) = \begin{cases} 1 \\ 2 \\ 4 \end{cases}$

$x^2 \equiv 1 \quad (p)$

$ord_p(x) = 4 \qquad 4 = ord_p(x) \mid p-1 \qquad 4 \mid p-1$

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

$$x^2+4=y^3+27$$

$$x^2 \equiv y^3+3 \quad (4)$$

$$x^2-3 \equiv y^3$$

$$-3 \equiv 1 \equiv y^3 \quad (4)$$

$$2 \equiv y^3 \quad (4)$$ ~~2 | y~~ IMOSS

x = pari = $2k$ y = dispari

$4k+1$ ~~$4k+3$~~

$$x^2+4=y^3+27=(y+3)(y^2-3y+9)$$

$$4(k^2+1)$$

$$y+3 \equiv 2 \quad (4)$$

$$y^2-3y+9 \equiv 1 \quad (4)$$

$$y+3 \equiv 0 \quad (4)$$

$$y^2-3y+9 \equiv 1-3+9=3 \quad (4)$$

0
1

Es: Quanti sono i generatori mod p?

$$\phi(p-1) = \phi(\phi_p)$$

$$g^{p-1} \equiv 1 \quad (p)$$

$$g^m \not\equiv 1 \quad (p) \quad \text{per } m < p$$

g^α $\qquad (\alpha, p-1) = 1 \qquad \phi(p-1)$ $\qquad \phi(\phi_m)$

$$\left(g^\alpha\right)^\beta \equiv 1 \quad (p) \qquad \beta < p-1$$

$$g^{\alpha\beta} \equiv 1 \quad (p) \qquad p-1 \mid \alpha\beta \qquad p-1 \mid \beta$$