N2 – BASIC SENIOR 2012

Titolo nota 05/09/2012

23 $\qquad m = 30$

$23 \equiv 23 \pmod{30} \qquad 30 = 5 \cdot 6$

$23 \equiv 3 \pmod 5$

$23 \equiv 5 \pmod 6$

Possiamo fare viceversa

$x \equiv 3 \pmod 5$

$x \equiv 5 \pmod 6$ $\qquad 5 \cdot 6$

SI!

Teorema Cinese del Resto

Moduli $m_1, m_2, \dots m_k$ a due a due primi tra loro $MCD(m_i, m_j) = 1$

Resti $r_1, r_2, \dots r_k$

Esiste un'unica classe di resto x modulo $m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_k$ tale che

$$x \equiv r_1 \pmod{m_1}$$
$$x \equiv r_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv r_k \pmod{m_k}$$

Esiste un unico intero che fa questo tra 1 e $m_1 m_2 \dots m_k$ (estremi inclusi)

α_i $\quad \alpha_i \equiv 0 \pmod{m_1}$
$\alpha_i \equiv 0 \pmod{m_2}$
$\vdots$
$\alpha_i \equiv 1 \pmod{m_i}$
$\vdots$
$\alpha_i \equiv 0 \pmod{m_k}$

$\alpha_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k \beta_i$

$\exists \beta_i$ t.c. $\cdot \beta_i \equiv 1 \pmod{m_i}$

$r_1 \alpha_1 + r_2 \alpha_2 + \cdots + r_k \alpha_k = x$

α_1: 1 modulo m_1, 0 modulo m_2, $\ldots$, 0 modulo m_k
α_2: 0 modulo m_1, 1 modulo m_2, 0 modulo m_3, $\ldots$, 0 modulo m_k
α_k: 0 modulo m_1, $\ldots$, 0 modulo m_{k-1}, 1 modulo m_k

modulo m_1 $\quad r_1$
modulo m_2 $\quad r_2$
$\vdots$

$1 \le x < y \le m_1 \cdots m_k$

$y - x \equiv r_1 - r_1 \equiv 0 \pmod{m_1}$
$\equiv r_2 - r_2 \equiv 0 \pmod{m_2}$
$\vdots$
$\equiv r_k - r_k \equiv 0 \pmod{m_k}$

- $m_1 \cdots m_k \mid y - x$ NO!

---

m, d, k interi positivi

Successione aritmetica di
- lunghezza m
- ragione d
- ogni termine sia divisibile per una

potenza k-esima perfette

$$n \equiv 0 \pmod{p_1^k}$$
$$n+d \equiv 0 \pmod{p_2^k}$$
$$n+2d$$
$$\vdots$$
$$n+(m-1)d \equiv 0 \pmod{p_m^k}$$

$p_1, \dots, p_m$ primi distinti

$$n \equiv 0 \pmod{p_1^k}$$
$$n \equiv -d \pmod{p_2^k}$$
$$\vdots$$
$$n \equiv -(m-1)d \pmod{p_m^k}$$

TCR: Tale n esiste

$$\begin{cases} n \equiv 3 \pmod 6 \\ n \equiv 2 \pmod 4 \end{cases}$$

$$n \equiv 0 \pmod 3$$
$$n \equiv 1 \pmod 2$$
$$n \equiv 2 \pmod 4$$

NO

$$\begin{cases} m \equiv 5 \pmod 6 \\ m \equiv 3 \pmod 4 \end{cases}$$

- $m \equiv 2 \pmod 3$
- $\begin{cases} m \equiv 1 \pmod 2 \\ m \equiv 3 \pmod 4 \end{cases}$
- $m \equiv 3 \pmod 4$

$$m \equiv 11 \pmod{12}$$

$\mathrm{mcm}(6,4)$

---

m, d

Successione aritmetica di
- lunghezza m
- ragione d
- nessun termine è una potenza

perfetta

$$n \equiv p_1 \pmod{p_1^2}$$
$$n+d \equiv p_2 \pmod{p_2^2}$$
$$\vdots$$
$$n+(m-1)d \equiv p_m \pmod{p_m^2}$$

$p_1 \dots p_m$ primi distinti

$$a^h = (q_1^{\alpha_1} \cdots q_s^{\alpha_s})^h$$

φ φ

↑ GIUSTO

$\varphi(n)$ = numero degli interi tra 1 e n estremi inclusi coprimi con n

$\varphi(1) = 1$ $\varphi(2) = 1$ $\varphi(3) = 2$

$\varphi(p) = p-1$ p primo

$\varphi(6) = 2$ $\varphi(4) = 2$

[$MCD(m,n) = 1$

$\varphi(mn) = \varphi(m)\varphi(n)$

→ SE NO, È FALSO

MOLTIPLICATIVA

φ è moltiplicativa MA NON COMPLET. MOLTIPLICATIVA

$f(mn) = f(m)f(n)$ per ogni m,n intero positivo

f è completamente moltiplicativa

$MCD(m,n) = 1$

Chi sono gli interi coprimi con mn?

a coprimo con mn $\Rightarrow$ a coprimo con m

$\Rightarrow$ a coprimo con n

Scelgo $1 \le r_1 \le m$ coprimo con m

$1 \le r_2 \le n$ coprimo con n

Esiste unico $1 \le r \le mn$

tale che $r \equiv r_1 \pmod m$

$r \equiv r_2 \pmod n$

Viceversa $1 \le s \le mn$ coprimo con mn

$s \equiv s_1 \pmod m$

$s \equiv s_2 \pmod n$

Interi tra 1 e mn coprimi con mn

Coppie di interi (c,d)

$1 \le c \le m$ c coprimo con m

$1 \le d \le n$ d coprimo con n

$\varphi(mn) = \varphi(m)\varphi(n)$

$\varphi(p) = p - 1$

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

$\varphi\left(p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}\right) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p_\ell^{k_\ell}\right) =$

$$= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_\ell^{k_\ell} - p_\ell^{k_\ell-1}\right) =$$

$$= p_1^{k_1}\cdots p_\ell^{k_\ell}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_\ell}\right)$$

Numero di divisori (positivi)

Moltiplicativa ma NON completamente moltiplicativa

$$p_1^{\alpha_1}\cdots p_r^{\alpha_r} \times q_1^{\beta_1}\cdots q_s^{\beta_s}$$

$$(\alpha_1+1)\cdots(\alpha_r+1) \times (\beta_1+1)\cdots(\beta_s+1)$$

Somma dei divisori (positivi)

Moltiplicativa ma NON completamente moltiplicativa

$MCD(m,n) = 1$

$c \mid m \qquad d \mid n$

$MCD(c,d) = 1$

$cd \mid mn$

$h \mid mn$

$MCD(h,m) \mid m$

$MCD(h,n) \mid h$

$MCD(h,m)\cdot MCD(h,n) = h$

$$\underbrace{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}_{m}\ \underbrace{q_1^{\beta_1}\cdots q_s^{\beta_s}}_{n}$$

Divisori di mn

Coppie (divisore di m, divisore di n)

$$\sigma(mn) = \sigma(m)\sigma(n)$$

---

n intero positivo

$$\sum_{d|n} \varphi(d) = n$$

$n = p^k$ $\quad 1, p, p^2, \dots, p^{k-1}, p^k$

$$\varphi: 1 + (p-1) + (p^2-p) + (p^3-p^2) + \dots + (p^{k-1}-p^{k-2}) + (p^k - p^{k-1}) = p^k$$

$p_1^{k_1} \cdots p_h^{k_h} \; p_{h+1}^{k_{h+1}}$

$d \cdot 1 \longrightarrow \sum \varphi = p_1^{k_1} \cdots p_h^{k_h} \cdot 1$

$d \cdot p_{h+1} \longrightarrow \sum \varphi(d \cdot p_{h+1}) =$

$d \cdot p_{h+1}^2$ * $\quad = \sum \varphi(d)\varphi(p_{h+1}) =$

$= \sum (p_{h+1} - 1)\varphi(d) =$

$d \cdot p_{h+1}^{k_{h+1}} \quad = (p_{h+1} - 1)\, p_1^{k_1} \cdots p_h^{k_h}$

* $\sum \varphi(d\, p_{h+1}^2) = \sum \varphi(d)\varphi(p_{h+1}^2) =$

$= (p_{h+1}^2 - p_{h+1}) \sum \varphi(d) = (p_{h+1}^2 - p_{h+1}) p_1^{k_1} \cdots p_h^{k_h}$

$p_1^{k_1} \cdots p_k^{k_h} \left(1 + (p_{h+1} - 1) + (p_{h+1}^2 - p_{h+1}) + \cdots \right.$

$\left. \cdots + (p_{h+1}^{k_{h+1}} - p_{h+1}^{k_{h+1}-1}) \right) =$

$$= p_1^{k_1} \cdots p_k^{k_k} p_{k+1}^{k_{k+1}}$$

$n \geq 2$ intero

a intero

$a, a^2, a^3, a^4, \ldots$

modulo n

$a^k \; a^{k+1} \ldots$ $\quad a^h \equiv a^k \pmod{n}$

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

$a^{h+2} \equiv a^{k+2} \pmod{n}$

La successione è periodica modulo n da un certo punto in poi

$MCD(a,n) = 1$ allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$ord_n(a) =$ il più piccolo intero positivo r tale che

$a^r \equiv 1 \pmod{n}$

$ord_n(a) \leq \varphi(n)$ $\quad ord_n(a) \mid \varphi(n)$

$\varphi(n) = d \cdot ord_n(a) + b \quad 0 \leq b < ord_n(a)$

$a^{ord_n(a)} \equiv 1 \pmod{n}$

$\left(a^{ord_n(a)}\right)^d \equiv 1 \pmod{n}$

$a^{\underbrace{ord_n(a) \cdot d + b}_{\varphi(n)}} \equiv 1 \pmod{n}$

$$a^{\mathrm{ord}_n(a)} a^b \equiv 1 \pmod n$$

$a^{\mathrm{ord}_n(a)} \equiv 1$

$$a^b \equiv 1 \pmod n$$

$$\mathrm{ord}_n(a) \mid \varphi(n)$$

Può essere $\mathrm{ord}_n(a) = \varphi(n)$?

dipende da n

$n = 2$ sì

$n = 4$ sì

$n = 2^k$ $k \geq 3$ NO

p primo dispari: tale a esiste

p^k, $2 \cdot p^k$ $k \geq 1$ sì

TUTTI GLI ALTRI: NO

$$n = p_1^{\alpha_1} \cdots p_h^{\alpha_h} \cdot 2^{k \geq 2}$$

$\mathrm{MCD}(a, n) = 1$

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}}$$

$\varphi(2^k)$ = $k-1$

$a^2 \equiv 1 \pmod{2^k}$

$$\vdots$$

$$a^{\varphi(p_h^{\alpha_h})} \equiv 1 \pmod{p_h^{\alpha_h}}$$

$$a^{\mathrm{mcm}(\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_h^{\alpha_h}), 2^{k-1})} \equiv 1 \pmod n$$

$\leq \varphi(n)$

$$\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$$

$$\varphi(2^k) = 2^{k-1}$$

Prendo n t.c. esiste a coprimo con n t.c. $\text{ord}_n(a) = \varphi(n)$

Un tale a è detto generatore modulo n.

Sia g un generatore modulo n

$$g, g^2, g^3, g^4, \dots, g^{\varphi(n)} \pmod n$$

SONO DIVERSI MODULO N

$$g^k \equiv g^h \pmod n \qquad 1 \le k < h \le \varphi(n)$$

Esiste $(g^k)^{-1} \pmod n$

$$\equiv (g^{-1})^k$$

$$g^k \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{k \text{ volte}} \equiv 1$$

$$1 \equiv g^k (g^k)^{-1} \equiv g^h \underbrace{(g^{-1})^k}_{g^{-k}} \equiv g^{h-k} \qquad h-k < \varphi(n)$$

ASSURDO

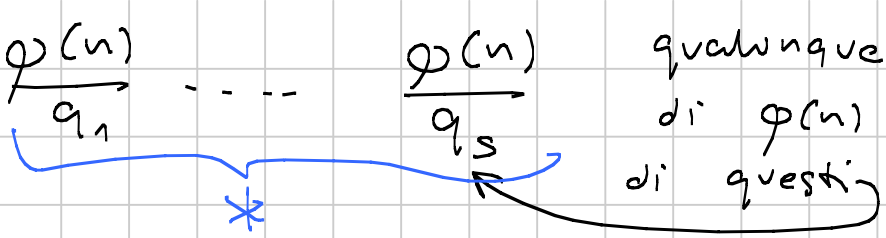
Quindi

$$g, g^2, g^3, \dots, g^{\varphi(n)}$$ sono <u>tutte</u> le classi di resto modulo n coprime con n

n che ha un generatore

a t.c. $MCD(a,n) = 1$ a è un generatore

$$\varphi(n) = q_1^{\beta_1} \cdots q_s^{\beta_s}$$



Se a non è un generatore,

$\text{ord}_n(a)$ divide uno tra *

$$a^{\text{ord}_n(a)} \equiv 1 \pmod n$$

$$a^{k \cdot \text{ord}_n(a)} \equiv \underbrace{\left(a^{\text{ord}_n(a)}\right)^k}_{1} \equiv 1$$

Se a non è generatore, uno tra

$a^{\frac{\varphi(n)}{q_1}}, a^{\frac{\varphi(n)}{q_2}}, \dots a^{\frac{\varphi(n)}{q_s}}$ è $\equiv 1 \pmod n$

È UN SE E SOLO SE

Quindi se tutti questi sono $\not\equiv 1 \pmod n$, a è un generatore

$$a^m \equiv 1 \pmod n \iff \text{ord}_n(a) \mid m$$

Dimostrazione: $m = d \cdot \text{ord}_n(a) + r$

$0 \le r < \text{ord}$

se $r \neq 0$ $a^r \equiv 1$, ASSURDO

---

n tale che esiste generatore modulo n

$$g, g^2, g^3, \dots g^{\varphi(n)} \equiv 1 \pmod n$$

Quanti sono gli elementi con un determinato ordine (in particolare, quanti sono i generatori?)

$1 \le k \le \varphi(n)$ g^k. che ordine ha g^k?

$$\frac{\varphi(n)}{MCD(\varphi(n),k)}$$

$$g^{k \cdot \mathrm{ord}_n(g^k)} \equiv 1 \pmod n$$

$$\varphi(n) \mid k \cdot \mathrm{ord}_n(g^k)$$

$$g^{mcm(k,\varphi(n))} \equiv 1 \pmod n$$

$$mcm(k,\varphi(n)) = \frac{k\varphi(n)}{MCD(\varphi(n),k)}$$

Perché g^k sia un generatore, il suo ordine deve essere $\varphi(n)$, quindi

$$\frac{\varphi(n)}{MCD(\varphi(n),k)} = \varphi(n) \qquad MCD(\varphi(n),k) = 1$$

Ci sono $\varphi(\varphi(n))$ esponenti per g con questa proprietà, e quindi $\varphi(\varphi(n))$ generatori

Fissiamo $d \mid \varphi(n)$. Quanti sono le classi di resto modulo n coprime con n e con ordine d?

Avendo g generatore g^k ha ordine $\frac{\varphi(n)}{MCD(\varphi(n),k)}$

$$\frac{\varphi(n)}{MCD(\varphi(n),k)} = d \qquad MCD(\varphi(n),k) = \frac{\varphi(n)}{d}$$

$$k = \frac{\varphi(n)}{d}, 2\frac{\varphi(n)}{d}, \dots\dots (d-1)\frac{\varphi(n)}{d}, \varphi(n)$$

$$k = h\frac{\varphi(n)}{d} \qquad MCD(h,d) = 1$$

$$k = h_1 \cdot \underset{>1}{MCD(h,d)} \frac{\varphi(n)}{d} = h_1 \frac{\varphi(n)}{d/MCD(h,d)}$$

$$\frac{\varphi(n)}{d/MCD(h,d)} \mid k \qquad \frac{\varphi(n)}{d/MCD(h,d)} \mid \varphi(n)$$

$$\frac{\varphi(n)}{d/MCD(h,d)} \mid MCD(\varphi(n),k) \qquad \frac{\varphi(n)}{d/MCD(h,d)} > \frac{\varphi(n)}{d}$$

se $MCD(h,d) > 1$

Se invece $MCD(h,d) = 1$

Allora $MCD\left(h\frac{\varphi(n)}{d}, \varphi(n)\right) = \frac{\varphi(n)}{d}$

Se h è coprimo anche con $\varphi(n)$ siamo a posto

Se no, tutti i fattori primi di $\varphi(n)$ in h ci sono già in $\frac{\varphi(n)}{d}$

Conclusione: Gli elementi di ordine d sono $\varphi(d)$ perché mi vanno bene tutti gli h coprimi con d

n che ha un generatore g modulo n

$g, g^2, \dots g^{\varphi(n)}$

Quanti sono i residui delle potenze k-esime coprimi con n

Sono $\frac{\varphi(n)}{MCD(\varphi(n),k)}$

$g^k, g^{2k}, g^{3k}, \dots g^{\varphi(n)\cdot k}$

Questi esponenti modulo $\varphi(n)$ sono

$MCD(\varphi(n),k)$, $2\cdot MCD(\varphi(n),k)$, $\dots$ $\frac{\varphi(n)}{MCD(\varphi(n),k)}\cdot MCD(\varphi(n),k)$

$MCD(\varphi(n),k) = b\varphi(n) + ck$ Bezout

$(g^c)^k = g^{ck}\cdot 1 = g^{ck} g^{b\cdot\varphi(n)} =$

$= g^{b\varphi(n)+ck} = g^{MCD(\varphi(n),k)}$

$\alpha \mid \beta$ $\quad \alpha, 2\alpha, 3\alpha, \dots \frac{\beta}{\alpha}\alpha$

$MCD(k,\varphi(n)) \mid \varphi(n)$

I possibili esponenti sono i multipli di k modulo $\varphi(n)$

$1 \leq tk - t\varphi(n) \leq \varphi(n)$

$MCD(k, \varphi(n)) \mid tk$

$MCD(k, \varphi(n)) \mid t\varphi(n)$

I residui k-esimi sono "i multipli" di $MCD(k, \varphi(n))$ Modulo $\varphi(n)$ e sono

$$\frac{\varphi(n)}{MCD(k, \varphi(n))}$$

---

p primo dispari

-1 è un residuo quadratico modulo p?

Lo è se e solo se $p \equiv 1 \pmod 4$

$p = 4h+1$

$g, g^2, \dots g^{2h}, \dots g^{4h} \equiv 1$ ($g^{2h} \to (g^h)^2$)

-1

$(g^{2h})^2 \equiv 1 \pmod p$ $\quad$ $g^{2h} \not\equiv 1 \pmod p$

$x^2 \equiv 1 \pmod p$ $\quad$ $x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \pmod p$

$x \equiv -1 \quad x \equiv 1$

$p = 4h+3$

$g, g^2, g^3, \dots, g^{2h+1}, \dots g^{4h+2} \equiv 1$

$\uparrow$

-1

$MCD(2, 4h+2) \cdot l$

$2 \cdot l$

$g^2, g^4, g^6 \dots g^{4h+2}$ sono residui quadratici

$p \equiv 3 \pmod 4$

$p \mid x^2+y^2 \Rightarrow \begin{matrix} p \mid x \\ p \mid y \end{matrix}$

$p \nmid x \Rightarrow MCD(p,x) = 1$

$\uparrow$ p primo

esiste $x^{-1} \bmod p$

$(x^{-1})^2 \equiv (x^2)^{-1} \equiv x^{-2}$

$p \mid x^2+y^2$ prendo z t.c. $z \equiv x^{-1}$

$p \mid z^2(x^2+y^2)$

$(x^2)^{-1} x^2 + (x^2)^{-1} y^2 \equiv 0 \pmod p$

$1 + y^2 x^{-2} \equiv 0 \pmod p$

$y \cdot x^{-1}$ sarebbe tale che

$(y \cdot x^{-1})^2 \equiv -1 \pmod p$

"square - free"

$p \mid a$: $a, a^2, a^3, \equiv 0 \equiv 0 \equiv 0 \pmod p$

$p \nmid a$: $a, a^2, \dots \underbrace{a^{\mathrm{ord}_p(a)}}_{\equiv 1}, a, a^2$

$p_1 p_2 \cdots p_s$ a intero

La successione $a, a^2, a^3, \dots$ è periodica modulo ciascun p_i, quindi modulo il loro prodotto per TCR

periodo modulo p_1 —

1 se $p_1 \mid a$

$\mathrm{ord}_{p_1}(a)$ se $p_1 \nmid a$

periodo modulo p_2 - —

Il periodo modulo il prodotto è il mcm dei periodi modulo i fattori

$p^{\alpha > 1} \cdot K$

$a = p$ $\quad p, p^2, \dots p^{\alpha-1}, 0 \dots \to$

n intero positivo

$2 \nmid n \qquad 5 \nmid n$

Allora esiste m tale che

$\underbrace{1111\ldots11}_{m \text{ "uni"}}$ è divisibile per n

$\underbrace{9999\ldots99}_{m \text{ "nove"}} = 10^m - 1$

$10^m \equiv 1 \pmod{n} \pmod{9n}$

$MCD(10, n) = 1$

$m = ord_n(10)$

$(9n)$

Dato p primo, esistono infiniti n tali che

$p \mid 2^n - n$

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

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

$n = p-1 \qquad 2^{p-1} - (p-1) \equiv 1 - (p-1) \equiv 2 \pmod{p}$

$a^p \equiv a \pmod{p}$ per qualunque a

$a^{\varphi(n)+1} \equiv a \pmod{n}$ se n è square-free per qualunque a

$$2^{(p-1)^2} - (p-1)^2 =$$

$$= \cancel{1} - p^2 + 2p - \cancel{1} \equiv 0 \pmod{p}$$

$(p-1)^2$

$$2^{(p-1)^{2h}} - (p-1)^{2h} \equiv$$

$$\equiv 1 - (\text{Mutipli di } p + 1)$$

2^n è periodica modulo p di periodo divisore di $p-1$

$-n$ è periodica modulo p con periodo p

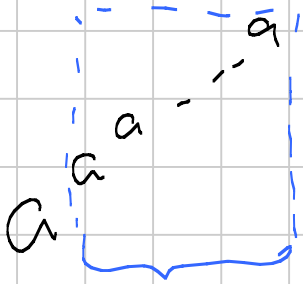
$2^n - n$ è periodica modulo p di periodo mcm dei periodi sicuramente $p(p-1)$

---

a intero positivo, m intero positivo

$$a,\ a^a,\ \underbrace{a^{a^a}}_{a^{(a^a)}},\ a^{a^{a^a}},\ \underbrace{a^{a^{(a^a)}}}_{a^{(a^{(a^a)})}},\ \dots$$

Definitivamente (Da un certo in) poi costante modulo m



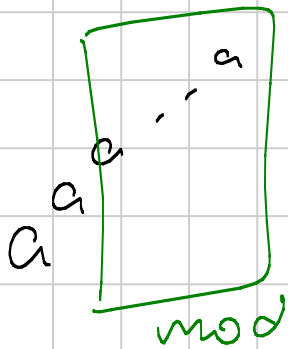
$a^{a^{\cdot^{\cdot^{a}}}} \pmod m$

mi basta l'esponente modulo $\varphi(m)$

$$a = \underbrace{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}_{\text{stanno in } m} \underbrace{q_1^{\beta_1} \cdots q_s^{\beta_s}}_{\text{non ci stanno}}$$

$$m = p_1^{\gamma_1} \cdots p_r^{\gamma_r} K$$

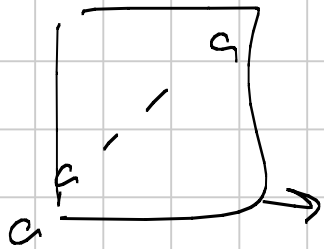
$$a^{a^{\cdot^{\cdot^{a}}}} \equiv 0 \mod p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$



$\varphi(n) < n$ tranne per $n=1$

modulo $\varphi(\varphi(m))$

$\varphi(n)$ $\varphi(\varphi(n))$, $\varphi(\varphi(\varphi(n)))$ - -



costante modulo 2

definitivamente costante modulo $\varphi(\varphi(\ldots\varphi(n)\ldots))$

$a^{a^{a^{\cdots}}}$

$n \mid 2^n + 1$ Allora $3 \mid n$

$2^n \equiv -1 \pmod n$

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

$\operatorname{ord}_n(2) \mid 2n$ $\operatorname{ord}_n(2) \mid \varphi(n)$

PPP sia p il ppp rimo che divide n (più piccolo)

$p \mid 2^n + 1$

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

$\operatorname{ord}_p(2) \mid 2n$ $\operatorname{ord}_p(2) \mid p-1$

$\operatorname{ord}_p(2) \mid \operatorname{MCD}(2n, p-1) \to 1, 2$

$\operatorname{ord}_p(2) = 1, 2$

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

$p = 3$ $2^3 + 1 = 3^2$

$2^9+1 = 513$

$3^h \mid 2^{3^h}+1 \qquad 2^{3^h} = k3^h - 1$

$$2^{3^{h+1}} = \underbrace{k^3 3^{3h} - 3k^2 3^{2h} + k3\cdot 3^h}_{\text{qui c'è } 3^{h+1}} - 1$$

$q > 3$

$3q \mid 2^{3q}+1$

$2^{3q} \equiv -1 \pmod q$

$2^{6q} \equiv 1 \pmod q$

$\text{ord}_q(2) \mid 6q \qquad \text{ord}_q(2) \mid q-1$

$\text{ord}_q(2) = 1, 2, 3, 6 \rightarrow 2^6 \equiv 1 \pmod q$

$2^3 \equiv 1 \pmod q$

$q = 7$

$21 \mid 2^{21}+1$? NO, MODULO 7

2, 4, 1 sono le potenze di 2 modulo 7

$3^2 \cdot 19 = 171$

Quali sono

Qual è il modulo comodo per i residui cubici?

7, 9 $\quad -1, 0, 1$

n con generatore modulo n

I residui k-esimi modulo n

Le classi g^h con h residui dei multipli di $MCD(k, \varphi(n))$ modulo $\varphi(n)$

$$\varphi(7) = \varphi(9) = 6$$

g_7 generatore modulo 7, allora g_7^3 (≡ −1) e g_7^6 (≡ 1) sono i residui modulo 7 coprimi con 7. Poi c'è lo 0

g_9 generatore modulo 9

$g_9^3 \equiv -1$, $g_9^6 \equiv 1$ sono i residui cubici modulo 9 coprimi con 9 Ricordatevi lo 0

Massimo ordine possibile modulo 2^k con $k \geq 3$ è 2^{k-2}

Provate, dando per noto p, a mostrare per induzione che modulo p^k esiste il generatore