Senior 2013 N1 – Medium

SIMONE DI MARINO

IMO 2009/1 (CONGRUENZE)

Sia $n>0$ e $a_1, a_2, \dots, a_k$ $(k \geq 2)$ interi distinti nell'insieme $\boxed{\{1, 2, \dots, n\}}$ tutti e soli i residui modulo n

tali che $n \mid a_i(a_{i+1}-1)$ $(i=1,2,\dots,k-1)$

Dimostrare che $\left[n \nmid a_k(a_1-1)\right]$.

Dim. Proviamo a scrivere i dati sotto forma di congruenze $(\mathrm{mod}\ n)$. $1 \leq a_1, \dots, a_k \leq n$ e distinti, in particolare $a_1 \not\equiv a_2$ (n).

L'altra ipotesi si scrive come

$$a_i(a_{i+1}-1) \equiv 0 \quad (n)$$

$$a_i a_{i+1} - a_i \equiv 0 \quad (n)$$

$$a_i a_{i+1} \equiv a_i \quad (n) \quad \forall\, i=1,\dots,k-1$$

$$a_1 \equiv a_1 a_2 \qquad \underbrace{a_2 \equiv a_2 a_3} \qquad a_3 \equiv a_3 a_4 \quad \cdots \quad a_{k-1} \equiv a_{k-1} a_k$$

$$a_1 \equiv a_1 \boxed{a_2} \equiv a_1 \boxed{a_2 a_3} \equiv a_1 a_2 a_3 a_4 \cdots \equiv \underline{a_1 a_2 a_3 \cdots a_{k-1} a_k}$$

Supp. per assurdo che $\left[a_k a_1 \equiv a_k \quad (n)\right]$

$$a_2 \equiv a_2 a_3 \equiv a_2 a_3 a_4 \cdots \equiv a_2 a_3 a_4 \cdots a_{k-1} \boxed{a_k} \equiv$$

$$\equiv \underline{a_2 a_3 a_4 \cdots a_{k-1} \boxed{a_k a_1}}$$

Quindi avremmo che $a_2 \equiv a_1 \ (n)$. ↯

- Supponete che n sia primo. Poi. $n = pq$. ecc...

Polinomi in $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}$

~~$\mathbb{Z}_p$~~

① $p(x)$ polinomio di grado d, ha al più d radici. $(a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0)$

② $\exists$ $q(x)$ tale che $q(x) \neq 0$ come polinomio

ma $q(i) = 0 \quad \forall i$

$q(x) = x^{p-1} - 1 \longrightarrow$ $(0) \equiv -1 \quad (p)$

$(1) \equiv 0 \quad (p)$

$(2) \equiv 0 \quad (p) \leftarrow$ LFT / PTF

$q(x) = x^p - x$

$\rightarrow q(0) \equiv q(1) \equiv q(2) \equiv \cdots \equiv q(p-1)$

Se $r(0) \equiv r(1) \equiv \cdots \equiv r(p-1) \equiv 0 \quad (p)$

in $\mathbb{Q}$ $\rightarrow r(x) = x(x-1)(x-2) \cdots (x-(p-1)) \cdot q(x) + r_1(x)$

$r_1(x)$ ha tutti coeff. multipli di p

$r(x) \equiv x(x-1) \cdots (x-(p-1))\, q(x)$

$\hookrightarrow$ polinomio monico di grado p che ha come radici $\{0, 1, ..., p-1\}$

$\equiv (x^p - x)\, q(x)$

Sia $q(x)$ un polinomio di grado $\leq p-2$.

Dimostrare che $q(0)+q(1)+\dots+q(p-1)\equiv 0\ (p)$.

Step I Basta dimostrarlo per $q_m(x)=x^m$:

supponiamo sia vero per essi

$$q(x)=a_d x^d + a_{d-1}x^{d-1}+\dots+a_1 x + a_0$$

$$\sum_{i=0}^{p-1} q(i) \equiv \left(a_d\cdot 0^d + a_{d-1}\cdot 0^{d-1}+\dots+a_1\cdot 0 + a_0\right)+$$
$$\left(a_d\cdot 1^d + a_{d-1}\cdot 1^{d-1}+\dots+a_1\cdot 1 + a_0\right)+$$
$$\left(a_d\cdot 2^d + a_{d-1}\cdot 2^{d-1}+\dots+a_1\cdot 2 + a_0\right)+$$
$$\vdots$$
$$\left(a_d\cdot (p-1)^d + a_{d-1}\cdot (p-1)^{d-1}+\dots+a_1 (p-1) + a_0\right);$$

$$\equiv a_d\cdot 0 + a_{d-1}\cdot 0 - \dots + a_1\cdot 0 + a_0\cdot 0$$

$$\equiv 0.$$

Step II $0^m+1^m+2^m+\dots+(p-1)^m\equiv 0\ (p)$.

(a) sia g un generatore modulo p $\begin{pmatrix} g^{p-1}\equiv 1\ (p) \\ g^k\not\equiv 1\ (p) \\ k<p-1\end{pmatrix}$

$$\{g^0, g^1, \dots, g^{p-2}\}=\{1,\dots,p-1\}$$

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

poiché $1 \le m \le p-2$, so che $g^m \not\equiv 1$ (g generatore)

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

(b) $\{1, 2, \ldots, p-1\} = \{a, 2a, 3a, \ldots, a(p-1)\}$

$(a,p) = 1$ so che $a \not\equiv 0$, $2a \not\equiv 0$, $\vdots$, $a(p-1) \not\equiv 0$ $\quad ia \not\equiv ja$ se $i \neq j$

$$S_m = 1^m + 2^m + \cdots + (p-1)^m \overset{\text{mod } p}{\equiv} a^m + (2a)^m + \cdots + ((p-1)a)^m$$

$$S_m \equiv a^m S_m \quad (p) \qquad \forall\ (a,p) = 1$$

$$S_m (a^m - 1) \equiv 0 \quad (p)$$

<u>Fatto</u> se $1 \le m \le p-2$ $\exists\ a$ t.c. $a^m \not\equiv 1$ (p)

ad esempio è vero per $a = g$.

Esistenza di un generatore (mod. p) (p primo)

Sia x tale che $x^{24} \equiv 1$ (61).

è vero che $x^{36} \equiv 1$ (61) ?

$\text{ord}_{61}(x)$?

$$\mathcal{O}_x = \{ k \mid x^k \equiv 1 \ (61) \}$$

$0 \in \mathcal{O}_x$ $\qquad$ $60 \in \mathcal{O}_x$ $\Leftarrow$ piccolo teorema di fermat.

$k \in \mathcal{O}_x \Rightarrow 2k \in \mathcal{O}_x, \ 3k \in \mathcal{O}_x \ \ldots$

$k, J \in \mathcal{O}_x \Rightarrow k + J \in \mathcal{O}_x$

$x^k \equiv 1 \quad x^J \equiv 1 \Rightarrow x^{k+J} \equiv 1$

$$\mathcal{O}_x = \{0, m, 2m, 3m, \ldots\}$$

$m = ord_{61}(x)$

Sia m il minimo di $\mathcal{O}_x \setminus \{0\}$.

Ora, dato $n \in \mathcal{O}_x$ $\qquad$ $n = qm + r$

$$1 \equiv x^n \equiv x^{qm+r} \equiv x^{qm} \cdot x^r = (x^m)^q \cdot x^r$$
$$\equiv x^r \ (61) \qquad r \in \mathcal{O}_x$$

$0 \le r < m \Rightarrow r = 0. \Rightarrow m \mid n.$

$x^k \equiv 1 \ (61) \Rightarrow ord_{61}(x) \mid k$

$x^{60} \equiv 1 \ (61) \qquad ord_{61}(x) \mid 60$

$$x^{24} \equiv 1 \quad (61) \qquad \mathrm{ord}_{61}(x) \mid 24$$

$$\Rightarrow \mathrm{ord}_{61}(x) \mid (24, 60) = 12^{*}$$

$$^{*}\, x^{12} \equiv 1 \quad (61) \qquad \mathrm{ord}_{61}(x) \mid 60$$

$$x^{36} \equiv 1 \quad (61)\ ? \quad \text{Sí porque } (x^{12})^3 \equiv 1^3 \equiv 1.$$

$$31 \mid x^{19} - y^{19} \Rightarrow 31 \mid x^{9} - y^{9}$$

$$\left(\frac{x}{y}\right)^{19} \equiv 1 \quad (31) \Rightarrow \mathrm{ord}_{31}\left(\frac{x}{y}\right) \mid 19 \;/\!\!\mid 30 \quad = 1.$$

$$\mathrm{ord}_p(a) = k \qquad \mathrm{ord}_p(b) = J$$

$$\mathrm{ord}_p(ab) \overset{?}{=} \mathrm{mcm}$$

$$\boxed{b = a^{-1}}$$

$$\mathrm{ord}_p(a) = k \qquad \mathrm{ord}_p(a^{-1}) = k \qquad \mathrm{ord}_p(\underbrace{a \cdot a^{-1}}_{1}) = 1 \neq k$$

$$(ab)^{\mathrm{mcm}(k,J)} \equiv a^{\mathrm{mcm}(k,J)} \cdot b^{\mathrm{mcm}(k,J)} \equiv 1 \cdot 1 \equiv 1 \quad (p)$$

$$m = \mathrm{ord}_p(ab) \mid \mathrm{mcm}(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$$

$$(ab)^{mJ} \equiv 1^J = 1^J \qquad \mathrm{ord}_p(a) \mid mJ$$

$$\overset{\shortparallel}{a^{mJ} \cdot b^{mJ}} \equiv a^{mJ} \cdot (b^J)^m \equiv a^{mJ}$$

$$k \mid m j \qquad \text{mcm}(k, j) \mid m\, \text{MCD}(k,j)$$
$$j \mid m k$$

$$k^2 \mid m j k$$
$$j^2 \mid m j k \implies \text{mcm}(k^2, j^2) \mid m j k$$
$$\text{mcm}(k, j)^2 \mid m j k$$

$$jk = \text{mcm}(j,k)\, \text{MCD}(j,k) \qquad \text{mcm}^{\cancel{2}} \mid m \cdot \cancel{\text{mcm}} \cdot \text{MCD}$$

$$\left(p^a \cdot p^b = p^{\max\{a,b\}} \cdot p^{\min\{a,b\}} \right) \qquad \frac{\text{mcm}}{\text{MCD}} \mid m$$

Th.
$$\boxed{\frac{\text{mcm}}{\text{MCD}} \mid ord_p(ab) \mid \text{mcm}}$$

Corollario

in particolare se $\text{MCD}(ord_p(a), ord_p(b)) = 1$ allora $ord_p(ab) = \text{mcm} = ord_p(a) \cdot ord_p(b)$.

Esercizio a, b coprimi con p, mostrare che $\exists$ c coprimo con p tale che
$$ord_p(c) = \text{mcm}(ord_p(a), ord_p(b)).$$

Caso facile $(ord_p(a), ord_p(b)) = 1$ so che $c = ab$ risolve per il Cor. precedente.

$$c = a^i b^h \to (ord_p(a^i), ord(b^h)) = 1$$
$$\to ord_p(a^i) \cdot ord(b^h) = \text{mcm}(k, j)$$

$$\frac{ord_p(a)}{(ord_p(a), i)} = ord_p(a^i) < \begin{matrix} ord_p(a) & (i, ord_p(a)) = 1 \\ \frac{ord_p(a)}{i} & (i \mid ord_p(a)) \end{matrix}$$

$$m = ord_p(a^i) = \min\{ n : (a^i)^n \equiv 1 \ (p) \}$$

$$= \min\{ n : a^{in} \equiv 1 \ (p) \}$$

$$\min\{ n : ord_p(a) \mid in \}$$

$$m = \frac{ord_p(a)}{(ord_p(a), i)} .$$

$M = \{$ il più grande intero che sia ordine moltiplicativo per qualche x mod p $\}$

$$= \max\{ ord_p(x) : x \in 1, \dots, p-1 \} = ord_p(g)$$

<u>Cor.</u> $x^M \equiv 1 \ (p) \quad \forall \ x \in 1, \dots, p-1.$

supp. per assurdo che $\exists \ y$ t.c.

$$y^M \not\equiv 1 \ (p) \qquad ord_p(y) \nmid M$$

$$mcm(ord_p(y), ord_p(g)) > M$$

$$\overset{\shortparallel}{ord_p(c)} \qquad ord_p(c) > M \qquad \underline{\text{Assurdo}}.$$

$q(x) = x^M - 1$ ha per radici $1, 2, 3, \dots, p-1$

$\Rightarrow \quad M \geq p-1 \qquad M \leq p-1$ (piccolo th. di Fermat)

$\Rightarrow \quad M = p-1 \quad \rightsquigarrow \quad \mathrm{ord}_p(g) = p-1$ (generatore)

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

piccolo th. di fermat: $x^{p-1} \equiv 1 \ (p) \quad \forall\ x = 1, \dots, p-1$

$$\underbrace{\mathrm{ord}_p(x) \mid p-1}_{\leq p-1}.$$

$$n < p \leq \frac{4n+3}{3} \Rightarrow p \mid \sum_{i=0}^{n} \binom{n}{i}^4$$

$n = p-1$

$$\binom{p-1}{i} = \frac{(p-1)\cdot(p-2)\cdot(p-3)\cdots(p-i)}{1\cdot 2\cdot 3 \cdots i} \equiv$$

$$\equiv \frac{(-1)}{1}\cdot\frac{(-2)}{2}\cdot\frac{(-3)}{3}\cdots\frac{}{(i-1)}\cdot\frac{(-i)}{i} = (-1)^i \ (p)$$

$$\sum_{i=0}^{p-1} \left((-1)^i\right)^4 = p \equiv 0 \quad (p) \quad . \text{ ok.}$$

$n = p-2$

$$\binom{p-2}{i} = \frac{(\cancel{p}-\cancel{2})(\cancel{p}-\cancel{3})\cdots/(\cancel{p}-i-1)}{1\cdot\cancel{2}\cdot\cancel{3}\cdots\cancel{i}} = (-1)^i(i+1)$$

$$\sum_{i=0}^{p-2} \binom{p-2}{i}^4 = \sum_{i=0}^{p-2} \left(\quad (i+1) \right)^4 = \sum_{i=0}^{p-1} q(i) \equiv 0 \ (p)$$

$$\text{se} \quad \partial q \overset{\leq 5}{\leq} p-2$$

$$p \leq \frac{4(p-2)+2}{3} \Rightarrow 3p \leq 4p - \cancel{6}$$

$$\cancel{6} \leq p$$

$$n = p - r$$

$$\binom{p-r}{i} = \frac{\overset{(p-i-1)(p-i-2)\cdots}{\cancel{(p-r)}(\cancel{p-r-1}) \cancel{-} - - (p-r-i+1)}}{1 \cdot 2 \cdot 3 \cdots r-1 \cdot \cancel{r} \cdot \cancel{\cdot} \cancel{i}} =$$

$$= (-1)^i \frac{(p-i-1)(p-i-2)\cdots(p-i-(r-1))}{1 \cdot 2 \cdot 3 \cdots (r-1)} \overset{(-1)^i}{=} q_r(i)$$

$$\sum_{i=0}^{p-r} \binom{p-r}{i}^4 = \sum_{i=0}^{p-r} q_r(i)^4 = \sum_{i=0}^{p-1} q_r(i)^4 \overset{?}{\equiv} 0$$

$$\partial q_r^4 = 4(r-1)$$

$$4(r-1) \overset{?}{\leq} p-2$$

$$p \leq \frac{4n+2}{3} \qquad p \leq \frac{4(p-r)+2}{3}$$

$$3p \leq 4p - 4r + 2$$

$$\Downarrow$$

$$4(r-1) \leq p-2 \quad . \quad \text{ok.}$$

Lifting the exponent lemma.

Lemma (LTE) Sia p un primo dispari e siano a, b numeri interi coprimi con p. Allora se $p \mid a-b$ allora

$$v_p\left(a^{p^k} - b^{p^k}\right) = v_p(a-b) + k$$

altrimenti $v_p\left(a^{p^k} - b^{p^k}\right) = 0$.

Def. (valutazione p-adica) Dato un primo p e un intero a, si definisce $k = v_p(a)$ il massimo numero naturale tale che $p^k \mid a$

Esempi:

$$v_2(10) = 1 \qquad v_3(1001) = 0$$

$$v_5(100) = 2 \qquad v_3(10101012) = 1$$

$$v_7(49^3) = 6$$

nei razionali $v_2\left(\frac{1}{10}\right) = -1$ $\qquad v_2\left(\frac{1}{1000}\right) = -3$

$$v_5\left(\frac{17}{3}\right) = 0$$

Proprietà di v_p: • $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

• $v_p(a \cdot b) = v_p(a) + v_p(b)$

Dim. $$(a^{p^k} - b^{p^k}) = (a-b)(\text{Mostriciattolo})$$

chiaramente $$v_p(a^{p^k} - b^{p^k}) \geq v_p(a-b)$$

$\boxed{k=1}$ $$a^p - b^p = (a-b)\underbrace{(a^{p-1} + a^{p-2}\cdot b + \dots + b^{p-2}\cdot a + b^{p-1})}$$

So che $a \equiv b \ (p)$ $$a^{p-1} + a^{p-1} + \dots + a^{p-1} = p \cdot a^{p-1} \equiv 0 \ (p)$$

Ah! Ma allora $$v_p(a^p - b^p) \geq v_p(a-b) + 1$$

$$a = b + kp^s \qquad (\text{dove } (k,p) = 1,\ s = v_p(a-b))$$

$$a - b = k \cdot p^s$$

$$a^p - b^p = (b + kp^s)^p - b^p =$$

$$= p \cdot (kp^s) \cdot b^{p-1} + \overbrace{\underbrace{\binom{p}{2}(kp^s)^2 \cdot b^{p-2}}_{\frac{p(p-1)}{2}\cdot p^{2s}\cdot k^2 \cdot b^{p-2}} + \dots}^{\text{multiplo di } p^{s+2}}$$

$$p^{s+1} \cdot p^s$$

$$= p^{s+1} \cdot k' + p^{s+2} \cdot k'',$$

$$= p^{s+1}(k' + p \cdot k'')$$

sicuramente NON ha fattori p.

$$v_p(a^p - b^p) = v_p(a-b) + 1$$

Per induzione: $v_p(a^{p^k} - b^{p^k}) = v_p(a-b) + k$

(a, b sono coprimi con p e $p \mid a-b$)

$\boxed{p=2}$ $v_p(a^{2^k} - b^{2^k}) = v_p(a^2 - b^2) + k - 1$

$$= v_p(a-b) + v_p(a+b) + k - 1$$

Teo Sia g generatore modulo p tale che $p^2 \nmid g^{p-1} - 1$. Allora g è generatore modulo p^k $\forall k$.

Esempio 2 mod 5

$2 = 2$
$2^2 = -1$
$2^3 = 3$
$2^4 = 1$

(anche 3 è generatore)

$25 \nmid 2^4 - 1 = 15$

$\rightsquigarrow$ 2 è generatore modulo 5^k per ogni k.

Dim. Voglio stabilire $\mathrm{ord}_{5^k}(2)$. So che $\mathrm{ord}_{5^k}(2) \mid \varphi(5^k)$ (teo eulero)

$$x^{\varphi(n)} \equiv 1 \quad (n) \qquad \forall \quad (x,n) = 1$$

$$\Rightarrow \quad ord_n(x) \mid \varphi(n)$$

$$ord_{5^k}(2) \mid 5^{k-1} \cdot 4$$

$$ord_5(2) \mid ord_{5^k}(2) = m_k$$

$$2^{m_k} \equiv 1 \quad (5^k)$$

$$2^{m_k} \equiv 1 \quad (5)$$

$$4 \mid ord_{5^k}(2) \mid 5^{k-1} \cdot 4$$

$$\Rightarrow \quad ord_5(2) \mid m_k$$

$$ord_{5^k}(2) = 5^s \cdot 4$$

s lo dobbiamo trovare

$$s \leq k-1$$

$$V_5\left(2^{5^s \cdot 4} - 1\right) = V_5\left((2^4)^{5^s} - (1)^{5^s}\right) =$$

$$\overset{LTE}{=} V_5(2^4 - 1) + s = s+1$$

$$2^{5^s \cdot 4} \equiv 1 \quad (5^k)$$

$$5^k \mid 2^{5^s \cdot 4} - 1$$

$$V_5(5^k) \leq V_5\left(2^{5^s \cdot 4} - 1\right)$$

$$s \geq k-1 \quad \Leftarrow \quad k \leq s+1$$

$$s = k-1$$

$$\Rightarrow \quad ord_{5^k}(2) = 5^{k-1} \cdot 4 = \varphi(5^k)$$

$\Rightarrow$ 2 è generatore.

Cor. Esistenza di un generatore modulo p^k.

g generatore mod p t.c. $p^2 \mid g^{p-1}-1$

Ese. $(g+p)$ è generatore mod p

e $(g+p)^{p-1} \not\equiv 1 \quad (p^2)$.

$4p^k$ NON può avere generatori

perché $\mathrm{ord}_{nm}(x) = \mathrm{mcm}(\mathrm{ord}_n(x), \mathrm{ord}_m(x))$

quando n, m sono coprimi

in particolare $\mathrm{ord}_{4p^k}(x) \mid \varphi(p^k) \neq \varphi(4p^k)$

$$\varphi(4p^k) = 2\varphi(p^k)$$

$p\ q$ dispari $\quad \mathrm{ord}_{pq}(x) \mid \dfrac{(p-1)(q-1)}{2}$.

Residui modulo p:

residui quadratici

quanti sono? (escluso lo 0, $\frac{p-1}{2}$) $\quad \frac{p+1}{2}$

$0^2 \quad 1^2 \quad 2^2 \quad 3^2 \quad 4^2 \quad - - - \quad (p-2)^2 \quad (p-1)^2$

$$a^2 \equiv b^2 \quad (p) \quad \iff \quad p \mid (a-b)(a+b) \quad \begin{cases} a \equiv b \ (p) \\ a \equiv -b \ (p) \end{cases}$$

i residui quadratici sono $\frac{p+1}{2}$ e sono esattamente

$$0 \quad (\pm 1)^2 \quad (\pm 2)^2 \quad \dots \quad \left(\pm \frac{p-1}{2}\right)^2$$

Come faccio a sapere se a è un residuo quadratico?
- criterio di Eulero
- simbolo di Jacobi

Se $a \equiv b^2 \ (p)$ a residuo quadratico

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \quad (p) \quad \Rightarrow \quad a^{\frac{p-1}{2}} \equiv 1 \quad (p)$$

(I) a non è un residuo quadratico, allora $a = g^k$ k per forza dispari

$$a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \not\equiv 1 \qquad p-1 \nmid \frac{k(p-1)}{2}$$

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \quad \Rightarrow \quad a^{\frac{p-1}{2}} \equiv -1 \quad (p)$$

(II) $x^{\frac{p-1}{2}} - 1 = q(x)$ ha al più $\frac{p-1}{2}$ radici.

So che i residui quadratici sono radici ma allora non ce ne sono altre e quindi se a NON è residuo $\quad a^{\frac{p-1}{2}} \not\equiv 1 \ (p) \quad (\equiv -1)$.

-1 è res. quadratico $\iff (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } 4 \mid p-1 \\ -1 & \text{altrimenti} \end{cases}$

p primo dispari $\quad (a, p) = 1 \quad$ (simbolo di Jacobi)

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è res. quadratico} \\ -1 & \text{se } a \text{ non è res. quad.} \end{cases}$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p)$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Almeno uno tra 2, 3 e 6 è residuo quadratico modulo p.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

rec. quadratica (p, q primi) $\quad \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

$$\left(\frac{1787}{61}\right) = \left(\frac{-43}{61}\right) = \left(\frac{18}{61}\right) = \cancel{\left(\frac{3}{61}\right)}\cancel{\left(\frac{3}{61}\right)}\left(\frac{2}{61}\right) = (-1)^{d} = -1$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

$$2 \cdot 4 \cdot 6 \cdot 8 \cdots \frac{p-1}{2} \cdot \frac{p+3}{2} \cdots p-1 =$$

$$P = 2 \cdot 4 \cdot 6 \cdot \overset{11}{8} \cdot \cdots (p-1) =$$

$$= 2^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)$$

$$= 2 \cdot 4 \cdot \cdots \frac{p-1}{2} \cdot \left(\frac{p+3}{2} \cdots 1\right).$$

$$(-1)^{\lfloor\frac{p-1}{4}\rfloor}$$

$$= \left(\frac{p-1}{2}\right)!$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{\lfloor\frac{p-3}{4}\rfloor}.$$

$\frac{p^2-1}{8}$ < pari se $p \equiv {1 \atop 7}$ (8) ; dispari se $p \equiv {3 \atop 5}$ (8)

<u>TdN 2</u> : 10 $\quad D = \{ n \in \mathbb{N} : n \mid 2^n + 1 \}$

a) determinare tutti i primi p che stanno in D.

p.t.f. $\quad x^p \equiv x \quad (p)$

$$p \mid 2^p + 1 \equiv 2 + 1 = 3 \qquad p \mid 3$$

$p = 3$ va bene $\quad 3 \mid 9$

(b) Determ. potenze di primi che sono in D

$$p^k \mid 2^{p^k}+1 \qquad\qquad 2^p+1 \mid 2^{p^k}+1$$

$$0 \equiv 2^{p^k}+1 \equiv \left(2^{p^{k-1}}\right)^p + 1 \equiv 2^{p^{k-1}}+1 \ldots \equiv 2+1 \ (p)$$

$$\left(x^{p^2} = \left(x^p\right)^p \equiv x^p \equiv x \right) \qquad \boxed{p=3}$$

$$3^k \mid 2^{3^k}+1 = 2^{3^k} - (-1)^{3^k}$$

voglio i k t.c. $k \leq v_3\left(2^{3^k} - (-1)^{3^k}\right) =$

$$= v_3(2-(-1)) + k = k+1$$

$\forall k$. $\quad D \supseteq \{3, 3^2, 3^3, \ldots\}$.

(c) $n = pq$

$$pq \mid 2^{pq}+1$$

$$2^{pq} \equiv -1 \ (p) \qquad\qquad 2^{pq} \equiv -1 \ (q)$$

$$(2^p)^q \equiv 2^q \equiv -1 \ (p) \qquad\qquad 2^p \equiv -1 \ (q)$$

$2^{2q} \equiv 1 \quad (p)$ $\qquad$ $2^{2p} \equiv 1 \quad (q)$

$\text{ord}_p(2) \mid 2q$ $\quad$ ($\cancel{1}$, 2, $\cancel{q}$, 2q) $\qquad$ $\text{ord}_q(2) \mid 2p$

$p \leq q$

$\text{ord}_p(2) \nmid q$

$\text{ord}_p(2) \mid p-1$ $\qquad$ $\text{ord}_p(2) \mid (2q, p-1)$

$(2, p-1) = 2$

$\text{ord}_p(2) = 2$

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

$3 \equiv 0 \quad (p)$

$3 = p$

$3 \mid 2^q + 1$ $\qquad$ $q \mid 2^3 + 1 = 9$ $\qquad$ $q = 3$

(c): unico e' 9

(d):

$n = p^s \cdot A$ $\qquad$ p e' il più piccolo primo che divide n

$p^s A \mid 2^{p^s A} + 1$ $\qquad$ $2^{p^s A} \equiv -1 \quad (p)$

$2^{2p^s A} \equiv 1 \quad (p)$

$\text{ord}_p(2) \mid (2\cancel{p^s A}, p-1) \Leftarrow$

$(2, p-1) = 2$

$2^2 - 1 \equiv 0 \quad (p) \Rightarrow p = 3$

(e) $n = p^2 q$

$p=3 \longrightarrow n = 9q$

$9q \mid 2^{9q}+1$ $\quad 27 \cdot 19$

$q \mid 2^{9q}+1 \equiv 2^9+1$

$q = 19$

[e si verifica che funziona]

$q=3 \longrightarrow n = 3p^2$

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

$p \mid 2^{3p^2}+1 \equiv 2^3+1 = 9$ $\quad p=3$ $\lightning$.