

N1

$$n = p_1^{\alpha_1} + \dots + p_k^{\alpha_k} \quad p_i | m \quad \alpha_i \geq 0$$

$$n = p^{\alpha} + q^{\beta} \quad \text{No può: } p \nmid p^{\alpha} + q^{\beta}$$

proviamo con 3 primi tra cui p

$$n = p^{\alpha} + q^{\beta} + r^{\gamma} \quad p, q, r | m$$

$$r | p^{\alpha} + q^{\beta}$$

$$q | p^{\alpha} + r^{\gamma}$$

$$p | q^{\beta} + r^{\gamma}$$

operiamo che ni porta a

$$r^{\gamma} \equiv -1 \pmod{p}$$

$$p^{\alpha} \equiv -1 \pmod{q}$$

$$q^{\beta} \equiv -1 \pmod{p}$$

$$r | p^{\alpha} + q^{\beta}$$

per la prima, possiamo prendere $(p-1)(q-1) | \gamma$ e la scelta di r è arbitraria tra i divisori di $p^{\alpha} + q^{\beta}$ (che non è divisibile per p o q)

CRITERIO DI EULERO

$$p \in \mathbb{P}_{>2} \quad (a, p) = 1 \quad \left(\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right)^{\frac{p-1}{2}} \pmod{p}$$

$$\text{se } a \text{ non è residuo quadratico} \quad a^{\frac{p-1}{2}} \equiv -1$$

$$\text{Quindi, ci basterà avere che } \left(\frac{p}{q}\right) = -1 = \left(\frac{q}{p}\right) \text{ e } \begin{cases} \alpha \equiv \frac{q-1}{2} (q-1) \\ \beta \equiv \frac{p-1}{2} (p-1) \end{cases}$$

$$\text{Dimostreremo che } 1 = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}}$$

$$\text{se } q \equiv 1 \pmod{4} \quad \checkmark$$

Quindi ci basterà prendere $q \equiv \text{non residuo quadratico} \pmod{p}$,
che esiste. $\square$

N2

Per ogni a quanto vale $|S_a|$? Non porta a molto

Per ogni classe di resto r , per quanti a si ha che $r \in S_a$?

Guardarle in contemporanea funziona meglio:

(r, a) t.c. che $r \in S_a$. Sappiamo che

$$\sum |S_a| = \sum_{\substack{r, a \text{ t.c.} \\ r \in S_a}} 1$$

$$S_a \quad r \in S_a \Rightarrow \exists x \text{ t.c. } x^n + ax = r$$

$$\Rightarrow \lambda^n x^n + \lambda^n ax = r \lambda^n \quad \forall \lambda \text{ classe di resto.}$$

$$(\lambda x)^n + \lambda^{n-1} a (\lambda x) = r \lambda^n$$

$$(r, a) \text{ buona} \Rightarrow (r \lambda^n, a \lambda^{n-1}) \text{ è buona}$$

$$r=0: (0, a) \text{ è sempre buona } (x=0) \\ \Rightarrow p-1 \text{ coppie } (0, a).$$

$$r \neq 0: (r, a) \text{ buona, considero le coppie} \\ \text{buone } (\lambda^n r, \lambda^{n-1} a) \text{ al variare di} \\ \lambda = 1, \dots, p-1$$

$$\text{Se } (\lambda_1^n r, \lambda_1^{n-1} a) = (\lambda_2^n r, \lambda_2^{n-1} a)$$

$$\Rightarrow \frac{\lambda_1^n r}{\lambda_1^{n-1} a} = \frac{\lambda_2^n r}{\lambda_2^{n-1} a} \Rightarrow \lambda_1 = \lambda_2$$

Inoltre che se $(r, a) \rightarrow (\lambda^n r, \lambda^{n-1} a)$,

allora da $(\lambda^n r, \lambda^{n-1} a) \rightarrow (r, a)$

agendo sulla coppia $\frac{1}{\lambda}$ (che esiste perché λ è invertibile). Ho fatto una divisione

in gruppi che hanno tutti $p-1$ elementi.

N3

$$p - q = n^2$$

$$\forall t \mid p - t^2 > 0, \quad p - t^2 = 2^\alpha q^\beta$$

Solipsini

$$p - q = x^2 - 1 = (x-1)(x+1)$$

$$(x-1, x+1) = 2$$

Come tra $x-1$ e $x+1$ ha fattori primi
dispari $\Rightarrow x-1 = 2^n$ o $x+1 = 2^n$

$$x-1 = 2^{n+1}$$

$$x+1 = 2^{n+1} + 2 = 2(2^n + 1)$$

11 5e

$$2^n + 1 = 5^a$$

$$2^n = 5^a - 1$$

$$2 \mid 5-1$$

$$(5-1)(5+1)$$

$$\frac{2^n - 1}{1}$$

$$n \geq 3$$

$$n = 2$$

$$\Rightarrow a = 1$$

$$2^n \pm 1$$

$$a \mid n$$

$\downarrow$ ipotesi

$$\Rightarrow n = 2^{n'}$$

$$2^a + 1 \mid 2^n - 1$$

$$k-1 = 2^{n+1}$$

$$n+1 = 2(2^{2^n} + 1)$$

↙ prime

$$p = (2^{2^n + 1} + 1)^2 + 8$$

↙
 2^n

$$(2^{1+1})^2 + 8 = 3^2 + 8 = 17$$

OG

$$k+1 = 2^{q+1}$$

$$k-1 = 2^{q+1} - 2 = 2(2^q - 1)$$

↙
 s^β

$$2^q = s^\beta + 1$$

$$s=2 \quad \beta=1$$

$$\Rightarrow \beta=1$$

$$\text{Ie } q = ru$$

$$2^r - 1 \mid 2^q - 1 \quad \text{non ve been}$$

$$\Rightarrow q \in \text{prime.}$$

$$k-1 = 2^{q+1} - 2$$

$$n = 2^{q+1} - 1$$

$$P = (2^{q+1} - 1)^2 + 8 \quad \equiv \quad 1 + 8 \equiv 9 \pmod{16}$$

$\forall x$
 super
 $p = k^2$

Se over in due punti r, s piccoli con
 $\left(\frac{p}{r}\right) = \left(\frac{p}{s}\right) = 1$, una CRT e ho vinto.

$$r = \frac{1}{c} \sqrt{p} \quad c \text{ oblatore grande } c > 10^{10^{10}}$$

$$\left(\frac{p}{r}\right) = 1$$

$$k = \sqrt{p} \quad (r)$$

$$k = 1 \quad (r)$$

$$k^2 = c_1 r^2 \quad c_1 \leq r_h$$

$$p r^n = p - k^2 = p - c_1 r^2 \quad p - \frac{c_1}{c^2} r = p \left(1 - \frac{c_1}{c^2}\right)$$

$$p r^m = p - (k + \delta r)^2 = p - k^2 - \underbrace{(16kr + 64r^2)}_{c_2 r^2} = p \left(1 - \frac{c_1}{c^2} - \frac{c_2}{c^2}\right)$$

$$r \leq 3$$

$$c_2 \leq 1000$$

$$r < \frac{1}{c} \sqrt{p} \quad \left(\frac{p}{r}\right) = 1$$

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

$$r \mid p - k^2$$

$$r < \frac{1}{2} \sqrt{p} \quad \left(\frac{p}{r}\right) = -1$$

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

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

$r \mid \underbrace{\quad \quad \quad}$

$$\left(\frac{p}{r}\right) = 1$$

$$r \mid z^s - 1, \quad s \text{ odd}$$

$$z = g^h \quad g^{xs} = 1, \quad p-1 \mid ks$$

$$z \mid p-1 \Rightarrow z \mid h$$

$$q_{f-1} = 2^{\omega}$$

$$p \equiv 7 \pmod{8}$$

$$p = 7 \mid 8$$

$$\text{ord}_{17}(2) = 8$$

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

$$(1 - 1)^2 + 8 = 8$$

$$\left(\frac{2}{17}\right) = 1$$

oppure $q \perp 1$ ma è potenza di 2

$$(2^{\frac{q+1}{2}} - 1)^2 (2^{\frac{q+1}{2}} + 1)^2 + 1 = 16$$

$$5 \mid q+1 \quad r \mid 2^8 - 1 \mid 2^{\frac{q+1}{2}} - 1$$

Per questo $r, \left(\frac{p}{r}\right) = 1$ e abbiamo finito. $\square$