N 1 MEDIUM / parte 2 [Gallo]

Titolo nota

Esiste un generatore mod p^n (con p primo dispari, $n \geq 1$)

- Se g genera mod p, allora g oppure $g+p$ genera mod p^2.

Dim.

- Sia g che $g+p$ generano mod p
- x è gen. mod p^2 $\iff$ $\mathrm{ord}_{p^2} x = \varphi(p^2) = p(p-1)$

$\iff$ $p^2 \nmid x^{p-1}-1$ e $p^2 \nmid x^{dp}-1$ dove $d \mid p-1$

Supponiamo che $g^{p-1} \equiv 1 \mod p^2$,

è vero quando x è gen mod p

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}\cdot p + \cancel{\ldots}^{0} \mod p^2$$
$$\equiv 1 + (p-1)\cdot g^{p-2}\cdot p \mod p^2$$
$$\equiv 1 - g^{p-2}\cdot p \mod p^2$$

$\not\equiv 1$ mod p^2 e quindi soddisfa!

2 genera mod 3 $\longrightarrow$ 2 ~~5~~ generano mod 9 !

4
8 = -1
-2
-4
1

- Se g genera mod p^2, allora genera mod p^n.

x genera $\iff$ $\mathrm{ord}_{p^n}(x) = \varphi(p^n) = p^{n-1}(p-1)$

$\iff$ $p^n \nmid x^{p^{n-1}d}-1$ e $p^n \nmid x^{p^{n-2}(p-1)}-1$

$d \mid p-1$, $d < p-1$

Vero quando x è gen mod p

$$x^{p^{n-1}\cdot d} \equiv (x^d)^{p^{n-1}} \equiv x^d \not\equiv 1 \mod p$$

$$v_p\left(x^{p^{n-2}\cdot(p-1)}-1\right) = v_p\left((x^{p-1})^{p^{n-2}}-1\right) =$$
$$= v_p(x^{p-1}-1) + v_p(p^{n-2})$$
$$= 1 + (n-2)$$ per la dim nel caso p^2
$$= n-1$$

$\longrightarrow$ 2 genera mod 3^n

Problema 6. [BMO 2018-4] Trovare (p,q) di primi t.c.

$$3p^{q-1}+1 \mid 11^p+17^p.$$

LHS $\equiv 4 \mod q$

$v_p(11^p+17^p)$ con $p\neq 2,7$ non posso

$v_2(11^2+17^2)=1$ mod 4

$v_7(11^7+17^7)=2$ LTE

- Prendo r primo che divide $3p^{q-1}+1$

$$11^p+17^p \equiv 0 \mod r$$
$$\left(11/_{-17}\right)^p \equiv 1 \mod r$$

$r=2,7$

$\Longrightarrow \text{ord}_r(11/_{-17})$ → 1: $11/_{-17}\equiv 1 \mod r$, $28\equiv 0 \mod r$

→ p: $p \mid r-1$

- $3p^{q-1}+1 = 2^m\cdot 7^k\cdot t$ con t prodotto di primi $\equiv 1 \mod p$, $(t,14)=1$

$m=0,1,2$ $\quad$ $k=0,1$

$$1 \equiv 2^{m} \cdot 7^{k} \cdot 1 \mod p$$

con p dispari

$$V_2(11^p + 17^p) = V_2(28) + V_2(p)$$
$$= 2$$

LTE

$$m = V_2(3p^{q-1}+1) \leq V_2(11^p + 17^p) \leq 2$$

$$k \leq V_7(11^p + 17^p) \overset{LTE}{=} V_7(28) = 1$$

$\Longrightarrow$ p è un primo ≤ 28

$\longrightarrow$ $p = 2, 3$ e finisco coi casi piccoli!

Problema 7. Dimostrare che qualunque sia $n > 0$ intero esiste $m > 0$ intero tc

$$7^n \mid 5^m + 3^m - 1$$

$n=1$ $\quad 7 \mid 5+3-1$ ü.

$n=2$ $\quad 7^2 \mid 5^m + 3^m - 1$?

Vorrei avere uno strumento che mi calcola $V_7(5^m + 3^m - 1)$

$$5 \equiv -2 \qquad 3 \equiv -4 \mod 7$$

$$5^m + 3^m - 1 \equiv -1 + (-2)^m + (-4)^m \mod 7$$
$$= -\phi_3(2^m) \quad \text{quando } m \text{ è disp.}$$

Nope

? Posso sostituire 5^m con $(-2)^m$ mod 7^n??

Ho usato LTE per ottenere delle congruenze ~~prostaferesi~~ esotiche

$$5^m \equiv (-2)^m \mod 7^n$$
$$7^n \mid 5^m - (-2)^m$$

$$n \le v_7\left(5^m-(-2)^m\right) = v_7(7)+v_7(m) = v_7(m)+1$$

$m = 7^{n-1}$

$$5^{7^{n-1}} + 3^{7^{n-1}} - 1 \equiv (-2)^{7^{n-1}} + (-4)^{7^{n-1}} - 1 \mod 7^n$$
$$\equiv -\frac{8^{7^{n-1}}-1}{2^{7^{n-1}}-1} \mod 7^n$$

lui $=0$ FACCIO LTE!

lui $\neq 0$!

per ASSURDO $2^{7^{n-1}} \equiv 1 \mod 7^n$??

$$v_7\left(8^{7^{n-1}}-1\right) = v_7(8-1) + v_7\left(7^{n-1}\right) = n$$

$2^{7^{n-1}} - 1 \not\equiv 0 \mod 7$.

$3 = \mathrm{ord}_7(2) \mid 7^{n-1}$ no

GUADAGNO DI UN PRIMO

p primo DISPARI, x,y interi positivi

$\frac{x^p+y^p}{x+y}$ ha un fattore primo che $(x+y)$ non aveva

ECCETTO IN CASI "PICCOLI" $x=2,\ y=1,\ p=3$; $x=1,\ y=1,\ p$

Meglio

$$(x^p+y^p) = (x+y)\left(\frac{x^p+y^p}{x+y}\right)$$

divide lui

$\exists\ q$ non divide

Dim.

- Scelgo r che divide $x+y$ e uso LTE
$$v_r(x^p+y^p) = v_r(x+y) + v_r(p)$$
- Se $r \neq p$ allora divide entrambi con la stessa molt.

• se $r = p$ allora $v_p(x^p + y^p) = v_p(x+y) + v_p(p)$

• Se, per assurdo, non ce ne fossero altri, allora avrei

$$x^p + y^p = p(x+y)$$ CASO I

(forse c'è un altro caso con $p = 1$) FACILE

cresce MOLTO più in fretta

• $x, y \geq 2$

$\rightarrow x^p \geq px$

$x^p + y^p \geq p(x+y)$

con $=$ solo se $x^p = px$, $y^p = py$

che non succede mai!!

• $y = 1$ WLOG

cresce troppo

$x^p + 1 = p(x+1)$

INDUZIONE

$x^p + 1 > p(x+1)$ se $x \geq 3$

$\longrightarrow$

Problema SNS/2014. $a^7 + b^7 = 7^c$ con $(a,b,c) \in \mathbb{N}_0^3$

$(a+b) \mid a^7 + b^7 = 7^c \implies a+b = 7^m$

$$\left(\frac{a^7+b^7}{a+b}\right)(a+b) = 7^c$$

7^m

ma lui ha un fattore primo $q \neq 7$ per LETTA GUAD. DI PRIM

[P di prima $3^k = x^k + y^k$]

Problema. [BRCO?] $x^5 + 4^y = 2013^z$ (x, y, z) interi pos

$[2013 = 3 \cdot 11 \cdot 61]$

$\frac{10}{(10,5)} = 2 \longrightarrow$ $x^5 + 4^y \equiv 0 \mod 11$

$n \equiv 3 \mod 4$

± 1 $\quad$ 4^y è un $\square$, -1 non è $\square$ mod 4

DEVO AVER $4^y \equiv 1 \mod 11 \leftarrow \mathrm{ord}_{11}(4) = 5$ (per Eulero)

$x^5 \equiv -1 \mod 11$

$y = 5a$

Qui dev'essere piccolo! non può avere fattori 11

Quindi $\frac{2013^z}{11} = \left(x^5 + 4^{5a} \right. = (x+4^a)\left(\frac{x^5+4^{5a}}{x+4^a}\right)$

$3^z \cdot 11^z \cdot 61^z$

sono coprimi!!

$p \mid x + 4^a$

• Se $x + 4^a \equiv 0 \mod 11^z$ allora

MEDIE

$$x^5 + 4^{5a} \geq \left(\frac{x+4^a}{2}\right)^5 \cdot 2$$

$$\geq \left(\frac{11^z}{2}\right)^5 \cdot 2 = 11^{5z} \cdot (2^{-4}) \gg 2013^z$$

• $x + 4^a = 3^z$

$$2013^z = x^5 + 4^{5a} \leq (x+4^a)^5 = 3^{5z} = 243^z$$ ↳ no

PROBLEMI. [IMO 2022/5] $a^p = b! + p$

→ Quasi tutto a dis: QUANTO CRESCONO EXP E !

QUANTO CRESCONO LE LORO v_p

→ $p \leq b < 2p \rightsquigarrow a = p$

$p^p - p = b!$

LTE con v_2

Legendre

PROBLEMI [ISL 2021 / 5] $n! = a^{n-1} + b^{n-1} + c^{n-1}$

ha finite soluzioni

→ dis scema $\frac{n-1}{2} \geq a,b,c$

→ Voglio v_p. Voglio fare LTE.] ← Vedo se riesco a ottenere queste hp

$p \mid a+b$

Serve p dispari!..

$a+b$, $b+c$, $c+a$ sono tutte potenze di 2

→ $v_2 \,\underline{\underline{n}}$

Problema. [IMO 2000] $\exists n$ con esattamente 2000 fattori primi

tc $n \mid 2^n+1$??

trovo $p \mid 2^n+1$ ma che non divide n,

allora $np \mid 2^{np}+1$

DEVO TROVARE IL MODO DI USARE IL

LEMMA DI GUADAGNO DI UN PRIMO