Senior 2013 - N2 medium

Titolo nota 06/09/2013

"Lemma del guadagno di un primo" LGP

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

$f(n)$ $\qquad m^p \equiv 1 \pmod q$

$$\Updownarrow$$

$$q \mid f(m)(m-1)$$

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

$f(n)$ ha come divisori primi solo $\begin{cases} p \\ q \equiv 1 \pmod p. \end{cases}$

$f(1) = p$ può capitare

$$q \mid f(n) \Rightarrow q \mid n^p - 1 \Rightarrow n^p \equiv 1 \pmod q$$

$\mathrm{ord}_q n$ $\begin{cases} 1 \to n \equiv 1 \bmod q \to f(1) = p \text{ e simili, } p=q \\ p \quad \text{ma } \mathrm{ord}_q n \mid \varphi(q) = q-1 \end{cases}$

$$\Rightarrow p \mid q-1 \Rightarrow q \equiv 1 \pmod p$$

e $q^2 \mid f(n)$? $\qquad q=p$ no

$n \equiv 1 \pmod p \qquad n = kp+1$

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

$$= \big(\overbrace{1+1+\cdots+1}^{p}\big) + k\,(1+2+3+\cdots+p-1)\,p + Np^2 =$$

$$= p + kp\cdot p\,\frac{p-1}{2} + Np^2 = p + \Big(k\,\underset{\text{se } p>2}{\frac{p-1}{2}} + N\Big)p^2 \equiv$$

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

$q \equiv 1 \mod p$? Era necessario prima, quindi anche adesso.

$\exists$ el. di ordine $p \pmod q$ $[q \equiv 1 \pmod p]$?

prendo g generatore mod q

$g^{q-1} \equiv 1 \pmod q$ $\quad g^k \not\equiv 1 \pmod q$ $0<k<p-1$

$p \mid q-1$ $\quad \underbrace{g^{\frac{q-1}{p}}}_{a} \not\equiv 1$ $\quad \frac{q-1}{p} < q-1$

$a^p \equiv g^{q-1} \equiv 1$ $\quad$ quanti sono questi elementi

x che mod q fanno $x^p \equiv 1 \pmod q$?

$g^{\frac{q-1}{p}} = a_1$ $\quad (p>2)$ $\left[g^{\left(\frac{q-1}{p}\right)}\right]^2 \equiv g^{2\frac{q-1}{p}} \equiv a^2$

$(a_1^2)^p \equiv (a_1^p)^2 \equiv 1 \pmod q$ $\quad a_1^i$ $\quad i = 1, \dots, p-1$

Come risolvendo $p \cdot x \equiv 0 \pmod{q-1}$

$(g^x)^p \equiv g^{xp} \equiv g^{(q-1)k'} \equiv 1$ $\quad x = k\,\frac{q-1}{p}$ $\quad k = 0, \dots, p-1$ No

E se volessi a_2 t.c. $a_2^p - 1 \equiv 0 \pmod{q^2}$?

$(\mathbb{Z}/q^2\mathbb{Z})^*$ ha un generatore ($\to$ un sistema di generatori fatto da 1 solo elemento)

g_2 sia il generatore. $(g_2^x)^p \equiv 1 \pmod{q^2}$

$$g_2^{\frac{q(q-1)}{p}} \equiv a_2 \not\equiv 1 \quad a_2^p \equiv 1 \pmod{q^2}$$

$$g_2^k \not\equiv 1 \quad k < q(q-1) = \varphi(q^2).$$

Così per trovare a_k t.c. $a_k^p \equiv 1 \pmod{q^k}$

LGP

x intero

$x^p - 1 = (x-1)f(x)$ Allora $\exists$ un divisore primo di $f(x)$ che non divide $x-1$ a meno che non sia $3^2 - 1 = (3-1)(3+1)$.

Dim. $q \mid f(x)$ $\qquad q \equiv 1 \bmod p \quad$ o $\quad q = p$

e $q \mid x-1$ $\qquad x \equiv 1 \pmod q$

$$q \mid f(x) \equiv 1 + (1+kq) + \ldots \qquad (1+kq)^{p-1} \equiv p$$

$q = p \qquad (x-1) f(x) \qquad (x-1) = p^a$

$f(x) = p^b$

$$p \mid f(x) \Rightarrow f(x) \equiv p \pmod{p^2} \Rightarrow f(x) = p \quad b = 1$$

$(x-1) = p^a \quad f(x) = p$

$p = 2 \to (3-1)(3+1)$

$p \neq 2 \quad a = 0$ ass.

Conclusione: da $x-1$ a x^p-1 si "guadagna" almeno un nuovo divisore primo.

Polinomi a coeffi interi visti in $\mathbb{Z}/p\mathbb{Z}$.

① $f(x)$ non può assumere solo valori primi.

$f(0)=0$ no $\quad f(0) = p \quad f(p) = p \cdot g(p)$
composto
$g \neq 1$

② $S = \{ p_i \text{ primi} \mid \exists n \ \ p_i \mid f(n) \}$ deve essere infinito

$f(0)=0 \quad f(x) = x \cdot g(x) \quad x = p_i$

$f(0) = 1$ Se $\bar{p} = \max S \quad f(\bar{p}!) = N \cdot \prod_{p_i \in S} p_i + 1$

$\Rightarrow p_i \nmid f(\bar{p}!)$ per nessun i

$f(0) = a \qquad f(ax) = c_n a^n x^n + c_{n-1} a^{n-1} x^{n-1} + \dots + c_1 a x + a =$

$= a \cdot g(x) \qquad g(0) = 1$ e mi riduco al caso precedente

③ $\forall f(x)$ polinomio $\exists$ infiniti p primi t.c.

$f(x)$ in $\mathbb{Z}/p\mathbb{Z}$ ha una radice.

$\exists \infty \, p$ t.c. $\exists n \quad p \mid f(n) \iff f(\bar{n}) \equiv 0 \pmod p$

Oss. pol. ciclotomico di grado $n \overset{\Phi_n(x)}{=}$ pol.

che ha come radici tutte le radici primitive

n-esime dell'unità $\lambda^n = 1 \quad \lambda^k \neq 1 \quad k < n$

$\Phi_n(x)$ ha coeff. interi (non sempre 0 e 1)

$$x^p - 1 = (x-1)\,\Phi_p(x)$$

$$x^n - 1 = \Phi_n(x) \cdot \Phi_{d_1}(x)\, \Phi_{d_2}(x) \cdots \underset{\underset{x-1}{\parallel}}{\Phi_1(x)} = \prod_{d \mid n} \Phi_d(x)$$

Equazioni diofantee di secondo grado in due variabili

$$ax^2 + bx + c \equiv 0 \pmod p$$

1 var.: $x^2 \equiv a$ — a res. quadr. risolubile; a non lo è, no.

Δ — è res. quadr. risolubile; non lo è, no.

$$ax^2 + bxy + cy^2 + dx + ey + f$$

$$x^2 + ay^2 = f$$

- $a > 0$ — # fin. di soluzioni se ci sono
- $a = -b^2$ — $(x-by)(x+by) = f$

  Fattorizzo $f = f_1 \cdot f_2$ e faccio molti conti facili
- $a < 0$ — $-a$ non quadrato ?

$x^2 - 2y^2 = 1$ è antica $\qquad x^2 - ay^2 = b$

1. $b := 1 \qquad \lambda \in \mathbb{C}$ t.c. $\lambda^2 = -a$

$$x^2 + \lambda^2 y^2 = b \qquad x^2 + \lambda^2 y^2 = \|(x, \lambda y)\|^2.$$

$$\mathbb{Z}[\sqrt{-a}] = \mathbb{Z}[\lambda]$$

Caso paradigmatico $\lambda = i$

$$x^2 - y^2 = b \qquad x^2 + y^2 = b$$

$$\shortparallel$$

$$(x + iy)(x - iy) = b$$

$\mathbb{Z}[i]$ = interi di Gauss. Ma come funziona la fattorizzazione negli interi di Gauss?

(Devo fattorizzare anche b in $\mathbb{Z}[i]$)

$$2 = (1+i)(1-i)$$

2 non è irriducibile

$\doteqdot$ non si può scriverlo come $a \cdot b$ a meno che a o b non siano invertibili (in $\mathbb{Z}$, ± 1)

Invertibili in $\mathbb{Z}[i]$?

2 non è primo

$\doteqdot \quad 2 \mid a \cdot b \Rightarrow 2 \mid a$ o $2 \mid b$

primo $\Rightarrow$ irriducibile:

WLOG

$p = a \cdot b \Rightarrow p \mid a \cdot b \Rightarrow p \mid a \Rightarrow a = k \cdot p \Rightarrow p = k \cdot p \cdot b$

$\Rightarrow k \cdot b = 1 \Rightarrow b$ invertibile

$\cancel{\Leftarrow}$ non sempre vero

Fatt. in $\mathbb{Z}$
1) dividendo, numero diminuisce
2) unicità a meno dell'ordine

$N(a+ib) = a^2+b^2 \in \mathbb{Z}_+$ $\quad N((a+ib)(c+id)) = N(a+ib)N(c+id)$

Se $a+ib$ è invertibile? Sia $c+id$ l'inverso.

$N(a+ib)N(c+id) = N(1) = 1 \Rightarrow N(a+ib) = 1.$

Invertibili: $1, -1, i, -i$

$N(a+ib) = p$ e fattorizzassi $(a+ib) =$
$= z_1 \cdot z_2$

$p = N(z_1) \cdot N(z_2)$
$\Rightarrow$ o $N(z_1)=1$ o $N(z_2)=1 \Rightarrow$ o z_1 o z_2 è invert.
$\Rightarrow a+ib$ irriducibile. (= primo in $\mathbb{Z}[i]$)

$a+ib \in \mathbb{Z}$ $\quad b=0$ $\quad$ a non primo $\to$ niente
$a=2 \to$ non primo $\quad -i(1+i)=(1-i)$
$a=p$? $\quad$ Se $p = z_1 \cdot z_2$

$N(p) = N(z_1) \cdot N(z_2)$

$p^2 = N(z_1) \cdot N(z_2)$
- $N(z_1)=1 \quad p$
- $N(z_2)=1 \quad p$
- $N(z_1)=p \quad N(z_2)=p$

NON È FATTORIZZ.

$N(z_1)=p \quad p = a^2+b^2 \quad (a+ib)(a-ib)$

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

$\Leftrightarrow \left(\frac{-1}{p}\right)=1$ Ma $\mathbb{Z}/_{p\mathbb{Z}}^{*}$ ha $p-1$ elem. e un gen. g

$$g^k \equiv -1 \Longleftrightarrow g^{2k}\equiv 1 \quad g^k \not\equiv 1$$

Voglio k pari $\Longleftrightarrow 4 \mid p-1 \Rightarrow p\equiv 1 \pmod 4$

Se ora $\exists\ a$ $\quad a^2\equiv -1 \pmod p \qquad a^2+1\equiv 0 \pmod p$

$$(ka)^2+k^2 \equiv 0 \pmod p \quad \forall k$$

Tutti i $p\equiv 1 \pmod 4$ sono somme di due quadrati $\Rightarrow$ non sono primi in $\mathbb{Z}[i]$. Viceversa, $p\equiv 3 \pmod 4$ sono ancora primi. (Così, sono primi $1+i$ e $1-i$).

Fattorizzando, la norma diminuisce $\Rightarrow$ # finito di fattori.

2) Unicità? $\qquad \mathbb{Z}[\sqrt{-5}]$

$$6=2\cdot 3=(1-\sqrt{-5})(1+\sqrt{-5})$$

$$e\ 3, 2 \neq (1-\sqrt{-5})\cdot \text{invertibile}$$

Ma in $\mathbb{Z}[i]$ la fattorizzazione è unica

$\mathbb{Z}[\sqrt{-1}]$ (anche $\sqrt{-2}, \sqrt{-3}, \ - \ --- \ \sqrt{-163}$)
9 casi

$x^2+y^2=b \qquad b=2^a\cdot \underbrace{p_1^{k_1}\cdots p_e^{k_e}}_{\equiv 1 \pmod 4}\ \underbrace{q_1^{h_1}\cdots q_n^{h_n}}_{\equiv 3 \pmod 4}$

$$(x+iy)(x-iy)=(-i)^a(1+i)^{2a}\prod (c_j+id_j)^{k_j}(c_j-id_j)^{k_j}\cdot\prod q_j^{h_j}=$$

$$=(A+iB)(C+iD)$$

in tutti i modi possibili (inclusi gli invertibili) e con MOLTI conti e sistemi trovo tutte le soluzioni

$x^2 - d y^2 = b \quad d > 0$ $\qquad \mathbb{Z}[\sqrt{-d}]$

$\sqrt{-d} = \lambda \qquad x^2 + \lambda^2 y^2$

$a + \sqrt{-d}\, b \qquad a^2 + d b^2 \qquad a^2 - d b^2\ ?$

$x^2 - d y^2 = 1 \qquad N(z_1 \cdot z_2) = N(z_1) N(z_2)$

$(a + \sqrt{-d}\, b)(m + \sqrt{-d}\, n) =$

$(am - d bn) + \sqrt{-d}(an + bm)$

$a^2m^2 - 2\cancel{d}abmn + d^2b^2n^2 + (da^2n^2 + 2\cancel{d}\,\cancel{an}bm + db^2m^2) = (am - d\, bn)^2 \pm d(an + bm)^2 \stackrel{?}{=}$

$\stackrel{?}{=} (a^2 \pm d b^2)(m^2 \pm d n^2)$

$\| $

$a^2m^2 \pm a^2 d n^2 \pm d b^2 m^2 + d^2 b^2 n^2$

$x^2 - d y^2 = 1 \qquad x^4 - 2d\cancel{y^2x^2} + d^2 y^4 = 1$

$m^2 - d n^2 = 1$

$x^2m^2 + d^2n^2y^2 - dm^2y^2 - dn^2x^2 = 1$

$a^2 - db^2\ ?$ $\qquad \|$

$(x^2m^2 \pm 2d\, xymn + d^2n^2y^2) - d(m^2y^2 \mp 2xymn + n^2x^2)$

$\|$

sol. $\quad (xm \pm dny)^2 - d(my \mp nx)^2$

$(x, y) \to (x + \sqrt{-d}\, y) \quad (m + \sqrt{-d}\, n)$

$x \pm \sqrt{-d}\, y$

$(x, y) \to (x + \sqrt{-d}\, y)^k \to (x', y')$ che è ancora soluz.

$$x^2 - dy^2 = a$$
$$m^2 - dn^2 = b \longrightarrow (xm \pm dny)^2 - d(my \mp nx)^2 = ab.$$

$$(x, y, a) \ (m, n, 1) \longmapsto (x', y', a)$$

Trovo così ∞ soluzioni, (tante quante quelle con 1) ma ATTENZIONE ci possono essere più famiglie infinite.

$$x^2 - dy^2 = 1 \qquad a^2 - db^2 = k \qquad (m, 1, m^2 - d)$$

$$am + db, \ a + bm, \ k(m^2 - d)$$

Se $am+db$ e $a+bm$ sono multipli di k,

$$\left(\frac{am+db}{k}, \frac{a+bm}{k}, \frac{m^2-d}{k}\right)$$

Cerco m $\begin{cases} am + db \equiv a + bm \equiv 0 \pmod{k} \\ \dfrac{m^2-d}{k} \text{ "piccolo".} \end{cases}$

Se $\dfrac{m^2-d}{k} \neq 1$, lo rifaccio: Teo arrivo sempre.

Minimizzando la $N(z)$, le soluzioni di

$x^2 - dy^2 = 1$ sono potenze di una fondamentale.

Dopo ne trovo una particolare di

$x^2 - dy^2 = b$ e moltiplico.

Spesso è utile "stringere tra due quadrati"

Se $f: \mathbb{N} \to \mathbb{N}$ e $\forall m,n$ $nf(n) + 2nm + mf(m)$ è un quadrato

Allora $f(n) = n$.

Dim [$f(n) = n$ va bene ow.]

$a = p$ (primo) $b = 0$ $\qquad pf(p)$ è quadrato

$$\Rightarrow p \mid f(p) \qquad f(p) = p \cdot g^2(p)$$

$p, 1 \qquad pf(p) + 2p + f(1) = a^2$

$p, 2 \qquad pf(p) + 4p + 2f(2) = b^2 \qquad a \neq b$

$$2p + 2f(2) - f(1) = b^2 - a^2 \geq 2a + 1 > 2\sqrt{2}p + 1$$

se $f(p) \neq p$ $\quad f(p) \geq 2p \qquad a, b \geq \sqrt{2} \cdot p$

per infiniti p!

$p > 100^{100} \dfrac{2f(2) - f(1)}{\sqrt{2}}$ assurdo.

$$2p + K > 2\sqrt{2}p + 1$$

"Più piccolo primo" $\qquad n = p_1^{a_1} \cdots p_k^{a_k}$

prendo il p_i più piccolo.

IMO 1990/3

Quando $\dfrac{2^n + 1}{n^2}$ è intero? $\qquad n$ dispari

$2^n \equiv -1 \pmod{n}$ $\qquad 2^{2n} \equiv 1 \mod n$

$\mathrm{ord}_n(2) \mid 2n$ $\qquad$ n primo $= p$

$$\mathrm{ord}_p(2) \mid (2p, p-1) \begin{cases} 1 \\ 2 \end{cases}$$

$p = 3$ $\qquad \dfrac{2^3+1}{3^2} = 1 \qquad \dfrac{2^1+1}{1} = 3$

$n = 3^k \cdot m \qquad 2^{3^k m} \equiv -1 \quad (3^{2k} m^2)$

quando $3^a \parallel 2^{3^k m} + 1$? $= (2^{3^{k-1}m}+1)\underbrace{(2^{2\cdot 3^{k-1}m} - 2^{3^{k-1}m} + 1)}_{1 \text{ solo } 3}$

$a = k+1$ per induzione

$\Rightarrow$ le uniche sol. sono $k = 0, 1$

Tra gli altri, prendo il minimo primo p_i a parte 3

$\mathrm{ord}_{p_i}(2) \mid (2p_i, p_i - 1)$

$\Rightarrow$ solo poche scelte: $2^1-1 \quad 2^2-1 \quad 2^3-1 \quad 2^6-1$

$1 \quad 3 \quad 7 \quad 63$

$7 \cdot 9$

ma modulo 7 non funziona

$\Rightarrow$ solo 3.

Teorema di Chevalley

"Vieta jumping" $\qquad$ IMO 1988/6 $\quad \dfrac{a^2+b^2}{1+ab}$ se è intero è quadr.