N2 MEDIUM

Titolo nota

- ESTENSIONI QUADRATICHE
- INTERI DI GAUSS (SOMME DI QUADRATI)
- APPROSSIMAZ. DIOFANTEE,
- EQ. DI PELL
- SIMBOLI DI LEGENDRE
- RECIPROCITÀ QUADRATICA

ANELLI

ins. A con somma e prodotto $\rightarrow$ prop. comm. (+, ×) distrib.

es. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C},$

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

$\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

INTERI GAUSSIANI

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

$\alpha = a + bi \rightarrow \bar{\alpha} := a - bi$

$N(\alpha) = \alpha \cdot \bar{\alpha} = (a+bi)(a-bi) = a^2 + b^2 = |\alpha|^2$

$\searrow$ NORMA $\quad N : \mathbb{Z}[i] \rightarrow \mathbb{N}$

MOLTIPLICATIVA $\rightarrow N(\alpha)N(\beta) = \alpha\bar{\alpha}\beta\bar{\beta} = (\alpha\beta)(\overline{\alpha\beta}) = N(\alpha\beta)$

$\mathbb{Z}[i]$ è un dominio a fattorizz. unica, cioè
- esistono i numeri primi (p è primo se $p \neq ab$, $N(a), N(b) > 1$)
- ogni α si può scrivere in modo "unico" come prodotto di primi

$\alpha = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$p \mid ab \Rightarrow p \mid a \vee p \mid b$

$5 = (1+2i)(1-2i) = (2+i)(2-i)$

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

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

in $\mathbb{Z}$:
$-15 = (-3)5 = (-5)\cdot 3$

a meno di fattori invertibili ($N(u)=1$) a, b associati $\iff a = u \cdot b \iff b = u^{-1} \cdot a$

$N(u) = 1 \longrightarrow u \in \mathbb{Z}[i]$

$u \cdot \bar{u} = 1 \to \bar{u} = u^{-1}$

Vogliamo vedere quali primi in $\mathbb{Z}$ lo sono anche in $\mathbb{Z}[i]$

$p = \alpha\bar{\alpha}$ se p non è primo in $\mathbb{Z}[i]$

$p = \alpha\beta \to p^2 = N(p) = N(\alpha)N(\beta)$

$\to N(\alpha) = N(\beta) = p \to \alpha = \bar{\beta}$

vogliamo cercare

$\to p = (a+ib)(a-ib) = a^2 + b^2$

Thm (Fermat): $p = a^2 + b^2 \iff p = 2 \vee p \equiv 1 \pmod 4$

DIM $p = 2 = 1^2 + 1^2$

$p > 2$

$(\Rightarrow)$ $p \nmid a, b$, altrimenti $p^2 \mid a^2 + b^2 = p$ ↯

$\rightarrow a^2 + b^2 \equiv 0 \pmod p$

$(a/b)^2 \equiv -1 \ (p)$

$(a/b)^4 \equiv 1 \ (p)$

$\rightarrow$ Fermat

$\rightarrow 4 = \mathrm{ord}_p(a \cdot b^{-1}) \mid p-1$

$4 \mid p-1 \rightarrow p \equiv 1 (4)$

$(\Leftarrow)$ Lemma di Thue

Dato $s \not\equiv 0 (p)$ primo allora $\exists (x,y)$ t.c.

$0 < |x|, |y| < \sqrt{p}$ $\wedge$ $x \equiv sy \pmod p$

DIM: Consideriamo $x \equiv -sy \pmod p$

per $0 \le x \le \lfloor \sqrt{p} \rfloor$ $\quad \lfloor \sqrt{p} \rfloor^2 \le p < (\lfloor \sqrt{p} \rfloor + 1)^2$

$(\lfloor \sqrt{p} \rfloor + 1)^2 > p$

$\rightarrow$ per Pigeonhole, $\exists (x_1, y_1) \neq (x_2, y_2)$ t.c.

$x_1 - s y_1 \equiv x_2 - s y_2$

$\rightarrow (x_1 - x_2) \equiv s (y_1 - y_2)$

x $\qquad$ y

$0 \le |x_1 - x_2| \le \lfloor \sqrt{p} \rfloor$ $\quad 0 \le |y_1 - y_2| \le \lfloor \sqrt{p} \rfloor$

↳ se avessimo $x_1 \equiv x_2 \Rightarrow y_1 \equiv y_2$ ma

Torniamo al problema

$\exists s \quad s^2 + 1 \equiv 0 \ (p)$

se $p \equiv 1 (4)$, allora $s = \left(\frac{p-1}{2}\right)!$ funziona

$p = 4k+1$

$$\left(\frac{p-1}{2}\right)!^2 \underset{p}{\equiv} 1 \cdot \ldots \cdot \left(\frac{p-1}{2}\right) \cdot -(p-1) \cdot -(p-2) \cdot \ldots \cdot -\left(p - \frac{p-1}{2}\right)$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (p-1)! \equiv (-1)^{\frac{p-1}{2}} \cdot (-1)$$

$$\equiv (-1)^{\frac{p+1}{2}} \equiv (-1)^{2k+1} \equiv -1 \ (\mathrm{mod}\, p)$$

[N.B. se g gen. mod p, anche $s = g^{\frac{p-1}{4}}$ $s^2 \equiv g^{\frac{p-1}{2}} \equiv -1$]

→ ora applichiamo Thue a ciò che è stato

$\exists x, y, \ 0 < |x|, |y| \leq \lfloor \sqrt{p} \rfloor$ t.c.

$$x/y \equiv s \ (p) \rightarrow x^2/y^2 \equiv s^2 \equiv -1$$

$$\rightarrow x^2 \equiv -y^2 \rightarrow x^2 + y^2 \equiv 0 (p)$$

$$0 < x^2 + y^2 \leq \lfloor \sqrt{p} \rfloor^2 + \lfloor \sqrt{p} \rfloor^2 \leq \sqrt{p}^2 + \sqrt{p}^2 = 2p$$

$$p \mid x^2 + y^2 \ \wedge \ 0 < x^2 + y^2 < 2p$$

→ $x^2 + y^2$ dev'essere esattamente p

$$p = x^2 + y^2$$

Possiamo dimostrare che questa scrittura è unica [a meno di permutazioni / negativi, es. $5 = 2^2+1^2 = (-1)^2+2^2$]

$$p = x^2+y^2 = z^2+w^2 \quad (\text{WLOG } x>y>0,\ z>w>0)$$

$$(x+iy)(x-iy) \quad (z+iw)(z-iw)$$

$N(\ ) = p$ — primi

$\to$ fatt. unica $\to$ $x+iy = u\cdot(z\pm iw)$, $u \in \{\pm 1, \pm i\}$

$\to$ $x+iy = z+iw$ $\vee$ $x+iy = i(z-iw)$

$= w+iz \to (x,y) = (w,z)$

In generale possiamo vedere per quali M esistono x, y t.c. $M = x^2+y^2$

$M_1 = x^2+y^2$ $M_2 = z^2+w^2$

$$M_1 \cdot M_2 = N(x+iy)N(z+iw) = N\big((xz-yw)+i(yz+xw)\big) =$$
$$= (xz-yw)^2+(yz+xw)^2$$

$\to$ ci interessano solo i fatt. primi di M

$\to$ se possiamo generare i primi della scomposizione, allora possiamo generare anche il loro prodotto

Se $q \mid M$ t.c. $q \equiv 3 \pmod 4$ cosa succede?

$x^2+y^2 = M \equiv 0 \pmod q$ se x, y sono coprimi con q allora $4 \mid q-1$

$\rightarrow x \equiv y \equiv 0 \ (q) \rightarrow \underline{q^2 \mid x^2+y^2 = M}$

$\rightarrow q^2 \mid M \qquad M' = M/q^2 = (x/q)^2 + (y/q)^2$

$v_q(M) = 2k \rightarrow M/q^{2k} = (x')^2 + (y')^2 \rightarrow x = q^k x' \quad y = q^k y'$

$v_q(M) = 2k+1 \rightarrow M/q^{2k} = (x')^2 + (y')^2$

$\max\{t : q^t \mid M\}$

$M = M/q^{2k}$ poss. $\downarrow$ $q \mid M'$, ma $q^2 \nmid M'$ $\forall$

$q^{2k} = (q^k)^2 + 0^2$

$\rightarrow$ Conclusione: M è somma di quadrati se i suoi primi che lo dividono $\equiv 3 \ (4)$ sono contenuti un numero pari di volte in M

es: $3 \cdot 5^2$ NO

$2 \cdot 3^2 \cdot 7^2 \cdot 11^1 \cdot 31^2$ NO

$2 \cdot \underline{3}^2 \cdot \underline{7}^2 \cdot \underline{3}1^2$ SI

ES: $p = x^2 + xy + y^2$ se $p = 3 \vee p \equiv 1 \ (3)$

$(\Rightarrow)$ $p \mid x, y$ (altrimenti $p \nmid x^2 + xy + y^2 = p$)

$\left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right) + 1 \equiv 0$

se fosse $1 \rightarrow \frac{x}{y} \equiv 1 \rightarrow x \equiv y$ $\rightarrow p \equiv 3x^2 \ (p) \rightarrow p = 3$

$\left(\frac{x}{y}\right)^3 - 1 \equiv 0 \ (p) \rightarrow \text{ord}_p\left(\frac{x}{y}\right) = 3 \mid p-1$

$\rightarrow 3 \mid p-1 \rightarrow p \equiv 1 \ (3)$

($\Leftarrow$) $\exists s \quad s^2+s+1 \equiv 0 \pmod p$ se $p \equiv 1 \pmod 3$

se $g = \text{gen. mod } p$

$$s \equiv g^{\frac{p-1}{3}}$$

$$\to s^2+s+1 \equiv g^{2\frac{p-1}{3}} + g^{\frac{p-1}{3}} + 1 \equiv \frac{g^{3\frac{p-1}{3}} - 1}{g^{\frac{p-1}{3}} - 1} \equiv 0 \pmod p$$

$$\hookrightarrow \not\equiv 0 \pmod p$$

$\to$ Usiamo Thue

$\to \exists x, y \quad 0 < |x|, |y| \le \lfloor \sqrt{p} \rfloor < \sqrt{p}$ t.c. $\frac{x}{y} \equiv s \pmod p$

$\to \left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right) + 1 \equiv 0 \pmod p \to x^2+xy+y^2 \equiv 0 \pmod p$

$0 < x^2+xy+y^2 < \sqrt{p}^2 + \sqrt{p}\cdot\sqrt{p} + \sqrt{p}^2 = 3p$

$\to x^2+xy+y^2 \in \{p, 2p\}$

$\to$ se $x^2+xy+y^2 = 2p \to 2 \mid x, y$

$\to 2^2 \mid x^2+xy+y^2 = 2p$

$\to p = 2$, ma $p \equiv 1 \pmod 3$

$\to x^2+xy+y^2$ deve essere esattamente p

[NOTA x^2+xy+y^2 è la norma di $x+y\omega$ in $\mathbb{Z}[\omega]$, dove $\omega = \frac{-1+\sqrt{3}i}{2}$, una rad. 3 dell'unità, infatti $(x+y\omega)(x+y\bar{\omega}) = \dots = x^2+xy+y^2$]

APPROSSIMAZIONE DIOFANTEA

Successioni di Farey

$\mathcal{F}_n$ $\frac{h}{k}$ con $(k,h)=1$, $0 \le h \le k \le n$

$\mathcal{F}_1 = \frac{0}{1}, \frac{1}{1}$ $\mathcal{F}_2 = \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$ $\mathcal{F}_3 = \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$

1) $\forall n$ $\mathcal{F}_n$ abbiamo $\frac{h}{k}, \frac{h'}{k'}$ consecutivi $kh'-hk'=1$

2) $\frac{h}{k}, \frac{h'}{k'}, \frac{h''}{k''}$ cons., allora $\frac{h'}{k'} = \frac{h+h''}{k+k''}$

⇓

3) $k+k'>n$: se $k+k' \le n$ $\frac{h+h'}{k+k'} \in \mathcal{F}_n$ (ai minimi termini), sta tra $\frac{h}{k}$ e $\frac{h'}{k'}$ ↯.

4) $k \neq k'$: $\frac{h}{k} < \left(\frac{h}{k-1}\right) < \frac{h+1}{k} \le \frac{h'}{k}$ √

Successioni di Beatty

$x>0$, $B_x = \{\lfloor nx \rfloor \mid n \in \mathbb{N}^+\}$, $r,s>1$

$\frac{1}{r}+\frac{1}{s}=1$ e $r,s \in \mathbb{R}\setminus\mathbb{Q}$ ⇔ B_r e B_s partizionano $\mathbb{N}^+$

⇒: Consideriamo la successione dei $\frac{k}{r}$ e $\frac{k}{s}$ con $k \in \mathbb{N}^+$ messi in ordine crescente:

- $\frac{k}{r} \neq \frac{j}{s}$: per assurdo $\frac{s}{r} = \frac{j}{k} \in \mathbb{Q}$ (ma $\frac{s}{r} = s-1 \notin \mathbb{Q}$) ↯
- $\frac{k}{r}$ è preceduto da k termini $\frac{j}{r}$ e da $\lfloor \frac{ks}{r} \rfloor$ termini $\frac{j}{s}$ ($\frac{j}{s} < \frac{k}{r} \Leftrightarrow j < \frac{ks}{r} \Leftrightarrow j \le \lfloor \frac{ks}{r} \rfloor$), la posizione di $\frac{k}{r}$ è la $k + \lfloor \frac{ks}{r} \rfloor = k + \lfloor k(s-1) \rfloor = \lfloor ks \rfloor$
- analogamente $\frac{k}{s}$ è in posizione $\lfloor kr \rfloor$

Lemma di Dirichlet: $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, $n \in \mathbb{N}^+$ allora
$\exists p,q \in \mathbb{Z}$ con $q \in \{1,\dots,n\}$ tali che $|\alpha - \frac{p}{q}| < \frac{1}{(n+1)q}$:

$0, \{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}, 1$ stanno in $[0,1]$ e sono $n+2$, quindi

$\exists k,l \mid 1 \le k,l \le n$, $k > l$ tale che $|\{k\alpha\} - \{l\alpha\}| < \frac{1}{n+1}$ (a parte casi con 0 e 1)

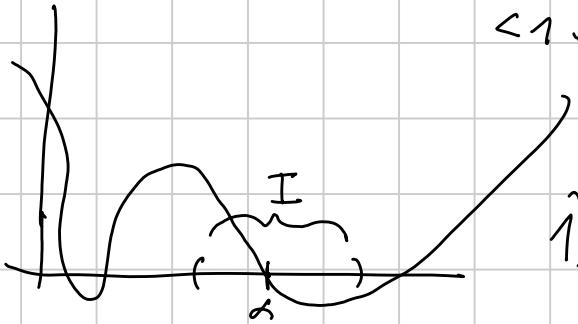
poniamo $q = k - l$ $\quad |k\alpha - \lfloor k\alpha \rfloor - l\alpha + \lfloor l\alpha \rfloor| < \frac{1}{n+1}$

$$\left|\alpha - \frac{\lfloor k\alpha \rfloor - \lfloor l\alpha \rfloor}{k-l}\right| < \frac{1}{(n+1)(k-l)}$$

Dirichlet pt. 2: $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ $\exists \infty$ (p,q) tali che $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$

Teorema di Liouville: α algebrico di grado n (ovvero $\exists p \in \mathbb{Z}[x]$ con $\deg(p) = n \mid p(\alpha) = 0$), allora $\exists K > 0$ tale che $\forall p,q \in \mathbb{Z}$

$|\alpha - \frac{p}{q}| > \frac{K}{q^n}$: $P \in \mathbb{Z}[x]$, consideriamo I (chiusa) centrato in α di raggio < 1 e in cui non ci sono altre radici di P.



Fissiamo $p,q \in \mathbb{Z}$ tali $\frac{p}{q} \in I$;

1) Scegliamo $M > 0 \mid |P'(x)| < M \ \forall x \in I$

2) $\left|P\left(\frac{p}{q}\right)\right| \ge \frac{1}{q^n}$; $P(x) = a_n x^n + \dots + a_0$, $P\left(\frac{p}{q}\right) = \frac{a_n p^n + \dots + \dots + a_0 q^n}{q^n}$ ($\neq 0$)

$\Rightarrow \left|P\left(\frac{p}{q}\right)\right| \ge \frac{1}{q^n}$

3) intervallo da $\frac{p}{q}$ a α, allora $\exists c$ in esso tale che

$$P\left(\frac{p}{q}\right) - 0 = \left(\frac{p}{q} - \alpha\right) f'(c) \Rightarrow \frac{\left|P\left(\frac{p}{q}\right)\right|}{|f'(c)|} = \left|\frac{p}{q} - \alpha\right| \Rightarrow \left|\frac{p}{q} - \alpha\right| > \frac{1}{Mq^n} \quad \left(\frac{1}{M} = K\right)$$

P1.1: $k_1, \dots, k_n \in \mathbb{N}$ maggiori di 1 definitivamente crescente, allora

$S := \sum_{j=1}^{\infty} \prod_{i=1}^{j} \frac{1}{k_i} \in \mathbb{Q} \Leftrightarrow \{k_n\}_{n \in \mathbb{N}}$ è definitivamente costante

Lemmino: $\frac{a}{b} \in \mathbb{Q}$ allora $\left|p\frac{a}{b} - q\right| < \frac{1}{b} \Rightarrow |\sim| = 0$!

$\Leftarrow$ è chiara per $\sum_{n=1}^{\infty} x^n = \frac{x}{1-x}$

$\Rightarrow$:

$$S\prod_{i=1}^{n} K_i = \underbrace{\sim}_{\text{in } \mathbb{Z}} + \overbrace{\frac{1}{K_{n+1}} + \frac{1}{K_{n+1}K_{n+2}} + \dots}^{0}$$

$$\leq \sum_{i=1}^{\infty} \frac{1}{(K_{n+1})^i} = \frac{1}{K_{n+1} - 1}$$ ← questa parte frazionaria tende a 0.

BMO 4/2015: Ogni 20 interi positivi consecutivi $\exists d$ tale che $n\sqrt{d}\{n\sqrt{d}\} > \frac{5}{2}$ $\forall n \in \mathbb{N}^+$;

pongo $m = \lfloor n\sqrt{d} \rfloor \Rightarrow \underbrace{2n\sqrt{d}(n\sqrt{d} - m)}_{(*)} > 5$

speriamo di trovare $(n\sqrt{d}+m)(n\sqrt{d}-m) > 5 \Leftrightarrow dn^2 - m^2 > 5$

sappiamo che $dn^2 - m^2 \geq 0$

Dobbiamo escludere $dn^2 - m^2 = 0, 1, 2, 3, 4, 5$

$d \equiv 3$ (4) (ad esempio $dn^2 - m^2 = 1 \Rightarrow -n^2 - m^2 \equiv 1$ (4) $\Leftrightarrow n^2 + m^2 \equiv 3$ (4), assurdo)

$d \equiv 0$ (5) (ad esempio $dn^2 - m^2 = 2, 3 \Rightarrow m^2 \equiv 3, 2$ (5), assurdo)

$d \neq \square$ perché $d \equiv -1$ (4)

Per sistemare s notare che (*) a LHS c'è un irrazionale.

EQUAZIONI DI PELL

$x^2 - dy^2 = 1$ con $d \neq \square$ e cerchia $x, y \in \mathbb{Z}$

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

$N(a+b\sqrt{d}) = a^2 - db^2 = (a+b\sqrt{d})(a-b\sqrt{d}) = (a+b\sqrt{d})\overline{(a+b\sqrt{d})}$

$N(a)N(b) = N(ab)$!

$N\left(\frac{1}{a}\right) = \frac{1}{N(a)}$ per a invertibile $\left(a \cdot \frac{1}{a} = 1\right)$

$z \in \mathbb{Z}[\sqrt{d}] \Rightarrow \frac{1}{z} \in \mathbb{Q}[\sqrt{d}]$ perché $a + b\sqrt{d} = \frac{a^2 - db^2}{a - b\sqrt{d}}$

se $\frac{1}{2} \in \mathbb{Z}[\sqrt{d}]$ $N(\frac{1}{2}) \in \mathbb{Z} \Rightarrow N(z) = \pm 1$, e $N(z) = \pm 1$ è sufficiente per $\frac{1}{z} \in \mathbb{Z}[\sqrt{d}]$ perché in tale caso abbiamo $a - b\sqrt{d} = \frac{1}{a+b\sqrt{d}} = \frac{1}{z}$.

invertibile $\Leftrightarrow N(z) = \pm 1$

$N(a + b\sqrt{d}) = 1 \Leftrightarrow a^2 - b^2 d = 1$ (cerco sol. non banali: $(1,0), (-1,0)$)

Consideriamo p_0 e q_0 tali che $|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$

$|q\sqrt{d} - p| < \frac{1}{q} \Rightarrow |q\sqrt{d} - p|\,|q\sqrt{d} + p| = |p^2 - dq^2| < \sqrt{d} + \frac{p}{q} \leq 2\sqrt{d} + 1$

$\exists \infty (p,q)$ tali che $|p^2 - dq^2| < 2\sqrt{d} + 1$

$\Rightarrow \exists n \in \mathbb{Z}, n \neq 0 \mid \exists \infty (p,q)$ per cui $p^2 - dq^2 = n$

$\Rightarrow \exists (p_1, q_1)$ e (p_2, q_2) come sopra con $p_1 \equiv p_2 \ (n)$ e $q_1 \equiv q_2 \ (n)$

$z_1 = p_1 + q_1\sqrt{d}$ e $z_2 = p_2 + q_2\sqrt{d} \Rightarrow N\left(\frac{z_1}{z_2}\right) = 1$

$z_0 := \frac{z_1}{z_2} = (p_1 + q_1\sqrt{d})\,\underbrace{(p_2 - q_2\sqrt{d})}_{n} = \underbrace{(p_1 p_2 - d q_1 q_2)}_{n} + \underbrace{(q_1 p_2 - p_1 q_2)}_{n}\sqrt{d}$

$p_1 p_2 - d q_1 q_2 \equiv p_1^2 - d q_1^2 \equiv 0 \ (n)$ $\quad q_1 p_2 - p_1 q_2 \equiv q_1 p_1 - p_1 q_1 \equiv 0 \ (n)$

$\Rightarrow z_0 \in \mathbb{Z}[\sqrt{d}]$ $z_0 = a + b\sqrt{d}$, ho che (a,b) è una sol. non banale di $x^2 - dy^2 = 1$.

Chiamiamo $z_0 \in \mathbb{Z}[\sqrt{d}]$ la più piccola (per norma) soluzione con $z_0 > 1$

se z è tale che $|N(z)| = 1$ e $|z| > 1$ allora $z = a + b\sqrt{d}$ con $a, b > 0$

soluzione generale: $z = \pm z_0^k$ con $k \in \mathbb{Z}$

PROOF: $z > 0$ soluzione $\Rightarrow \exists! \, k \in \mathbb{Z} \mid z_0^k \leq z < z_0^{k+1}$

$\Leftrightarrow 1 \leq z z_0^{-k} < z_0$ $\quad N(z z_0^{-k}) = 1 \Rightarrow z z_0^{-k} = 1 \Rightarrow z = z_0^k$

stesso per $z < 0$...

In termini di coppie mi dice che le soluzioni in $\mathbb{N}^+$ le trovo con

$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ in cui $x_1 + y_1\sqrt{d} = z_0$

$x^2 - dy^2 = -1$, non sempre ci sono soluzioni

Es: $x^2 - 3y^2 = -1 \Rightarrow x^2 \equiv 2 (3)$, impossibile

LEMMA: $x^2 - dy^2 = -1$ ha soluzione $\Leftrightarrow \exists\, z_1 \in \mathbb{Z}[\sqrt{d}]$, $z_1 > 1$ tale che $z_1^2 = z_0$

$\Leftarrow$: $N(z_1) = \pm 1$, ma z_0 è minimale per $N(z) = 1 \Rightarrow N(z_1) = -1$

$\Rightarrow$: prendiamo $z \in \mathbb{Z}[\sqrt{d}] \mid N(z) = -1$, $z > 0$, $\exists!\, k \mid z_0^k < z \leq z_0^{k+1}$

$\Rightarrow 1 < z z_0^{-k} \leq z_0$, $N(\underbrace{z z_0^{-k}}_{z_1}) = -1$, noto che $1 < z_1^2 \leq z_0^2$, $N(z_1^2) = 1$

$\Rightarrow z_1^2 \in \{z_0, z_0^2\}$ $z_1^2 = z_0^2 \Rightarrow z_1 = z_0$, impossibile $\Rightarrow z_1^2 = z_0$. $\surd$

$x^2 - dy^2 = a$: (a lo assumiamo positivo, su aggiusto per i negativi)

LEMMA: se ci sono soluzioni esiste $z_2 = x_2 + y_2\sqrt{d}$ soluzione con $|x_2| \leq \frac{\sqrt{|a|}}{2}\left(\sqrt{z_0} + \frac{1}{\sqrt{z_0}}\right)$;

$z = x + y\sqrt{d}$ con $x, y \in \mathbb{N}^+$, $\exists!\, k \in \mathbb{Z} \mid \frac{\sqrt{a}}{\sqrt{z_0}} \leq z z_0^k \leq a\sqrt{z_0}$, voglio dire che $z_2 := z z_0^k$ $(N(z_2) = a)$

$$2|x_2| = \left|z_2 + \frac{a}{z_2}\right| \leq \max_{\left[\frac{a}{\sqrt{z_0}}, a\sqrt{z_0}\right]} \left|t + \frac{a}{t}\right| = \sqrt{a}\left(\sqrt{z_0} + \frac{1}{\sqrt{z_0}}\right)$$

$$\Rightarrow |x_2| \leq \frac{\sqrt{a}}{2}\left(\sqrt{z_0} + \frac{1}{\sqrt{z_0}}\right)$$

Chiamo $z_2 > 0$ la sol. minimale di $N(z_2) = a$, allora le soluzioni sono tutte e sole quelle della forma $\pm z_2 z_0^k$.

1) N6 2019 (Beatty)

2) in $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$ con $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, la migliore A è $\sqrt{5}$: negare $A > \sqrt{5}$. ← TEO DI HURWITZ

3) $\exists\, \infty\, (n,m) \in \mathbb{N}^2$ tali che $n^2 = \lfloor m\sqrt{2} \rfloor$.

4) $\exists_\infty\, n \in \mathbb{N} \mid n^2 + 1 \mid n!$

5) $\exists \infty\, n \in \mathbb{N}$ tali che n^2+1 ha due divisori con differenza n.

SIMBOLI DI LEGENDRE

↳ RECIPROCITÀ QUADRATICA

$$\left(\frac{a}{p}\right)_{\text{primo}} = \begin{cases} +1 & \text{se } a \text{ è res. quad. mod } p \ (\neq 0) \ (QR) \\ 0 & \text{se } p \mid a \\ -1 & \text{se } a \text{ non è res. quad. mod } p \ (NQR) \end{cases}$$

es.: $\left(\frac{0}{3}\right)=0$, $\left(\frac{1}{3}\right)=1$, $\left(\frac{2}{3}\right)=-1$, $\left(\frac{2}{7}\right)=+1$

PROPRIETÀ

1) $a \equiv b \pmod p \to \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

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

$QR \cdot QR = QR \quad (x^2 \cdot y^2 = (xy)^2)$

$QR \cdot NQR = NQR$

$NQR \cdot NQR = QR$

3) $\left(\frac{a^2}{p}\right)=\left(\frac{a}{p}\right)^2=+1$

$\forall p \nmid 2$

4) $\left(\frac{a^{-1}}{p}\right)=\left(\frac{a}{p}\right)^{-1}=\left(\frac{a}{p}\right)$ (perché $\left(\frac{a}{p}\right)\cdot\left(\frac{a^{-1}}{p}\right)=\left(\frac{1}{p}\right)=1$)

$x \in \{\pm 1\},\ x=x^{-1}$

es. $\left(\frac{6}{7}\right)=\left(\frac{2}{7}\right)\cdot\left(\frac{3}{7}\right)=+1\cdot(-1)=-1$

CRIT. DI EULERO : $\forall a \not\equiv 0 \pmod p$, $\forall p$ primo > 2

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

DIM : notiamo che $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \rightarrow a^{\frac{p-1}{2}} \in \{\pm 1\}$

$\rightarrow$ se $a = x^2 \rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$

Thm di Lagrange in $\mathbb{F}_p[x]$: se $f \in \mathbb{F}_p[x]$ e $\deg f = n$, allora il # di sol. di $f = 0$ è $\leq n$

$\rightarrow$ i QR sono $\frac{p-1}{2}$, e soddisfano $x^{\frac{p-1}{2}} - 1 \equiv 0 \ (p)$

$\rightarrow$ sono esattamente tutte le soluzioni $\rightarrow$ non ce ne sono altre

$\rightarrow$ se x è NQR $\rightarrow x^{\frac{p-1}{2}} \equiv -1$

Questo teor. ci permette di dim. la moltiplicatività :

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

Lemma di Gauss

$a \not\equiv 0 \ (p)$, $p > 2$

Sia $A = \{ ak \pmod p \mid 0 < k < p/2 \}$ e sia N il # di residui in A compresi tra $p/2$ e p.

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

DIM: Chiamiamo "positivi" i residui tra 0 e $p/2$ e negativi gli altri. Definiamo un "valore assoluto"

con $|x| = \begin{cases} x & \text{se } x \text{ è pos} \\ -x & \text{se } x \text{ è neg.} \end{cases}$

es. mod 11 allora $|3|=3$ $|9|=2$

Consideriamo la sg. espans. (mod p)

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \underline{(1\cdot a)}\cdot(2\cdot a)\cdot\ldots\cdot\left(\tfrac{p-1}{2}\cdot a\right) \overset{d}{\equiv} (-1)^N \cdot 1\cdot 2\cdot\ldots\left(\tfrac{p-1}{2}\right)$$

se $0 < r \neq s < p/2$

$\rightarrow |ar| = |as| \iff ar \equiv \pm as \iff r \equiv \pm s \rightarrow r = s$

i moduli di ak sono distinti e $\in \{1, 2, \ldots, \frac{p-1}{2}\}$

$\hookrightarrow$ ciascun modulo è preso una sola volta

$$(1\cdot a)\cdot\ldots\left(\tfrac{p-1}{2}\cdot a\right) = \pm 1 \cdot \pm 2 \cdot \ldots \pm \tfrac{p-1}{2} = (-1)^N \cdot \left(\tfrac{p-1}{2}\right)!$$

$$\hookrightarrow a^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \equiv (-1)^N \left(\tfrac{p-1}{2}\right)! \rightarrow \text{abbiamo finito}$$

Thm: (RECIPROCITÀ QUADRATICA): se p e q sono primi dispari distinti, allora

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1 & \text{se } p \equiv 1 \,(q) \vee q \equiv 1 \,(4) \\ -1 & \text{altrimenti } (p \equiv q \equiv 3 \,(4)) \end{cases}$$

DIM: lasciata al lettore (esistono più di 100 modi)

Gauss due "supplementi"

1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ per crit. di Eulero

$$= \begin{cases} +1 & \text{se } p \equiv 1 \ (4) \\ -1 & \text{se } p \equiv 3 \ (4) \end{cases}$$

$\exists s : s^2 \equiv -1 \ (p) \iff p \equiv 1 \ (4)$

2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{se } p \equiv 1,7 \ (8) \\ -1 & \text{se } p \equiv 3,5 \ (8) \end{cases}$

DIM: con il lemma di Gauss:

$p/2 < 2k < p$ (con $0 < k < p/2$)

$2k < 2 \cdot p/2 = p$

$p/2 < 2k \to k > p/4 \Rightarrow N = \frac{p-1}{2} - \lfloor p/4 \rfloor$

ci interessa $N \bmod 2 \to$ si fanno un po' di conti $\to$ $2k+1$, $8k+3$, $8k+5$, $8k+7$

es. $\left(\frac{30}{37}\right) = \left(\frac{2}{37}\right)\cdot\left(\frac{3}{37}\right)\cdot\left(\frac{5}{37}\right) = (-1)\left(\frac{37}{3}\right)(+1)\cdot\left(\frac{37}{5}\right) =$

$= -\left(\frac{1}{3}\right)\cdot\left(\frac{2}{5}\right) = -1 \cdot 1 \cdot (-1) = +1 \to 30$ è QR mod 37

ESERCIZI

1) BMO 2021/3

2) Trova il # di sol. (mod p) a $x^2 + y^2 \equiv 1$

[Guardare la somma $\sum_{x=0}^{p-1}\left(\left(\frac{1-x^2}{p}\right)+1\right)$ e usa il crit. di Eulero]

3) USAMTS T 2010/9 Se $p = 6k+1$ é primo, então

$$\binom{3k}{k} \not\equiv 1 \pmod{p}$$

4) $k = 2^n + 1$ $\quad$ k é primo $\Leftrightarrow$ $k \mid 3^{\frac{k-1}{2}} + 1$