TEORIA DEI NUMERI 3

- GRUPPO

$G \times G \to G \qquad f(a,b) = a \cdot b$

$\exists$ ELEMENTO NEUTRO

$e \in G: \quad a \cdot e = e \cdot a = a \quad \forall a \in G$

- ASSOCIATIVA: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists$ INVERSO: $\forall a \, \exists b: \; ab = ba = e$

$b = a^{-1}$

COMM. $ab = b \cdot a$

ANELLO COMMUTATIVI

A 2 operazione

A è un gruppo rispetto al +

prodotto:

- ASSOCIATIVO
- DISTRIBUTIVO $a(b+c) = ab + ac$
- COMMUTATIVO $ab = b \cdot a$

A ANELLO CON UNITÀ

SE $\exists \, e: \quad a \cdot e = e \cdot a = a \quad \forall a \in A$

- EL NEUTRO SOMMA = 0
- EL NEUTRO PRODOTTO = 1

DOMINI DI INTEGRITÀ

A anello è un dominio

se $\forall a, b \neq 0$, $a \cdot b \neq 0$

a PUÒ NON AVERE INVERSO MOLTIPLICATIVO

$ab = ac \not\Rightarrow b = c$

$2 \cdot 4 = 2 \cdot 1$ $\mathbb{Z}_6$

→ VERA NEI DOMINI

$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a \cdot (b - c) = 0$

$a \neq 0$, ✓ $b = c$

CAMPI $\mathbb{K}$

- SOMMA GRUPPO ABELIANO
- PRODOTTO $\mathbb{K} \setminus \{0\}$ $\mathbb{K}^*$

GRUPPO ABELIANO COMMUTATIVO

$a \cdot (b + c) = ab + ac$

I CAMPI SONO DOMINI.

DOMINI EUCLIDEI D

ESISTE UNA FUNZIONE (GRADO)

$g: D \setminus \{0\} \to \mathbb{N}$

$\forall\, m, n \in D \quad \exists\, k, r \in D$:

$m = kn + r$ E $g(r) < g(n)$

DIVISIONE CON RESTO — OPPURE $r = 0$

$\forall\, a, b \neq 0$

$g(ab) \geq g(a)$

CON L'UGUALE SSE b INVERTIBILE

ESERCIZIO

GRUPPO $\mathbb{Z}_n$ RISPETTO ALLA SOMMA

ANELLO $\mathbb{Z}_n$ $+, \cdot$ ANELLO CON UNITÀ

$\mathbb{Z}_n, +, \cdot$ NON È UN DOMINIO

$n \mid ab \quad n \nmid a \wedge n \nmid b \quad n$ COMPOSTO

PRIMO $\neq$ IRRIDUCIBILE

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

IRRIDUCIBILE SE NON SI FATTORIZZA

$n = a \cdot b \qquad a = \pm 1 \vee b = \pm 1$

$n \mid ab \qquad n \mid a \vee n \mid b$

$\Downarrow$ $\mathbb{Z}_p$ È UN DOMINIO

DOMINIO FINITO $\Rightarrow$ CAMPO

$\mathbb{Z}_p, +, \cdot$ È UN CAMPO, p PRIMO

FATTORIZZAZIONE UNICA (DOMINIO D)

def: $u \in D$ SI DICE UNITÀ SE È INVERTIBILE SE $\exists u^{-1}$ $u \cdot u^{-1} = 1$

def: DOMINIO D È A FATT. UNICA (UFD) SE OGNI $d \in D$ SI ESPRIME COME PRODOTTO DI PRIMI IN MODO UNICO (A MENO DI UNITÀ).

RISOLVERE DIOFANTEE CI SERVE!!

- DOMINI EUCLIDEI SONO UFD!!

1) PRIMO $\Leftrightarrow$ IRRIDUCIBILE

PRIMO $\Rightarrow$ IRRIDUCIBILE

$p \in D$ PRIMO NON IRRIDUCIBILE

$p = a \cdot b$ a, b NON SONO UNITÀ

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

$p = p \cdot c \cdot b$ $1 = c \cdot b$

---

2) IRRIDUCIBILE $\Rightarrow$ PRIMO

$d \in D$ IRRIDUCIBILE

SUPPONIAMO $d \mid ab$ $d \nmid a \wedge d \nmid b$

$d \nmid a$ $\exists\, s, k \in D:$ $sd + ak = 1$

$I = \{ na + md \mid n, m \in D \}$

$(a, d) = c$ L'ELEMENTO DI I A GRADO MINORE

$a \in I$ $d \in I$

$\forall i \in I$, $c \mid i$

$c = sa + kd$ $s, k \in D$

$i = s_1 a + k_1 d$

$i = q \cdot c + r$ $g(r) < g(c)$ $\vee$ $r = 0$

$g(r) < g(c)$

$s_1 a + k_1 d = q(sa + kd) + r$

$a(s_1 - qs) + d(k_1 - kq) = r \in I$ $g(r) < g(c)$

ES VIEN FUORI LO STESSO A MENO DI UNITA'

$a, d \in D$ EUCL. (a, d) = $\exists\, s, k$ $sa + kd \mid a$ $sa + kd \mid d$

(a, d) SIA TALE CHE!

$c \mid a$ e $c \mid d \Rightarrow c \mid (a, d)$

$(a, d) \mid a$ $\quad (a, d) \mid d$

$d \mid ab$ $\quad (d \nmid a \wedge d \nmid b)$

$c_1 = J_1 d + K_1 a$

$c_1 \mid d$ $\quad c_1 \mid a$

$d = c_1 \cdot c$ $\quad c_1 = d \cdot c^{-1} \Rightarrow d \mid c_1 \Rightarrow d \mid a$

c_1 INVERTIBILE $\quad \exists\, c_1^{-1}$

$c_1^{-1}(J_1 d + K_1 a) = c_1 \cdot c_1^{-1}$

$c_1^{-1} J_1 d + c_1^{-1} \cdot K_1 a = 1$

d IRR. $\quad d \nmid a$ $\quad d \nmid b$

$\Rightarrow \exists\, m_1, n_1 :$ $\quad m_1 d + n_1 a = 1$

$m_2 d + n_2 b = 1$

$(m_1 d + n_1 a)(m_2 d + n_2 b) = 1$

$m_1 m_2 d^2 + m_1 d \cdot n_2 b + n_1 a \cdot m_2 d + n_1 n_2 \cdot ab = 1$

$d \mid ab \Rightarrow d \mid 1$ ASSURDO

PRIMO $\Leftrightarrow$ IRRIDUCIBILE

$d \in D$ INDUCO SU $g(d)$

$g(a) < g(d)$ $\quad a = \prod_{i=1}^{n} q_i$ $\quad q_i$ IRR.

$d = a \cdot b$ $\quad a, b$ NON UNITARI!

$g(d) > g(a)$, $\quad g(d) > g(b)$

$a = \prod_{i=1}^{n} q_i$ $\quad b = \prod_{i=1}^{m} p_i$

$ab = \left(\prod_{i=1}^{n} q_i\right)\left(\prod_{i=1}^{m} p_i\right)$

OGNI d SI FATTORIZZA IN PRIMI

$d = \prod_{i=1}^{n} q_i = \prod_{i=1}^{m} p_i$

$q_n \mid p_j$ $\quad q_n \cdot u = p_j$

SEMPLIFICO E HO CONTROESEMPIO + PICCOLO!!!

$g(ab) = g(a) \iff b$ INV.

$\Rightarrow$

$a = k\,ab + r$ $\quad g(r) \geq g(a)$ $\quad r = 0$

$a = k\,ab$ $\quad 1 = kb$

ESEMPIO

$g(n) = |n| \qquad |mn| \geq |m| \qquad \checkmark$

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

$\overline{a+bi} = a - bi \qquad z \in \mathbb{Z}[i] \quad \bar{z}$

$|z| = z \cdot \bar{z}$

$A \xrightarrow{f} B$

omom. $\begin{cases} f(a+b) = f(a) + f(b) & f(0) = 0 \\ f(a \cdot b) = f(a) \cdot f(b) & f(-a) = -f(a) \end{cases}$

ISOMORFISMO = OMOMORFISMO BIGETTIVO

$A \quad f^{-1}$

$\overline{(a+bi) + (c+di)} = \overline{(a+bi)} + \overline{(c+di)}$

$\overline{(a+bi)(c+di)} = \overline{(ac - bd + bci + adi)}$

$= (ac - bd - bci - adi)$

$= (a - bi)(c - di)$

$|a+bi| = (a+bi)(a-bi) = a^2 + b^2$

w, z $\qquad |wz| = wz \cdot \overline{wz} = w \cdot z \cdot \overline{w} \cdot \overline{z}$

$= w\overline{w} \cdot z \cdot \overline{z}$

$g(wz) \geq g(w)$

$a \neq 0$

$b \neq 0$

$m + ni$ $\qquad$ DIVIDERLO $\qquad a+bi$

$(m + ni) = (a+bi)\boxed{(\alpha + \beta i)}$ $\qquad \alpha, \beta$ NON INTERI

$\alpha \quad \exists A : |\alpha - A| \leq \frac{1}{2}$

$A + Bi$

$|(m+ni) - (a+bi)(A+Bi)| =$

$= |(a+bi)(\alpha+\beta i) - (a+bi)(A+Bi)| =$

$= |(a+bi)((\alpha - A) + (\beta - B)i)| < |a+bi|$

$|a+bi| \, |(\alpha - A) + (\beta - B)i| < |a+bi|$

$\Updownarrow$

$|(\alpha - A) + (\beta - B)i| < 1$

$(\alpha - A)^2 + (\beta - B)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$

$x^2 + 1 = y^3$ $\qquad x, y \in \mathbb{Z}$

$(x+i)(x-i) = y^3$

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

PRIMO IN $\mathbb{Z}$

$p \in \mathbb{Z}[i]$ $\quad |p| = 9$

p PRIMO $\quad p \neq a \cdot b \quad |p| = |a| \cdot |b|$

$9 = 1 \cdot 9$

3 $\quad$ 9

$2 = -i(1+i)^2 \quad (1+i)(1-i)$ $\quad$ $1+i$ PRIMO

$p \mid n^2+1 = (n+i)(n-i)$

$a \mid b \quad \exists c \in D : ac = b$

$\exists a, b \quad p(a+bi) = n+i$

$p = (a+bi)(c+di)$

$(a+bi)(c+di) \in \mathbb{R}$

$c+di = \lambda(a-bi) \quad \lambda \in \mathbb{R}$

$(a+bi)(c+di) = |a+bi| \cdot \lambda$

$p = (a+bi)(a-bi) \cdot n$

$p^2 = |a+bi|\,|a-bi| \cdot |n| \quad p \quad \uparrow$

$p^2 = (|a+bi|\, n)^2 \quad p = |a+bi| \cdot n'$

$p = (a+bi)(a-bi)$

$p \equiv 1 \ (4)$ $\qquad \exists a, b \in \mathbb{Z} : p = a^2 + b^2$

$p \equiv 3 \ (4)$ $\qquad$ SONO IRRIDUCIBILI $\Rightarrow$ PRIMI

$(a+bi)(a-bi) = m \cdot n$ $\qquad (a, b) = 1$

WLOG $a+bi \mid m$ $\qquad = l(a-bi)$

$m = (a+bi)(c+di) = l \cdot (a+bi)(a-bi)$

$m = l \cdot m \cdot n$

$y^3 \equiv 2 \ (4)$

$(x+i)(x-i) = y^3$ $\qquad x^2+1 = y^3$

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

$\qquad = (i, 2)$

$1 = 1^3$

$-1 = (-1)^3$

$i = (-i)^3$

$-i = i^3$

$(x+i) = (a+bi)^3$

$x + i = a^3 + 3a^2bi - 3ab^2 - ib^3$

$1 = 3a^2b - b^3$ $\qquad b \mid 1$ $\qquad b = \pm 1$

$1 = 3a^2 - 1$

$0^2 + 1 = 1^3$

$1 = -3a^2 + 1 \Rightarrow a = 0$

p PRIMO ≥ 3

$x^2+1 = y^p$

x PARI

$(x+i)(x-i)$

$(x+i,\ x-i) = 1$

$y^p = (a+bi)^p (a-bi)^p$

$(x+i) = (a+bi)^p$

$y^p = (a^2+b^2)^p$

$$i = \sum_{k=0}^{\frac{p-1}{2}} a^{2k} (bi)^{p-2k} \cdot \binom{p}{2k}$$

$p-2k>0$

$b \mid 1$

$b = \pm 1$

$$\cancel{i} = \cancel{(\pm i)^p} + (\pm i)^{p-2} \cdot a^2 \binom{p}{2} + \dots$$

$$0 = \sum_{k=1}^{\frac{p-1}{2}} a^{2k} (\pm i)^{p-2k} \binom{p}{2k} \quad a \qquad a$$

$k > 1$

$$v_2\left(a^{2k}\binom{p}{2k}\right) > v_2\left(a^2\binom{p}{2}\right)$$

$$a^{2(k-1)} \frac{(p-2)!\ 2!}{(2k)!\ (p-2k)!} = a^{2(k-1)} \cdot \binom{p-2}{2k-2} \cdot \frac{2}{2k\cdot(2k-1)}$$

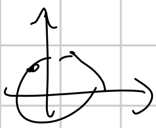
$$v_2\left(a^{2(k-1)} \binom{p-2}{2k-2} \frac{\cancel{2}}{\cancel{2}k\cancel{(2k-1)}}\right) > 0$$

$$v_2\left(a^{2(k-1)} \binom{p-2}{2k-2}\right) > v_2(k)$$

$$\geq v_2\left(a^{2(k-1)}\right) \geq 2(k-1)$$

È POSSIBILE CHE $v_2(k) \geq 2(k-1)$?

$4^{k-1} \mid k$ $\qquad k \le 1$ $\qquad$ ASSURDO!



ω RADICE 3^e DI 1

$\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$, $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$

$\mathbb{Z}[\sqrt{-5}]$ $\qquad 1+\sqrt{-5}$, $1-\sqrt{-5}$ $\qquad (1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3$

UFD, EUCLIDEI

PRIMI $\qquad$ $|p|$ PRIMA IN $\mathbb{Z}$

$p \in \mathbb{Z}$ PRIMI IN $\mathbb{Z}$ $\qquad$ $q(X)$ NON HA RADICI mod p

α $\qquad \mathbb{Z}[\alpha]$ $\qquad a + b\alpha + c\alpha^2 + \dots$

$a_0 + a_1 X + \dots + a_n X^n$ $\qquad q(x)$ POL.

$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] = \mathbb{Q}(\sqrt{-7}) \cap$ INT. ALG. (ESERCIZIO)

$\mathbb{Z}[\alpha]$ $\qquad (X-\alpha)(X-\bar{\alpha})$ $\qquad |z| = z\cdot\bar{z}$

$a + b\alpha \to a + b\bar{\alpha}$ $\qquad$ ISOMORFISMO!!!

$x^2 + 2 = y^3$

$(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$

$\sqrt{-1}$, $\sqrt{-2}$, $\frac{1+\sqrt{-3}}{2}$, $\frac{1+\sqrt{-7}}{2}$

$\frac{1+\sqrt{-19}}{2}$, $\frac{1+\sqrt{-47}}{2}$, $\frac{1+\sqrt{-163}}{2}$

$$(x+\sqrt{-2}, x-\sqrt{-2}) = (x+\sqrt{-2}, 2\sqrt{-2}) = (x+\sqrt{-2}, \sqrt{-2}^3)$$

$$x+\sqrt{-2} = (a+b\sqrt{-2})^3$$

$$= a^3 + 3a^2 b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2}$$

$b \mid 1 \qquad b = \pm 1$

$1 = 3a^2 - 2 \qquad\qquad 3 = 3a^2 \qquad a = 1$

$1 = -3a^2 + 2 \qquad (\text{mod } 8)$

$a = 1 \qquad b = -1 \qquad\qquad -5$

$(1 - \sqrt{-2})^3 =$

$5^2 + 2 = 27$

$a^2 + 2 = 3^b$

$(a+\sqrt{-2})(a-\sqrt{-2}) = (1+\sqrt{-2})^b(1-\sqrt{-2})^b$

$(1+\sqrt{-2})^b = \pm(a \pm \sqrt{-2})$

$\operatorname{Im}(1+\sqrt{-2})^b = \pm 1$

$b = 1$

$$\frac{(1+\sqrt{-2})^b - (1-\sqrt{-2})^b}{(1+\sqrt{-2}) - (1-\sqrt{-2})} = \pm 1 \qquad\qquad 5^2 + 2 = 3^3$$

$(1-\sqrt{-2})^2 = 1 - 2 - 2\sqrt{-2} = -\boxed{(1+2\sqrt{-2})}$

$\uparrow 2\sqrt{-2}$

$$(1+\sqrt{-2})^h - (1-\sqrt{-2})^h = \pm\left[(1+\sqrt{-2}) - (1-\sqrt{-2})\right]$$

$$(1+\sqrt{-2})^h \equiv \pm(-1) \quad (\text{mod } 1+2\sqrt{-2})$$

$$(-1+2\sqrt{-2})^h \equiv 1$$

$$(-2)^h \equiv 1 \quad (\text{mod } 1+2\sqrt{-2})$$

$$1+2\sqrt{-2} \mid (-2)^h - 1$$

$$9 \mid (-2)^h - 1$$

$$a+b\sqrt{-2} \mid n \Rightarrow \frac{|a+b\sqrt{-2}|}{(a,b)} \mid n$$

$$3 \mid h$$

$$a^2+2 = 3^{3h}$$

$$\frac{(1+\sqrt{-2})^h - (1-\sqrt{-2})^h}{(1+\sqrt{-2}) - (1-\sqrt{-2})}$$

$a_0 = 0$

$a_1 = 1$

$$a_{n+2} = K a_{n+1} + J \cdot a_n$$

$a_0 = 0$

$a_1 = 1$

$$(a_n, a_m) = a_{(n,m)}$$

m' + нaи. инд. $a \mid a_m$

$$\Rightarrow \boxed{a \mid a_n \Leftrightarrow m \mid n}$$

$a_n = 3^k$

$$a_n = \frac{a^n - 1}{a - 1}$$

$a_0 = 0 \quad a_1 = 1 \quad a_{n+2} = K a_{n+1} + J a_n$

$(K, J) = 1$

$$a_n = \frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}} \qquad (x-\alpha)(x-\bar{\alpha}) = x^2 - Kx - J$$

$\mathbb{Z}[\alpha]$

$a + b\alpha$

$\| \quad \alpha^{n-1} + \alpha^{n-2}\bar{\alpha} + \dots + \bar{\alpha}^{n-1}$

LASCIATA FISSA DAL CONIUGIO

$m = Kn$

$a_n \mid a_m \qquad \overline{\alpha^n} = \bar{\alpha}^n$

$$\frac{\alpha^{Kn} - \bar{\alpha}^{Kn}}{\alpha^n - \bar{\alpha}^n} \in \mathbb{Z} \qquad F_n \mid F_{Kn}$$

$n = dx \quad m = dy \quad d = (n, m)$

$$b_i = \frac{a_{di}}{a_d} = \frac{\alpha^{di} - \bar{\alpha}^{di}}{\alpha^d - \bar{\alpha}^d} \in \mathbb{Z} \qquad x^2 - cx - e = 0$$

$(c, e) = 1$

$a_{(n,m)} \mid (a_n, a_m) \qquad (\alpha\bar{\alpha}, \alpha+\bar{\alpha}) = 1$

$((\alpha\bar{\alpha})^d, (\alpha+\bar{\alpha})^d) \neq 1$

$$\left(\frac{a_n}{a_{(n,m)}}, \frac{a_m}{a_{(n,m)}}\right) = 1 \qquad \Downarrow$$

$(\alpha\bar{\alpha}, (\alpha+\bar{\alpha})^d) \neq 1$

$\|$

$b_n \quad b_0 = 0 \quad b_1 = 1 \qquad (\alpha\bar{\alpha}, \alpha+\bar{\alpha}) \neq 1$ ASSURDO

$b_{n+2} = c b_{n+1} + e b_n$

PER INDUZIONE: $(b_n, b_{n+1}) = 1$

$n = dx$
$m = dy$
$(x, y) = 1$

$p \mid \left(\frac{a_n}{a_d}, \frac{a_m}{a_d} \right)$ $\quad p \mid a_x$

$p \mid b_y$ $\quad p \mid b_{kx}$ $\quad p \mid b_{jx}\ \forall j$

$kx + 1 = jy$ ASSURDO!! $\quad p \mid b_{kx}$ $\quad p \nmid b_{kx+1}$

$X_0 = 2$ $\quad X_{n+1} = 2X_n^2 - 1$

$(n, X_n) = 1$

$$\cosh(\theta \cdot 2^n) = \frac{(e^\theta)^{2^n} + (e^\theta)^{-2^n}}{2}$$

$e^\theta = 2 + \sqrt{3}$

$$X_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}$$

p DISP. $\quad p \mid X_n$ $\quad \left(\frac{3}{p}\right) = 1$ $\quad p \mid X_n$

$\sqrt{3}$ ESISTE IN $\mathbb{Z}_p$ $\quad \Downarrow$

$a \quad \frac{1}{a} \quad 2^{n+2} \mid p-1$

$a^{2^n} \equiv -a^{-2^n}$ $\quad a^{2^{n+1}} \equiv -1$

$\left(\frac{3}{p}\right) = -1$ $\quad \operatorname{ord}(a) = 2^{n+2}$

$$\{a + b\sqrt{+3} \mid a, b \in \mathbb{Z}_p\} = \mathbb{Z}_p[\sqrt{3}]$$

$$|\mathbb{Z}_p[\sqrt{3}] \setminus \{0\}| \mid p^2-1$$

$$p \mid \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}$$

$$(2+\sqrt{3})^{2^n} = -(2-\sqrt{3})^{2^n} \qquad \text{ord}(2+\sqrt{3}) = 2^{n+2}$$

$$(2+\sqrt{3})^{2^{n+1}} = -1 \qquad 2^{n+2} \mid p^2-1$$

$$2^{n+1} \mid p-1 \ \vee\ 2^{n+1} \mid p+1$$

$$2^n - 1 \mid X_{n-2} \iff 2^n-1 \text{ è PRIMO}$$

Equazioni tipo Pell

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

$z = a + b\sqrt{d}$ $\qquad$ $\bar{z} = a - b\sqrt{d}$

$N(z) = a^2 - db^2 = z\bar{z}$ (moltiplicativa:

$N(z_1 z_2) = N(z_1) N(z_2)$)

$(x + \sqrt{d}\, y)(a + \sqrt{d}\, b) = 1$

$x^2 - dy^2 = 1$ $\qquad$ (d non quadrato)

$\exists$ una soluzione $z_0 = x_0 + y_0\sqrt{d}$ $\quad N(z_0) = 1$

con z_0 minima tra le soluzioni $N(z) = 1$

e $z > 1$, con la proprietà che ogni altra

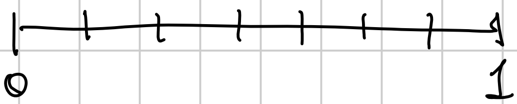
si scrive $\pm z_0^n$, $n \in \mathbb{Z}$

Teo (Dirichlet) $\forall \alpha$ irrazionale, $\exists$ infiniti

$p/q \in \mathbb{Q}$ t.c. $|\alpha - p/q| < 1/q^2$

Idea $|\alpha - p/q| < \dfrac{1}{q(n+1)}$ $\qquad$ $|\alpha q - p| < \dfrac{1}{n+1}$

$(q \leq n)$ $\qquad$ $0, \{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}, 1$



$$\left|\sqrt{d} - p/q\right| < \frac{1}{q^2}$$

$$p^2 - dq^2 = (p + q\sqrt{d})(p - q\sqrt{d}) =$$

$$\leq q \cdot \frac{1}{q^2}(p + q\sqrt{d}) \leq (p/q + \sqrt{d}) \leq 2\sqrt{d} + 1$$

$\exists$ un $M \leq 2\sqrt{d}+1$ t.c.

$$x^2 - dy^2 = M \leftarrow$$

ha ∞ soluz.

(p, q) mod M ha M^2 possibilità

$p_1 \equiv p_2 \ (M)$, $q_1 \equiv q_2 \ (M)$, $p_i^2 - dq_i^2 = M$

$N(p_1 + \sqrt{d}\, q_1) = M$, $N(\ ---) = M$

$$\frac{p_1 + \sqrt{d}\, q_1}{p_2 + \sqrt{d}\, q_2} \cdot \frac{p_2 - \sqrt{d}\, q_2}{p_2 - \sqrt{d}\, q_2} = \frac{(p_1 p_2 - d q_1 q_2) + \sqrt{d}\,(q_1 p_2 - q_2 p_1)}{M}$$

$\circledast$ $q_1 p_2 \equiv q_2 p_1 \ (M)$

$\circledast$ $p_1 p_2 \equiv d q_1 q_2 \ (M) \iff M = p_1^2 - dq_1^2 \equiv 0 \ (M)$

$$z_0 = \min\{z \text{ t.c. } N(z) = 1,\ z > 1\}$$

Prendiamo una soluzione a $N(z) = 1$.

Osserviamo che $N(z \cdot z_0) = N(z)\, N(z_0) = 1 \cdot 1 = 1$

$$z_0 = x_0 + y_0\sqrt{d} \longrightarrow \overline{z_0} = z_0^{-1}$$

$$(x_0 + y_0\sqrt{d})(x_0 - y_0\sqrt{d}) = 1$$

$$1 \leq \underbrace{z \cdot z_0^{-k}}_{} < z_0$$

Soluzione della Pell → è 1

$$z = z_0^{k}$$

$$z = \pm z_0^{k}$$

$$x^2 - dy^2 = m$$

Caso $m = -1$

Ha soluz. $\iff$ z_0 è un quadrato in $\mathbb{Z}[\sqrt{d}]$.

Se $z_0 = z_1^2$, allora $N(z_1) = -1$

$$\begin{cases} (N(z_1))^2 = N(z_1^2) = N(z_0) = 1 \\ z_1 < z_0 \longrightarrow N(z_1) \neq 1 \end{cases}$$

Viceversa, se z_1 è t.c. $N(z_1) = -1$, allora $N(z_1^2) = 1$

Tutte le soluzioni: $z = \pm z_1 \cdot z_0^{n}$ $\quad k = n$

$$= \pm z_1^{2k+1}$$

Caso $x^2 - dy^2 = m$ generico

Esistono al più $\varphi(|m|)$ soluzioni,

$z_1, z_2, \ldots, z_\ell$ con $\ell \leq \varphi(|m|)$

con la proprietà che z è soluzione prim. $\iff$

$$z = \pm z_k \cdot z_0^n \qquad k \in \{1, \dots, \ell\}, \quad n \in \mathbb{Z}$$

z si dice primitiva se $(z = x + \sqrt{d}\,y)$ si ha

$$(x, y) = 1$$

$$s(z = x + \sqrt{d}\,y) = x y^{-1} \pmod{m}$$

1) $s(z \cdot z_0^n) = s(z)$

$$z \cdot z_0^n = (x + y\sqrt{d})(a + b\sqrt{d}) \qquad N(a + b\sqrt{d}) = 1$$

$$= (ax + bdy) + \sqrt{d}\,(ay + bx) \qquad a^2 - b^2 d = 1$$

$$\frac{ax + bdy}{ay + bx} \cdot \frac{ax - bdy}{ax - bdy} = \qquad a^2 = 1 + db^2$$

$$= \frac{a^2x^2 - b^2d^2y^2}{a^2xy + abx^2 - abdy^2 - b^2dxy} = \frac{db^2(x^2 - dy^2) + x^2}{xy + Nab}$$

($a^2xy - b^2dxy$ circled: xy)

$$= \frac{Ndb^2 + x^2}{Nab + xy} \equiv x/y \ (N)$$

Se $s(w_1) = s(w_2)$, $\frac{w_1}{w_2} \in \mathbb{Z}[\sqrt{d}]$

$$N\left(\frac{w_1}{w_2}\right) = \frac{N(w_1)}{N(w_2)} = 1 \longrightarrow w_2 = w_1 \cdot z_0^n$$

Remark Se $z \in \mathbb{Z}[\sqrt{d}]$, $N(z) = m$,

$$X = \frac{z + \bar{z}}{2}, \qquad y = \frac{z - \bar{z}}{2\sqrt{d}}$$

$z = z_0^n \longrightarrow x, y$ rispettano relaz. per ricorrenza

$$X_0 = 1, \quad y_0 = 0$$

$$X_{n+2} = (z_0 + \bar{z}_0)\, X_{n+1} - (z_0 \bar{z}_0)\, X_n$$

Bound sulle soluzioni

Se $x^2 - dy^2 = m$ ha una soluzione, allora ne ha una in cui $|x| \leq \frac{1+z_0}{2\sqrt{z_0}} \sqrt{|m|}$

Moltiplicando per z_0^n opportuno, troviamo una soluzione $\in \left[\sqrt{\frac{m}{z_0}}, \sqrt{m \cdot z_0} \right)$ che chiamo w

$$2|x| = |w + \overline{w}| = \left| w + \frac{m}{w} \right| \leq$$

$$\leq \max_{w \in \left[\sqrt{\frac{m}{z_0}}, \sqrt{m \cdot z_0} \right]} \left| w + \frac{m}{w} \right| \qquad (m > 0)$$

$$= \sqrt{|m| \cdot z_0} + \sqrt{\frac{|m|}{z_0}} = \sqrt{|m|} \, \frac{z_0 + 1}{\sqrt{z_0}}$$

Trovare z_0 + successioni di Farey

FAREY

$$\mathcal{F}_n = \left\{ \frac{a}{b} : (a,b)=1,\ 0<b\le n,\ 0\le \frac{a}{b}\le 1 \right\}$$

$\frac{0}{1}$ $\frac{1}{1}$

$\frac{0}{1}$ $\frac{1}{2}$ $\frac{1}{1}$

$\frac{0}{1}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{1}{1}$

Algoritmo:

* $\frac{n}{1} < \sqrt{D} < \frac{n+1}{1}$

* Ad ogni passo, se $\frac{a}{b} < \sqrt{D} < \frac{c}{d}$, calcolate $\frac{a+c}{b+d}$.
  - Se $x=(a+c), y=(b+d)$ è soluzione Pell → FINE
  - Altrimenti, $\frac{a}{b} < \sqrt{D} < \frac{a+c}{b+d}$ o $\frac{a+c}{b+d} < \sqrt{D} < \frac{c}{d}$

Lavoriamo in $\mathcal{F}_n$. Diciamo che $\frac{a}{b} < \frac{c}{d}$ siano consecutive. Allora

i) $b+d > n$

ii) $(a,c) = (b,d) = 1$

iii) $bc - ad = 1$

i) $\frac{a}{b} < \underbrace{\frac{a+c}{b+d}}_{\leq n} < \frac{c}{d}$ ASSURDO

ii) Segue da iii + Bézout

iii) Induzione su n. $\frac{a}{b} < \frac{c}{d}$ in $\mathcal{F}_n$

* o $\frac{a}{b}$, c/d restano consecutive in $\nearrow \mathcal{F}_{n+1}$
* o $\frac{a}{b} < \frac{M}{n+1} < c/d$

$$\frac{M}{n+1} - \frac{a}{b} = \frac{k_1}{b(n+1)}, \quad \frac{c}{d} - \frac{M}{n+1} = \frac{k_2}{d(n+1)}$$

$$\frac{1}{bd} \overset{ii}{=} \frac{c}{d} - \frac{a}{b} = \frac{k_1 d + k_2 b}{bd(n+1)}$$

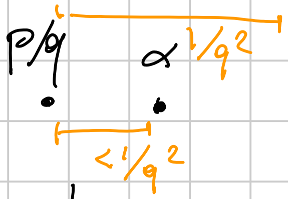
$$\underbrace{-b-d+n+1}_{\leq 0} = k_1 d + k_2 b - b - d$$

$$= d(k_1 - 1) + b(k_2 - 1) \longrightarrow k_1 = k_2 = 1$$

Teo (Hurwitz) α irraz.

$$\exists \infty \ p/q \ \text{t.c.} \ |\alpha - p/q| < \frac{1}{\sqrt{5}\, q^2}$$

$\frac{a}{b} < \alpha < \frac{c}{d}$ una tra a/b, c/d, $\frac{a+c}{b+d}$ va bene nel Teo. Hurwitz



$$\alpha - p/q < 1/q^2$$

Esisterà a/b t.c. $\alpha > a/b > p/q$, e $b \leq q$?

$$\frac{a}{b} - p/q \geq \frac{1}{bq} \geq 1/q^2$$

Se $x + y\sqrt{d}$ risolve la Pell, $x^2 - dy^2 = 1$

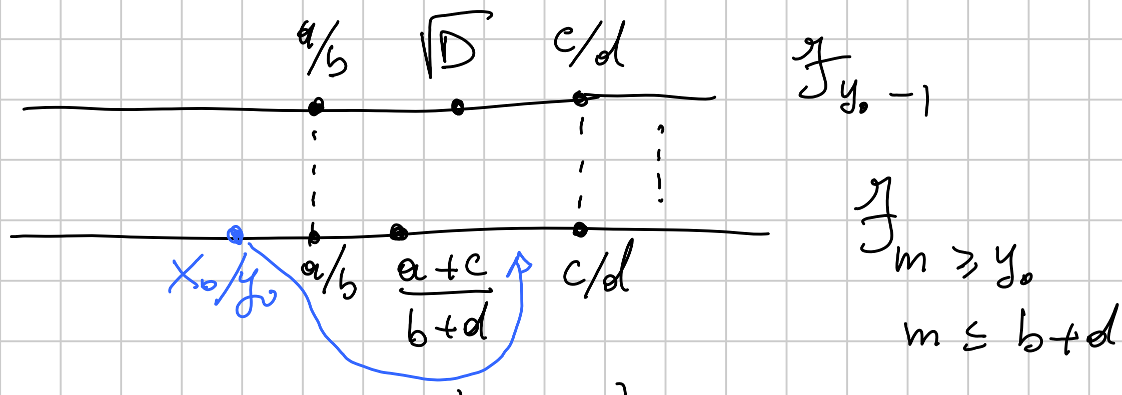
$$x/y > \sqrt{d}$$

$$\frac{x}{y} - \sqrt{d} = \frac{1}{y}\frac{(x - y\sqrt{d})(x + y\sqrt{d})}{(x + y\sqrt{d})} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{d}\right)} < \frac{1}{2y^2\sqrt{d}}$$

$$< \frac{1}{2y^2}$$

Sia x_0, y_0 la più piccola soluz. Pell; x_0/y_0

starà in una $\mathcal{F}_n = \mathcal{F}_{y_0}$.



Sappiamo $\left|x_0/y_0 - \sqrt{D}\right| < \frac{1}{2y_0^2}$. Se $\frac{x_0}{y_0} \notin \left(\frac{a}{b}, \frac{c}{d}\right)$

succede che a/b è un'approx di $\sqrt{D}$ migliore

di x_0/y_0 (IMPOSSIBILE, perché $b \leq y_0$)

$$\frac{c}{d} - \frac{a+c}{b+d} = \frac{cb + \cancel{cd} - ad - \cancel{cd}}{d(b+d)} = \frac{1}{d(b+d)}$$

Esempio $a^2 = 19n+1$ e $b^2 = 95n+1$ sono quadrati

$$b^2 = 5a^2 - 4 \qquad b^2 - 5a^2 = -4$$

$$\varphi(|4|) = 2 \qquad b \equiv a \quad (4)$$

$$b \equiv 3a \quad (4)$$

$$(1 + \sqrt{5} \cdot 1)(1 - \sqrt{5} \cdot 1) = -4$$

$$(11 + 5\sqrt{5})(11 - 5\sqrt{5}) = -4$$

Mancano: * non primitive $x^2 - 5y^2 = -1$

* z_0 $\quad x^2 - 5y^2 = 1$

$$\frac{2}{1} < \sqrt{5} < \frac{3}{1}$$

$$\frac{2}{1} < \sqrt{5} < \frac{5}{2} \qquad 7/3 > \sqrt{5}$$

$$\frac{2}{1} < \sqrt{5} < 7/3 \qquad 9/4$$

Non primitive: $(2+\sqrt{5})^{2k+1}$

$$(1+\sqrt{5})(9+4\sqrt{5})^k, \qquad (11+5\sqrt{5})(9+4\sqrt{5})^k$$

$$(2+\sqrt{5})^{2k+1} \qquad \varphi^2 = \varphi + 1$$

$$(1+\sqrt{5})^2 = 6 + 2\sqrt{5}$$

$$(1+\sqrt{5})^3 = 16 + 8\sqrt{5} = 8(2+\sqrt{5})$$

$$(2+\sqrt{5})^2 = 9 + 4\sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^6$$

$$(1+\sqrt{5})^5 = 16(3+\sqrt{5})(2+\sqrt{5}) = 16(11+5\sqrt{5})$$

$$11+5\sqrt{5} = 2\left(\frac{1+\sqrt{5}}{2}\right)^5$$

$$z = 2\left(\frac{1+\sqrt{5}}{2}\right)^{2k+1}$$

$$y = \frac{2\left(\frac{1+\sqrt{5}}{2}\right)^{2k+1} - 2\left(\frac{1-\sqrt{5}}{2}\right)^{2k+1}}{2\sqrt{5}} = F_{2k+1}$$

$$F_{2k+1}^2 - 1 \equiv 0 \ (19) \qquad \left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1$$

<u>Es</u> $3^n - 2 = X^2$ $\qquad$ X dispari $\rightarrow$ n dispari

$$3y^2 - 2 = X^2$$

$$X^2 - 3y^2 = -2 \qquad (1+\sqrt{3})$$

$$X^2 - 3y^2 = 1 \qquad (2+\sqrt{3})$$

$$y_n = \frac{(1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2-\sqrt{3})^n}{2\sqrt{3}} = (\star)$$

$$(1+\sqrt{3})^2 = 4+2\sqrt{3} = 2(2+\sqrt{3})$$

$$(\star) \quad \frac{(1+\sqrt{3})^{2n+1} - (1-\sqrt{3})^{2n+1}}{2^{n+1}\sqrt{3}}$$

$$9 \mid y_n \iff n \equiv 4 \ (9)$$

$$y_4 = 153 = 9 \cdot 17$$

$$b_{2n+1} = 2^n y_n = \frac{(1+\sqrt{3})^{2n+1} - (1-\sqrt{3})^{2n+1}}{2\sqrt{3}}$$

$$(b_{2n+1}, b_9) = b_{(9,2n+1)} = b_9 \equiv 0 \ (17)$$

$$17 \mid 2^n y_n \qquad 17 \mid y_n$$