N 1 - ADVANCED   Guido

Titolo nota   03/09/2015

$\mathbb{Z}[\sqrt{5}]$, $\subseteq \mathbb{C}$

A è dominio se $ab = ac \overset{\text{e } a \neq 0}{\Rightarrow} b = c$

$A \ni u$ è unità se $\exists\, v \in A$ t.c. $u \cdot v = 1$

$\{\text{unità}\} = A^\times$

$\mathbb{Z}^\times = \{\pm 1\}$ $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

$\mathbb{Z}[i]$ "Interi di Gauss"

$\overset{\shortparallel}{\{a + bi : a, b \in \mathbb{Z}\}} \subseteq \mathbb{C}$

Per dire che è un anello abbiamo verificare che ($0, 1 \in A$) è chiuso per

1. opposto
2. somma
3. prodotto

$x \in \mathbb{Z}[i] \Longrightarrow -x \in \mathbb{Z}[i]$

1 ✓ $x = a + bi$ $\overset{\shortparallel}{-a + (-b)i}$

2: $x = a + bi$ $y = c + di$ $x + y \overset{?}{=} (a+c) + (b+d)i$

3. " " $x \cdot y = (ac - bd) + (bc + ad)i$

$\mathbb{Z}[i]^\times = ?$ $\pm 1, \pm i$ $(i)(-i) = 1$

$(a+bi)(c+di) = 1$ -

$$\begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$$

$x = a + bi \longrightarrow a^2 + b^2 = N(x)$

$N(xy) = N(x) \cdot N(y)$

$x \mid z \qquad z = xy \qquad N(z) = N(x)\,N(y)$

$\Rightarrow N(x) \mid N(z)$

$\Rightarrow$ Se $u \in \mathbb{Z}[i]^\times \qquad N(u) \in \mathbb{Z}^\times$

$u = a + ib \qquad a^2 + b^2 = \pm 1 \qquad a = \pm 1 \quad b = 0$

$a = 0 \quad b = \pm 1$

$D \in \mathbb{Z} \qquad D \neq \square$

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

3 $\qquad (a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$

$\cancel{\sqrt{\tfrac{1}{3}} \quad \tfrac{i}{3}}$

Esempio a parte $\{a + b\tfrac{i}{3}\}$ ($a, b \in \mathbb{Z}$) non è un anello

$\tfrac{i}{3} \cdot \tfrac{i}{3} \in$

$\mathbb{Z}[\sqrt{D}]^\times \ni \pm 1 \qquad D = 2$

cerchiamo un metodo per trovare $\mathbb{Z}[\sqrt{2}]^*$

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

$a+b\sqrt{2}$ $\qquad (1+\sqrt{2})(1+\sqrt{2}) = 3+2\sqrt{2}$

- Idea generalizzare il concetto di Norma su $\mathbb{Z}[\sqrt{D}]$

- Definire un coniugio

$x \longmapsto \sigma(x)$

Definiamo un coniugio $\sigma : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}]$

$a+b\sqrt{D} \longrightarrow a-b\sqrt{D}$

1. $\sigma(x+y) = \sigma(x)+\sigma(y)$
2. $\sigma(x\cdot y) = \sigma(x)\cdot\sigma(y)$ $\qquad \sigma$ è omomorfismo

$x = a+b\sqrt{D}$ $\qquad y = c+d\sqrt{D}$ $\qquad x+y = (a+c)+(b+d)\sqrt{\ }$

$\sigma(x+y) = (a+c)-(b+d)\sqrt{D}$

$\sigma(x)+\sigma(y) = a - b\sqrt{D} + c - d\sqrt{D} \Rightarrow$

Definiamo $N(x)$ $\qquad x \in \mathbb{Z}[\sqrt{D}]$

$x\cdot\sigma(x) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2$

$x = a+b\sqrt{D}$

$N(xy) = xy\,\sigma(xy) = x\,y\,\sigma(x)\,\sigma(y) = (x\sigma(x))(y\sigma(y))$

$\mathbb{Z}[\sqrt{D}]^\times = a+b\sqrt{D} = u$

$N(u) = \pm 1 = u \cdot \sigma(u) = \pm 1$

le unità $\mathbb{Z}[\sqrt{D}] = \{ a + b\sqrt{D} \cdot a, b \in \mathbb{Z} : a^2 - Db^2 = \pm 1 \}$

Se $D > 0 \longrightarrow$ ci siamo ricondotti alle equazioni di Pell

Se $D < 0 \longrightarrow$ è una diofantea facile

$D = -1 \longrightarrow$ fatto ✓

$D < -1$ $\qquad \mathbb{Z}[\sqrt{D}]^* = \{\pm 1\}$

<u>Def</u> $\qquad A$ dominio

- $a \in A$ è <u>irriducibile</u> se non si può scrivere come $a = x \cdot y$ e x, y non sono unità di A e $a \in A^\times$

- $a \in A$ è <u>primo</u> se $a \mid x \cdot y \Longrightarrow a \mid x$ oppure $a \mid y$ e $a \notin A^\times$

primo $\Rightarrow$ irriducibile

$p = ab \Rightarrow p \mid a \qquad a = p \cdot c$

$\Rightarrow p = p \cdot cb \qquad c \cdot b = 1$

$A = \mathbb{Z}[\sqrt{-5}]$ $\qquad a = 2$

- 2 è irrid
- ma 2 non è primo

Supponiamo $\quad 2 = a \cdot b \quad \Rightarrow \quad N(2) = N(a) \cdot N(b)$

$$\begin{matrix} N(2) \\ \shortparallel \\ 4 \end{matrix}$$

$N(a) = N(b) = 2 \qquad a = x + y\sqrt{-5}$

$x^2 + 5y^2 = 2 \qquad$ Ass!

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

$\frac{1+\sqrt{-5}}{2} \in A \quad$ oppure $\quad \frac{1-\sqrt{-5}}{2} \in A$

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

su $\mathbb{Z}$ vale

- ogni n si può scrivere come prodotto di irrid e la scomposizione è unica (a meno di ordine e di unità)

Che succede su $\mathbb{Z}[\sqrt{D}]$?

$\alpha \in \mathbb{Z}[\sqrt{D}]$ $\qquad \alpha = x \cdot y$

$\cancel{p_1} \cdots p_n = \cancel{q_1} \cdots q_s\, u_j$

$\hat{j}$

$p_1 \mid q_1 \qquad q_1 = p_1 \cdot x$

Se $\{\text{primi}\} = \{\text{irred.}\}$ $\Rightarrow$ A è UFD

$x \mid ab \qquad xy = ab =$

$x(p_1 \cdots p_s) = (q_1 \cdots q_r)(t_1 \cdots t_l)$

WLOG $\quad x = q_1 \cdot$ unità $\Rightarrow x \mid a$.

$\mathbb{Z}[\sqrt{D}]$

- $\mathbb{Z}[i]$ è UFD

In generale

- $\mathbb{Z}[\sqrt{-2}]$ è UFD

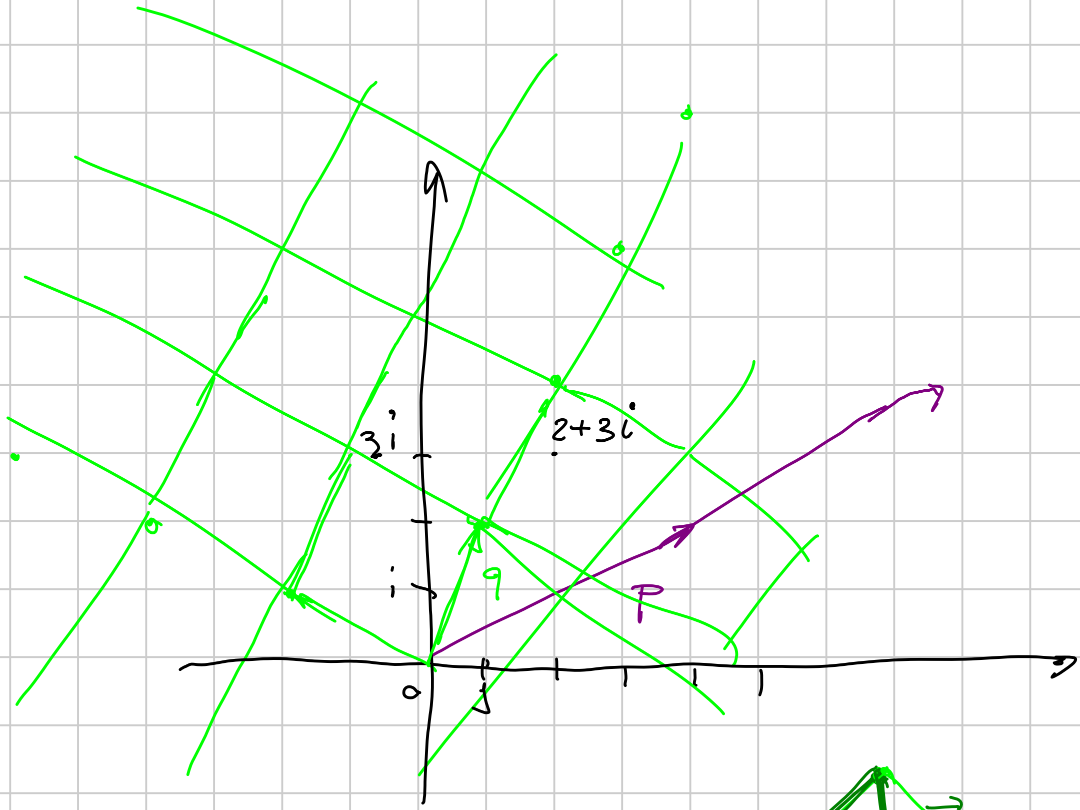
$\boxed{\text{TEO}}$

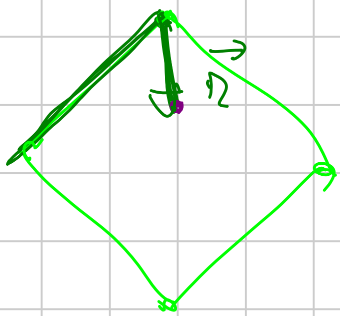
Tutti gli anelli con una divisione col resto sono UFD

Diciamo che su $A = \mathbb{Z}[\sqrt{D}]$ c'è la divisione col resto se

$\forall\, p, q \qquad \exists\, r, d \qquad p = q \cdot d + r$

e $|N(r)| < |N(p)|$

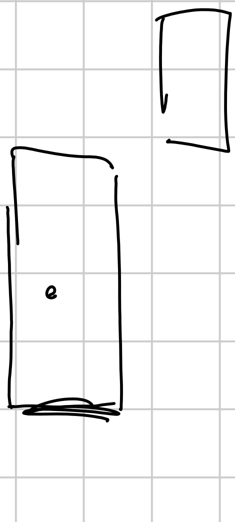




$\exists\, d$

$p = r + q \cdot d$

Esercizio $\quad \mathbb{Z}[\sqrt{-2}]$ è UFD



$\mathbb{Z}[\sqrt{-3}]$

2 è irrid ma non primo

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

Se $\mathbb{Z}[\sqrt{-3}]$ fosse UFD

$\omega \in \frac{1+\sqrt{-3}}{2} \in_{blue} \mathbb{Z}[\sqrt{-3}]$

$B = \{a+b\omega : a,b \in \mathbb{Z}\} =$

$\omega^2 \in B \qquad \omega^2 = \omega - 1$

$(a+b\omega)(c+d\omega) = ac + bc\omega + ad\omega + bd\omega^2 =$

$(ac-bd) + (bc+ad+bd)\omega$

Se $D \equiv 1 \ (4) \qquad D < 0$

2 non è primo

$2 \cdot 2 = D - 1 = (\sqrt{D} - 1)(\sqrt{D} + 1)$

Se $D \equiv 1 \mod 4$

$\omega = \dfrac{\sqrt{D} - 1}{2} \qquad$ ~~Bcrvon~~ $B = \{a+b\omega : a,b \in \mathbb{Z}\}$

$\omega^2 = \dfrac{D+1}{4} - \dfrac{\sqrt{D}}{2} = -\dfrac{\sqrt{D}-1}{2} + \dfrac{D-1}{4} = \dfrac{D-1}{4} + \omega$

Se $D \equiv 1$ non ci conviene considerare $\mathbb{Z}[\sqrt{D}]$

$\mathbb{Z}\left[\dfrac{\sqrt{D}+1}{2}\right]$

$\hat{\iota}$

$a+b\omega \to a-b\omega \qquad x + y\sqrt{D}$

$(a+b\omega)(c+d\omega)$

$N(\omega) = \omega(-\omega) = -\omega^2 = \frac{D-1}{4} - \omega \notin \mathbb{Z}$

$\omega = \frac{1+\sqrt{D}}{2} \longrightarrow \frac{1-\sqrt{D}}{2} = \bar{\omega}$

$\varphi(a+b\omega) \longrightarrow a+b\bar{\omega}$

$x\,\varphi(x)$

A è un <u>dominio euclideo</u> se · è un dominio
se $\exists$ una funzione $\varphi : A\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ t.c.
$\forall\, p, q \in A\setminus\{0\}$ $\exists\, d, r$ tali che
$p = qd + r$ e $\varphi(r) < \varphi(q)$

<u>TEO</u> Se A è un dominio euclideo, allora vale il teo di fattorizzazione unica

---

<u>Esercizio</u> $x^2 + 1 = y^p$ con p numero primo

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

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

$(x+i, x-i)$ $MCD(a, b) = MCD(a, b-ka)$

$M.C.D(10, 16) = 2$ $\mathbb{Z}i$

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

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

oss. $\quad 1-i = -i(1+i)$

Per capire l'M.C.D (- -) dobbiamo capire se $x+i$ è multiplo di $1+i$

Se x fosse pari M.C.D $= 1$

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

2) $N(x+i) = x^2+1$

1 (o 3) $\quad x+i \equiv 2m+i \equiv i \pmod{1+i}$

Se x fosse dispari $x^2+1 \equiv 2 \pmod 4$

$\Rightarrow$ $x+i$ e $x-i$ sono coprimi

$$(x+i)(x-i) = y^p = \alpha_1^p \cdots \alpha_k^p$$

$$\Rightarrow \begin{cases} x+i = \alpha^p \cdot u \\ x-i = \beta^p \cdot v \end{cases} \qquad u = \pm 1, \pm i$$

$$\overline{x+i} = x-i$$

se $\quad x+i = \alpha^p u \Rightarrow x-i = \overline{\alpha^p u} = \bar{\alpha}^p \cdot \bar{u}$

$p = 2 \longrightarrow \quad x = \pm \quad y = 0$

$p > 2$ $\qquad -\alpha^p = (-\alpha)^p$

$$x+i = \alpha^p$$

$$x+i = i\alpha^p \qquad \alpha = \cancel{a} \pm i$$

$$\alpha = a+bi \Rightarrow \alpha^p = \sum_{k=0}^{p} b^k i^k a^{p-k}\binom{p}{k} =$$

$$\underbrace{\sum_{\substack{k=0\\ k \text{ pari}}}^{p} b^k (-1)^{\frac{k}{2}} a^{p-k}\binom{p}{k}}_{\text{1 altro}} + \underbrace{\sum_{\substack{k=0\\ k \text{ dispari}}}^{p} b^k a^{p-k}(-1)^{\frac{k-1}{2}} i \binom{p}{k}}_{\text{intero} \cdot i}$$

$k = 2m+1$

$i^k = i(-1)^m$

$$= x+i$$

i

$$\sum_{\substack{k=0\\ k \text{ dispari}}}^{p} b^k (-1)^{\frac{k-1}{2}} a^{p-k}\binom{p}{k} = 1$$

$$= \underbrace{b a^{p-1}\binom{p}{1} - b^3 a^{p-3}\binom{p}{3} + \dots}_{\text{divid...}} + \underbrace{b^p(-1)^{\frac{p-1}{2}}}_{=1} = 1$$

$b = \pm 1$

$$b^p(-1)^{\frac{p-1}{2}} = 1 \quad \begin{cases} (-1)^{\frac{p-2}{2}} \\ -(-1)^{\frac{p-2}{2}} \end{cases}$$

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

$b = \dots$

$\pm \quad \underbrace{\overbrace{a^{p-1}\binom{p}{1} \pm a^{p-3}\Big(\qquad}} \pm \overbrace{a^2\binom{p}{2}} = 0$

$p \mid a \qquad v_p(a^2) < v_p(\dots)$

a deve essere pari

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

ci vuole $\quad v_2\binom{p}{k} \geq v_2\binom{p}{2} - 1$

$\dfrac{p(p-1)\dots(p-k+1)}{k!} \qquad \dfrac{p(p-1)}{2} \qquad$ se $p \equiv 3 \pmod 4$ ✓

$$\boxed{\begin{gathered} v_2\binom{p}{k+2} \geq v_2\binom{p}{k} - 2 \\ v_2\left(a^{k+2}\binom{p}{k+2}\right) \geq v_2\left(\binom{p}{k} a^k\right) \\ \frac{p \dots (p-k-1)}{} \\ v_2(p-k-1)(p-k) + 2 \geq v_2(k+1)(k+2) \end{gathered}}$$

$\dots \qquad ? \qquad$:(

Trovare tutte le soluzioni a

$2^n = x^2 + 7y^2$ $\qquad x, y$ dispari

$8 = 1+7 \rightsquigarrow \alpha$

$16 = 9 + 7 \cdot 1 \rightsquigarrow \beta$

$32 = 25 + 7 \cdot 1$

$2^n = (x + \sqrt{-7}\,y)(x - \sqrt{-7}\,y) = N(x + \sqrt{-7}\,y)$

per quale n $\quad 2^n = N(\alpha)$ con $\alpha \in \mathbb{Z}[\sqrt{-7}]$?
α non divisibile per 2

$8 = N(\alpha)$ $\qquad \cancel{64} = N(\alpha^2)$ $\qquad \alpha = 1 + \sqrt{7}$

$2^7 = 16 \cdot 8 = N(\alpha \cdot \beta)$

$2^n = N(\gamma) \Rightarrow 2^{n+3} = N(\alpha \cdot \gamma)$

Abbiamo ms. l'ex per induzione a patto

di dimostrare che $2 \mid \alpha \cdot \gamma$

$\alpha = 1 + \sqrt{-7}$ $\qquad \gamma = a + b\sqrt{-7}$

$\alpha\gamma = (a - 7b) + (a+b)\sqrt{-7}$

$2^{n+3} = N(\alpha\gamma)$ $\qquad N\left(\frac{\alpha\gamma}{2}\right) = \frac{2^{n+3}}{4} = 2^{n+1}$

$\nexists \; \frac{\alpha\gamma}{2} = \gamma \; \frac{\sqrt{-7}+1}{2}$

$$A = \mathbb{Z}[\sqrt{-7}] \subseteq B = \mathbb{Z}\left[\frac{\sqrt{-7}+1}{2}\right] = \mathbb{Z}[\omega]$$

$$x + y\sqrt{-7} \in B \qquad y = \frac{b}{2}, \quad x = a + \frac{b}{2}$$

Scopo: $\quad \cdot\ \alpha \in B \qquad \alpha = a + b\omega = x + y\sqrt{-7}$

$\cdot\ \alpha\bar{\alpha} = 2^n$

$\cdot\ \alpha \in A \qquad 2 \mid b \qquad a \nmid b$

$$\omega = \frac{1+\sqrt{-7}}{2} \qquad (1+\sqrt{-7})(1-\sqrt{-7}) = 8$$

$$2\omega \quad 2\bar{\omega} = 8$$

$$\omega\bar{\omega} = 2$$

$$\alpha\bar{\alpha} = 2^m = \omega^n \bar{\omega}^n$$

$$\mathbb{Z}[\omega]^\times = ?$$

$$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) =$$

$$= a^2 + b^2 \underset{2}{\omega\bar{\omega}} + ab\,\underset{\frac{1+\sqrt{-7}}{2} + \frac{1-\sqrt{-7}}{2} = 1}{(\omega+\bar{\omega})}$$

$$= a^2 + 2b^2 + ab = \left(a + \frac{b}{2}\right)^2 + b^2\left(1 + \frac{3}{4}\right) = 1$$

$\Rightarrow a = \pm 1, \quad b = 0 \qquad a + b\omega = \pm 1$

$$\alpha\bar{\alpha} = \omega^n \bar{\omega}^n$$

$$\alpha = \omega^a \bar{\omega}^b \qquad \alpha = \pm \omega^a \bar{\omega}^b$$

$\alpha\bar\alpha = \omega^a\bar\omega^b\,\bar\omega^a\omega^b = (\omega\bar\omega)^{a+b}$.

$a+b=n$

$\omega^a\bar\omega^b = \qquad (\omega\bar\omega)^2 = 4 \mid \alpha \quad$ in B

$a, b \geq 2 \quad$ No

$\alpha = 4\beta = 2(2\beta) = 2$ (un mult in $\mathbb{Z}[\sqrt{-7}]$)

$\beta \in B \qquad 2\beta \in A$

$a = \pm\omega^n, \ \pm\omega^{n-1}\bar\omega, \ \pm\bar\omega^{n-1}\omega, \ \pm\bar\omega^n$

$\omega^n \qquad \omega^3 = \left(\frac{1+\sqrt{-7}}{2}\right)^3 =$

$\frac{1+(-7)\sqrt{-7}+3\sqrt{-7}-7\cdot 3}{8} = \frac{-20+4\sqrt{7}}{8} \notin A$

Guess $\omega^n \notin B$

$\Downarrow$

$\omega^n = a_n + b_n\omega \qquad b_n \equiv 1 \pmod 2$

Dim $\times$ induzione: $a_n \equiv 0 \quad b_n \equiv 1 \pmod 2$

$\omega^{n+1} = (a_n + b_n\omega)\omega = a_n\omega + b_n\omega^2 = *$

$\omega^2 = ? \qquad \omega^2 - (\omega+\bar\omega)\omega + \omega\cdot\bar\omega = 0$

$\omega^2 - \omega + 2 = 0 \qquad \omega^2 = \omega - 2$

$* \quad a_n\omega - 2b_n + b_n\omega =$

$\Rightarrow a_{n+1} = -2b_n \qquad b_{n+1} = a_n + b_n$

$= \omega^n \qquad \pm \bar{\omega}^n \not\in A$

$n \geq 2$

$$\bar{\omega}\omega^{n-1} = (\omega\bar{\omega})\,\omega^{n-2} = 2\,\omega^{n-2}$$

$$\bar{\omega}\,\omega^{n-1} \in A \setminus 2A$$

$\pm \bar{\omega}\cdot\omega^{n-1}$ è una soluzione al nostro problema

$\pm\, \omega\, \bar{\omega}^{n-1}$

$\forall n \geq 2 \qquad \omega\bar{\omega} = 2$

$x^2 + 7y^2$

$$\left\{\begin{array}{l} \omega\,\bar{\omega}^{n-1} = x + y\sqrt{-7} \\ \bar{\omega}\,\omega^{n-1} = x - y\sqrt{-7} \end{array}\right.$$

$$x = \bar{\omega}^{n-2} + \omega^{n-2}$$

Consolazione della faccina $\frown \to \smile$

$$v_2\left[\binom{p}{2} a^2\right] < v_2\left[\binom{p}{2k} a^{2k}\right]$$

$$v_2\ \frac{p(p-1)}{2}\, a^2 \ \lneq\ v_2\left[\frac{p\cdots(p-2k+1)}{2k!}\, a^{2k}\right] = \binom{p-2}{2k-2}\frac{p(p-1)}{2k(2k-1)}\, a^{2k}$$

$\geq$

$$V_2\left(\frac{p(p-1)}{2k(2k-1)}\, a^{2k}\right)$$

$$\geq$$

$$V_2\left(\underbrace{p(p-1)}_{u}\, a^2\right) + V_2\left(\frac{a^{2k-2}}{k}\right)$$

Hope: $V_2\left(\dfrac{a^{2k-2}}{k}\right) > 0$

$$\geq$$

$$V_2\left(\frac{2^{2k-2}}{k}\right) > 0$$

$y^2 + 2 = x^3$ $\leftarrow$ Esercizio

Eq. di Pell

$x^2 - Dy^2 = 1$ $\qquad x, y \in \mathbb{Z}$ $\qquad D > 0$, $D \neq \square$

$(x + \sqrt{D}\, y)(x - \sqrt{D}\, y) = 1$

$\cancel{x} + y\sqrt{D} \in \mathbb{Z}[D]^\times$

$x^2 - \varepsilon y^2 = 1$ $\qquad g - \varepsilon = 1$

Se u è unità di $\mathbb{Z}[\sqrt{D}]$ anche u^n è unità $\forall n$

Se $u, v \in \mathbb{Z}[\sqrt{D}]^\times \longrightarrow u \cdot v \in \mathbb{Z}[\sqrt{D}]^\times$

1) Esistono unità non banali

2) Che struttura ha $\mathbb{Z}[\sqrt{D}]^\times$

È vero che sono tutte della forma $\pm u_0^n$ per una certa u_0?

1) Risp.: Sì

2) Risp: Sì

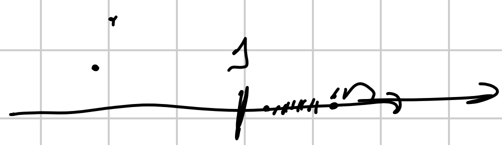
$$\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{R}$$

$\alpha \in \mathbb{Z}[\sqrt{D}]$ $\quad |\alpha|$

Definisco u_0 = minimo tra $\{ u \in \mathbb{Z}[\sqrt{D}]^\times : u > 1 \}$

$u = a + b\sqrt{D}$ $\quad u > 1$

$\frac{\Delta}{u_0}$ $\quad a - b\sqrt{D}$



$u > \sqrt{D} > 1$

$u_n \ \forall \ \alpha$

$\frac{u_n}{u_{n+1}} > 1$ $\qquad \frac{u_n}{u_{n+1}} = v < \sqrt{D}$

$\searrow 1$

u_0

$u = \pm u_0^n$? uno tra $\pm u$ $\quad \pm u^{-1}$ è > 1

per assurdo $\qquad u > 1 \qquad u > u_0$

$\exists n \qquad u_0^n \leq u < u_0^{n+1}$

Se $u_0^n < u \qquad u_0 > \frac{u}{u_0^n} > 1$ ✓

Per dimostrare la 1) cerchiamo di giocare con le divisibilità in $\mathbb{Z}[\sqrt{D}]$

$u_0 > 1$

$\alpha \quad N(\alpha) = M \qquad \alpha, \alpha u_0, \alpha u_0^2$

- Idea vado in cerca di ∞ $\alpha_n \in \mathbb{Z}[\sqrt{D}]$

a) che hanno tutti la stessa norma

b) se 2 di questi si dividono a vicenda per finito

$\alpha = \beta\gamma \qquad \beta = \alpha\delta = \beta\gamma\delta \qquad \Rightarrow \delta\gamma = 1$

Per il passo a) dimostro che $\exists$ ∞ ele di $\mathbb{Z}[\sqrt{D}]$ $N(\alpha) \leq 2\sqrt{D}+1$

$\alpha = a + b\sqrt{D} \qquad N(\alpha) = a^2 - Db^2 < cost$

$\Leftrightarrow \frac{a^2}{b^2} - D < \frac{cost}{b^2}$

$\frac{a}{b}$ approssima bene $\sqrt{D}$

Lemma (Teo di Dirichlet)

ogni irrazionale α ammette ∞ $\frac{p}{q}$ (p, q coprimi)

t.c. $\left| \frac{p}{q} - \alpha \right| \leq \frac{1}{q^2}$

Dim FATTA DA POL ☺

$$\left| \frac{p}{q} - \sqrt{D} \right| < \frac{1}{q^2} \Longrightarrow \frac{p}{q} < \sqrt{D} + 1$$

$$\frac{p^2}{q^2} - D = \left(\frac{p}{q} - \sqrt{D} \right) \left(\frac{p}{q} + \sqrt{D} \right) \leq \frac{1}{q^2} \left(2\sqrt{D} + 1 \right)$$

$$p^2 - D q^2 \leq 2\sqrt{D} + 1$$

$\Longrightarrow$ troviamo infinite α_n : $N(\alpha_n) = M$

M costante $< 2\sqrt{D} + 1$

$$\alpha_n = a_n + b_n \sqrt{D} \qquad m \text{ e } n$$

$$a_n \equiv a_m \pmod{M}$$

$$b_n \equiv b_m \pmod{M}$$

$\exists\ \alpha, \beta$ t.c. $N(\alpha) = N(\beta) = M$

$\alpha - \beta$ è divisibile per M

$$\alpha \equiv \beta \ (M)$$

$$\beta = \alpha + M\gamma$$

$$\bar{\beta} = \bar{\alpha} + M\bar{\gamma} = \bar{\alpha} + M\bar{\gamma}$$

$$\frac{\alpha}{\beta} = \frac{\alpha\bar\beta}{\beta\bar\beta} = \frac{\alpha\bar\beta}{\alpha\bar\alpha} = \frac{\alpha\bar\beta}{n} = \frac{\alpha\bar\alpha + n\bar\gamma\alpha}{n}$$

$$= 1 + \bar\gamma\alpha \in \mathbb{Z}[\sqrt{D}]$$

$\beta \mid \alpha \qquad \alpha \mid \beta$

$\Longrightarrow \exists$ una unità non banale in $\mathbb{Z}[\sqrt{D}]$

- $x^2 - y^2 D = n$

$\alpha = x + y\sqrt{D} \qquad \alpha_1, \dots, \alpha_k$ t.c.

tutte le soluzioni sono del tipo

$\alpha_i\, u_0^n$

$\alpha > 0 \qquad \alpha\, u_0^n \qquad n \in \mathbb{Z}$

$\{1, u_0\}$

$(x, y) \qquad \frac{x}{y} \quad \hat{=} \quad ,$