TEORIA DEI NUMERI 2 MEDIUM (DARKCRYSTAL)

Titolo nota 05/09/2015

SOMME DI QUADRATI (& ancora residui)

a è RQ mod p $\iff$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

Cor: -1 è RQ mod p $\iff$ $p \equiv 1 \pmod 4$
$p = 2$

Lemma: a, b interi, $p \mid a^2 + b^2$ e $p \equiv 3 \pmod 4$

Allora $p \mid a$ E $p \mid b$

Dim Se $p \mid a$ FINE, quindi supponiamo $p \nmid a$.

L'ipotesi è $a^2 \equiv -b^2 \pmod p$

$\iff -1 \equiv (b \cdot a^{-1})^2 \bmod p$

Ma questo è impossibile (perché $p \equiv 3 \bmod 4$) ⊗

Oss Supponiamo $x^2 \equiv -1 \bmod p$. (*)

$\operatorname{ord}_p(x) = 4 \mid p-1$

perché $x^4 \equiv 1 \pmod p$, quindi ord $\mid 4$, ma

ord $\neq 2$ ($\neq 1$) per (*)

Primi $\equiv 1 \mod 4$

$5 = 2^2 + 1^2$ ma $5 \nmid 2$, $5 \nmid 1$

Fatto Se $p \equiv 1 \mod 4$, $\exists$ a e b t.c. $p = a^2 + b^2$

Dim Per induzione: siano $p_1, p_2, \dots$ i primi $\equiv 1\ (4)$. $p_1 = 5 = 1^2 + 2^2$

Sia p il prossimo primo $\equiv 1\ (4)$

Esiste $c \in \mathbb{N}$ t.c. $p \mid c^2 + 1$, perché -1 è RQ.
$\left(0 \le c \le \frac{p-1}{2}\right)$

$0 < c^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + 1 < p^2$, quindi

$$c^2 + 1 = Kp \quad \text{con } K < p$$

Idea Passare da $m^2 + n^2 = Kp$ a $(m')^2 + (n')^2 = K'p$ con $K' < K$ (se $K \ge 2$)

Come si scrive: prendo K minimo per cui esistono $m, n \in \mathbb{N}_{>0}$ t.c. $m^2 + n^2 = Kp$

Identità $(x^2+y^2)(z^2+w^2) = (xz - yw)^2 + (xw + yz)^2$

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

Sia q un divisore primo di K $\left(q \le K < p\right)$

- se $q \equiv 3\ (4)$, $q \mid m, n$ quindi

$$\left(\frac{m}{q}\right)^2 + \left(\frac{n}{q}\right)^2 = \left(\frac{K}{q^2}\right) \cdot p,$$

assurdo perché k era minimo possibile

- se $q \equiv 1 \ (4)$ o $q = 2$. Per hp. induttiva

$$q = a^2 + b^2$$

Partiamo da $\dfrac{m^2+n^2}{a^2+b^2} = \left(\dfrac{k}{a^2+b^2}\right) p$

$$m^2+n^2 = N(m+ni) \qquad a^2+b^2 = N(a+bi)$$

$$\frac{m+ni}{a+bi} = \frac{(m+ni)(a-bi)}{a^2+b^2} = \frac{(am+bn)+i(an-bm)}{a^2+b^2}$$

↓ Norme

$$\frac{m^2+n^2}{a^2+b^2} = \frac{(am+bn)^2+(an-bm)^2}{q^2} =$$

$$= \left(\frac{am+bn}{q}\right)^2 + \left(\frac{an-bm}{q}\right)^2$$

Basta mostrare che $\dfrac{am+bn}{q}$ e $\dfrac{an-bm}{q}$ sono interi.

- $q = a^2+b^2$ divide m^2+n^2, e possiamo supporre $q \nmid m$, $q \nmid n$ (e $q \neq 2$)

$m^2 \equiv -n^2 \ (q)$, cioè $m \equiv (\pm)\alpha n \ (q)$, dove $\pm\alpha$ sono le radici quadrate di -1 mod q

- $q \mid a^2+b^2 \implies b \equiv \pm\alpha a \ (q)$ (1)

Tesi: $\frac{am+bn}{q}$ intero e $\frac{an-bm}{q} \in \mathbb{Z}$

$$am+bn \equiv a\cdot \alpha n + bn \equiv n(b+\alpha a) \quad (2)$$

Cambiando b in $-b$, possiamo supporre (1) che $b \equiv -\alpha a \pmod q$, quindi $(2) \equiv 0 (q)$

$$an - bm \equiv an + \alpha a m \equiv a(n+\alpha m)$$

$$\equiv a\alpha(m+\alpha^{-1}n)$$

$$\equiv a\alpha(m-\alpha n) \equiv 0 \quad (q)$$

$$\alpha^2 \equiv -1 \pmod q \implies \alpha \equiv -\alpha^{-1} \quad (q)$$ ☒

Simbolo di Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è Res. Quad mod } p \\ -1 & \text{se } a \text{ NON è R. Q. mod } p \\ 0 & \text{se } p \mid a \end{cases}$$

Se $a, b \not\equiv 0 \pmod p$, abbiamo

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

(Eulero)

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

$$\Rightarrow \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Esempio Modulo $p \neq 2,3$ almeno uno tra 2, 3 e 6 è un quadrato: se $\left(\frac{2}{p}\right) = -1$ e $\left(\frac{3}{p}\right) = -1$, allora

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = +1 \quad (\text{cioè } 6 \equiv \square \ (p))$$

Esempio X^4+1 è irriduc / $\mathbb{Q}$ ma riducibile mod p per ogni p.

- X^4+1 è irrid / $\mathbb{Q}$ (è ciclotomico)
- $X^4+1 = \left(X - \frac{1+i}{\sqrt{2}}\right)\left(X - \frac{1-i}{\sqrt{2}}\right)\left(X - \frac{-1+i}{\sqrt{2}}\right)\left(X - \frac{-1-i}{\sqrt{2}}\right)$

$$X^4+1 = (X^2+i)(X^2-i)$$

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

$$= (X^2-1+\sqrt{2}\,i\,X)(X^2-1-\sqrt{2}\,i\,X)$$

Oss: uno tra -1, 2 e -2 è un RQ mod p

$p = 5$ $\quad 2^2 \equiv -1 \ (5)$ $\quad$ " $\quad i \equiv 2 \ (5)$ "

$$X^4 + 1 = (X^2 + 2)(X^2 - 2) \mod 5$$

Se p è t.c. $\left(\frac{-1}{p}\right) = 1$, sia $a \in \mathbb{N}$ t.c. $a^2 \equiv -1 \ (p)$.

Allora $\quad X^4 + 1 \equiv (X^2 + a)(X^2 - a) \mod p$

RECIPROCITÀ QUADRATICA

p, q primi dispari. Allora

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

In soldoni: • se $p \equiv 1\ (4)$ o $q \equiv 1\ (4)$ abbiamo

p quadrato mod q $\iff$ q quadrato mod p

• se invece $p \equiv q \equiv 3\ (4)$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

$$\left(\frac{17}{347}\right) = \left(\frac{347}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$$

$$= -\left(\frac{7}{3}\right) = -1$$

$$\left(\frac{10}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{5}{7}\right)$$

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

Dim

$$\begin{aligned} 1 &\equiv (-1)(-1) \quad (p) \\ 2 &\equiv (2)(-1)^2 \quad (p) \\ 3 &\equiv (-3)(-1)^3 \quad , \\ &\vdots \quad \vdots \\ s := \tfrac{p-1}{2} &\equiv \left((-1)^{s-1} s\right)(-1)^s \quad (p) \end{aligned}$$

$$s! \equiv (-1)(2)(-3) \cdots (\pm s)\ (-1)^{s(s+1)/2}$$

$$\frac{p-1}{2}! \equiv (2)(4)(6)\cdots(p-1)\cdot(-1)^{\frac{p(p+1)}{2}} \pmod p$$

$$\equiv 2^{\frac{p-1}{2}}\cdot(1\cdot 2\cdot\ldots\cdot\tfrac{p-1}{2})\cdot(-1)^{(p^2-1)/8} \pmod p$$

$$\equiv 2^{\frac{p-1}{2}}\cdot\tfrac{p-1}{2}!\cdot(-1)^{(p^2-1)/8} \pmod p$$

$$\left(\frac{2}{p}\right) \equiv (2)^{\frac{p-1}{2}} \equiv (-1)^{(p^2-1)/8} \pmod p$$ ∎

Esercizio $2b^2+3 \mid a^2-2$

Soluzione • Idea 1: $2b^2+3 \equiv \begin{cases} 5 \pmod 8 \\ 3 \pmod 8 \end{cases}$

$\Rightarrow \exists\, p \mid 2b^2+3, \quad p \equiv \pm 3 \pmod 8$

Assurdo, perché $a^2 \equiv 2 \ (p) \Rightarrow \left(\frac{2}{p}\right) = +1$

$\Rightarrow p \equiv \pm 1 \pmod 8$

• Idea 2: $\forall p \mid 2b^2+3, \quad \left(\frac{2}{p}\right) = 1$

$p \mid 2b^2+3 \iff 2b^2 \equiv -3 \ (p)$

$\iff (2b)^2 \equiv -6 \ (p)$

$\iff \left(\frac{-6}{p}\right) = 1$

$$\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) \Rightarrow \left(\frac{-3}{p}\right) = 1$$

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$$ ("perché -3 è un primo $\equiv 1 \pmod 4$")

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$$

$$= \left(\frac{p}{3}\right) \implies p \equiv 1 \ (3)$$

In generale: se $q \equiv 3 \ (4)$, $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$

Assurdo: ogni primo che divide $2b^2+3$ è $\equiv 1 \ (3)$,

ma $2b^2 + 3 \equiv 2 \mod 3$

Esempio Calcoliamo $\sum_{n \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1-3n^2}{p}\right) \pmod p$

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} (1-3n^2)^{\frac{p-1}{2}} \equiv \sum_{n \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{p-1}{2}\right)(-3n^2) + \underset{\text{ROBE}}{\cdots} + (-3n^2)^{\frac{p-1}{2}}\right)$$

$$\overset{\text{LEMMONE}}{\equiv} \sum_{n \in \mathbb{Z}/p\mathbb{Z}} (-3)^{\frac{p-1}{2}} n^{p-1} \equiv -\left(\frac{-3}{p}\right) \mod p$$

Ex (ADVANCED) $p > 100$, $r \in \mathbb{N}$. Allora $\exists a, b \in \mathbb{N}$

t.c. $r \equiv a^2 + b^5 \mod p$

Idea: tesi $\iff \exists b$ t.c. $\left(\frac{r-b^5}{p}\right) = +1$

Calcolare $\sum_{b=0}^{p-1} \left(\frac{r-b^5}{p}\right)$

e mostrare che è $\not\equiv 0 \mod p$

IMO SL (2006)

$$\frac{x^7-1}{x-1} = y^5 - 1 \qquad x \geq 2 \qquad y \in \mathbb{N}$$

Soluzione Sia p un divisore di $\frac{x^7-1}{x-1}$.

Claim: se $p \mid x-1$, allora $p = 7$

Dim: sta nel guadagno di un primo. Comunque,

$$v_p(x^7-1) \overset{LTE}{=} v_p(x-1) + v_p(7)$$

$$v_p\left(\frac{x^7-1}{x-1}\right) = v_p(7) \quad e^{\text{c}} \neq 0 \text{ solo se } p=7$$

Per $p=2$: se $x \equiv 1 \ (4)$, $v_2(x^7-1) = v_2(x-1) + v_2(7)$

$$\Downarrow$$

$$v_2\left(\frac{x^7-1}{x-1}\right) = 0$$

Altrimenti $x \equiv 3 \ (4)$, $x^7 \equiv 3 \ (4)$, quindi

$$v_2(x^7-1) = 1 \qquad v_2(x-1) = 1$$

$$v_2\left(\frac{x^7-1}{x-1}\right) = 0$$

$$x^7 - 1 = (x-1)(x^6 + x^5 + \dots + 1)$$

Claim Se $p \mid x^7 - 1$ ma non $x - 1$, allora

$$\text{ord}_p(x) = 7 \mid p - 1$$

Dim: $x^7 \equiv 1 \pmod p$, quindi $\text{ord}_p(x) \mid 7$, quindi

o $\boxed{\text{ord}_p(x) = 1}$ o $\text{ord}_p(x) = 7$ (SI)

$\Downarrow$

$x \equiv 1 \pmod p$ contro l'ipotesi (NO)

FATTO I fattori primi di $\frac{a^p - 1}{a - 1}$ sono o uguali

a p o $\equiv 1 \pmod p$

$$\frac{x^7 - 1}{x - 1} = \boxed{(y - 1)}\boxed{(y^4 + y^3 + y^2 + y + 1)}$$

che valori può assumere mod 7?
Soltanto 0 o 1

che valori assume mod 7?
0 o 1

Cioè: $y \equiv 1, 2 \mod 7$

Ma $1^4 + 1^3 + 1^2 + 1^1 + 1 \equiv 5 \mod 7$

e $2^4 + 2^3 + 2^2 + 2^1 + 1 \equiv 3 \mod 7$

contraddizione!

NON CI SONO SOLUZIONI

ESERCIZIO $b^a \mid a^b - 1$

Soluzione • Studiare $v_p(a^b - 1)$

• soluzioni piccole: $a = 1$, b qualunque
$b = 1$, $a = 2$
$b = 2$, $a = 3$

• Applichiamo LTE(?) NO: non sappiamo che $p \mid a - 1$.

Idea: se $d = \text{ord}_b(a)$, posso applicare LTE a

$$(a^d)^{b/d} - 1$$

• $\text{ord}_p(a) \mid (b, p-1)$

Riflesso condizionato da Senior basic: prendo p il PIÙ PICCOLO PRIMO

Per questo p, $(b, p-1) = 1$ e quindi $a \equiv 1 \ (p)$

$$v_p(a^b - 1) = v_p(a - 1) + v_p(b)$$

IV

$$v_p(b^a) = a\, v_p(b)$$

$$\Rightarrow \quad v_p(b) \cdot (a-1) \leq v_p(a-1) < (a-1)$$

Puzza di assurdo! Cosa può andare storto?

• $a = 1$ $\quad (v_p(a-1) = 0)$ ✓

- non esiste p, cioè $b = 1$ ✓
- magari la disug. è vera! no, non succede
- $p = 2$, non posso (proprio...) usare LTE
  b è pari

Uso LTE per $p = 2$

$$v_2(b^a) \leq v_2(a^b - 1) = v_2\left((a^2)^{b/2} - 1\right)$$

$v_2(b)$ $= v_2(a^2 - 1) + v_2(b/2)$

$= v_2(a^2 - 1) + v_2(b) - 1$

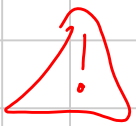
$$v_2(b) \cdot (a-1) + 1 \leq v_2(a^2 - 1)$$

$$\Downarrow$$

$$2^{1 + v_2(b)(a-1)} \leq 2^{v_2(a^2-1)} \leq a^2 - 1$$

- Se $v_2(b) \geq 2$, $LHS = 2^{2a-1} \leq a^2 - 1$ MAI
- Quindi $v_2(b) = 1$, $2^a \leq a^2 - 1$, che è vera solo per $a = 3$

Quindi ci siamo ridotti a $b^3 \mid 3^b - 1$



Achtung: NON abbiamo dimostrato che $b = 2$!

Guardo (di nuovo) $\text{ord}_b(3)$, anzi $\text{ord}_p(3)$ dove p è un eventuale divisore dispari di b.

$$\text{ord}_p(3) \mid (b, p-1)$$

Se scelgo p minimo, $(b, p-1) = 2$, cioè

$$3^2 \equiv 1 \mod p$$
$$8 \equiv 0 \mod p$$

che è improbabile per p dispari.

Quindi b è una potenza di 2 (non ha divisori dispari), quindi $b = 2^{v_2(b)} = 2$.

IMO 2000) Esiste $n \in \mathbb{N}$ t.c. $n \mid 2^n+1$ e n ha esattamente 2000 divisori primi distinti.

Soluzione $n=3$ divide 2^n+1

$$9 \mid 2^3+1 \mid 2^9+1 = 513 = 9 \cdot 57 = 27 \cdot 19$$

Oss: $v_3\left(2^9+1\right) = v_3(2+1) + v_3(9) = 3$

$n = 9 \cdot 19$ funziona: $9 \cdot 19 \mid 2^9+1 \mid 2^{9 \cdot 19}+1$

Sia p_3 un fattore primo di $2^{9 \cdot 19}+1$ diverso da 3 e da 19 (esiste per guadagno di un primo)

Allora $n_3 = 9 \cdot 19 \cdot p_3$ funziona:

$$9 \cdot 19 \cdot p_3 \mid 2^{9 \cdot 19}+1 \mid 2^{9 \cdot 19 \cdot p_3}+1$$

Iterazione: se ho costruito n_k, $2^{n_k}+1$ ha un fattore primo "nuovo" (p_{k+1}) e pongo $n_{k+1} = n_k \cdot p_{k+1}$. n_{2000} funziona.

PUTNAM QUALCOSA Sia $n \in \mathbb{N}$ e $p \in \left(n, \frac{4n+2}{3}\right]$. ($p$ primo)

Allora $p \mid \sum_{j=0}^{n} \binom{n}{j}^4$

Oss. $\sum_{j=0}^{n} \binom{n}{j}^2 = \binom{2n}{n}$. Tutti i primi nell'intervallo $(n, 2n]$ dividono questa somma

Soluzione

Scriviamo $p = n+k$ con $k \geq 1$

$k=3$

$$\binom{p-k}{j} \equiv \frac{(p-k)(p-k-1)\cdots(p-k-j+1)}{j!}$$

$$\equiv \frac{(-k)(-k-1)\cdots(-k-j+1)}{j!} \quad (p)$$

$$\equiv (\pm 1)\frac{(k+j-1)\cdots(k+1)(k)}{j!} \quad (p)$$

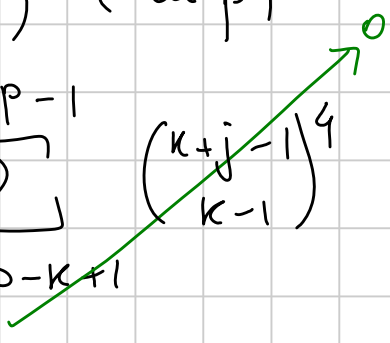
$$\equiv (\pm 1)\binom{k+j-1}{j} \mod p$$

$$\equiv (\pm 1)\binom{k+j-1}{k-1} \mod p$$

Quindi:

$$\sum_{j=0}^{n}\binom{n}{j}^4 \equiv \sum_{j=0}^{n=p-k}\binom{k+j-1}{k-1}^4 \pmod p$$

$$\equiv \sum_{j=0}^{p-1}\binom{k+j-1}{k-1}^4 - \sum_{j=p-k+1}^{p-1}\binom{k+j-1}{k-1}^4$$



$$\equiv \sum_{j=0}^{p-1} \underbrace{\binom{k+j-1}{k-1}^4}_{Q(j)}$$

$$\deg Q(j) = 4(k-1) \overset{?}{\leq} p-1 = n+k-1$$

$$\Leftrightarrow \quad (k-1) < n/3$$

$$\Leftrightarrow \quad p-1 < 4n/3$$

$$\Leftrightarrow \quad p \leq \frac{4n+2}{3}$$

□

Es (test iniziale)

$p_1, \dots, p_{2015}$ primi distinti > 100

Sia $\sum_{i=1}^{2015} \frac{1}{p_i^6 + 1} = a/b$ con $(a,b) = 1$

Sia $c = b a^5$. Calcola $16^c \bmod 29$.

$\| \; 2^{4c}$

Domanda: $c \bmod 7$ $\quad c \equiv b a^5 \equiv b/a$,

quindi basta $a/b \bmod 7 \equiv \sum_{i=1}^{2015} \frac{1}{2} \equiv$

$\equiv 4 \cdot 2015 \equiv 3$

$c \equiv b/a \equiv 5 \; (7)$ $\quad$ Risposta: $2^{20} \bmod 29$

$\|\|$

23

Interi di Gauss

$$\mathbb{Z}[i] = \{ m + i \cdot n \mid m, n \in \mathbb{Z} \}$$

$2+3i \in \mathbb{Z}[i]$

Domanda: $2+3i$ divide 13? Sì, perché

$$13 = (2+3i)(2-3i)$$

Divisibilità: $a+bi$ divide $c+di$ se esiste $e+fi$ tale che $c+di = (a+bi)(e+fi)$

$$\frac{13}{2+3i} = \frac{13(2-3i)}{(2+3i)(2-3i)} = \frac{13(2-3i)}{4+9} = 2-3i$$

Primi (di Gauss) $p = m+ni$ è primo se vale una (e quindi entrambe) tra:

- se $p \mid a \cdot b$ allora $p \mid a$ oppure $p \mid b$
- se $p = a \cdot b$ allora o a o b è invertibile

(in soldoni: uno tra a e b è $\pm 1, \pm i$)

⚠ 13 non è un primo di Gauss! Infatti

$$13 = (2+3i)(2-3i)$$

⚠⚠ 2 non è un primo di Gauss

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

TEOREMA (FATTORIZZAZIONE UNICA)

$\forall n \in \mathbb{Z}[i]$ esistono primi (di Gauss) $p_1, \dots, p_k$, esponenti $e_1, \dots, e_k$, e un invertibile u tali che $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$

(unità)

e questa scrittura è (essenzialmente) unica: se $u_1 p_1^{e_1} \cdots p_k^{e_k} = u_2 q_1^{f_1} \cdots q_k^{f_k}$, allora (a meno di permutare) $e_1 = f_1, \dots, e_k = f_k$,

$p_1 = v_1 q_1, \dots, p_k = v_k q_k$ con v_i unità.

Esempio $13 = (2+3i)(2-3i) = -i(-3+2i)(2-3i)$

differiscono per i (che è un'unità)

Esercizio $2+3i$ è primo. (e $2-3i$ anche)

Supponiamo che $2+3i = (a+bi)(c+di)$.

$2-3i = (a-bi)(c-di)$

$13 = (a^2+b^2)(c^2+d^2)$

Siccome 13 è primo (in $\mathbb{Z}$), $a^2+b^2 = 1$, cioè $a+bi \in \{1, -1, i, -i\}$

Definizione $N(a+bi) = a^2+b^2$

Conseguenza Se $N(a+bi)$ è un primo (in $\mathbb{Z}$),

allora $a+bi$ è primo (in $\mathbb{Z}[i]$)

Fatto 3 è un primo di Gauss (ma $N(3)=9$)

Dim $3 = (a+bi)(c+di)$

$9 = (a^2+b^2)(c^2+d^2)$ ← Norma

Wlog $3 \mid a^2+b^2$. Ma allora $3 \mid a$, $3 \mid b$, quindi $9 \mid a^2+b^2$, quindi $c^2+d^2=1$, cioè $c+di$ è un'unità

Teorema I primi di Gauss sono:

- i primi (di $\mathbb{Z}$) congrui a 3 mod 4
- gli $a+bi$ t.c. $N(a+bi)$ è un primo di $\mathbb{Z}$ (necess. $=2$, o $\equiv 1 (4)$)

Conseguenza della fattorizzazione unica

Sia $p \equiv 1 (4)$. Sappiamo che $\exists\, c \in \mathbb{N}$ t.c. $p \mid c^2+1$

Negli interi di Gauss, $p \mid (c+i)(c-i)$ ma

$p \nmid c+i$ e $p \nmid c-i$

(Infatti: $p \mid c+i$ vuol dire che Re e Im di $\frac{c+i}{p}$ sono intere, il che è falso)

Cioè p non è primo di Gauss, quindi non è irriducibile: $p = (a+bi)(c+di)$

Prendo le norme: $p^2 = (a^2+b^2)(c^2+d^2)$, dove $a^2+b^2 \neq 1$ e $c^2+d^2 \neq 1$, perché $a+bi$ e $c+di$ non sono unità.

$$\Rightarrow \boxed{a^2+b^2 = p}$$

Unità: se u è invertibile sia v l'inverso

$$1 = u \cdot v$$

$$1 = N(1) = N(u \cdot v) = N(u) \cdot N(v)$$

$$\Rightarrow N(u) = 1 \Rightarrow u \in \{\pm 1, \pm i\}$$

Esempio In quali modi si può scrivere 65 come somma di quadrati?

$$65 = 13 \cdot 5 = (2+3i)(2-3i)(2+i)(2-i)$$

$$a^2+b^2 = N(a+bi) = 65$$

$$a+bi = p_1^{e_1} \cdots p_k^{e_k}$$

$$65 = a^2+b^2 = N(p_1)^{e_1} \cdots N(p_k)^{e_k}$$

$e_1 = 1$, $e_k = 1$

$N(p_1) = 5$, $N(p_k) = 13$

$$a+bi \in \{ (2+3i)(2+i),\ (2+3i)(2-i),\ (2-3i)(2+i),\ (2-3i)(2-i) \}$$

$$= \{ 1+8i,\ 7+4i,\ 7-4i,\ 1-8i \}$$

CATALAN DEI POVERI

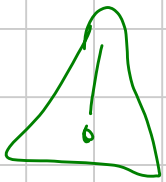
Risolvere $x^2+1 = y^n$ (NO SOLUZIONI) tranne $x=0$

Dimostrazione $(x+i)(x-i) = y^n$

Oss preliminari
- basta fare il caso $n = p$ primo
- $p=2$ $\quad 1 = (y-x)(y+x)$
- Parità di x e y? Modulo 4 $\Rightarrow$ x pari e y è dispari

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

$$= \gcd(x+i, 2)$$



Tentazione → $= 1$, perché $\frac{x+i}{2} \notin \mathbb{Z}[i]$

ma questo è come dire $(15, 6) = 1$ perché $15/6$ non è intero

$$= \gcd(x+i, (1+i)^2)$$

Oss: $1+i$ è primo, perché $N(1+i) = 2$

Voglio dimostrare che $(x+i, 1+i) = 1$, cioè che nessun primo divide entrambi.

$$(x+i, 1+i) = (x-1, 1+i) = \begin{cases} 1+i \\ 1 \end{cases}$$

Domanda: $1+i \mid x-1$?

Se sì, $(X-1) = (1+i)(a+bi)$

$\downarrow N$

$(X-1)^2 = 2\cdot(a^2+b^2)$,

assurdo modulo 2 (x è pari)

$(X+i)(X-i) = y^p \Rightarrow \quad X+i = u(a+bi)^p$

$X-i = \bar{u}(a-bi)^p$

Oss: ogni unità è una potenza p-esima

$$\left[ab = y^3 \qquad a = c^3 \quad b = d^3 \right.$$
$$\left. a = -c^3 \rightsquigarrow \quad a = (-c)^3 \right]$$

1 ok $\qquad -1 = (-1)^p \qquad i = (\pm i)^p$

$-i = (\mp i)^p$

Quindi $X+i = (a+bi)^p$ per qualche $a, b \in \mathbb{Z}$

$$X+i = a^p + p\cdot a^{p-1} bi + \binom{p}{2} a^{p-2}(bi)^2 + \dots + (bi)^p$$

Considerando Im, $1 = b$ (un sacco di roba)

$\Rightarrow \quad b = \pm 1$

$$(a+bi)^3 = a^3 + 3a^2 bi + 3a(bi)^2 + (bi)^3$$
$$= (a^3 - 3ab^2) + ib(3a^2 - b^2)$$

$3a^2 - 1 = 1$

Se prendo Im e poi modulo p, ottengo

$$1 \equiv \frac{1}{i}(bi)^p \pmod p$$

$$\equiv b^p \cdot i^{p-1}$$

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

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

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

$$X + i = (a \pm i)^p \xrightarrow{N} X^2 + 1 = (a^2+1)^p$$

$\Rightarrow a$ pari

Prendiamo di nuovo la parte immaginaria:

$$1 = \mathrm{Im}\left(\sum_{j=0}^{p} \binom{p}{j} a^j (\pm i)^{p-j}\right)$$

$$= \sum_{\substack{j=0 \\ j \text{ pari}}}^{p} \binom{p}{j} a^j (\pm i)^{p-j-1}$$

Hope: magari non torna per congruenze modulo 2^k.

$$\cancel{1} = \cancel{1} + \sum_{\substack{k=1 \\ j=2k}}^{\frac{p-1}{2}} \binom{p}{2k} a^{2k} (\pm i)^{p-1-2k}$$

Claim: $v_2\left(\binom{p}{2k} a^{2k}\right) > v_2\left(\binom{p}{2} a^2\right) \quad \forall k > 1$

Oss 1: wlog $v_2(a) = 1$ (caso peggiore)

Oss 2: $$v_2\left(\binom{p}{2} a^2\right) = v_2\left(\frac{p(p-1)}{2}\right) + 2$$

$$= v_2(p-1) + 1$$

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

$$\geq 2k + v_2(p-1) - 1 - v_2(k)$$

Disug. da dimostrare:

$$2k + v_2(p-1) - 1 - v_2(k) > v_2(p-1) + 1$$

$$2(k-1) > v_2(k)$$

Basta $k < 2^{2(k-1)}$ vera $\forall k \geq 2$

∎