Teoria dei Numeri

Note Title 9/5/2016

Medium 2

Troleito br00tal

$\mathbb{Z}[i]$ ← INTERI DI GAUSS

$a+ib$ CON $a,b \in \mathbb{Z}$ $(i^2=-1)$

$+, \cdot$ EREDITATI DA $\mathbb{C}$

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$

$$(a+ib)\cdot(c+id) = (ac-bd)+i(bc+ad)$$

$(ib)\cdot(id) = -bd$

$\mathbb{Z}[i]$ AMMETTE UNA STRUTTURA LEGATA AI PRIMI (MOLTIPLICATIVA) MOLTO SIMILE A QUELLA DI $\mathbb{Z}$.

$\mathbb{Z}$: FATTORIZZAZIONE UNICA A MENO DEL $\pm$

$\mathbb{Z}[i]$: FATTORIZZAZIONE UNICA A MENO DI $\pm 1, \pm i$

EL. INVERTIBILI: POSSO SCRIVERE $1 = ab$ CON

$a \in \{1, -1, i, -i\}$

$1 \cdot 1 = 1 \quad (-1)\cdot(-1) = 1 \quad i \cdot (-i) = 1$

$(-i) \cdot i = 1$

QUALI SONO I PRIMI DI $\mathbb{Z}[i]$?

$$N(a+ib) = a^2+b^2 \in \mathbb{N}$$

$$N\big((a+ib)(c+id)\big) =$$

$$N\big((ac-bd)+i(ad+bc)\big) =$$

$$= (ac-bd)^2 + (ad+bc)^2 =$$

$$= a^2c^2 + b^2d^2 - 2abcd +$$

$$+ a^2d^2 + b^2c^2 + 2abcd =$$

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

$$= N(a+ib)\cdot N(c+id)$$

LA NORMA N È MOLTIPLICATIVA.

Th. (CHE NON DIMOSTRIAMO)

IN $\mathbb{Z}[i]$ ESISTONO DEI NUMERI PRIMI E OGNI ELEMENTO DI $\mathbb{Z}[i]$ SI SCRIVE IN MODO UNICO (A MENO DI $1, -1, i, -i$) COME PRODOTTO DI TALI PRIMI.

QUALI INTERI POSSONO ESSERE PRIMI IN $\mathbb{Z}[i]$?

QUELLI COMPOSTI NO! PERCHÉ SI POSSONO SCOMPORRE ANCHE IN $\mathbb{Z}[i]$.

CI RESTANO I PRIMI.

Es. $5 = (2+i)(2-i)$

↳ NON È PRIMO

$3 \stackrel{?}{=} (a+ib)(c+id)$

IDEA FURBA: NORMA!

$N(3) = N(a+ib) \cdot N(c+id)$

$9 = (a^2+b^2)(c^2+d^2)$

$1 \quad 0 \quad 3 \quad 0$

FATTO DA EVITARE: $a+ib$ PUÒ ESSERE UN INVERTIBILE

NON VANNO BENE $(1,0)$ $(0,1)$ $(-1,0)$ $(0,-1)$

a^2+b^2 $\begin{cases} 1 \\ 3 \\ 9 \end{cases}$ NO: SAREBBE INVERTIBILE

VORREMMO CHE FOSSE 3

NO: $c^2+d^2=4$

$0\ 1\ 0\ 1$

$a^2+b^2=3$ NON HA SOLUZIONE MODULO 4.

3 È UN PRIMO IN $\mathbb{Z}[i]$

SE $p\equiv 3(4)$ COSA SUCCEDE?

$p=(a+ib)(c+id)$

$\downarrow$ NORMA

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

a^2+b^2 $\begin{cases} 1 & N_0 \\ p & N_0 \pmod 4 \\ p^2 & N_0 \end{cases}$

QUINDI $p\equiv 3(4)$ È PRIMO IN $\mathbb{Z}[i]$

SE $p \equiv 1(4)$

SE $p = a^2 + b^2$ ALLORA

$p = (a+ib)(a-ib) = a^2 + b^2 + \cancel{ab}$

LEMMA OGNI $p \equiv 1(4)$ SI SCRIVE COME SOMMA DI DUE QUADRATI.

SE $p \equiv 1(4)$ $\exists\, k \in \mathbb{Z}$ TALE CHE

$k^2 \equiv -1 (p)$.

CONSIDERIAMO I NUMERI DELLA FORMA

$a + bk$ CON $0 \le a, b \le \lfloor \sqrt{p} \rfloor$ E

$(a,b) \neq (0,0)$

QUANTE SONO? $(\lfloor\sqrt{p}\rfloor+1)^2-1$ → (0,0)

(A LO POSSO PRENDERE IN $1+\lfloor\sqrt{p}\rfloor$ MODI)

b IDEM

SARÀ CIRCA p. ANZI, ALMENO p

$$(\lfloor\sqrt{p}\rfloor+1)^2-1 \overset{?}{\geq} p$$

$$\lfloor\sqrt{p}+1\rfloor \overset{?}{\geq} \sqrt{p+1}$$

p NON È MAI □

p

n^2 $(n+1)^2$

$\lfloor\sqrt{p}\rfloor = n$ $\quad n+1 \overset{?}{\geq} \sqrt{p+1}$

VERA PERCHÉ $p+1 \leq (n+1)^2$ PERCHÉ

$n^2 < p < (n+1)^2$

QUINDI GLI $a+bk$ SONO ALMENO p

CE NE SONO DUE CONGRUI?

(SE FOSSERO $p+1$)

- CE N'È UNO $\equiv 0 \ (p)$
- CE NE SONO $2 \equiv \ (p)$

HO p NUMERI: SE NESSUNO $\equiv 0 (p)$

CI POSSO METTERE SOLO IN $\{1, \dots, p-1\}$:

PIGEONHOLE

$a+kb \equiv 0 \ (p)$ $\qquad$ $k^2 \equiv -1 \ (p)$

$a \equiv -kb \ (p)$ $\qquad$ $a^2 \equiv -b^2 \ (p)$

$p \mid a^2+b^2$

$(a,b) \neq (0,0) \rightarrow a^2+b^2 \neq 0$

$a^2+b^2 <$ $\quad (a, b \leq \lfloor \sqrt{p} \rfloor < \sqrt{p})$

$p+p = 2p \rightarrow a^2+b^2 = p$

$a_1 + b_1 k \equiv a_2 + b_2 k \pmod{p}$

$(a_1 - a_2) \equiv (b_2 - b_1) k \pmod{p}$

$(a_1 - a_2)^2 + (b_2 - b_1)^2 \equiv 0 \pmod{p}$

$a_1 - a_2 \neq 0 \quad o \quad b_2 - b_1 \neq 0$

↳ ALMENO UNA DELLE DUE È VERA, ALTRIMENTI $(a_1, b_1) = (a_2, b_2)$ MA IO AVEVO DUE COPPIE DISTINTE

A PRIORI $b_2 - b_1$ PUÒ ESSERE NEGATIVO

CONSIDERO $|a_2 - a_1|$ E $|b_2 - b_1|$

O $|a_2 - a_1|, |b_2 - b_1| < \sqrt{p}$?

a_2 E b_1 STANNO IN $[0, \sqrt{p})$:

LA DIFFERENZA DEV'ESSERE AL PIÙ LA LORO DISTANZA, DUNQUE $|b_2 - b_1| < \sqrt{p}$

$(|a_2 - a_1|)^2 + (|b_2 - b_1|)^2$ È MULTIPLO DI p, NON È 0, È $< 2p$: È p. □

$p \equiv 1 \pmod 4$ $\quad p = a^2 + b^2 = (a+ib)(a-ib)$

→ NON È PRIMO IN $\mathbb{Z}[i]$

$a+ib$ È PRIMO

$$a+ib = (x_1+iy_1)(x_2+iy_2)$$

$$\downarrow \text{NORMA}$$

$$p = a^2+b^2 = (x_1^2+y_1^2)(x_2^2+y_2^2)$$

$\hookrightarrow$ WLOG È 1:

DUNQUE x_1+iy_1 $\begin{cases} 1 \\ -1 \\ i \\ -i \end{cases}$ $\leftrightarrow$ INVERTIBILE.

IN EFFETTI $a+ib$ È PRIMO

RAGIONEVOLMENTE $a-ib$ È PRIMO

SE $p \equiv 1 \ (4)$, $a+ib$ E $a-ib$ SONO PRIMI ASSOCIATI.

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

$1+i$ E $1-i$ SONO PRIMI DISTINTI:

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

UNICA ECCEZIONE: $1+i$ È LO STESSO PRIMO DI $\overline{1+i} = 1-i$

ALTRIMENTI NO: SONO PRIMI DISTINTI:

$a+ib = \begin{cases} 1\,(a-ib) : & -b = b \to b = 0 \\ i\,(a-ib) : & a = b,\ b = a \\ -1\,(a-ib) & -a = a,\ b = b \\ -i\,(a-ib) & -a = b,\ -b = a \end{cases}$

$a+ib = K(1+i)$

$= K(1-i)$

$K = \pm 1$

SE $K > 1$: $K(1+i) = \underbrace{K \cdot (1+i)}$

NESSUNO INVERTIBILE

- $b=0 \rightarrow a$ È PRIMO

  $\overline{a}=a \rightarrow$ ENTRAMBI PRIMI

  $(a \rightarrow p \equiv 3 \ (4))$

- $a=0 \rightarrow ib$ È PRIMO

  $\downarrow$

  b È PRIMO

ib PRIMO $\leftrightarrow \overline{ib} = -ib$ PRIMO

PERCHÉ $3+4i$ NON È PRIMO

$N(3+4i)=25$ NON È PRIMO

HOPE: $a+ib$ È PRIMO SE E SOLO SE

$N(a+ib) \begin{cases} p^2 & \text{CON } p \equiv 3 \ (4) \\ p & \text{CON } p \equiv 1 \ (4) \end{cases}$

$a^2+b^2 \equiv p^2, \quad p \equiv 3 \ (4)$

Sε $0 < a, b < p$

$a^2+b^2 \equiv 0 \ (p) \to a^2 \equiv -b^2 \ (p)$

$\equiv 1$

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

$(a \cdot b^{-1})^2 \equiv -1 \ (p)$ ΜΑ $p \equiv 3 \ (4)$

Δινω αυτ $(a,b) = (0,p) = (p,0)$

Sε $N(a+ib) = p^2, \quad p \equiv 3 \ (4)$

$a+ib \mid p$

$\equiv -ip$

$N(a+ib) = p \ (\equiv 1 \ (4))$

SE $c+id$ DIVIDE $N(c+id)$ $\Big/$ p

QUINDI $a+ib$ È PRIMO

$$p = a^2+b^2 = c^2+d^2$$

$$p = (a+ib)(a-ib) = (c+id)(c-id)$$

(NON PRIMI)

$$a+ib = \begin{cases} \pm(c+id) \\ \pm i(c+id) \\ \pm(c-id) \\ \pm i(c-id) \end{cases}$$

$a+ib = -ic+d \rightarrow$ $a=b$, $b=-c$

SE $N(a+ib) \neq \begin{cases} p^2 & \equiv 3 \pmod 4 \\ p & \equiv 1 \pmod 4 \end{cases}$

$\Rightarrow$? $\Rightarrow$ ~~$p \equiv 3 \pmod 4$~~

$N(a+ib)$ NON È UN p^2 O UN p

↓

CONE PRODOTTO DI DUE INTERI

$N(a+ib) = q \times$ CON q PRIMO

$(a+ib)$ DIVIDE $q \times$

$(a-ib)$ DIVIDE $q \times$

$$q \times = \prod_{j=1}^{k} (m_j + i n_j)$$

$$a+ib = \prod_{j=1}^{R} (m_j + i n_j)$$

A PRIORI PUÒ ESSERE 1

$$a-ib = \prod_{j=1}^{R} (m_j - i n_j)$$

$$a^2+b^2 = \prod_{j=1}^{R} (m_j^2 + n_j^2) =$$

$$= \prod_{j=1}^{R} (m_j + i n_j)(m_j - i n_j)$$

$$N(a+ib) = qX$$

$$q = \prod_{j=1}^{V_+} (m_j + i n_j) \cdot \prod_{j=1}^{V_-} (m_j - i n_j)$$

$$K = \prod_{j=1}^{U_+} (m_j + i n_j) \cdot \prod_{j=1}^{U_-} (m_j - i n_j)$$

$a+ib$ È PRIMO $\rightarrow$ AL PIÙ 2 PRIMI CHE SONO PROPRIO $a+ib$ E $a-ib$

$a-ib$ È PRIMO

$p \equiv 1 \ (4)$

Ho 2 primi:

$$q = \prod (m + in) = (a+ib)(a-ib)$$

$$a^2 + b^2 = p$$

$$x = \prod (m + in) \rightarrow 0 \text{ primi}$$

I due primi che avevo ($a+ib$ e $a-ib$) stanno in $q \rightarrow x = 1$

$$N(a+ib) = q$$

$p \equiv 3 \ (4)$

1 primo $a+ib$

$$q = \prod (m + in)$$

$$x = \prod (m + in)$$

$a = 0 \vee b = 0$

$q = \pm 1 / \pm i \ (a+ib)$

$x = \pm 1 / \pm i \ (a+ib)$

WLOG $b>0$ $\rightarrow$ $q=\prod(m+in)=$ $m+0$

$x=q$ $\qquad$ $x=\prod(m+in)=$ $=n-0$

$N(n+ib)=xq=q^2$, con $q\equiv 3\ (4)$

ORA ABBIAMO TUTTI I PRIMI $p^2p\equiv 3\ (4)$

$a+ib$ t.c. / $N(a+ib)$ $\qquad$ $p,\ p\equiv 1\ (4)$

TROVARE PER QUALI $(x,y)\in\prod$ VALE

$x^2+y^2=13^2$ $\qquad$ $N(3+2i)\in\mathbb{P}$: non si scompone

$(x+iy)(x-iy)=13^4=(3+2i)^4(3-2i)^4$

$(x+iy)=(3+2i)^{\alpha}(3-2i)^{\beta}$

$(x-iy)=(3+2i)^{4-\alpha}(3-2i)^{4-\beta}$

$$(3-2i)^{\alpha}(3+2i)^{\beta}$$

$$(3-2i)^{\alpha}(3+2i)^{\beta} = (3+2i)^{4-\alpha}(3-2i)^{2-\beta}$$

$$\boxed{\alpha+\beta=4}$$

$$x+iy = (3+2i)^{\alpha}(3-2i)^{4-\alpha}$$

$\alpha = 0, 1, 2, 3, 4$

conviene

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

$\Rightarrow (3+2i)(3-2i)^3$

$$x+iy = (3+2i)^4 = -119+120i$$

$$x+iy = (3+2i)^3(3-2i) = 13(5+12i)$$

$$x+iy = (3+2i)^2(3-2i)^2 = 13^2 = 169$$

Sim. in (a,b)

VIÈTA JUMPING

$$\frac{a^2+b^2+1}{ab} = k$$

a, b INTERI POSITIVI E k INTERO POSITIVO.

DIMOSTRARE CHE $k=3$

$a^2 - kab + b^2 + 1 = 0$

(a,b) È SOLUZIONE

$x^2 - mx + q = 0$ HA α COME SOLUZIONE. L'ALTRA SOLUZIONE È $m - \alpha$ (OPPURE q/α.)

$$a^2 - (kb)\,a + (b^2 + 1) = 0$$

a È SOLUZIONE $\rightarrow$ $kb - a$ È SOLUZIONE

$$(a, b) \longrightarrow (kb - a, b)$$

(b, a)

$$(a, b) \begin{cases} \nearrow (kb - a, b) \\ \searrow (ka - b, a) \end{cases}$$

UNO SPERA CHE SE $a > b$ ALLORA

$Ka - b$ o $Kb - a$ SIANO $< b$ E

> 0.

$$\frac{a^2 + b^2 + 1}{ab} = K$$

$$\frac{(Kb - a)^2 + b^2 + 1}{(Kb - a)\, b} \stackrel{?}{=} \frac{K^2 b^2 - 2Kab + a^2 + b^2 + 1}{Kb^2 - ab} =$$

$$= \frac{K^2 b^2 - Kab}{Kb^2 - ab} + \frac{-Kab + a^2 + b^2 + 1}{Kb^2 - ab}$$

K

$$-Kab + a^2 + b^2 + 1 = 0$$

$$K = \frac{a^2 + b^2 + 1}{ab}$$

(a,b) SOLUZIONE CON $a>b>1$.

QUALI COPPIE RESTANO?

- $b>a$ (SIMMETRIA)
- $a=b$
- $b=1$

$a=b \rightarrow \dfrac{a^2+a^2+1}{a^2} = 2+\dfrac{1}{a^2}$

$a \to 1 \quad \to K=3$

$a=b=1 \to K=3$

$b=1 \to \dfrac{a^2+1+1}{a} = a+\dfrac{2}{a}$

$a=2 \to a=2, b=1, K=3$

$a=1 \to a=1, b=1, K=3$

Con $a > b > 1$

$$a^2 - a(kb) + (b^2+1)$$

$$(a,b) \to (b,\ kb-a)$$

RAPPORTO ✓

$$kb - a \overset{?}{<} b \qquad kb \overset{?}{<} a+b$$

$$\frac{(a^2+b^2+1)b}{ab} \overset{?}{<} a+b$$

$$a^2b + b^3 + b \overset{?}{<} a^2b + ab^2$$

$$b^2 + 1 \overset{?}{<} ab$$

$$1 \overset{?}{<} b(a-b)$$

$1 \le b$; $a - b \ge 1$

PERCHÉ $Kb-a$ NON È NEGATIVO,
ANZI, PERCHÉ È ≥ 1

$$(Kb-a)\cdot a \equiv (b^2+1)$$

LE 2 RADICI DI $x^2 - x(Kb) + (b^2+1)$

$$(a,b) \rightarrow (b, Kb-a)$$

$a > b > 1$ $\quad b > Kb-a \geq 1$ $\quad \geq 1$ $\quad = 1$ ✓

$a > b > 1$

$\downarrow$

$b > Kb-a > 1$

$\downarrow$ VADO AVANTI...

K SI CONSERVA

UNA SUCCESSIONE DI INTERI POSITIVI DECRESCENTE È FINITA: IL MECCANISMO FINISCE QUANDO ARRIVO A 1

QUINDI K DEVE RISOLVERE ALMENO UNA SOL. ESTREMALE $\Rightarrow$ $K = 3$.

QUALI (a, b)?

PASSAGGIO AL CONTRARIO

$(a, b) \rightarrow (b, 3b - a)$

(x, y)

$(3x - y, x)$

RISALIRE È SCEGLIERE FISSANDO L'ALTRA DELLE DUE

ALG. SU $a > b \rightarrow$ SCENDO

ALG. SU $a < b \rightarrow$ SALITO

METTIAMO CHE (a, b) CON $(a < b)$

SCENDA: $(a, b) \rightarrow (b, c)$

SE FACCIO IL PASSAGGIO AL CONTRARIO SU (b, c) SCENDO

$(1,1)$ $(2,1)$

$(y, x) \longrightarrow (3y - x, y)$

$(x_{n+1}, x_n) \longrightarrow (3x_{n+1} - x_n, x_{n+1})$

$x_{n+2} = 3x_{n+1} - x_n$

SI RISOLVE

1 1 2 5 13 34 ...

EQ. DI PELL

$x^2 - dy^2 = 1$ $\quad (x, y)$ INTERI

SE $d = \square \rightarrow (x+\sqrt{d}y)(x-\sqrt{d}y) = 1$

$\downarrow$

$x = 1,\ y = 0$

SE $\oplus x 0$ VABBÈ

$x^2 - dy^2 = 1, \qquad d \neq \square$

CI SONO SEMPRE ∞ SOLUZIONI.

ES.

$2a^2 + 27a + 91 = b^2$

(a/b) SONO INFINITE

$x^2 + x$ HA SENSO SCRITTO COME $\left(x + \frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2$

$2a^2 + 27a + 91 = \frac{1}{2}\left(4a^2 + 54a + 182\right) =$

$= \frac{1}{2}\left(\left(2a + \frac{27}{2}\right)^2 - \frac{1}{4}\right) =$

$$\frac{1}{8}(4a+27)^2 - \frac{1}{8} = b^2$$

$$(4a+27)^2 - 1 = 8b^2$$

$$(4a+27)^2 - 8b^2 = 1$$

$x^2 - 8y^2 = 1$ (SO CHE HA INFINITE SOLUZIONI).

↳ DISPARI

VORREI $x = 4a+27$ ∞ VOLTE

$x \equiv 3 \ (4)$ ∞ VOLTE

$x \equiv 3 \ (4)$ ✓

$x \equiv 1, 3 \ (4)$

$x \equiv 1 (4) \rightarrow -x \equiv 3 (4)$

$x^2 - dy^2 = 1$ HA INFINITE SOLUZIONI!

$(1, 0)$

SUPPONIAMO CI SIA UNA SOL. NON BANALE (a, b).

$$a^2 - d b^2 = 1$$

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

$$\left((a^2 + b^2 d) + (2ab)\sqrt{d} \right) \left((a^2 + b^2 d) - (2ab)(\sqrt{d}) \right) = 1$$

$$(a^2 + b^2 d)^2 - d (2ab)^2 = 1$$

$$(a, b) \to (a^2 + b^2 d, 2ab)$$

MOLTO GROSSA

$(a, b) \quad (x, y) \to (ax + by d, \; bx + ay)$

$(a + b\sqrt{d})(x + y\sqrt{d}) = (ax + by d) + (bx + ay)\sqrt{d}$

$x^2 - 3y^2 = 1 \qquad (2, 1) \qquad (2+\sqrt{3})^n = a + b\sqrt{3}$

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

$$(a+b\sqrt{d})(x+y\sqrt{d}) = u+v\sqrt{d}$$

$$u = ax+bdy$$
$$v = bx+ay$$

$$(ax+bdy)^2 - d(bx+ay)^2 =$$

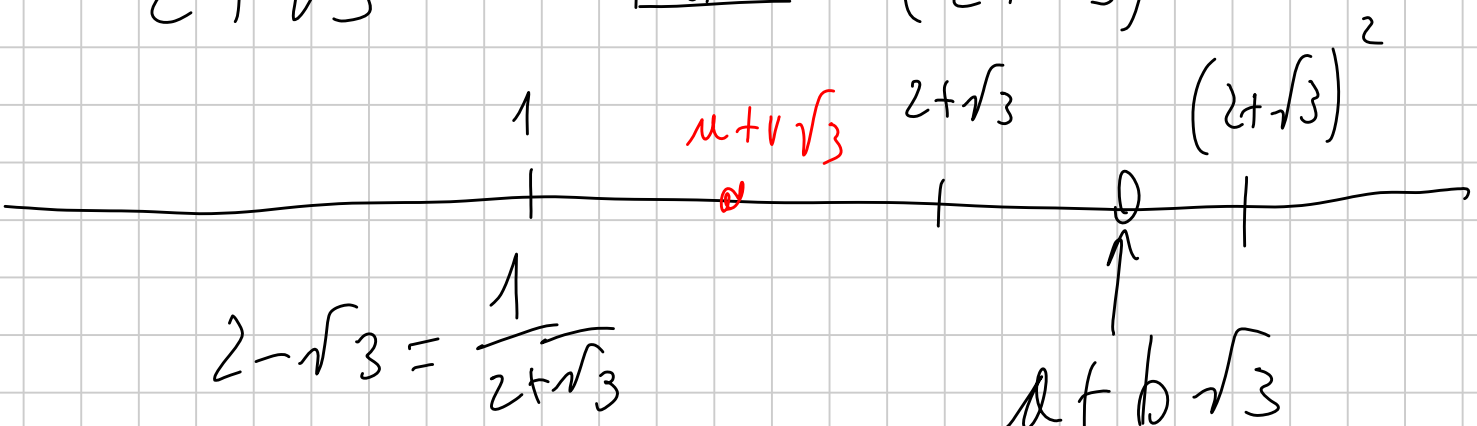
$$= a^2x^2 + 2abdxy - db^2x^2 -$$
$$+b^2y^2d^2 - 2abdxy - da^2y^2 =$$

$$= (a^2 - b^2d)(x^2 - y^2d) = 1$$

$$(a+b\sqrt{d})(x+y\sqrt{d}) = u+v\sqrt{d}$$
$$(a-b\sqrt{d})(x-y\sqrt{d}) = u-v\sqrt{d}$$
$$(a^2-db^2)(x^2-dy^2) = u^2-dv^2$$

$$x^2 - 3y^2 = 1$$

$2+\sqrt{3}$ — Идея: $(2+\sqrt{3})^n$

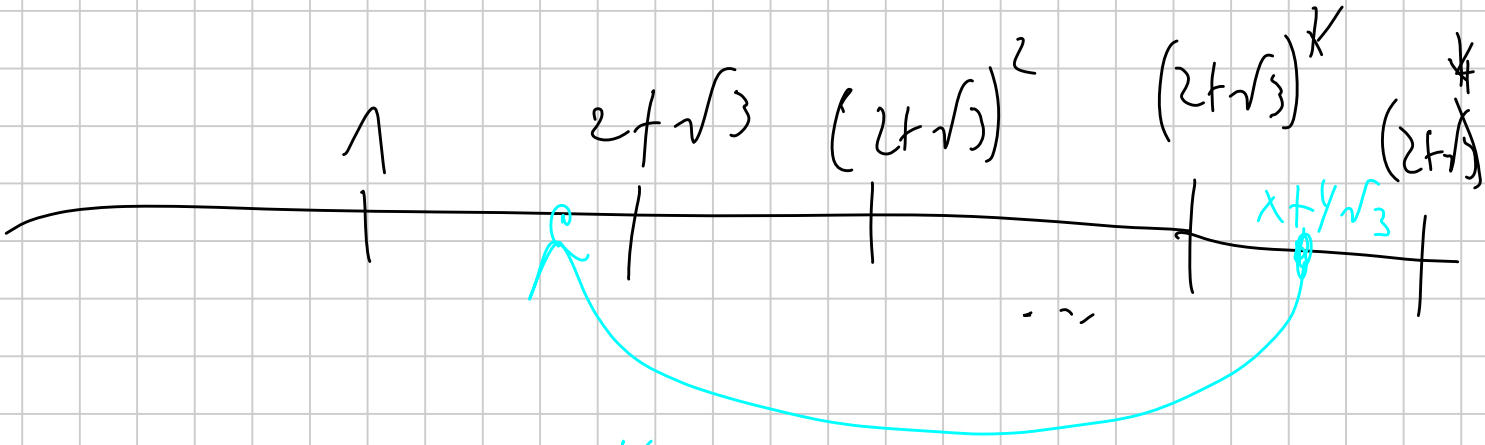


$$2-\sqrt{3} = \frac{1}{2+\sqrt{3}}$$

$$(a+b\sqrt{3})(2-\sqrt{3}) = u+v\sqrt{3}$$

$$(a-b\sqrt{3})(2+\sqrt{3}) = (u-v\sqrt{3})$$

$\|$ $\|$ $\quad u^2-3v^2=1$



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

$$\downarrow$$

$$u^2-3v^2=1$$

$$1 < u + v\sqrt{3} < 2 + \sqrt{3}$$

$$u^2 - 3v^2 = 1$$

$$\| $$

$$(u + v\sqrt{3})(u - v\sqrt{3}) = 1$$

$$2 - \sqrt{3} < u - v\sqrt{3} < 1$$

$$0 < 3 - \sqrt{3} < 2u < 3 + \sqrt{3} < 6$$

$u = 1, 2$

$u = 1 \rightarrow v = 0$

$u = 2 \rightarrow v = \pm 1$

$u = 2 \quad v = -1 \quad 2 - \sqrt{3} < 1$ ASSURÉ

$u = 2 \quad v = 1 \quad 2 + \sqrt{3}$ É

LA SOL. BASE

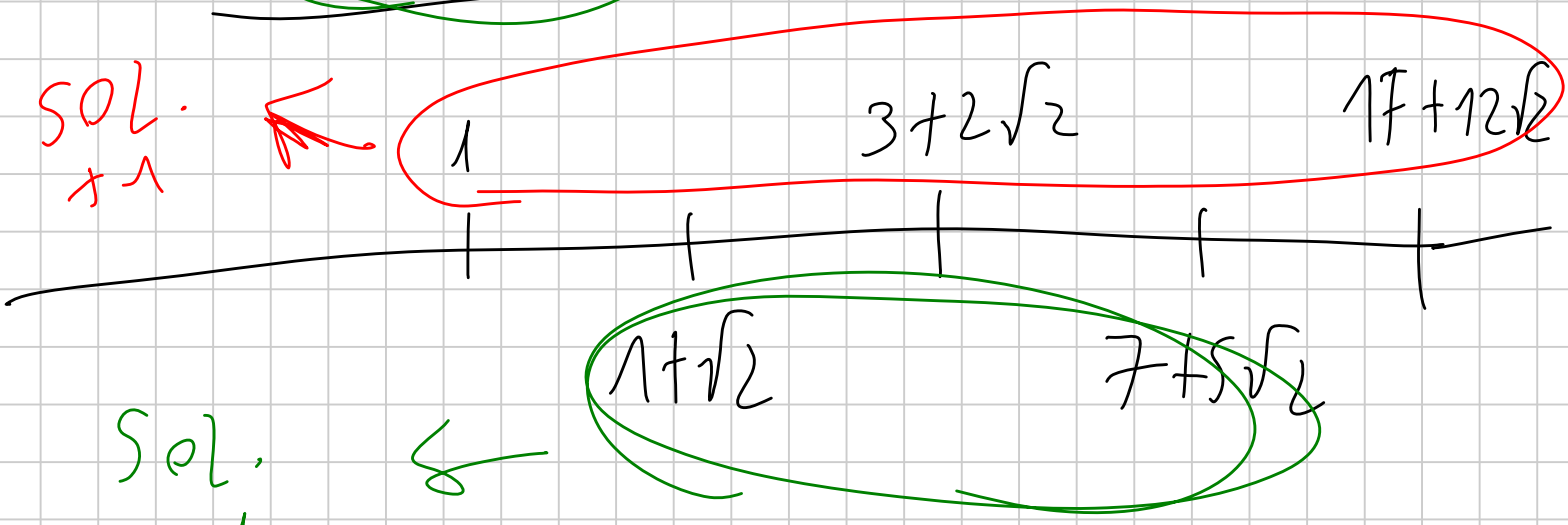
CON $x^2 - dy^2 = -1$ È MOLTO PIÙ PROBLEMATICO CAPIRE COSA SUCCEDE.

$x^2 - 2y^2 = -1$

$x^2 - 2y^2 = 1$

$(1+\sqrt{2})^2$

$3+2\sqrt{2}$



LE SOL. DI $x^2 - dy^2 = 1$ SONO SEMPRE POTENZE DELLA SOL. MINIMA

$x^2 - y^2 d = 1$ HA SOLUZIONE?

SIANO a_1, b_1 t.c. $a_1^2 - b_1^2 d = m$

a_2, b_2 t.c. $a_2^2 - b_2^2 d = m$

$$\frac{(a_1 + b_1\sqrt{d})}{(a_2 + b_2\sqrt{d})} = \frac{(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d})}{m} =$$

$= x \quad m \qquad = y \quad m$

$$\frac{(a_1 a_2 - d\, b_1 b_2) + \sqrt{d}(a_2 b_1 - a_1 b_2)}{m}$$

$$x^2 - d y^2 = ?$$

$$\frac{1}{m^2}\left((a_1 a_2 - d\, b_1 b_2)^2 - d(a_2 b_1 - a_1 b_2)^2 \right) =$$

... CONTI

$$\frac{1}{m^2}\left((a_1^2 - d b_1^2)(a_2^2 - d b_2^2) \right) = 1$$

VOREI CHE m DIVIDESSE

$$a_1 a_2 - d b_1 b_2 \quad \text{E} \quad a_2 b_1 - a_1 b_2$$

SE $a_1 \equiv a_2 \ (m)$ E $b_1 \equiv b_2 \ (m)$

$\Rightarrow$ $a_1^2 - d b_1^2 = m \equiv 0 \ (m)$

$a^2 - d b^2 \equiv 0 \ (m)$

$\equiv 0 \ (m)$

$ab - ab \equiv 0 \ (m)$

PER TROVARE UNA SOLUZIONE A $x^2 - d y^2 = 1$ CE NE BASTANO DUE A $x^2 - d y^2 = m$ CON $x_1 \equiv x_2 \ (m)$ E $y_1 \equiv y_2 \ (m)$.

OSS: SE HO ∞ SOLUZIONI A $x^2 - d y^2 = m$, DI SICURO, TRA LE COPPIE (a, b) DI SOL. MOD m, CE NE SONO 2 UGUALI.

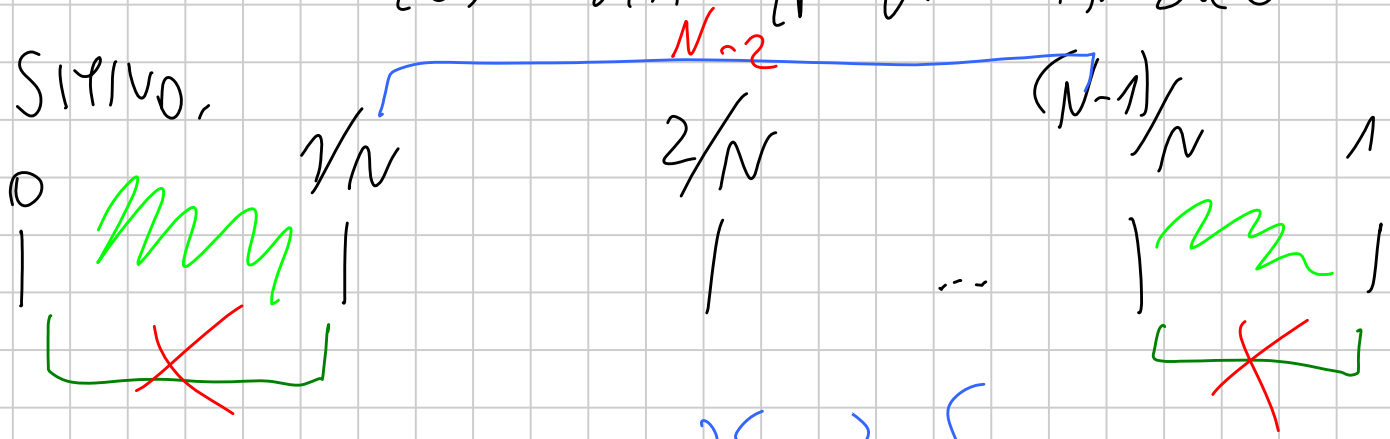
QUINDI O DA VOLERO TROVARE ∞ SOLUZIONI

LEMMA (DIRICHLET)

SIA α UN NUMERO IRRAZIONALE, ALLORA ESISTONO INFINITI INTERI POSITIVI p, q TALI CHE

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

PER DIMOSTRARLO, SIA N UN INTERO POSITIVO.



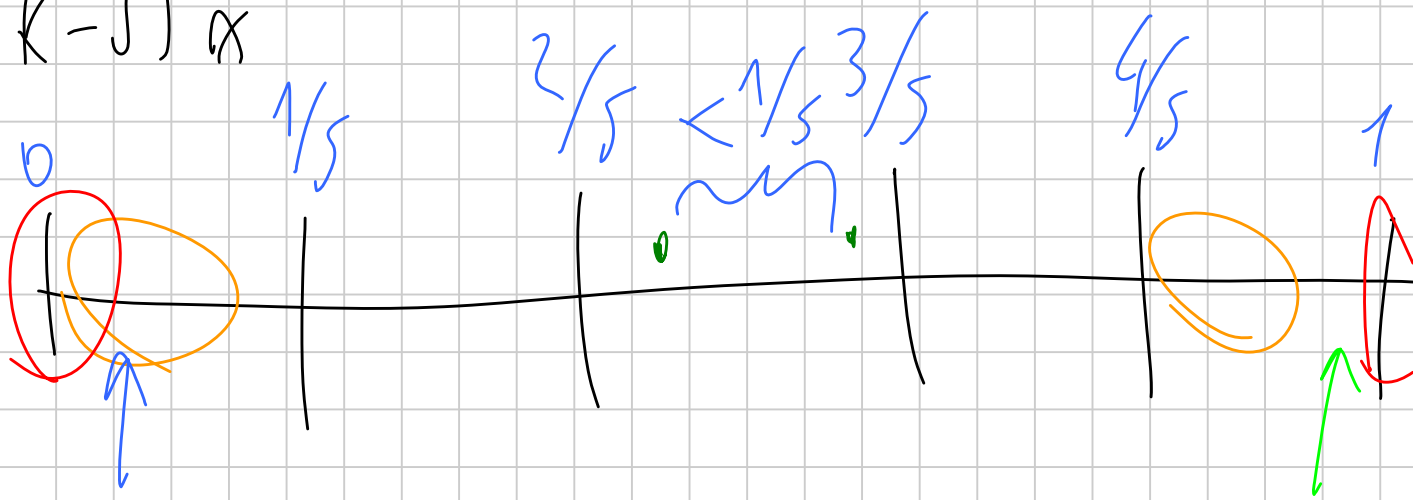
E CONSIDERIAMO $\{\alpha\}, \{2\alpha\}, \ldots, \{(N-1)\alpha\}$

POICHÉ SONO IRRAZIONALI NON SONO i/N

PER PIGEON HOLE DUE SONO NELLO STESSO INTERVALLO. SE $K\alpha$ E $J\alpha$ SONO

NELLO STESSO INTERVALLO $(K > J)$

$(K-J)\alpha$



C'È N' È UNO IN UNO DEGLI

$$|\alpha K - J| \leq \frac{1}{N} \rightarrow \left|\alpha - \frac{J}{K}\right| \leq \frac{1}{NK} <$$

$K < N$

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

$$\left|\alpha - \frac{J}{K}\right| < \frac{1}{NK}$$

SUPPONIAMO CHE GLI K_i, K_j SIANO FINITI. ALLORA

$\left|\alpha - \frac{K_i}{K_j}\right|$ HA UN MINIMO >0 PERCHÉ α È IRRAZIONALE

SE SCELGO N TALE CHE

$\frac{1}{N}$ SIA $<$ DEL MIN

AVREI $\left|K - \frac{k}{K}\right| < \frac{1}{KN} < \min$

ASSURDO

LEMMA SU $\sqrt{d}$

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

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

$$\left(q\sqrt{d} + p\right)\left|q\sqrt{d} - p\right| < \frac{q\sqrt{d} + p}{q}$$

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

$$|p^2 - d q^2| < 2\sqrt{d} + 1$$

INFINITE VOLTE

CI SARANNO A SOL. A $x^2 - dy^2 = m$

CON $|m| < 2\sqrt{d} + 1$

$m \neq 0$ DENNÒ $x^2 = dy^2 \rightarrow d = \square$

QUALCOSA DI ANALITICO

COSA VUOL DIRE CHE UNA SOMMATORIA DI TERMINI POSITIVI DIVERGE? O CONVERGE

$$\sum_{i=1}^{+\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$$

$$\sum_{i=0}^{+\infty} a_i = C \iff$$

$$\forall \varepsilon > 0 \quad \exists N \text{ t.c. } \sum_{i=0}^{N} a_i > C - \varepsilon$$

$$\forall N \quad \sum_{i=0}^{N} a_i \leq C$$

$$\sum_{n=1}^{+\infty} \frac{1}{n}$$ DIVERGE (VA A INFINITO)

$$1 \qquad \geq \frac{1}{2} = \frac{1}{2}$$

$$\frac{1}{2} \quad \frac{1}{3} \qquad \geq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

$$\frac{1}{4} \quad \frac{1}{5} \quad \frac{1}{6} \quad \frac{1}{7} \geq \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}$$

$$\sum_{i=1}^{2^K-1} \frac{1}{i} \geq \frac{K}{2}$$

$$\forall N \quad \exists K \text{ t.c. } \sum_{i=1}^{K} \frac{1}{i} > N$$

CONDENSAZIONE DI CAUCHY

DIVERGE

DATA UNA SUCCESSIONE DEBOLMENTE DECRESCENTE DI REALI POSITIVI $a_1, a_2, \ldots$ ALLORA

$$\sum_{n=1}^{+\infty} a_n \text{ CONVERGE} \iff \sum_{n=1}^{+\infty} 2^{n-1} \cdot a_{2^n} \text{ CONVERGE}$$

1/2 SERIE DI CAUCHY | SERIE NORMALE | SERIE DI CAUCHY

$a_2 \leq a_1 \leq a_1$

$a_4 \leq a_2 \leq a_2$

$a_4 \leq a_3 \leq a_2$

$a_8 \leq a_4 \leq a_4$

$a_8 \leq a_5 \leq a_4$

$a_9 \leq a_6 \leq a_4$

$a_8 \leq a_7 \leq a_4$

$a_{18} \leq a_8 \leq a_8$

SE CONVERGE

SE CONVERGE CONVERGONO TUTTE

LE I CONVERGE

LE I CONVERGE

PERCHÉ

$DX = a_{1+2}SX$

$$\sum_{n=1}^{+\infty} \frac{1}{n^s}$$ CONV. $s>0$

CONV. (SE E SOLO SE $s>1$)

$$\sum_{n=1}^{+\infty} 2^n \cdot \frac{1}{(2^n)^s}$$ CONV.

$$\sum_{n=1}^{+\infty} \left(2^{1-s}\right)^n$$

SE $x<1$

$$\sum_{i=0}^{+\infty} x^i = 1 + x + x^2 + \dots = \lim_{n\to+\infty} \frac{x^n - 1}{x-1} = \frac{1}{1-x}$$

SE $x<1$

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1} = \frac{1-x^{n+1}}{1-x}$$

$$\frac{1}{1-x} \cdot \left(1-x^{n+1}\right) \leftarrow \frac{1}{1-x}$$

VICINO AD 1 QUANTO VOGLIO

$$\sum_{i=0}^{+\infty} x^i \geq \sum_{i=0}^{+\infty} 1 = +\infty \qquad x \geq 1$$

$$\sum_{n=1}^{+\infty} \left(2^{1-s}\right)^n \quad \text{CONV.} \iff 2^{1-s} < 1 \iff s > 1$$

CESENATICO 5, 2014

s È L'INSIEME DEI VALORI CHE ASSUME LO

$$x_1^{2014} + \ldots + x_{2015}^{2014}$$

STESSO VALORE PER DUE 2015-UPLE DISTINTE DI INTERI POSITIVI.

SUPPONIAMO CHE GLI $x_1^{2014} + \ldots + x_{2015}^{2014}$ SIANO TUTTI DIVERSI.

(È UN SOTTOINSIEME DEGLI INTERI POSITIVI)

SE IO CHIAMO S QUESTO INSIEME

(CIOÈ QUELLO DEI VALORI CHE ASSUME)

$$\sum_{n \in S} \frac{1}{n^{(2015/2014)}}$$ CONVERGE PERCHÉ

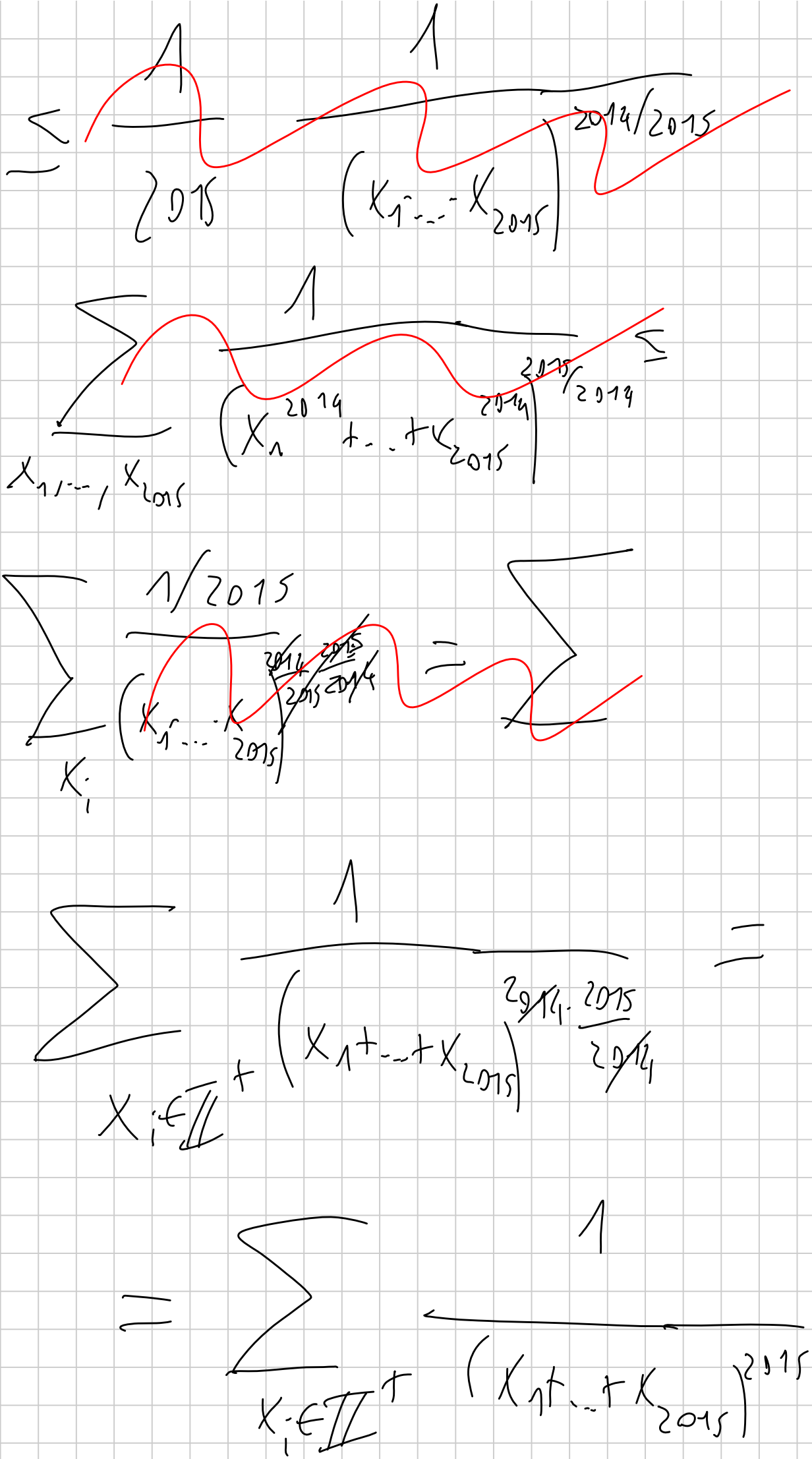
$$\frac{2015}{2014} > 1 \qquad \text{E } S \subseteq \mathbb{N}^+$$

$$\sum_{n \in \mathbb{N}^+} \frac{1}{n^{(2015/2014)}}$$

OGNI $x_1^{2014} + \dots + x_{2015}^{2014}$ APPARE SOLO UNA VOLTA

$$\sum_{n \in S} \frac{1}{n^{\left(\frac{2015}{2014}\right)}} = \sum_{x_1, \dots, x_{2015} \in \mathbb{N}^+} \frac{1}{\left(x_1^{2014} + \dots + x_{2015}^{2014}\right)^{2015/2014}}$$

$$\frac{1}{x_1^{2014} + \dots + x_{2015}^{2014}} \geq \frac{1}{\left(x_1 + \dots + x_{2015}\right)^{2014}}$$



K LO POSSO OTTENERE IN $K_1 + \dots + K_{2015}$ IN

$$\binom{K}{2015} \text{ MODI}$$

$$\sum_{x_i \in \mathbb{Z}^+} \frac{\binom{K-1}{2014}}{K^{2015}}$$

$$\binom{K-1}{2014} \text{ HA GRADO } 2014$$

$$\sum_{x_i \in \mathbb{Z}^+} \frac{\alpha K^{2014} + \text{ROBA}}{K^{2015}} \sim \sum_{K \in \mathbb{Z}^+} \frac{1}{K^{>}}$$

$> +\infty$