Lecture III   K. Conrad.

Factorisation to solve some Diophantine Equations

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

Suppose that $(x,y)=1$ $\left(\Rightarrow (x,z)=1 \text{ and } (y,z)=1\right)$

z is odd   Squares mod 4 : 0 or 1

If z were even then

$$x^2+y^2 \equiv 0 \bmod (4) \Rightarrow x, y \text{ even.}$$

Then $x^2+y^2 \equiv 1 \bmod 4 \Rightarrow$ x or y is even and the other is odd.

Whithout loss of generality, we can assume

x odd, y even $(z$ odd$)$

Write $$x^2 = z^2-y^2 = \underbrace{(z+y)}_{\text{odd}}\underbrace{(z-y)}_{\text{odd}}$$

and factors are relatively prime.

How can $c^2=ab$ with $(a,b)=1$?

then a and b are both squares. ~~[illegible]~~ (up to sign!)

Non example $6^2=(-4)(-9)$

So. $z+y=m^2 \quad z-y=n^2, \quad x^2=m^2n^2$

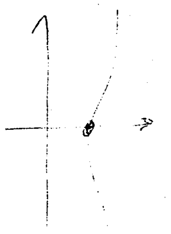
for some $m,n \in \mathbb{Z}$ with $(m,n)=1$.

Then $\quad x=mn, \quad y=\dfrac{m^2-n^2}{2}, \quad z=\dfrac{m^2+n^2}{2}$

Set $k=\dfrac{m+n}{2}, \quad \ell=\dfrac{m-n}{2} \quad (\text{in } \mathbb{Z})$

$x=k^2-\ell^2 \quad y=2k\ell \quad z=k^2+\ell^2$

A new diophantine equation



$y^2=x^3-1 \qquad (1,0)$ integer solutions.

What are $\mathbb{Z}$-solutions?

Since is not a quadratic equation the "geometric" method not work.

Rewrite as $\quad x^3=y^2+1 \; =(y+i)(y-i)$

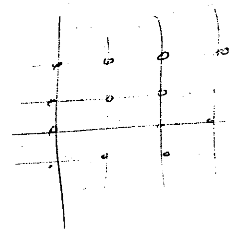
In $\mathbb{Z}$, if $c^3=ab$ with $(a,b)=1$

what can we say?

a,b are both cubes (and since $(-1)=(-1)^3$ not problems with signs)

Q: Are $y+i$ and $y-i$ relatively prime in a suitable sense?

Definition: The Gaussian integers are cpx numbers $a+bi$ with $a,b\in\mathbb{Z}$, noted by $\mathbb{Z}[i]$



Examples of factorizations in $\mathbb{Z}[i]$

$10=(3+i)(3-i)$

$3+4i=(2+i)^2$

In $\mathbb{Z}$ we have trivial factorizations

$n=n\cdot 1=(-n)(-1)$.

In $\mathbb{Z}[i]$ trivial factorizations are

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

Def: We call two gaussian integers relatively prime if their only common factors are $1,-1,i,-i$.

Examples of relatively prime gaussian integers:

Are $1+3i$ and $2+5i$ relatively prime?

<u>Def</u>: The <u>norm</u> of $\alpha = a+bi \in \mathbb{Z}[i]$ is defined by

$$N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$$

<u>Note</u> $N(1+3i) = 10$ $N(2) = 4$

$N(2+5i) = 29$.

<u>Key property</u>: The norm is multiplicative.

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Observe, if δ is a common factor of α and β then $N(\delta)$ divides $N(\alpha)$ and $N(\beta)$ <u>in $\mathbb{Z}$</u>.

<u>Ex</u> $1+3i$ and $2+5i$ are relatively prime in $\mathbb{Z}[i]$.

(since $N(\delta) / 10$, $N(\delta) / 29$ $\Rightarrow N(\delta) = 1 \Rightarrow \delta = 1,-1,i,-i$)

$\therefore$ Their only common factors are $1,-1,i,-i$.

So $N(\alpha), N(\beta)$ relatively prime $\Rightarrow \alpha, \beta$ relatively prime.

<u>Warning</u>! If $N(\alpha)$ and $N(\beta)$ are not relatively prime then it does not mean α and β are not rela. prime.

<u>Ex</u> $1+2i$, $1-2i$ have norms 5.

But, if $\delta / (1+2i)$ and $\delta / 1-2i$

then $N(\delta) = 1, 5$

If $N(\delta) = 5$ there are 8 numbers

$\{1+2i, 1-2i, 2+i, 2-i, -1+2i, -1-2i, -2+i, -2-i\}$

One can find that (checking)

$1+2i$ is divisible by 4 of the numbers

$1-2i$ is divisible by 4 of the numbers

but there is <u>not</u> <u>overlap</u>.

so $1+2i$ and $1-2i$ are relatively prime

(and their norms are not relatively prime)

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

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

Thm: The Gaussian integers $y+i$ and $y-i$ are relatively prime in $\mathbb{Z}[i]$ for any y fitting the equation $y^2 = x^3 - 1$

(Proof) Let $\delta \in \mathbb{Z}[i]$ be a common factor of $y+i$ and $y-i$. Then $N(\delta)$ is a factor of

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

δ is a factor of $2y$ and is a factor of $2i$

$\Rightarrow N(\delta) / 4y^2$ and $N(\delta)/4$ in $\mathbb{Z}$.

Let's show x odd, y even.

If x were even then $y^2 \equiv -1 \bmod 8$
$\equiv 7 \bmod 8$

This is impossible, the squares mod 8 are $0, 1, 4$,

so x is odd. $\Rightarrow y^2 = x^3 - 1$ even $\Rightarrow y$ even.

Since x^3 is odd, $N(\delta) = 1 \Rightarrow \delta = \pm 1$ or $\delta = \pm i$

Note
If it were the case in $\mathbb{Z}[i]$ that $\alpha\beta = \gamma^3$ and α and β being relatively prime $\Rightarrow \alpha$ and β are cubes! (*)

Then, in the example,

$$(y+i) = (m+ni)^3 \quad \text{for some } m, n \in \mathbb{Z}.$$

$$y + i = m^3 + 3m^2 ni - 3mn^2 - n^3 i$$
$$= m(m^2 - 3n^2) + n(3m^2 - n^2) i$$

Thus $y = m(m^2 - 3n^2)$

and $1 = n(3m^2 - n^2)$ in $\mathbb{Z}$

From the 2° equation $n = \pm 1$

$$1 = \pm (3m^2 - 1)$$

$1 = \cancel{3m^2 - 1}$ $\qquad$ $1 = -(3m^2 - 1) \Rightarrow m = 0$
$\Rightarrow y = 0 \Rightarrow x = 1$.

Provided the "note"(*), $(1,0)$ will be the only solution.
(integers)

How can we explain (*)?

In the integers is a consequence of unique factorization.

What does unique factorization look like in $\mathbb{Z}[i]$?

Def: A prime in $\mathbb{Z}[i]$ is any $\pi \in \mathbb{Z}[i]$ that is not 0 or ± 1 or $\pm i$ and its only factors ~~factorizations are~~ $\pm 1, \pm i, \pm \pi, \pm i\pi$.

Theorem: If $N(\alpha) = p$, p prime in $\mathbb{Z}$, then α is a prime in $\mathbb{Z}[i]$.

(proof) $\alpha = \beta\gamma$ $\quad N(\alpha) = p \Rightarrow p = N(\beta)N(\gamma)$

$\Rightarrow N(\beta)$ or $N(\gamma)$ is $1 \Rightarrow \beta$ or γ is ± 1 or $\pm i$

Warning: α can be a prime with $N(\alpha)$ not prime.

Ex: 3 is prime in $\mathbb{Z}[i]$ $\qquad N(3) = 9$

Suppose $3 = \beta\gamma$ with $N(\beta) > 1$, $N(\gamma) > 1$

then $9 = N(\beta)N(\gamma) \Rightarrow N(\beta) = 3 \Rightarrow a^2 + b^2 = 3$

impossible

Theorem

① Every $\alpha \in \mathbb{Z}[i]$ with $N\alpha > 1$ is a product of primes $\alpha = \pi_1 \pi_2 \cdots \pi_r$

② If $\pi_1 \pi_2 \cdots \pi_r = \pi_1' \cdots \pi_s'$ $\quad$ (π_i, π_k' primes)

then $r = s$ and after relabeling

$$\pi_j = u_j \pi_j' \quad \text{with } u_j \in \{1, -1, i, -i\}.$$

Note ② (Hard part).

Example $\quad 5 = (1+2i)(1-2i) = (2+i)(2-i)$

Corollary: If $\alpha\beta = \gamma^n$ in $\mathbb{Z}[i]$ and α and β are relatively primes then $\alpha = u\mu^n$, $\beta = v\lambda^n$ with $u, v \in \{1, -1, i, -i\}$.

III.6

Ex. $(4+3i)\,z = (3+i)^2$

$4+3i = i\,(2-i)^2 \qquad 2 = -i(1+i)^2$

(square up to ~~units~~ $1,-1,i,-i$) $\qquad \left(2 \neq (a+bi)^2,\ a,b\in\mathbb{Z}\right)$

Note ~~[illegible]~~ that with units not problem since $1,-1,i,-i$ are cubes

then $\alpha\beta = \gamma^3$ with α,β coprime implies α,β cubes

here: $\alpha = u\mu^3 = (\tilde{u}\mu)^3$

$u = \pm 1, \pm i \qquad \tilde{u} = \pm 1, \mp i$)