Factorization to Solve Diophantine Equations

$x^2 + y^2 = z^2$

suppose $\gcd(x, y) = 1$

$\Rightarrow \gcd(x, z) = 1$

$\Rightarrow \gcd(y, z) = 1$

z is odd: squares mod 4 : 0, 1

if z were even:

$x^2 + y^2 \equiv 0 \bmod 4$

$\Rightarrow x$ and y are even

$x^2 + y^2 \equiv 1 \bmod 4$

x & y is odd, the other is even.

WLOG

Without loss of generality, we can assume x odd, y even (z odd)

$x^2 = z^2 - y^2$

$= (z + y)(z - y)$ ← factors relatively prime.

($z + y$: odd, >0; $z - y$: odd, >0)

→ How can $e^2 = ab$ in $\mathbb{Z}^+$ with $\gcd(a, b) = 1$

$\Rightarrow a, b = \square$ (squares).

Non Ex: $6^2 = (-4)(-9)$

So $z + y = m^2$, $z - y = n^2$

$x^2 = m^2 n^2$

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

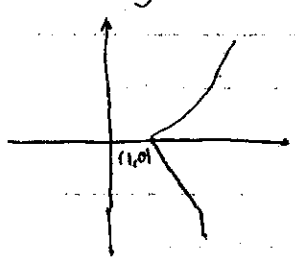
$x = mn$, $y = \frac{m^2 - n^2}{2}$, $z = \frac{m^2 + n^2}{2}$

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

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

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

sol: $(1, 0)$



What are $\mathbb{Z}$ sols?

Rewrite as

$x^3 = y^2 + 1$

$= (y + i)(y - i)$

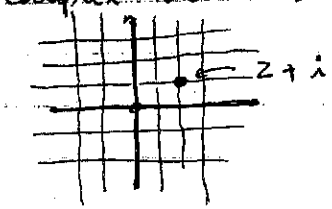
In $\mathbb{Z}$, if $c^3 = ab$ and $\gcd(a, b) = 1$,

what can we say?

a, b are both cubes $\square^3$ (since $-1 = (-1)^3$)

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

Defn: The Gaussian integers are complex numbers $a+bi$ with $a,b \in \mathbb{Z}$ ↖ $\mathbb{Z}[i]$



Factorizations: $10 = (3+i)(3-i)$
in $\mathbb{Z}[i]$ $\quad 3+4i = (2+i)^2$

In $\mathbb{Z}$ we have trivial factorizations
$n = n \cdot 1 = (-n)(-1)$
In $\mathbb{Z}[i]$ trivial factorizations are:
$\alpha = \alpha \cdot 1 = (-\alpha)(-1) = (i\alpha)(-i)$
$= (-i\alpha)(i)$

We call $\alpha, \beta, \in \mathbb{Z}[i]$ relatively prime if their only common factors are $1, -1, i, -i$.

How can we give examples?
→ Are $1+3i$ and $2+5i$ relatively prime?

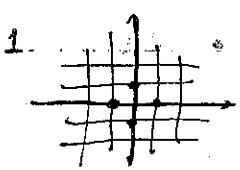
Def: The <u>norm</u> of $\alpha = a+bi \in \mathbb{Z}[i]$ is $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2$

$N(1+3i) = 1^2+3^2 = 10$
$N(2+5i) = 2^2+5^2 = 29$

* $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$
Observe if δ is a common factor of α and β in $\mathbb{Z}[i]$, so $\alpha = \delta\lambda$, $\beta = \delta\mu$ in $\mathbb{Z}[i]$
$\Rightarrow N(\alpha) = N(\delta)\,N(\lambda)$,
$N(\beta) = N(\delta) \cdot N(\mu)$
→ $N(\delta)$ is common factor of $N(\alpha)$, $N(\beta)$ in $\mathbb{Z}$.

If δ is factor of $1+3i$ and $2+5i$ in $\mathbb{Z}[i]$, then $N(\delta)$ is factor of 10 and 29 in $\mathbb{Z}$.
$\Rightarrow N(\delta) = 1$.
$\delta = a+bi$: $a^2+b^2 = 1$.

a	b	δ
1	0	1
-1	0	-1
0	1	i
0	-1	-i



Yes, relatively prime
$N(\alpha) = |\alpha|^2$

If $N\alpha$ and $N\beta$ are not relatively prime then it <u>does not</u> mean α and β are not relatively prime

(5)

Ex: $1+2i$ vs $1-2i$

Norms $= 5$. If $\delta \mid 1+2i$ and $\delta \mid 1-2i$, then $N(\delta) \mid 5$ in $\mathbb{Z} \Rightarrow N(\delta) = 1$ or 5

$\{1+2i, 1-2i, 2+i, 2-i, -1+2i, -1-2i, -2+i, -2-i\}$. $[(N(5) = 25)]$

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

$$x^3 = y^2 + 1 = (y-i)(y+i) \quad \Big\} \text{ assume } x, y \in \mathbb{Z}$$

Theorem: The gaussian integers $y+i$ and $y-i$ are relatively prime in $\mathbb{Z}[i]$.

$N(y+i) = y^2+1 \quad (N\alpha = N\bar{\alpha}) \downarrow$

(for any y fitting the equation above).

Proof:

Let $\delta \in \mathbb{Z}[i]$ be a common factor of $y+i$ and $y-i$

$\delta \mid y+i$ in $\mathbb{Z} \Rightarrow N(\delta) \mid N(y+i) = y^2+1 = x^3$ in $\mathbb{Z}$

$\delta \mid y+i, \delta \mid y-i \Rightarrow \delta \mid 2y$ and $\delta \mid 2i$ in $\mathbb{Z}[i]$

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

(6)

Let's show x odd, y even

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

No! squares mod 8 = 0, 1, 4 mod 8.

So, x odd.

$\Rightarrow y^2 = x^3 - 1 = \text{even}$

$\Rightarrow y$ even.

If it were the case in $\mathbb{Z}[i]$ then $\alpha\beta = \gamma^3$ and α and β being relatively prime: α and β are cubes

$$y + i = (m + ni)^3 \text{ for some } m, n \in \mathbb{Z}$$
$$= m^3 + 3m^2 ni - 3mn^2 - n^3 i$$
$$= m^3 - 3mn^2 + (3m^2 n - n^3) i$$
$$= m(m^2 - 3n^2) + n(3m^2 - n^2) i$$

Thus:

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

and $1 = n(3m^2 - n^2)$

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

integer ↗ $-3m^2 - 1$ or $1 = -(3m^2 - 1) = 1 - 3m^2$

$\Downarrow$

$m = 0$

$\Downarrow$

$y = 0$

$\Downarrow$

$x = 1$

This is (in $\mathbb{Z}$) a consequence of unique factorization.

$ab = c^3$ and $\gcd(a,b) = 1$ $\Rightarrow a, b = \square$ 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's not 0, ± 1, $\pm i$ and its only factors are $\pm 1, \pm i, \pm \pi, \pm i\pi$

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

Proof: write $\alpha = \beta\gamma$; then $p = N\beta \, N\gamma$ in $\mathbb{Z}^+$.

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

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

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

$\Rightarrow 9 = N\beta \, N\gamma$ in $\mathbb{Z}^+$

naw. $\Rightarrow N\beta = 3$

$a^2 + b^2 = 3$

Thm:

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 in $\mathbb{Z}[i]$

$\pi_1 \pi_2 \cdots \pi_r = \pi_1' \cdots \pi_s'$ (π_j, π_k' prime)

then $r = s$ and after relabeling we can say $\pi_j = u_j \pi_j'$ where $u_j = \pm 1$ or $\pm i$

Ex: $5 = (1+2i)(1-2i) = (2+i)(2-i)$

Cor: If $\alpha\beta = \gamma^n$ in $\mathbb{Z}[i]$ and α, β are rel. prime, then $\alpha = u\mu^n$, $\beta = v\lambda^n$ with $u, v \in \{\pm 1, \pm i\}$

Ex: $(4+3i) \cdot 2 = (3+i)^2$

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