Lecture 10: Gaussian Integers, from Stillwell's Elements of Number Theory Chapter 6

Notation $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$

Much the same as $\mathbb{Z}$,

- unique prime factorization
- $x^2+y^2 = (x+iy)(x-iy)$ makes $\mathbb{Z}[i]$ tool to study x^2+y^2.
- we'll see how the existence of Gaussian primes of particular type provide proof of Fermat's theorem: $p>2$ prime then $p = a^2+b^2$ for some $a,b \in \mathbb{N}$ iff $p = 4n+1$ for some $n \in \mathbb{N}$. (2-square th$^{\underline{m}}$ of Fermat)

§6.1 $\mathbb{Z}[i]$ and its norm

Diophantus knew $(a_1^2+b_1^2)(a_2^2+b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2$

we recognize this as $|z_1|^2|z_2|^2 = |z_1z_2|^2$ where $z_1 = a_1+ib_1$ and $z_2 = a_2+ib_2$ (I add squares to distinguish modulus from Stillwell's "norm")

$$\text{norm}(a+ib) = \underbrace{(a+ib)\overline{(a+ib)}}_{\text{(added by me.)}} = a^2+b^2$$

Since $\overline{zw} = \bar{z}\bar{w}$ and $\text{norm}(z) = z\bar{z}$ we find

$$\begin{aligned}\text{norm}(zw) &= zw\overline{zw} \\ &= zw\bar{z}\bar{w} \\ &= z\bar{z}\,w\bar{w} \\ &= \text{norm}(z)\,\text{norm}(w).\end{aligned}$$

Exercises from §6.1: explore concept of units in various contexts. You might find the def$^{\underline{n}}$ of a unit helpful: from pg. 183, a unit is a divisor of 1.

$\mathbb{N}: n \mid 1 \Rightarrow n = 1$

$\mathbb{Z}: x \mid 1 \Rightarrow x = \pm 1$

$\mathbb{Z}[i]: a+ib \mid 1 \Rightarrow a+ib = \pm 1, \pm i$

Comment on units continued

to say $3 \mid 1 \Rightarrow 1 = c3$ for some $c \in \mathbb{Z}[i]$

But $\text{norm}(1) = 1$ and $\text{norm}(1) = \text{norm}(c3)$ yields

$$1 = \text{norm}(c)\,\text{norm}(3) \leftarrow \text{eq}^{\underline{n}} \text{ in } \mathbb{Z}$$

But $\text{norm}(x+iy) = x^2+y^2 \geq 0$ hence

$\text{norm}(c) = \text{norm}(3) = 1$. We find that:

$$\boxed{\text{Th}^{\underline{m}}/\ a+ib \text{ is unit of } \mathbb{Z}[i] \Rightarrow \text{norm}(a+ib) = 1.}$$

In contrast, for $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ we find (by almost same argument)

$\text{norm}(a+b\sqrt{2}) = \pm 1$. But, this norm

is based on ~~nonstand.~~ $x^2 - 2y^2$...

$\text{norm}(a+b\sqrt{2}) = a^2 - 2b^2$ (not necessarily positive)

Units are sol$^{\underline{n}}$'s to $a^2 - 2b^2 = \pm 1$, but this

is Pell's Eq$^{\underline{n}}$ $a^2 - 2b^2 = 1$ or the related $a^2 - 2b^2 = -1$

$\exists\ \infty$ly many sol$^{\underline{n}}$'s ! (oh I've said too much, sorry to ruin your hwk ☺)

§6.2 Divisibility and Primes in $\mathbb{Z}[i]$ and $\mathbb{Z}$

We should remember much of the utility of $\text{norm}(a+ib) = a^2+b^2$ stems from fact $\text{norm}(z) \in \mathbb{Z}$ for $z \in \mathbb{Z}[i]$.

Th^m/ If $\alpha \mid \gamma$ then $\text{norm}(\alpha) \mid \text{norm}(\gamma)$
also.. if $\gamma = \alpha\beta$ then $\text{norm}\,\gamma = \text{norm}\,\alpha\,\text{norm}\,\beta$

Proof: Let $\alpha, \gamma \in \mathbb{Z}[i]$ such that $\alpha \mid \gamma$ then
$\Rightarrow \exists \beta \in \mathbb{Z}[i]$ s.t. $\gamma = \alpha\beta$ hence
$\text{norm}(\gamma) = \text{norm}(\alpha\beta) = \text{norm}(\alpha)\,\text{norm}(\beta)$
But $\text{norm}\,\beta \in \mathbb{Z}$ $\therefore$ $\text{norm}(\alpha) \mid \text{norm}(\gamma)$. //

Def^n/ A Gaussian Prime is an element of $\mathbb{Z}[i]$ which is not a product of Gaussian integers of smaller norm. ($\nexists\, u, v \in \mathbb{Z}[i]$ s.t. $z = uv$ and $\text{norm}(u), \text{norm}(v) < \text{norm}\, z$.
strict.)

① Example: $z = 4+i$ is a Gaussian prime.
$\text{norm}(4+i) = 16+1 = 17$. But 17 is prime in $\mathbb{Z}$ $\Rightarrow$ $4+i = uv$ has
$\text{norm}(4+i) = \text{norm}(u)\,\text{norm}(v) = 17$
$\Rightarrow \text{norm}(u), \text{norm}(v) = 1$ or 17.

② Example: $z = 2$ is not a Gaussian prime since
$2 = (1-i)(1+i)$ yet $\text{norm}(2) = 4$
and $\text{norm}(1 \pm i) = 2$ (both smaller norm than 4).

③ <u>Example</u>: $1-i$, $1+i$ are Gaussian prime factors of 2. Notice $\text{norm}(1\pm i) = 2 \leftarrow$ prime in $\mathbb{Z} \Rightarrow$ cannot nontrivially factor $1\pm i$ in $\mathbb{Z}[i]$ as only divisors of 2 are ± 1 and ± 2 in $\mathbb{Z}$.

Of course, $2 = (1-i)(1+i) = (-1+i)(-1-i)$ etc... we always face this sort of ambiguity due to units $\pm 1, \pm i$ in $\mathbb{Z}[i]$

my comment, Stillwell attends this point later.

Th^m/ <u>PRIME FACTORIZATON in $\mathbb{Z}[i]$</u>. Any Gaussian integer factorizes into Gaussian primes (uniqueness of factorization dealt with in §6.4)

<u>Proof</u>: Let $\gamma \in \mathbb{Z}[i]$ if γ is G. Prime then we're done. otherwise $\gamma = \alpha\beta$ for $\text{norm}(\alpha), \text{norm}\,\beta < \text{norm}(\gamma)$. If $\text{norm}(\alpha)$ or $\text{norm}(\beta)$ is prime $\Rightarrow$ the respective α or β is a G. Prime. Otherwise, if say $\text{norm}(\alpha)$ is composite $\overset{*}{\Rightarrow} \exists\, \alpha_1, \alpha_2$ s.t. $\alpha = \alpha_1\alpha_2$ and $\text{norm}(\alpha) = \text{norm}\,\alpha_1\, \text{norm}\,\alpha_2$. The size of the $\text{norm}(\gamma) > \text{norm}(\alpha), \text{norm}(\beta)$ and $\text{norm}(\alpha) > \text{norm}(\alpha_1), \text{norm}\,\alpha_2$ hence have decreasing seq of $\mathbb{N}$#'s, this must terminate $\Rightarrow \exists\, \alpha_1, .., \alpha_n$ for which $\gamma = \alpha_1\alpha_2 \cdots \alpha_n$ and $\alpha_1, .., \alpha_n$ are G. Primes. //

* actually, how do we <u>know</u> $\exists\, a_1, a_2, b_1, b_2$ s.t. $\alpha = (a_1 + ib_1)(a_2 + ib_2)$ with $\text{norm}\,\alpha_1 = a_1^2 + b_1^2$ etc... why can we be certain such integers exist? if they don't we're done!

§6.3 CONJUGATES

Def^{n}/ If $z = a+bi$ then $\bar{z} = a - bi$ [for $a, b \in \mathbb{R}$ but mostly $a, b \in \mathbb{Z}$ here]

Properties

$$z\bar{z} = |z|^2 = \text{norm}(z)$$

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$$

$$\overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2$$

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$$ -(or $\overline{z_1 \times z_2} = \bar{z}_1 \times \bar{z}_2$ to emphasize how conjugation preserves $\times$)-

Proof: left to reader, but, easy just set $z = a+ib$, $z_1 = a_1 + ib_1$, etc and work it out.//

$\boxed{\text{Th}^{m} \text{ (Real Gaussian Primes) An ordinary prime } p \in \mathbb{N} \text{ is a Gaussian Prime} \iff p \neq a^2+b^2.}$ extends to $-\mathbb{N}$ with ease.

-(also $p<0$ is Gaussian prime $\iff -p \in \mathbb{N}$ is Gaussian prime)-

Proof: $\Leftarrow$] Assume p is not the sum of two squares.
Suppose we have prime $p \in \mathbb{Z}$ that is not a Gaussian prime.
That is, $\exists \gamma \in \mathbb{Z}[i]$ such that $\underline{p = (a+bi)\gamma}_{*}$ with $\text{norm}(a+bi) = a^2+b^2$, $\text{norm}(\gamma) < p^2$. Conjugating $*$ yields,

$$\bar{p} = p = (a-bi)\bar{\gamma}$$

Hence $p^2 = (a+bi)\gamma(a-bi)\bar{\gamma} = (a^2+b^2)|\gamma|^2$
where $a^2+b^2, |\gamma|^2 > 1$. BUT, $p^2 = c_1 c_2 \Rightarrow c_1 = p, c_2 = p$ for $c_1, c_2 > 0$. Thus $p = a^2+b^2$ $\rightarrow\!\leftarrow$ $\therefore \nexists \gamma$ s.t. $p = (a+bi)\gamma$ thus p must be a Gaussian prime if it is an ordinary prime.

$\Rightarrow$] Conversely, if an ordinary prime $p = a^2+b^2$ with $a, b \in \mathbb{Z}$ then p is not a Gaussian prime because $p = (a+ib)(a-ib)$ and $\text{norm}(a \pm ib) = a^2+b^2 = p < p^2 = \text{norm}(p)$.//

- we know that a prime p is Gaussian prime only if $p \neq a^2+b^2$. (Th$^{\underline{m}}$ on pg. 5)

consider, if p is prime and $p = a^2+b^2$ then $p = (a+ib)(a-ib)$. Thus, while p is not a Gaussian prime, it has factors $a \pm ib$ for which $\text{norm}(a \pm ib) = a^2+b^2 = p$.

Th$^{\underline{m}}$/ If $a+ib$ is Gaussian prime then $a-ib$ is Gaussian prime.

Proof: $\S$ $a+ib$ is Gaussian prime and $\S$ $a-ib = \alpha\beta$ for $\text{norm}(\alpha), \text{norm}(\beta) < a^2+b^2$. Observe $\text{norm}\,\alpha = \text{norm}\,\bar{\alpha}$ and $\text{norm}\,\bar{\beta} = \text{norm}\,\beta$ and $a+ib = \overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ with $\text{norm}(\bar{\alpha}), \text{norm}(\bar{\beta}) < a^2+b^2 \Rightarrow a+ib$ not Gaussian prime $\rightarrow\leftarrow$. Hence $a-ib$ is <u>also</u> a Gaussian prime. //

But, do <u>all</u> Gaussian primes appear as part of such a pair with $a+ib$, $a-ib$ and $a^2+b^2 = \text{prime}$? It is conceivable that $a+ib$ is Gaussian prime yet a^2+b^2 is product of several ordinary primes (this is ruled out in next section)

- in §3.7 we saw primes in $4\mathbb{Z}+3$ are <u>not</u> sums of two squares.
- in §6.5 we'll see <u>every</u> prime in $4\mathbb{Z}+1$ <u>is</u> a sum of two squares.

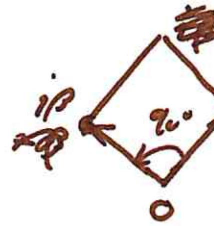
§6.4 Division in $\mathbb{Z}[i]$

You may recall the unique prime factorization of $\mathbb{Z}$ falls on the back of the Euclidean Algo. and hence at the base of things the Division Algorithm. There is also such a construction here in $\mathbb{Z}[i]$,

Thm (Division Property of $\mathbb{Z}[i]$). If $\alpha, \beta \neq 0$ are in $\mathbb{Z}[i]$ then $\exists \mu, \rho \in \mathbb{Z}[i]$ (μ is quotient, ρ is remainder) such that $\alpha = \mu\beta + \rho$ with $|\rho| < |\beta|$

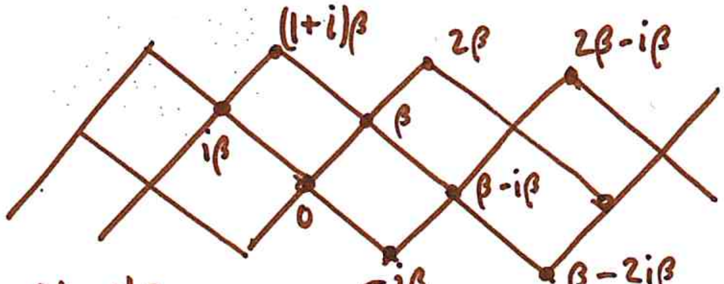
Proof: if $\beta \neq 0$ and $\mu \in \mathbb{Z}[i]$. We argue that $\mu\beta$ fall on square grid in complex plane.

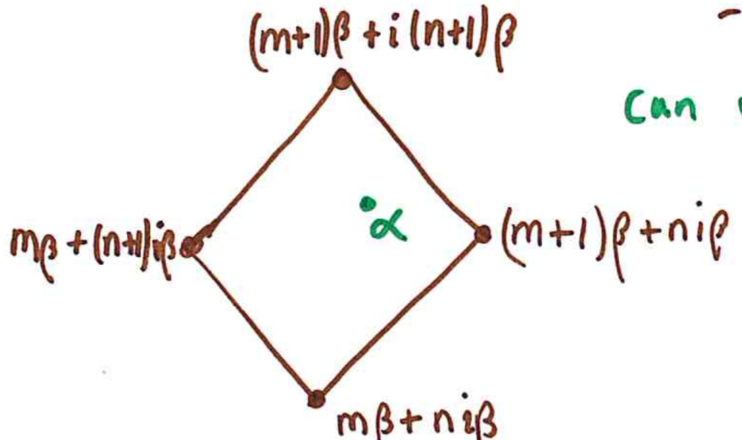
$\beta \longmapsto i\beta$ (rotation by $90°$)



$\beta = a + ib \qquad i\beta = ia - b$

$$\boxed{\underbrace{(c_1 + ic_2)}_{\mu}\beta = c_1\beta + c_2(i\beta) = \mu\beta}$$





can use $\mu \in \{m+ni,\ m+1+ni,\ m+(n+1)i,\ m+1+(n+1)i\}$ whichever is closest to α should work. Then set

$\rho = \alpha - \mu\beta$

this forces $|\rho| < |\beta|$ $\therefore$ //

Remark: the example on 8 $\longrightarrow$ 9 gives simple to see version of this...

Division in $\mathbb{Z}[i]$

Ex 1 Consider $z = 11+3i$ and $w = 1-i$. I wish to calculate $p, r \in \mathbb{Z}[i]$ for which

$$z = pw + r$$

where $|r| < |w|$. Of course, this amounts to $\frac{z}{w} = p + \frac{r}{w}$. $\mathbb{Z}[i] \subset \mathbb{C}$ so we can calculate directly.

$$\frac{z}{w} = \frac{11+3i}{1-i}\left[\frac{1+i}{1+i}\right] = \frac{11+11i+3i-3}{2} = \frac{8+14i}{2}$$

Great. My luck. $\boxed{z = (4+7i)w}$ $(r = 0)$ $p = 4+7i$.

Ex 2 $z = 11+3i$, $w = 3i+2$.

$$\frac{z}{w} = \frac{11+3i}{2+3i}\left[\frac{2-3i}{2-3i}\right] = \frac{22-33i+6i+9}{4+9} = \frac{31-27i}{13}$$

$$\frac{z}{w} = \frac{31}{13} - \left(\frac{27}{13}\right)i \quad \text{close to } p = 2-2i$$

~~Now calculate $pw = (2+2i)(2+3i) = 4+10i+6 = -2+10i$~~

~~Let $r = z - pw = (11+3i) - (-2+10i) = 13-7i$~~

$$pw = (2-2i)(2+3i) = 4+6i-4i+6 = \underline{10+2i}.$$

$$z - pw = (11+3i) - (10+2i) = \underline{1+i} = r$$

Thus, $11+3i = (10+2i) + 1+i \Rightarrow$

$$\underline{11+3i = (2-2i)(2+3i) + 1+i}.$$

EXAMPLE: **EUCLID'S ALGORITHM IMPLEMENTED IN $\mathbb{Z}[i]$**

$$(11+3i,\ 3i+2) = (z,\ w)$$

$$(3i+2,\ 1+i) = (w,\ z-(2-2i)w)$$

$$(1+i,\ -i) = \big(z-(2-2i)w,\ w-(3+i)[z-(2-2i)w]\big)$$

unit in $\mathbb{Z}[i]$

$$-i = w-(3+i)z+(3+i)(2-2i)w$$

$$-i = (9-4i)w-(3+i)z$$

$$1 = (4+9i)w + (\cancel{3}-3i+1)z$$

Thus, $\underline{1 = (4+9i)(3i+2) + (1-3i)(11+3i)}$.

Check it:

$$(4+9i)(3i+2) = 12i+8-27+18i = 30i-19$$

$$(1-3i)(11+3i) = 11+3i-33i+9 = -30i+20$$

Thus, $(4+9i)(3i+2)+(1-3i)(11+3i) = 1.$ ✓

$$\Rightarrow \underline{\gcd(11+3i,\ 3i+2) = 1}.$$