LECTURE 12 (QUADRATIC INTEGERS, from Chapter 7 of Stillwell's Elements of Number Theory.) ①

§7.1 THE EQUATION $y^3 = x^2 + 2$

Diophantus was aware of many rational sol^{ns} of $y^3 = x^2 + 2$ and also the integer sol^n $x = 5$ and $y = 3$. In 1657 Fermat ~~showed~~ claimed $\nexists$ any other sol^n in $\mathbb{N}$. As usual, Euler proved this claim (in 1770) by assuming unique prime factorization in

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$$

Let's retrace Euler's argument (we postpone proof of some of these assertions until later)

Suppose $y^3 = x^2 + 2$ for some $x, y \in \mathbb{Z}$ then we have factorization below in $\mathbb{Z}[\sqrt{-2}]$,

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

Assume $x - \sqrt{-2}$ & $x + \sqrt{-2}$ are relatively prime in $\mathbb{Z}[\sqrt{-2}]$ and a unique prime factorization, this implies these factors are themselves cubes. That is:

$$\begin{aligned} x - \sqrt{-2} &= (a + b\sqrt{-2})^3 \quad \text{for some } a, b \in \mathbb{Z} \\ &= a^3 + 3a^2b\sqrt{-2} + 3a(b\sqrt{-2})^2 + (b\sqrt{-2})^3 \\ &= a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2} \\ &= a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2} \end{aligned}$$

Equating real & imaginary parts of the above yields:

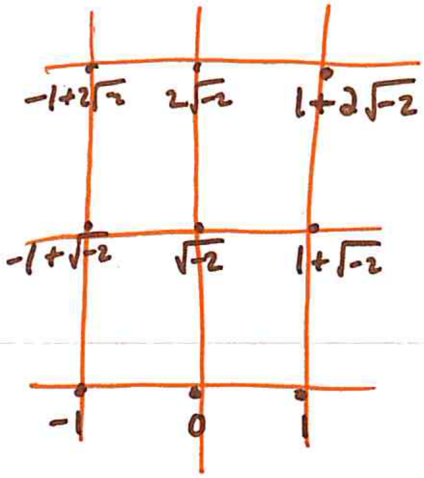
Re: $x = a^3 - 6ab^2$

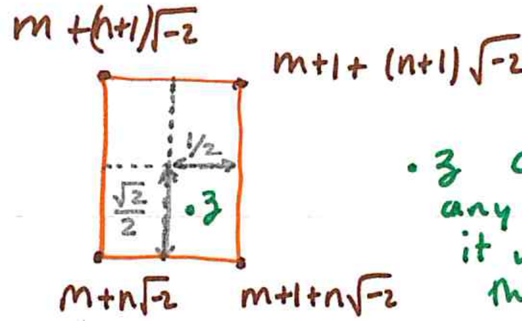
Im: $1 = 2b^3 - 3a^2b = b(2b^2 - 3a^2) \Rightarrow b \mid 1 \Rightarrow b = \pm 1$

Thus $2b^2 - 3a^2 = 2 - 3a^2 \Rightarrow 2b^2 - 3a^2 = -1$ & $b = -1$ (I think).

Therefore, $\boxed{\begin{array}{l} x = (-1)^3 - 6(-1)(-1)^2 = -1 + 6 = 5. \\ y = \sqrt[3]{5^2 + 2} = \sqrt[3]{27} = 3. \end{array}}$

§7.2 THE DIVISION PROPERTY IN $\mathbb{Z}[\sqrt{-2}]$:





• z could be in any quadrant, but it will be no more than $1/2$ horiz. and $\sqrt{2}/2$ vertically from nearest corner point.

$z = \dfrac{\alpha}{\beta} = x + y\sqrt{-2}$ choose $a + b\sqrt{-2} \overset{\text{def}}{=} \mu$ which is closest to z and see geometrically we have

$$|x-a| \leq \frac{1}{2} \quad \text{and} \quad |y-b| \leq \frac{\sqrt{2}}{2}$$

Let $\rho = \alpha - \mu\beta$. Observe

$$|\rho| < |\beta| \iff \left|\frac{\rho}{\beta}\right| < 1 \iff \left|\frac{\alpha}{\beta} - \mu\right| < 1 \iff |x-a+(y-b)\sqrt{-2}| < 1$$

But,

$$|x-a+(y-b)\sqrt{-2}| \leq \sqrt{\left(\tfrac{1}{2}\right)^2 + \left(\tfrac{\sqrt{2}}{2}\right)^2} = \frac{\sqrt{3}}{2} < 1$$

Thus $|\rho| < |\beta|$ and we have shown,

Th^m/ Division Property for $\mathbb{Z}[\sqrt{-2}]$. For nonzero $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ there exists $\mu = a + b\sqrt{-2}$ and $\rho \in \mathbb{Z}[\sqrt{-2}]$ for which $\alpha = \mu\beta + \rho$ and $\text{norm}(\rho) < \text{norm}(\beta)$

Def^n/ $\text{norm}(a + b\sqrt{-2}) = a^2 + 2b^2$.

<u>Notation</u>: $\sqrt{-2} = i\sqrt{2}$ so $a + ib\sqrt{2} = z$ and as before, $\text{norm}(z) = z\bar{z} \Rightarrow \text{norm}(zw) = \text{norm}\, z \;\text{norm}\, w$.

A <u>unit</u> in $\mathbb{Z}[\sqrt{-2}]$ is a divisor of 1. But, $u/1 \Rightarrow 1 = uv$ for $u, v \in \mathbb{Z}[\sqrt{-2}]$ and so $\text{norm}(1) = \text{norm}(u)\,\text{norm}(v)$. Notice $\text{norm}(z) \geq 0$ thus as $\text{norm}(1) = 1^2 = 1$ we need $\text{norm}(u) = 1$.

If $u = a + b\sqrt{-2}$ then $\text{norm}(u) = a^2 + 2b^2 = 1$ for $a, b \in \mathbb{Z}$ we obtain $a = \pm 1$, $b = 0$ thus,

the only units in $\mathbb{Z}[\sqrt{-2}]$ are simply ± 1

Suppose a cube $y^3 = st$ for s, t a relatively prime pair in $\mathbb{Z}[\sqrt{-2}]$. Since s, t share no factor except possibly ± 1 it follows that s, t are themselves cubes (± 1 also cubes so we can absorb them wlog)

Comment: relatively prime factors of a cube are themselves cubes inside $\mathbb{Z}[\sqrt{-2}]$.

§7.3 The gcd in $\mathbb{Z}[\sqrt{-2}]$

Prop: If $\alpha \mid \gamma$ then $\text{norm}(\alpha) \mid \text{norm}(\gamma)$

Proof: If $\alpha \mid \gamma$ then $\exists m \in \mathbb{Z}[\sqrt{-2}]$ s.t. $\gamma = m\alpha$ hence by multiplicative prop. of norm, $\text{norm}(\gamma) = \text{norm}(m)\,\text{norm}(\alpha)$ thus, as $\text{norm}(m) \in \mathbb{Z}$, we conclude $\text{norm}(\alpha) / \text{norm}(\gamma)$. //

Cor: if δ/α and δ/β then $\text{norm}(\delta)$ is a common divisor of $\text{norm}(\alpha)$ and $\text{norm}(\beta)$

In view of these facts we study $y^3 = x^2 + 2$ factoring to $y^3 = (x - \sqrt{-2})(x + \sqrt{-2})$

continuing, what is $\gcd(x-\sqrt{-2},\ x+\sqrt{-2})$?

(assuming x is part of sol$^{\underline{n}}$ to $y^3 = x^2+2$.)

Ok, if $y^3 = x^2+2$ then x must be odd. Why?

$$\boxed{\begin{array}{l}\text{If } x \text{ is even then } x^2+2 \equiv 2 \bmod 4 \\ \text{whereas } y^3 \equiv 0,1 \text{ or } 3 \bmod 4 \ \therefore\ x^2+2 \neq y^3 \\ \text{for any even } x.\ \ 0^3\equiv 0,\ 1^3\equiv 1,\ 2^3 \equiv 0,\ 3^3\equiv 3 \bmod 4.\end{array}}$$

$$\begin{aligned} \text{norm}(y^3) &= \text{norm}(x^2+2) \\ &= \text{norm}\big((x-\sqrt{-2})(x+\sqrt{-2})\big) \\ &= \text{norm}(x-\sqrt{-2})\ \text{norm}(x+\sqrt{-2}) \end{aligned}$$

If x odd then x^2 is odd $\Rightarrow x^2+2$ is odd

$\therefore\ y^3$ is odd and $\text{norm}(y^3) = (y^3)^2$ is also odd

$\Rightarrow$ $\text{norm}(x-\sqrt{-2})$ AND $\text{norm}(x+\sqrt{-2})$ odd.

Observe $(x+\sqrt{-2}) - (x-\sqrt{-2}) = 2\sqrt{-2}$. Since $\gcd(x-\sqrt{-2}, x+\sqrt{-2}) = d$ has $d \mid x-\sqrt{-2}$ & $d \mid x+\sqrt{-2} \Rightarrow d \mid 2\sqrt{-2}$.

The $\text{norm}(2\sqrt{-2}) = 8$. Observe $\gcd(8, \overbrace{x^2+2}^{\text{odd \#}}) = 1$

Hence, $\gcd(x-\sqrt{-2},\ x+\sqrt{-2}) = 1$.

- THIS COMPLETES EULER'S PROOF THAT $x=5$, $y=3$ IS THE ONLY SOLUTION IN $\mathbb{N}$ for $y^3 = x^2+2$; the cube y^3 factorizes into relatively prime $(x-\sqrt{-2})(x+\sqrt{-2})$ which are cubes by unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$ & the fact $1 = 1^3$, $-1 = (-1)^3$. Hence $x - \sqrt{-2} = (a+b\sqrt{-2})^3$ and we calculate as in §7.1.

§7.4 $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\zeta_3]$

We've had fun investigating $\mathbb{Z}[i]$ & $\mathbb{Z}[\sqrt{-2}]$. What next? Consider $\mathbb{Z}$ adjoin $\sqrt{-3}$,

$$\mathbb{Z}[\sqrt{-3}] = \{ a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \}$$

We find unique prime factorization fails in $\mathbb{Z}[\sqrt{-3}]$. Consider, we have at least two distinct factorizations of 4,

$$4 = 2 \times 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$$

The norm works as usual,

$$\text{norm}(a + b\sqrt{-3}) = |a + b\sqrt{-3}|^2 = a^2 + 3b^2$$

$$\alpha \mid \gamma \implies \text{norm}(\alpha) \mid \text{norm}(\gamma)$$

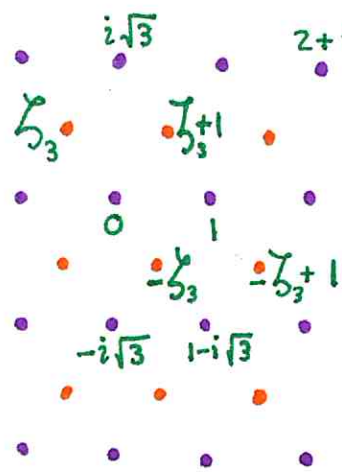
Notice, $\text{norm}(2) = 4$ and $a^2 + 3b^2 \nmid 4$ except $a^2 + 3b^2 = 1$ thus 2 is a prime in $\mathbb{Z}[\sqrt{-3}]$. Likewise

$$\text{norm}(1 \pm \sqrt{-3}) = 1 + 3 = 4 \implies 1 \pm \sqrt{-3} \text{ also prime in } \mathbb{Z}[\sqrt{-3}].$$

HOW TO FIX THIS?

As illustrated on p. 124 of Stillwell we can extend $\mathbb{Z}[\sqrt{-3}]$ to $\mathbb{Z}[\zeta_3]$ where $\zeta_3 = \frac{-1 + \sqrt{-3}}{2} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$

Eisenstein integers



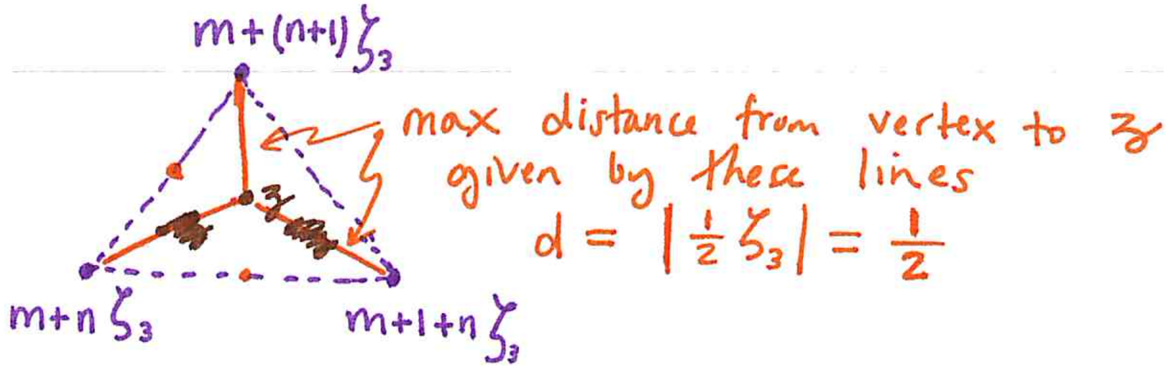
$\sqrt{-3} = i\sqrt{3}$ [sorry, I'm tired of $\sqrt{-3}$, I miss $\underbrace{i = \sqrt{-1}}$ 1777 Euler I think it's time to follow along.]

$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$$

$$\zeta_3 + 1 = \frac{1 + i\sqrt{3}}{2}$$

we can build all of $\mathbb{Z}[\sqrt{-3}]$ with ζ_3. $\longrightarrow$ $\boxed{2\zeta_3 + 1 = i\sqrt{3} = \sqrt{-3}}$

Thm/ Division Property for $\mathbb{Z}[\zeta_3]$. For any $\alpha, \beta \neq 0$ in $\mathbb{Z}[\zeta_3]$ there are μ, ρ in $\mathbb{Z}[\zeta_3]$ with
$$\alpha = \mu\beta + \rho \quad \text{and} \quad |\rho| < |\beta|$$



Consider $\frac{\alpha}{\beta} = \underbrace{x + y\zeta_3}_{z} \in \mathbb{Q}[\zeta_3]$

Let $\mu = a + b\zeta_3$ where $|x-a| \leq \frac{1}{2}$ and $|y-b| < \frac{1}{2}$ and $|z-\mu| \leq \frac{1}{2} < 1$. However, as usual, we seek to define ρ for which $|\rho| < |\beta|$. Let $\rho = \alpha - \mu\beta$

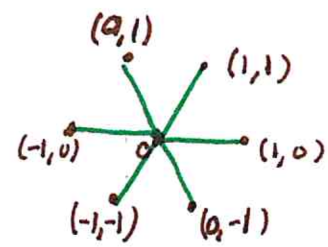
$$|\rho| < |\beta| \iff \left|\frac{\rho}{\beta}\right| < 1 \iff \left|\frac{\alpha}{\beta} - \mu\right| < 1 \iff |z - \mu| < 1$$

Hence $|\rho| < |\beta|$ and we've established the Thm. //

UNITS IN $\mathbb{Z}[\zeta_3]$? Need $\text{norm}(a + b\zeta_3) = 1$ for usual reasons.

$$\text{norm}(a+b\zeta_3) = \left|a + b\left(\frac{-1+i\sqrt{3}}{2}\right)\right|^2 = \left|\frac{2a-b}{2} + i\frac{b\sqrt{3}}{2}\right|^2$$
$$= \frac{1}{4}\left[(2a-b)^2 + 3b^2\right]$$
$$= \frac{1}{4}\left[4a^2 - 4ab + 4b^2\right]$$
$$= \underline{a^2 - ab + b^2 = 1}$$

all 6 points solve this eqn and clearly for $|a|, |b| > 1$ no soln can exist.



all distance 1 from zero hence units.

UNITS ARE $\pm 1, \pm\zeta_3, \pm(1+\zeta_3)$ a.k.a. $\pm\zeta_3^2$

QUADRATIC INTEGERS

The set $\mathbb{Z}[\zeta_3]$ is a set of <u>quadratic</u> <u>integers</u>, but, why is $\frac{-1+\sqrt{-3}}{2}$ an "integer". Let us be systematic in our nomenclature (aka name-calling)

Def^n/ A number $\alpha \in \mathbb{C}$ is an <u>algebraic</u> <u>integer</u> if it solves a monic polynomial eq^n with $\mathbb{Z}$-coeff, that is

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$$

where $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}$. In particular, a <u>quadratic</u> <u>integer</u> solves $x^2 + a_1 x + a_0 = 0$.

- <u>Chapter 10</u> we study algebraic integers and show the sum, difference, product of alg. integers is once more alg. integers.

$\zeta_3^3 = 1 \Rightarrow \zeta_3$ solves $x^3 - 1 = 0$

$\Rightarrow \zeta_3$ solves $x^2 + x + 1 = 0$ as we notice $x^3 - 1 = (x-1)(x^2+x+1)$

In fact $\mathbb{Z}[\zeta_3]$ is formed by $\mathbb{Z}$-linear comb. of 1 & ζ_3.

Th^m/ EVERY RATIONAL ALGEBRAIC INTEGER IS AN ORDINARY INTEGER.

<u>Proof</u>: we seek to show: if $r \in \mathbb{Q}$ solves $x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = 0$ where $a_{m-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ then $r \in \mathbb{Z}$. Consider $r = s/t$ in lowest terms, $\gcd(s,t) = 1$, which solves $x^m + \cdots + a_0 = 0$,

$$\frac{s^m}{t^m} = -a_{m-1}\frac{s^{m-1}}{t^{m-1}} - \cdots - a_1\left(\frac{s}{t}\right) - a_0$$

$$\Rightarrow s^m = (-a_{m-1}s^{m-1} - \cdots - a_1 s t^{m-2} - a_0 t^{m-1})t \Rightarrow t \text{ factor of } s^m$$

However, $\gcd(s,t) = 1$ hence a prime factor of t and s can only be ± 1

$\therefore t = \pm 1 \Rightarrow r = \frac{s}{t} = \pm s \in \mathbb{Z}$. $\hookrightarrow$ monic poly. $\mathbb{Z}$-coeff Eq^n have only $\mathbb{Z}$-sol^n's or <u>irrational</u> sol^n's.

§7.5 Rational Solutions of $x^3+y^3=z^3+w^3$

Hardy on Ramanujan:

"It was Littlewood who said that every positive integer was one of Ramanujan's personal friends. I remember going to see him once when he was lying ill at Putney. I had ridden in taxi-cab number 1729, and remarked that the number seemed to me a rather dull one, and I hoped it was not an unfavorable omen. "No" he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways"

$$1729 = 9^3+10^3 = 1^3+12^3$$

Brouncher (1657) gave

$$9^3+15^3 = 2^3+16^3 \quad (4104)$$
$$15^3+33^3 = 2^3+34^3 \quad (39312)$$
$$16^3+33^3 = 9^3+34^3 \quad (40033)$$
$$19^3+24^3 = 10^3+27^3 \quad (20683)$$

Also, noteworthy, $\underbrace{3^3+4^3=(-5)^3+6^3}$

$$3^3+4^3+5^3 = 6^3$$

(like $3^2+4^2=5^2$, neat)

- the remainder of §7.5 describes a rational parametric sol$^{\underline{n}}$ of $x^3+y^3=z^3+w^3$ due to (who else) Euler 1756.

§7.6 & 7.7 use $\mathbb{Z}[\zeta_3]$ to study $x^3+y^3=z^3$. Ultimately descent is used to show $\nexists$ interesting sol$^{\underline{n}}$'s. This is the start of the proof of Fermat's Last Theorem.

Fermat's Last Th$^{\underline{m}}$ (FLT for short): $\nexists$ interesting sol$^{\underline{n}}$'s to $x^n+y^n=z^n$ for $n \geq 3$. (Proof, somewhat recent by Andrew Wiles)

§7.8 DISCUSSION:

Algebraic numbers illuminate ordinary integer sol$^{\underline{n}}$'s to a variety of eq$^{\underline{n}}$'s. In particular, the norm and its multiplicative prop has been of fundamental use to study:

- generated sol$^{\underline{n}}$'s to Pell Eq$^{\underline{n}}$ $x^2 - ny^2 = 1$ via powers of $x_1 + y_1\sqrt{n}$ where (x_1, y_1) is smallest $\mathbb{N}$-sol$^{\underline{n}}$.
- find all rational sol$^{\underline{n}}$'s of $x^3 + y^3 = z^3 + w^3$

Certain rings of alg. integers have the more subtle prop. of unique prime factorization like $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$. This enabled us to capitalize on:

$$x^2 + y^2 = (x - yi)(x + yi)$$
$$x^3 + y^3 = (x+y)(x+\zeta_3)(x+\zeta_3^2)$$

to solve eq$^{\underline{n}}$'s which involve such algebra,

- primitive sol$^{\underline{n}}$'s to Pythagorean $x^2 + y^2 = z^2$ by factoring $x^2 + y^2$ in $\mathbb{Z}[i]$
- Fermat's theorem that each prime $p = 4n+1$ is a sum of two squares was proved by showing $p \mid m^2+1$ and factoring m^2+1 in $\mathbb{Z}[i]$
- integer sol$^{\underline{n}}$'s of $y^3 = x^2 + 2$ found by factoring x^2+2 in $\mathbb{Z}[\sqrt{-2}]$.
- nonexistence of sol$^{\underline{n}}$ of $x^3 + y^3 = z^3$ by factoring in $\mathbb{Z}[\zeta_3]$ (we did not cover details of this point, it's involved!)

We saw unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$. It turns out it fails for other cases like $\mathbb{Z}[\sqrt{-5}]$, but, $\nexists$ a nice way in $\mathbb{C}$ to fix it...

- Lamé published wrong proof of FLT based on assumed unique prime factorization of $x^n + y^n = (x+y)(x+\zeta_n y)\cdots(x+\zeta_n^{n-1}y)$
- Kummer realized error and introduced "ideal #'s" to fix it
- Dedekind cleaned-up ideal # concept & proved FLT for many n.