20. 4/3

20.1. Warm-up exercise: If $x, y, z \in \mathbf{Z}$ satisfy

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

then at least one of x, y, z must be even. Why? Next: At least one of x, y, z must be divisible by 5. Why?

20.2. *Gaussian congruences* As it turns out, Pythagorean triples of *Gaussian* integers enjoy similar properties. I want to use this idea to motivate some more practice with Gaussian congruence arithmetic.

We've already discussed the notion of divisibility in $\mathbf{Z}[i]$. Given $\alpha, \beta, \mu \in \mathbf{Z}[i]$, we say that α and β are *congruent modulo* μ, and write

$$\alpha \equiv \beta \pmod{\mu},$$

iff μ divides $\alpha - \beta$. The *congruence class* of α modulo μ is the set

$$\alpha + \mu\mathbf{Z}[i] = \{\alpha + \mu\lambda \mid \lambda \in \mathbf{Z}[i]\}.$$

We write $\mathbf{Z}[i]/\mu\mathbf{Z}[i]$ for the set of all congruence classe modulo μ.

20.3. How many congruence classes of Gaussian integers are there:

(1) ... modulo 2?
(2) ... modulo $2i$?
(3) ... modulo $1 + i$?
(4) ... modulo 3?
(5) ... modulo $2 + i$?

In each case, $|\mathbf{Z}[i]/\mu\mathbf{Z}[i]| = \mathbf{N}(\mu)$.

This takes some work to prove rigorously. But the basic idea is that $\mu\mathbf{Z}[i]$ is a rescaled, rotated version of the two-dimensional lattice $\mathbf{Z}[i]$. The scaling factor is $|\mu|$ along both axes, so the number of disjoint copies of $\mathbf{Z}[i]$ that fit inside $\mu\mathbf{Z}[i]$ is $|\mu|^2 = \mathbf{N}(\mu)$.

20.4. Notice that $\mathbf{Z}[i]/(2 + i)\mathbf{Z}[i]$ and $\mathbf{Z}/5\mathbf{Z}$ both have five elements. More strongly, I claim that these sets have identical arithmetic, in the sense that there is a bijection

$$f : \mathbf{Z}/5\mathbf{Z} \to \mathbf{Z}[i]/(2 + i)\mathbf{Z}[i]$$

which satisfies $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \pmod 5$. In fact, one candidate for f is

$$f(x + 5\mathbf{Z}) = x + (2 + i)\mathbf{Z}.$$

What does it mean for this map to be a bijection? It means f is both injective and surjective.

We can represent the five elements of $\mathbf{Z}/5\mathbf{Z}$ by the remainders $0, 1, \ldots, 4$. Injectivity of f means these integers are still pairwise distinct modulo $2 + i$. Surjectivity of f means every congruence class modulo $2 + i$ contains one of these integers. This whole discussion should remind you of our discussion of the Chinese Remainder Theorem.

20.5. In particular, statements about the arithmetic of integers modulo 5 can be translated into statements about the arithmetic of Gaussian integers modulo $2+i$, and vice versa.

If $x \in \mathbf{Z}$, then the possible congruence classes of x^2 modulo 5 are $0, 1, 4$ modulo 5. So if $\alpha \in \mathbf{Z}[i]$, then the congruence classes of α^2 modulo $2+i$ are $0, 1, 4$ modulo $2+i$. In particular, we deduce the analogue of the claim in the warm-up exercise: If $\alpha, \beta, \gamma \in \mathbf{Z}[i]$ satisfy

$$\alpha^2 + \beta^2 = \gamma^2,$$

then at least one of α, β, γ must be divisible by $2+i$.

(Note that 4 is too big to be a remainder of long division by $2+i$, because $\mathbf{N}(4) = 16 > 5 = \mathbf{N}(2+i)$. However, $4 \equiv -1 \pmod{2+i}$, and -1 is indeed a possible remainder.)

20.6. Notice that $\mathbf{Z}[i]/3\mathbf{Z}[i]$ has nine elements. So it cannot be in bijection with $\mathbf{Z}/p\mathbf{Z}$ for any prime p.

This is related in a funny way to the two-squares theorem. In the course of proving that theorem, we observed that if p is a positive prime, then $x^2 \equiv -1 \pmod{p}$ has a solution if and only if either $p \equiv 1, 2 \pmod 4$. In particular,

$$x^2 \equiv -1 \pmod 3 \tag{20.1}$$

has no solution for integer x. But it does have a solution if you allow x to be a Gaussian integer! Namely, take $x = i$.

In short, we can think of $\mathbf{Z}[i]/3\mathbf{Z}[i]$ as an enlargement of $\mathbf{Z}/3\mathbf{Z}$ where we gain the ability to solve (20.1). By contrast, $\mathbf{Z}[i]/(2+i)\mathbf{Z}$ is not an enlargement of $\mathbf{Z}/5\mathbf{Z}$, but this is fine, because we could already solve (20.1) in $\mathbf{Z}/5\mathbf{Z}$.

20.7. Let's move on to congruences in $\mathbf{Z}[\omega]$, where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Recall that the norm for this number system is

$$\mathbf{N}(x + y\omega) = (x + y\omega)(x + y\bar{\omega}) = x^2 - xy + y^2.$$

Following Stillwell §7.6, we study $\sqrt{-3}$. Since $\sqrt{-3} = 1 + 2\omega$, we have

$$\mathbf{N}(\sqrt{-3}) = 3.$$

Thus $\sqrt{-3}$ must be prime in $\mathbf{Z}[\omega]$, and moreover, there are exactly $\mathbf{N}(\sqrt{-3}) = 3$ congruence classes modulo $\sqrt{-3}$ in $\mathbf{Z}[\omega]$. They can be represented by the integers $0, 1, 2$. In fact, the map

$$f : \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}[\omega]/\sqrt{-3}\mathbf{Z}[\omega]$$

defined by $f(x + 3\mathbf{Z}) = x + \sqrt{-3}\mathbf{Z}[\omega]$ is a bijection that preserves addition and multiplication.

20.8. Note that $(\sqrt{-3})^4 = 9$. The following fact has no naive analogue in $\mathbf{Z}$:

Proposition 20.1. *If $\alpha \in \mathbf{Z}[\omega]$, then $\alpha^3 \equiv 0, \pm 1 \pmod 9$.*

Proof. We must have $\alpha \equiv 0, \pm 1 \pmod{\sqrt{-3}}$. We will handle the case where $\alpha \equiv 1$, leaving the others as exercises. So suppose $\alpha = 1 + \lambda\sqrt{-3}$, where $\lambda \in \mathbf{Z}[\omega]$. Then

$$\begin{aligned}\alpha^3 &= 1 + 3\lambda\sqrt{-3} + 3(\lambda\sqrt{-3})^2 + (\lambda\sqrt{-3})^3 \\ &= 1 + 3\lambda\sqrt{-3} - 9\lambda^2 + (3\sqrt{-3})\lambda^3 \\ &\equiv 1 + 3\sqrt{-3}(\lambda - \lambda^3) \pmod 9.\end{aligned}$$

But we can check that $\lambda - \lambda^3 \equiv 0 \pmod{\sqrt{-3}}$. So the last expression above simplifies to $1 \pmod 9$. □

The proof in Stillwell, at the bottom of page 130, contains a typo: The last two occurrences of the text $\pmod{\sqrt{-3}}$ should be $\pmod 9$.

20.9. We will use the following fact next time to prove a special case of Fermat's Last Theorem.

Corollary 20.2. *Let $\alpha, \beta, \gamma \in \mathbf{Z}[\omega]$. If*

$$\alpha^3 + \beta^3 + \gamma^3 = 0,$$

then at least one of α, β, γ must be divisible by $\sqrt{-3}$.

21. 4/5

21.1. Our goal today is to prove Fermat's Last Theorem in the case where the exponent is 3. Throughout, $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Theorem 21.1 ($\approx$ Euler)**.** *There do not exist $x, y, z \in \mathbf{Z}$, all nonzero, such that*

$$x^3 + y^3 = z^3.$$

Since z is an integer if and only if $-z$ is an integer, we can replace the above equation with $x^3 + y^3 + z^3 = 0$. Also, if any two of x, y, z share a common divisor d, then the third is divisible by d as well, so we can divide out by d^3, reducing to the case where x, y, z are pairwise coprime. So it suffices to show:

Theorem 21.2. *There do not exist $\alpha, \beta, \gamma \in \mathbf{Z}[\omega]$, all nonzero and pairwise coprime, such that*

$$\alpha^3 + \beta^3 + \gamma^3 = 0. \tag{21.1}$$

21.2. *Interlude* Why is $\mathbf{Z}[\omega]$ a more natural setting for the theorem? Over $\mathbf{Z}$, we have the factorization

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha^2 - \alpha\beta + \beta^2).$$

But over $\mathbf{Z}[\omega]$, we have the further, more symmetrical factorization

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta\omega)(\alpha + \beta\omega^2).$$

21.3. *Setting up the descent* Henceforth, we assume Theorem 21.2 is false in order to set up a contradiction.

Lemma 21.3. *If (21.1) holds, then one of α, β, γ must be divisible by $\sqrt{-3}$ in $\mathbf{Z}[\omega]$.*

Proof. By Proposition 20.1, a perfect cube in $\mathbf{Z}[\omega]$ must be congruent to one of $0, \pm 1$ modulo 9. So if three perfect cubes sum to 0 modulo 9, then exactly one of them, say α^3, must be 0 modulo 9 itself. But $9 = (\sqrt{-3})^4$, so 9 divides α^3 if and only if $\sqrt{-3}$ divides α. □

Let X be the set of tuples $(u, \alpha, \beta, \gamma) \in \mathbf{Z}[\omega]^4$ in which u is a unit, the other entries are all nonzero and pairwise coprime, and

$$\alpha^3 + \beta^3 + u\gamma^3 = 0.$$

We define the *Fermat power* of a tuple to be the largest integer n such that $(\sqrt{-3})^n$ divides γ. (This term is not standard.) By the lemma, the set of positive Fermat powers is nonempty. (If $\sqrt{-3}$ divides α or β, then relabel that variable γ.) By well-ordering, there is a minimal positive Fermat power m.

Let $(u, \alpha, \beta, \gamma)$ be a tuple with Fermat power m. Our goal is to create a tuple $(u', \alpha', \beta', \gamma')$ with an even smaller Fermat power.

21.4. *Reduction* We know that $\sqrt{-3}$ is prime and divides

$$-u\gamma^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta\omega)(\alpha + \beta\omega^2).$$

We also claimed earlier that $\mathbf{Z}[\omega]$ has long division, hence the prime divisor property. Therefore, $\sqrt{-3}$ must divide at least one of the three factors in the last expression. But we can check directly that for any $\alpha, \beta \in \mathbf{Z}[\omega]$, we have

$$\alpha + \beta \equiv \alpha + \beta\omega \equiv \alpha + \beta\omega^2 \pmod{\sqrt{-3}}.$$

Therefore, if $\sqrt{-3}$ divides one of them, then it divides them all. We conclude that the expressions

$$A = \frac{1}{\sqrt{-3}}(\alpha + \beta), \quad B = \frac{1}{\sqrt{-3}}(\alpha + \beta\omega), \quad C = \frac{1}{\sqrt{-3}}(\alpha + \beta\omega^2)$$

all define elements of $\mathbf{Z}[\omega]$.

We want to use A, B, C to build our new tuple $(u, \alpha', \beta', \gamma')$. We notice that since $1 + \omega + \omega^2 = 0$, we have

$$A + \omega B + \omega^2 C = 0.$$

So it would be great if A, B, C were all perfect cubes in $\mathbf{Z}[\omega]$, up to multiplication by units, and all nonzero and pairwise coprime.

21.5. *Structure of A, B, C* Since α and β are coprime in $\mathbf{Z}[\omega]$, we must have $\alpha \neq -\beta, -\beta\omega, -\beta\omega^2$. This shows $A, B, C \neq 0$.

Next, we show that A, B, C are pairwise coprime. We explain why A and B are coprime, the other cases being similar. The point is that α and β are themselves $\mathbf{Z}[\omega]$-linear combinations of A and B:

$$\begin{pmatrix} A \\ B \end{pmatrix} = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \implies \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -\omega^2 & \omega \\ \omega & -\omega \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix}.$$

So any common divisor of A and B would be a common divisor of α and β. Since α and β are coprime, A and B must be as well.

Finally, recall that $-u\gamma^3 = \alpha^3 + \beta^3 = (\sqrt{-3})^3 ABC$. Since A, B, C are pairwise coprime, uniqueness of prime factorization in $\mathbf{Z}[\omega]$ implies that A, B, C are each perfect cubes individually, up to multiplication by units.

So we have factorizations of the form

$$A = u_1(\alpha')^3, \quad B = u_2(\beta')^3, \quad C = u_3(\gamma')^3$$

in $\mathbf{Z}[\omega]$, where u_1, u_2, u_3 are units and α', β', γ' are pairwise coprime. We want to use α', β', γ' to build a tuple in X with smaller Fermat power than m.

21.6. *m is at least* 2 By assumption, we have $\gamma = (\sqrt{-3})^m \delta$ for some $\delta \in \mathbf{Z}[\omega]$ indivisible by $\sqrt{-3}$.

Lemma 21.4. *Above,* $m \geq 2$.

Proof. We have

$$\alpha^3 + \beta^3 + (\sqrt{-3})^{3m} \delta^3 = 0,$$

where none of α, β, δ can be divisible by $\sqrt{-3}$. By Proposition 20.1, each of α, β, δ is congruent to one of ± 1 modulo 9, so this identity cannot hold unless $(\sqrt{-3})^{3m} \equiv 0 \pmod 9$. □

We will finish the proof of Theorem 21.2 on Friday!

22. 4/7

22.1. Today we finish proving Theorem 21.2. I will implicitly fix some errors in Wednesday's lecture.

A recap: We introduced the set

$$X = \left\{ (u, \alpha, \beta, \gamma) \in \mathbf{Z}[\omega]^4 \;\middle|\; \begin{array}{l} u \text{ is a unit,} \\ \alpha, \beta, \gamma \text{ nonzero and pairwise coprime,} \\ \alpha^3 + \beta^3 + u\gamma^3 = 0 \end{array} \right\}.$$

For $(u, \alpha, \beta, \gamma) \in X$, we defined its *Fermat power* to be the largest $m \in \mathbf{N}$ such that $(\sqrt{-3})^m$ divides γ in $\mathbf{Z}[\omega]$.

We assume Theorem 21.2 is false. Then there is a smallest positive Fermat power m: say, coming from $(u, \alpha, \beta, \gamma) \in X$. We can write

$$\gamma = (\sqrt{-3})^m \delta,$$

where $\delta \in \mathbf{Z}[\omega]$ is indivisible by $\sqrt{-3}$. The aim of Wednesday was to show:

- $m \geq 2$.
- There are elements

$$A = u_1(\alpha')^3, \quad B = u_2(\beta')^3, \quad C = u_3(\gamma')^3$$

in $\mathbf{Z}[\omega]$, where:
  - u_1, u_2, u_3 are units.
  - $\alpha', \beta', \gamma' \in \mathbf{Z}[\omega]$ are nonzero and pairwise coprime.
  - We have

$$A + \omega B + \omega^2 C = 0, \tag{22.1}$$
$$(\sqrt{-3})^3 ABC = \alpha^3 + \beta^3 = -u\gamma^3.$$

We can rewrite the second identity as:

$$u_1 u_2 u_3 (\alpha')^3 (\beta')^3 (\gamma')^3 = -u(\sqrt{-3})^{3(m-1)} \delta^3.$$

22.2. *Conclusion* Since α', β', γ' are pairwise coprime, the prime $\sqrt{-3}$ must divide exactly one of them. After possibly relabeling, we can assume it divides γ'. Now we can rewrite (22.1) as

$$(\alpha')^3 + u_4(\beta')^3 + u_5(\gamma')^3 = 0,$$

where $u_4 = u_2/u_1$ and $u_5 = u_3/u_1$ are again units.

Observe that, since δ is indivisible by $\sqrt{-3}$, the largest power of $\sqrt{-3}$ that divides γ' must be $(\sqrt{-3})^{m-1}$.

We conclude that if $u_4 = \pm 1$, then $(u_5, \alpha', \pm\beta', \gamma')$ is an element of X with Fermat power $m - 1$, contradicting the minimality of m.

Lemma 22.1. $u_4 = \pm 1$.

Proof. Since $m \geq 2$ and $(\sqrt{-3})^{m-1}$ divides γ', we know that $(\sqrt{-3})^3$ divides $(\gamma')^3$. So we have

$$(\alpha')^3 + u_4(\beta')^3 \equiv 0 \pmod{(\sqrt{-3})^3}.$$

But α', β' are not divisible by $\sqrt{-3}$, so by Proposition 20.1, we know that $(\alpha')^3, (\beta')^3$ are each 1 or -1 modulo 9, hence also modulo $(\sqrt{-3})^3$. So the only way to get the congruence above is if $u_4 = \pm 1$. □

22.3. *Postscript* Fermat's Last Theorem says there are no solutions to $x^n + y^n = z^n$, where x, y, z, n are nonzero integers and $n > 2$. We have now seen a proof in the case where $n = 3$, which relied on the factorization

$$x^3 + y^3 = (x + y)(x + y\omega)(x + y\omega^2).$$

The 19th-century mathematician Lamé tried to generalize this proof using the factorization

$$x^n - (-y)^n = (x + y)(x + y\zeta_n)(x + y\zeta_n^2) \cdots (x + y\zeta_n^{n-1}),$$

where $\zeta_n = e^{2\pi i/n}$. This means generalizing from $\mathbf{Z}[\omega]$ to

$$\mathbf{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}\}.$$

This set is still closed under addition and multiplication! And it also has a notion of norm, defined using so-called Galois conjugates.

Unfortunately, when n is large, it does not have uniqueness of prime factorization, which we used in our $n = 3$ proof. So Lamé's proof breaks in general.

22.4. Before we discussed sums of perfect cubes, we discussed sums of perfect squares. We proved Fermat's two-squares theorem as part of a larger circle of equivalences:

Theorem 22.2. *Let p be a (positive) prime integer. Then the following are equivalent:*

(1) $p = x^2 + y^2$ for some integers x and y.
(2) p factors into smaller primes in $\mathbf{Z}[i]$.
(3) -1 is a quadratic residue modulo p.
(4) p is either 2 or congruent to 1 modulo 4.

Fermat also studied primes of the form $x^2 + 2y^2$ and $x^2 + 3y^2$. Here one finds very similar stories:

Theorem 22.3. *Let p be a (positive) prime integer. Then the following are equivalent:*

(1) $p = x^2 + 2y^2$ for some integers x and y.
(2) p factors into smaller primes in $\mathbf{Z}[\sqrt{-2}]$.
(3) -2 is a quadratic residue modulo p.
(4) p is either 2 or congruent to 1 or 3 modulo 8.

Example 22.4. If $p = 17$, then all of the items in Theorem 22.3 hold:

(1) $17 = 3^2 + 2(2^2)$.
(2) $17 = (3 + 2\sqrt{-2})(3 - 2\sqrt{-2})$. These factors are prime since they both have norm 17.
(3) $-2 \equiv 7^2 \pmod{17}$.
(4) $17 \equiv 1 \pmod{8}$.

By contrast, if $p = 13$, then none of the items hold.

Theorem 22.5. *Let p be a (positive) prime integer. Then the following are equivalent:*

(1) $p = x^2 + 3y^2$ for some integers x and y.
(2) p factors into smaller primes in $\mathbf{Z}[\omega]$, where $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.
(3) -3 is a quadratic residue modulo p and $p \neq 2$.
(4) p is congruent to 1 modulo 3.

Example 22.6. If $p = 13$, then all of the items in Theorem 22.3 hold:

(1) $13 = 1^2 + 3(2^2)$.
(2) $13 = (1 + 2\sqrt{-3})(1 - 2\sqrt{-3}) = (3 + 4\omega)(3 + 4\bar{\omega})$.
(3) $-3 \equiv 4^2 \pmod{13}$.
(4) $13 \equiv 1 \pmod{3}$.

By contrast, if $p = 17$, then none of the items hold.

Even though these stories are similar, the analogies look slightly messy at first. Nonetheless, the proofs are all roughly the same in structure, as explained in Stillwell §9.1.

Next week, we will focus on the case where p is odd, and on the equivalences (3) $\Leftrightarrow$ (4):

$$\begin{aligned} -1 \text{ is a QR modulo } p &\iff p \equiv 1 \pmod{4}, \\ -2 \text{ is a QR modulo } p &\iff p \equiv 1, 3 \pmod{8}, \\ -3 \text{ is a QR modulo } p &\iff p \equiv 1 \pmod{3}. \end{aligned}$$