15. 3/13

15.1. In Stillwell, we are turning from Chapter 5 to Chapter 6. A recap:

- We have been studying
$$\mathbf{Z}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbf{Z}\},$$
where n is a fixed, squarefree natural number.
- The norm function $\mathbf{N} : \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$ defined by
$$\mathbf{N}(x + y\sqrt{n}) = \mathbf{N}(x - y\sqrt{n}) = x^2 - ny^2$$
is multiplicative: $\mathbf{N}(\alpha\beta) = \mathbf{N}(\alpha)\mathbf{N}(\beta)$.
- The equation $\mathbf{N}(\alpha) = 1$ has a solution $\alpha \in \mathbf{Z}[\sqrt{n}]$ other than $\alpha = 1$. And if α is a solution, then α^k is also a solution for all $k \in \mathbf{Z}$.

15.2. *The Gaussian integers* What happens if we take n to be a negative integer, instead of a positive integer? Let $i = \sqrt{-1}$. Taking $n = -1$, we end up with the *Gaussian integers*

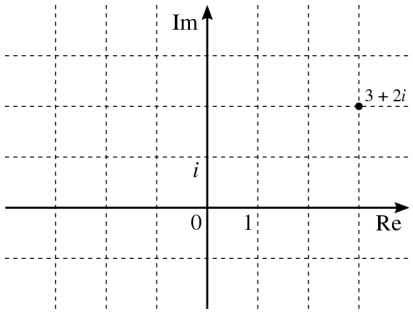
$$\mathbf{Z}[i] = \{x + yi \mid x, y \in \mathbf{Z}\}.$$

And the analogue of our earlier norm is the function $\mathbf{N} : \mathbf{Z}[i] \to \mathbf{Z}$ defined by

$$\mathbf{N}(x + yi) = x^2 + y^2.$$

It is again multiplicative by Brahmagupta's identity.

Unlike $\mathbf{Z}[\sqrt{n}]$ for positive n, we can visualize $\mathbf{Z}[i]$ using the complex plane:



Recall that the absolute value of a complex number $z = x + yi$ is its length as a vector in the complex plane: $|z| = \sqrt{x^2 + y^2}$. So the norm of an element of $\mathbf{Z}[i]$ is just the square of its absolute value.

15.3. For a squarefree positive integer n, we have seen that $\mathbf{Z}[\sqrt{n}]$ contains elements arbitrarily close to 0, and that $\mathbf{N}(\alpha) = 1$ has infinitely many solutions for $\alpha \in \mathbf{Z}[\sqrt{n}]$.

In $\mathbf{Z}[i]$, the reverse happens. The picture shows that the elements of $\mathbf{Z}[i]$ are evenly spaced in a grid; in particular, they do not accumulate near 0, or any other complex number. Moreover, solving $\mathbf{N}(\alpha) = 1$ for $\alpha = x + yi$ means solving the Diophantine equation $x^2 + y^2 = 1$, which only has 4 solutions: $(x, y) = (1, 0), (0, 1), (-1, 0), (0, -1)$. These correspond to $\alpha = 1, i, -1, -i$, respectively.

15.4. *Pythagorean triples* What about $x^2 + y^2 = N$ for other $N \in \mathbf{N}$?

In the case where $x, y > 0$ and N is a perfect square, say $N = z^2$ for an integer $z > 0$, the triple (x, y, z) is called a *Pythagorean triple*. Some small examples are:

$$3^2 + 4^2 = 5^2, \qquad 5^2 + 12^2 = 13^2,$$
$$8^2 + 15^2 = 17^2, \qquad 7^2 + 24^2 = 25^2.$$

But Pythagoras lived around 570–495 BCE, whereas people have been fascinated by these triples for much longer. The cover image on the course webpage is Plimpton 322, a Babylonian tablet from circa 1800 BCE written in Akkadian. It is currently the oldest known example of Pythagorean triples in writing.

There is a complete classification of Pythagorean triples. In this sense, the Diophantine equation

$$x^2 + y^2 = z^2 \tag{15.1}$$

has been totally solved.

15.5. *Digression: Fermat's Last Theorem* The problem of solving

$$x^n + y^n = z^n \qquad \text{for a fixed integer } n > 2$$

was posed by Fermat in a margin note to his copy of Diophantus' *Arithmetica*. He claimed that there were no solutions with x, y, z all positive integers. This claim is more widely known as Fermat's Last Theorem, though Fermat did not prove it. It was finally proved in the 90s by Andrew Wiles, building on work of André Weil, Yutaka Taniyama, Goro Shimura, Ken Ribet, Richard Taylor, and many others.

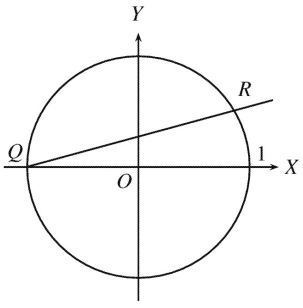
15.6. *Digression: The chord method* Following Stillwell §1.7, we will classify Pythagorean triples. First, solving (15.1) for $x, y, z \in \mathbf{N}$ is equivalent to solving

$$X^2 + Y^2 = 1 \tag{15.2}$$

for positive rational numbers X, Y, via the substitutions $X = x/z$ and $Y = y/z$. At the same time, the equation (15.2) describes the unit circle in the (X, Y)-plane. The key idea is: For any point R on this circle,

$$R \text{ has rational coordinates} \implies \text{the slope of the chord } \overline{QR} \text{ is rational}$$

in the figure from Stillwell below:



Indeed, if s is the slope of $\overline{QR}$, and $R = (X, Y)$, then

$$s = \frac{Y - 0}{X - (-1)} = \frac{Y}{X + 1},$$

from which the claim follows.

Rearranging, $Y = s(X + 1)$. At the same time, R lives on the unit circle, so

$$1 = X^2 + Y^2 = X^2 + (s(X + 1))^2 = (1 + s^2)X^2 + 2s^2X + s^2.$$

So using the quadratic formula, we can now express the rational number X as a function of the rational number s:

$$X = -1 \text{ or } \frac{1 - s^2}{1 + s^2}.$$

The case $X = -1$ is the degeneration where $R = Q$, so we exclude it. That leaves one other solution, which gives

$$(X, Y) = \left(\frac{1 - s^2}{1 + s^2}, \frac{2s}{1 + s^2}\right).$$

And now we see that any rational number s will give back rational values for both X and Y. As we run over all rational s, we get all rational solutions to $X^2 + Y^2 = 1$.

If $s = v/u$ with $u, v \in \mathbf{Z}$, then

$$(X, Y) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}\right)$$

after a little algebra. So every Pythagorean triple (x, y, z) must satisfy

$$\left(\frac{x}{z}, \frac{y}{z}\right) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}\right)$$

for some (u, v). Requiring $x, y, z > 0$ means requiring $u > v > 0$.

15.7. A funny consequence of the classification:

If $z^2 = x^2 + y^2$ for some $x, y, z \in \mathbf{N}$, then $z = u^2 + v^2$ for some $u, v \in \mathbf{N}$.

That is, a solution to the Diophantine equation in x, y, z implies a solution to the one in u, v. We can check this on our earlier examples:

$$\begin{aligned} 3^2 + 4^2 &= 5^2, & 1^2 + 2^2 &= 5. \\ 5^2 + 12^2 &= 13^2, & 2^2 + 3^2 &= 13. \\ 8^2 + 15^2 &= 17^2, & 1^2 + 4^2 &= 17. \\ 7^2 + 24^2 &= 25^2, & 3^2 + 4^2 &= 25. \end{aligned}$$

16. 3/15

16.1. Last time, we introduced the Gaussian integers

$$\mathbf{Z}[i] = \{x + yi \mid x, y \in \mathbf{Z}\}$$

and its norm $\mathbf{N}(x + yi) = x^2 + y^2$.

For a fixed integer $N \geq 0$, we raised the problem of finding all $x, y \in \mathbf{Z}$ such that $x^2 + y^2 = N$, or equivalently, $\alpha \in \mathbf{Z}[i]$ such that $\mathbf{N}(\alpha) = N$.

16.2. For small N, we can attack the problem by brute force. Note that if $\alpha \in \mathbf{Z}[i]$ is a solution, then so are $i\alpha, -\alpha, -i\alpha \in \mathbf{Z}[i]$. So it suffices to study the Gaussian integers α in the quadrant where $\mathrm{Re}(\alpha) > 0$ and $\mathrm{Im}(\alpha) \geq 0$.

α	$\mathbf{N}(\alpha)$	α	$\mathbf{N}(\alpha)$
0	0	$3 + i, 1 + 3i$	10
1	1	$3 + 2i, 2 + 3i$	13
$1 + i$	2	4	16
2	4	$4 + i, 1 + 4i$	17
$2 + i, 1 + 2i$	5	$3 + 3i$	18
$2 + 2i$	8	$4 + 2i, 2 + 4i$	20
3	9	$5, 4 + 3i, 3 + 4i$	25

The values of N for which $\mathbf{N}(\alpha) = N$ has no solution:

$$3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, \ldots$$

How can we characterize the numbers in this list?

Lemma 16.1. *If $N \equiv 3 \pmod 4$, then N is not a sum of two perfect squares.*

Proof. Modulo 4, we compute $0^2 \equiv 2^2 \equiv 0$ and $1^2 \equiv 3^2 \equiv 1$. So the only possible remainders for a perfect square modulo 4 are 0 and 1. For a sum of two perfect squares, they are $0, 1, 2$. □

This explains why $N = 3, 7, 11, 15, 19, 23, \ldots$ appear in the list. But the other numbers are trickier. For instance, $N = 21$ appears, yet $21 \equiv 1 \pmod 4$.

16.3. Since $\mathbf{N}$ is fully multiplicative, it may be natural to look at values for $\mathbf{N}(\alpha)$ that can't be factored any further.

In particular: What if we look the behavior of $\mathbf{N}(\alpha) = p$ for prime p? The list of p for which no solution exists:

$$3, 7, 11, 19, 23, \ldots$$

The list of p for which a solution exists:

$$2, 5, 13, 17, \ldots$$

Now a pattern is easier to see.

Theorem 16.2 (Fermat)**.** *Let p be prime. Then p is a sum of two perfect squares if and only if either $p = 2$ or $p \equiv 1 \pmod 4$.*

The "only if" direction follows immediately from Lemma 16.1. The "if" direction is much harder. Our proof will use the Gaussian integers.

16.4. *Divisibility of Gaussian integers* Let $\alpha, \beta \in \mathbf{Z}[i]$ be arbitrary. We say that β *divides* α in $\mathbf{Z}[i]$ iff there is some $\gamma \in \mathbf{Z}[i]$ such that $\beta\gamma = \alpha$. This immediately implies $\mathbf{N}(\beta)\mathbf{N}(\gamma) = \mathbf{N}(\alpha)$, so we deduce that

$$\beta \text{ divides } \alpha \implies \mathbf{N}(\beta) \text{ divides } \mathbf{N}(\alpha). \tag{16.1}$$

We say that α is *invertible* in $\mathbf{Z}[i]$, or a *Gaussian unit*, iff it divides 1. In this case, $\mathbf{N}(\alpha)$ divides 1, which implies $\mathbf{N}(\alpha) = 1$, which in turn implies $\alpha \in \{\pm 1, \pm i\}$. All four of these numbers are units.

We say that α is *prime* in $\mathbf{Z}[i]$, or a *Gaussian prime*, iff it is not a unit and, whenever $\beta\gamma = \alpha$ in $\mathbf{Z}[i]$, either β is a unit or γ is a unit.

Remark 16.3. In the first part of this course, we used the word "prime" to mean "positive prime". But in $\mathbf{Z}$, the units are ± 1. So in the analogy between $\mathbf{Z}[i]$ and $\mathbf{Z}$, the most accurate analogue of the Gaussian primes would include both positive and negative prime numbers.

Lemma 16.4. *If* $\mathbf{N}(\alpha)$ *is prime in* $\mathbf{Z}$*, then* α *is prime in* $\mathbf{Z}[i]$.

Proof. By (16.1). □

Example 16.5. The converse is false. As an element of $\mathbf{Z}[i]$, the number 3 satisfies $\mathbf{N}(3) = 9$. The only divisors of 9 are $1, 3, 9$. But we checked that there are no Gaussian integers of norm 3. Therefore, 3 must be prime in $\mathbf{Z}[i]$.

In general, the same argument shows that if p is prime in $\mathbf{Z}$, and $p \equiv 3 \pmod 4$, then p must remain prime in $\mathbf{Z}[i]$.

16.5. Recall that the *conjugate* of $\alpha = a + bi$ is $\bar{\alpha} := a - bi$.

Lemma 16.6. *If* α *is a Gaussian prime, then so is* $\bar{\alpha}$.

Proof. By symmetry. □

16.6. *Further analogies* The Gaussian integers enjoy analogues of many of the theorems we saw for integers: (1) long division, (2) the Euclidean algorithm, (3) the prime divisor property, and (4) unique prime factorization up to units. We only comment on (1) and (4).

First, when we do long division in $\mathbf{Z}[i]$, the notion of remainder involves the norm. The correct statement is:

Theorem 16.7. *For any* $\alpha, \beta \in \mathbf{Z}[i]$ *with* $\beta \neq 0$*, there are* $\mu, \rho \in \mathbf{Z}[i]$ *such that*

$$\alpha = \mu\beta + \rho \quad \textit{and} \quad \mathbf{N}(\rho) < \mathbf{N}(\beta).$$

(The second assertion is equivalent to $|\rho| < |\beta|$*.)*

Next, we note that in the proof of unique prime factorization in $\mathbf{Z}[i]$, the existence is easy but the uniqueness is hard. (When we studied prime factorization in $\mathbf{Z}$, we skipped the proof of uniqueness.) For $\mathbf{Z}[i]$, the uniqueness actually depends on the fact that long division still works.

16.7. Although the converse of Lemma 16.4 fails, we can salvage something close:

Lemma 16.8. *Suppose $\alpha = a + bi$ is a Gaussian prime.*

(1) If a, b are both nonzero, then $\mathbf{N}(\alpha)$ is prime in $\mathbf{Z}$.

(2) If one or both of a, b are zero, then $\mathbf{N}(\alpha)$ is the square of a prime in $\mathbf{Z}$.

Proof. In general,

$$\mathbf{N}(\alpha) = \alpha\bar{\alpha}. \tag{16.2}$$

We know from Lemma 16.6 that if α is a Gaussian prime, then so is $\bar{\alpha}$, so this equation actually gives a prime factorization of $\mathbf{N}(\alpha)$.

In case (2), either α is real, in which case $\alpha = \bar{\alpha}$ and $\mathbf{N}(\alpha) = \alpha^2$, or else α is totally imaginary, in which case $i\alpha$ is real and $\mathbf{N}(\alpha) = (i\alpha)^2$. Either way we get the desired conclusion.

In case (1), suppose that $\mathbf{N}(\alpha) = mn$ for some integers m, n such that $1 < m, n < \mathbf{N}(\alpha)$. Since (16.2) is a prime factorization, the uniqueness of the prime factorization of $\mathbf{N}(\alpha)$ up to units implies that m, n must differ from $\alpha, \bar{\alpha}$ by units. But by the assumption on a, b, this is not possible, so we get a contradiction. □

In case (1), we must have $\mathbf{N}(\alpha) = p$ with either $p = 2$ or $p \equiv 1 \pmod 4$, because we cannot have $p \equiv 3 \pmod 4$.

In case (2), we claim that $\mathbf{N}(\alpha) = p^2$ for some $p \equiv 3 \pmod 4$, in which case $\alpha = \pm p, \pm ip$. This will follow from Fermat's two-squares theorem.

17. 3/17

17.1. Reminder: There will be a test next Friday (3/24), the day before break.

17.2. Our goal is to prove Fermat's two-squares theorem. How is the statement related to $\mathbf{Z}[i]$?

Let p be a positive prime in $\mathbf{Z}$. Last time, we sketched a proof that if $p \equiv 3 \pmod 4$, then p remains prime in $\mathbf{Z}[i]$. We can reduce Fermat to the converse statement:

Theorem 17.1. *If $p > 0$ is prime and $p \equiv 1 \pmod 4$, then p does* not *remain prime in $\mathbf{Z}[i]$.*

Proof that Theorem 17.1 implies Fermat. If $p = \beta\gamma$ for some non-units β, γ in $\mathbf{Z}[i]$, then we must have $\mathbf{N}(\beta) = \mathbf{N}(\gamma) = p$. (In fact, we must also have $\beta = \bar{\gamma}$.) But any norm is a sum of two perfect squares. □

17.3. We further reduce Theorem 17.1 to:

Theorem 17.2 (Lagrange)**.** *If $p > 0$ is prime and $p \equiv 1 \pmod 4$, then p divides $x^2 + 1$ for some $n \in \mathbf{Z}$.*

Proof that Theorem 17.2 implies Theorem 17.1. Suppose that p divides $x^2 + 1$. We can write

$$x^2 + 1 = (x + i)(x - i).$$

But p cannot divide either $x + i$ or $x - i$ in $\mathbf{Z}[i]$, because that would mean $p(a \pm bi) = x \pm i$ for some $a, b \in \mathbf{Z}$, whereas $pb = 1$ is impossible. So by the Gaussian prime divisor property, p cannot be prime. □

17.4. *Quadratic residues* The conclusion of Theorem 17.2 can be rephrased using congruence arithmetic, as the statement that

$$x^2 \equiv -1 \pmod p$$

for some $x \in \mathbf{Z}$.

More generally, we say that the congruence class of a modulo m is a *quadratic residue (QR)* iff we can solve $x^2 \equiv a \pmod m$ for integer x. Otherwise, we say that it is a *quadratic non-residue (QNR)*.

Example 17.3. For any $m \in \mathbf{N}$, the congruence classes of 0 and 1 must be QRs mod m, because $0^2 \equiv 0$ and $1^2 \equiv 1$.

Example 17.4. Some lists of QRs:

(1) Modulo 3, they are (the congruence classes of) 0, 1.
(2) Modulo 4, they are 0, 1.
(3) Modulo 5, they are 0, 1, 4.
(4) Modulo 6, they are 0, 1, 3, 4.

17.5. The easiest QRs to understand are the invertible QRs modulo a prime. The proof of Theorem 17.2 will be a byproduct of our analysis.

Lemma 17.5. *If p is an odd prime and a is a nonzero QR mod p, then $x^2 \equiv a \pmod{p}$ has exactly two solutions mod p.*

Proof sketch. Using the prime divisor property, show that $x^2 \equiv a \pmod{p}$ has at most two solutions. If one solution is x, then the other is $-x$. It remains to show that $x \not\equiv -x$, or equivalently, that $2x \not\equiv 0$. Indeed, $p \neq 2$ implies that 2 is invertible mod p, and $a \not\equiv 0$ implies that $x \not\equiv 0$. □

Corollary 17.6. *If p is an odd prime, then exactly half the elements of $(\mathbf{Z}/p\mathbf{Z})^\times$ are QRs.*

Proof. Consider the map from $(\mathbf{Z}/p\mathbf{Z})^\times$ to itself that sends $x \mapsto x^2 \pmod{p}$. The image is the set of QRs mod p, and every element of the image has exactly two preimages in $(\mathbf{Z}/p\mathbf{Z})^\times$, by Lemma 17.5. □

Corollary 17.7. *Let p be any prime, and let $a, b \in (\mathbf{Z}/p\mathbf{Z})^\times$.*

(1) If a, b are both QRs, then ab is a QR.
(2) If exactly one of a or b is a QR, then ab is a QNR.
(3) If a, b are both QNRs, then ab is a QR.

Thus the map $\chi : (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$ defined by

$$\chi(a) \equiv \begin{cases} 1 & a \text{ is a QR} \\ -1 & a \text{ is a QNR} \end{cases}$$

is a group homomorphism (with respect to multiplication in both sets).

Proof. Basically the same as Non-Book Problem 4 from Problem Set 2, using the previous corollary. □

Theorem 17.8 (Euler's Criterion)**.** *If p is an odd prime and $a \in (\mathbf{Z}/p\mathbf{Z})^\times$, then*

$$\chi(a) \equiv a^{(p-1)/2} \pmod{p}$$

Proof. By Fermat's little theorem, we must have $a^{p-1} \equiv 1 \pmod{p}$, so by Lemma 17.5, we must have $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. And if $a \equiv x^2$, then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$.

It remains to show that if a is a QNR, then $a^{(p-1)/2} \equiv -1 \pmod{p}$. We do this by a clever counting argument. Indeed, for any $x \in (\mathbf{Z}/p\mathbf{Z})^\times$, the elements x and ax^{-1} must be distinct, because otherwise $x^2 \equiv a$. By pairing up these elements, we deduce that

$$a^{(p-1)/2} \equiv (p-1)! \pmod{p}.$$

By Wilson's theorem, the right-hand side is congruent to -1. □

Proof of Theorem 17.2. Suppose $p > 0$ is prime and $p = 4k + 1$ for some integer k. Then $(-1)^{(p-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p}$. So by Euler's Criterion, -1 is a QR mod p. □