UNIQUE FACTORIZATION AND FERMAT'S LAST THEOREM
LECTURE NOTES

JOSEPH RABINOFF

1. THE DIOPHANTINE EQUATION $x^n + y^n = z^n$

1.1. A history lesson. Diophantine equations are named after Diophantus of Alexandria, an ancient Greek mathematician who made a study of finding *integer* solutions indeterminate polynomial equations. For example, consider the equations:

$$x^2 + y^2 = 3(z^2 + w^2),$$
$$x^2 - ny^2 = \pm 1 \qquad \text{(Pell's equation)},$$

and of course, the Fermat equation

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

Here x, y, z, w are meant to be considered as indeterminates, and n is a fixed integer. The general problem is to find all integer values for x, y, z, w satisfying the given equation, or to show that no such values exist.

This is not something you can simply program a computer to do. In fact, the tenth of Hilbert's famous 23 open problems for 20th-century mathematicians, which he formulated in 1900, asks for the construction of an algorithm for determining the complete set of solutions of a given Diophantine equation. This remained open for 70 years, at which point it was proved that *no such algorithm exists*. Yet the problem of finding solutions to Diophantine equations can be solved in many interesting cases — although the solution is often extremely hard. Much of modern number theory can be regarded as an elaborate piece of machinery constructed in part to solve Diophantine equations.

The Fermat equation $x^n + y^n = z^n$ is the prime example of an extremely simple looking Diophantine equation which has spawned entire schools of mathematics. In around 1637, while reading the section of Diophantus' book *Arithmetica* treating the equation $x^2 + y^2 = z^2$ (more on this in today's homework), Pierre de Fermat scribbled in the margin that there are no (integer) solutions to $x^n + y^n = z^n$ for $n \geq 3$ and $xyz \neq 0$, but that the margin was too small for his "marvelous" proof of this fact. He even posed the cases $n = 3, 4$ as challenges to his mathematical correspondents (at the time, mathematics was a hobby for the intellectually-inclined gentry, and French and English gentleman-mathematicians loved sending each other challenge problems to see who was smarter).

Fermat's supposed proof notwithstanding, this problem remained open for the next 360 years, despite active research during much of that period. Fermat himself provided a proof (in his notes) for $n = 4$. The case $n = 3$ was proved by Leonhard Euler (1770), and $n = 5$ was proved independently by Dirichlet and Legendre (1825). But the first real breakthrough was made by Kummer in the mid-19th century, nearly 200 years after the conjecture became known. Kummer's theory of "ideal numbers" and unique factorization provided a proof for all so-called "regular" prime exponents. It is conjectured that approximately 61% of primes are regular, making Kummer's proof the first that (conjecturally) works for an infinite family of prime exponents. (On the other hand, it is not even known that infinitely many such primes exist!)

This course is about the ideas surrounding Kummer's approach, which form the foundations of modern algebraic number theory.

So, did Fermat indeed have a "marvelous" proof, lost to history? The most likely answer is that his proof was flawed. Many number theorists guess that Fermat's so-called proof ran along the lines of

Kummer's proof for $n = 3$ (which will appear in tomorrow's homework), but has a major gap, namely the existence of unique factorizations of cyclotomic integers. A full proof, no less marvelous, was provided by Andrew Wiles, with help from Richard Taylor, in the mid-1990's, and is one of the most impressive intellectual achievements of the 20th century. I cannot begin to describe the subtlety and edifice that goes into that theory, except to say that a large part of active number theorists today are working on ideas directly descended from Wiles' work, which has a wide range of other impressive applications.

1.2. Reduction steps. The first thing to notice about the equation

$$x^n + y^n = z^n$$

is that there are always infinitely many solutions! Indeed, if $x = 0$ then you can just take $y = z$. But these solutions are not very interesting; this Diophantine problem is about showing that there are no solutions with all of x, y, z *nonzero* and $n \geq 3$. The general strategy will be to assume that there do exist nonzero integers x, y, z and $n \geq 3$ such that $x^n + y^n = z^n$, and derive a contradiction.

There are several reduction steps that one can make right away. Suppose that n is not a prime number. If n has an odd prime divisor p, say $n = m \cdot p$, then we can rewrite our supposed solution as

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

This gives a solution to the Fermat equation with exponent p. If n has no odd prime factors then n is a power of 2; since $n \geq 3$ we must have $n = m \cdot 4$, so

$$(x^m)^4 + (y^m)^4 = (z^m)^4.$$

Therefore it suffices to show that the Fermat equation has no nonzero solutions for prime exponents and for the exponent 4. The latter was done by Fermat, and is outlined in today's homework; the former is the subject of Kummer's strategy.

Let's start off with the "easiest" case, the exponent $n = 3$. (Recall however that even this case wasn't solved for 130 years!) Suppose that we had nonzero integers x, y, z such that $x^3 + y^3 = z^3$. Let $\zeta = e^{2\pi i/3}$. The three *cube roots of unity*, i.e. the three numbers whose cube is 1, are 1 itself, ζ, and $\zeta^2 = e^{4\pi i/3} = \overline{\zeta}$. Thinking of these as the zeros of the polynomial $X^3 - 1$, we have the factorization

$$X^3 - 1 = (X - 1)(X - \zeta)(X - \zeta^2).$$

Letting $X = x/y$, we can write this as

$$\frac{x^3}{y^3} - 1 = \left(\frac{x}{y} - 1\right)\left(\frac{x}{y} - \zeta\right)\left(\frac{x}{y} - \zeta^2\right).$$

Multiplying both sides by y^3 and replacing y by $-y$, we obtain

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

The idea now is to show that the right side of this equation couldn't possibly be a cube by analyzing the "prime factors" of the numbers $x + y$, $x + \zeta y$, and $x + \zeta^2 y$. These are complex numbers though, not integers, so we have to think carefully about what we mean by prime factorization in this situation.

1.3. Prime factorization and Euclid's algorithm. Before we can start thinking about prime factorization of more "exotic" kinds of numbers, we have to have a very good understand of prime factorization of ordinary integers. The existence and uniqueness of prime factorization of ordinary integers is not a trivial theorem — your elementary school teacher (presumably) just didn't tell you the proof!

The story starts with division with remainder. Let a, b be nonzero integers, say with $|b| < |a|$. You know from your 3rd-grade math class that there exists integers q_0 and r_0 with $r_0 < |b|$ such that

$$a = q_0 b + r_0 \quad \text{i.e.} \quad r_0 = a - q_0 b;$$

here q_0 is the "quotient" and r_0 is the remainder. It is clear from the above equations that any common divisor of a and b will also divide r_0, and any common divisor of r_0 and b will divide a. Dividing b by r_0 with remainder, we obtain:

$$b = q_1 r_0 + r_1 \quad \text{i.e.} \quad r_1 = b - q_1 r_0$$

with $r_1 < r_0$. Again, any common divisor of a and b will also divide b and r_0, hence divides r_1, and any common divisor of r_1 and r_0 will divide r_0 and b, hence divides a. Continuing this procedure, we obtain a decreasing sequence of positive integers $r_0 > r_1 > r_2 > \cdots$ such that

$$r_{n-2} = q_n r_{n-1} + r_n$$

for all $n \geq 0$ (if we set $a = r_{-2}$ and $b = r_{-1}$); this will terminate when $r_N = 0$. The numbers $r_0, r_1, r_2, \ldots, r_{N-1}$ are all divisible by any common divisor of a and b, and any common divisor of r_n and r_{n-1} will also be a common divisor of a and b. The above procedure is called *Euclid's algorithm*.

If we substitute the definition of every r_n with $n \geq 0$, we have:

$$\begin{aligned} r_{N-1} &= r_{N-3} - q_{N-1} r_{N-2} \\ &= (r_{N-5} - q_{N-3} r_{N-4}) - q_{N-1}(r_{N-4} - q_{N-2} r_{N-3}) \\ &= \cdots = x \cdot a + y \cdot b \end{aligned}$$

for some integers x, y. Moreover, since $r_N = 0$ we have $r_{N-2} = q_N r_{N-1}$, i.e. r_{N-1} divides r_{N-2}; since r_{N-1} divides itself and r_{N-2}, it also divides a and b. Hence division with remainder has given us:

Proposition 1.4. *Let a, b be nonzero integers.*

(1) *There exists an integer $d = \gcd(a, b)$, called the* greatest common divisor *of a and b, such that $d \mid a$ and $d \mid b$, and such that any common divisor of a and b divides d.*
(2) *There exist integers x, y such that $d = x \cdot a + y \cdot b$.*

From this we can derive existence and uniqueness of prime factorization. Recall that a number $p > 1$ is called *prime* if its only divisors are 1 and itself. The following proposition is very non-obvious if you don't already know the existence of unique factorizations.

Proposition 1.5. *Let p be a prime number and let a, b be integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Suppose that $p \nmid b$. We must show that $p \mid a$. Since the only divisors of p are 1 and itself, and since $p \nmid b$, the greatest common divisor of p and b is 1. Therefore there exist integers x and y such that $x \cdot p + y \cdot b = 1$; multiplying both sides by a, we have

$$xap + yab = a.$$

Since $p \mid xap$ and $p \mid yab$, we have that $p \mid a$. ∎

The following Corollary is in today's homework.

Corollary 1.6. *Let $a > 1$ be an integer. Then a can be written as a product of prime numbers, and this factorization is unique, in that if*

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

where the p_i, q_j are (not necessarily distinct) prime numbers, then $n = m$ and one can reorder $(p_1, \ldots, p_n)$ to obtain $(q_1, \ldots, q_n)$.

Definition 1.7. We say that integers a, b are *relatively prime* or *coprime* provided that $\gcd(a, b) = 1$. Equivalently, a and b are coprime if there exist integers x, y such that $xa + yb = 1$.

2. The ring $\mathbf{Z}[\zeta]$

2.1. Definition and basic properties. Recall that if we had a solution to Fermat's equation

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

in nonzero integers x, y, z, then we could write

$$z^3 = (x + y)(x + \zeta y)(x + \zeta^2 y)$$

where $\zeta = e^{2\pi i/3}$. We would like to analyze the prime factors of the numbers $x-y$, $x-\zeta y$, and $x-\zeta^2 y$ in order to show that the right side of the equation cannot be a cube, and thus derive a contradiction. But what does it mean for one complex number to divide another? If we took the naïve definition "b divides a if there exists c such that $a = bc$", then any nonzero complex number divides any other complex number, since $a = b \cdot \frac{c}{b}$. So we have to be more restrictive about what kinds of complex numbers we allow.

Definition 2.2. The *ring of 3-cyclotomic integers* is the set

$$\mathbf{Z}[\zeta] = \{a + b\zeta \in \mathbf{C} \ : \ a, b \in \mathbf{Z}\},$$

where $\mathbf{Z} = \{\dots, -1, 0, 1, \dots\}$ is the set of integers and $\mathbf{C}$ is the set of complex numbers.

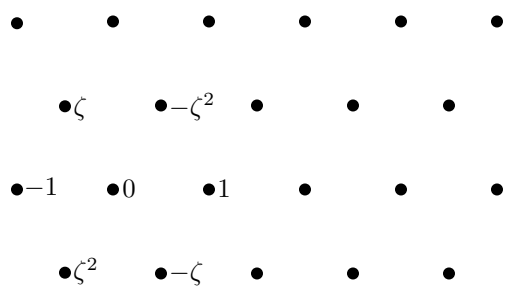

FIGURE 1. A picture of $\mathbf{Z}[\zeta]$, represented as dots in the complex plane.

A picture of this ring can be found in Figure 1. Note that if $a + b\zeta$ is a real number then $b = 0$, so that $\mathbf{Z}[\zeta] \cap \mathbf{R} = \mathbf{Z}$. Note also that since 1 is a root of the polynomial $X^3 - 1$, the polynomial $X - 1$ is a factor of $X^3 - 1$; doing polynomial long division, we have

$$X^3 - 1 = (X - 1)(X^2 + X + 1).$$

Therefore ζ is a root of $X^2 + X + 1$, so

$$\zeta^2 + \zeta + 1 = 0, \quad \text{i.e.,} \quad \zeta^2 = -1 - \zeta.$$

It follows that $\pm 1, \pm\zeta$, and $\pm\zeta^2$ are all contained in $\mathbf{Z}[\zeta]$. More generally:

Proposition 2.3. *The set $\mathbf{Z}[\zeta]$ has the following properties:*

(1) *The numbers $0, 1$ are in $\mathbf{Z}[\zeta]$.*
(2) *If $z, w \in \mathbf{Z}[\zeta]$ then $z + w \in \mathbf{Z}[\zeta]$.*
(3) *If $z, w \in \mathbf{Z}[\zeta]$ then $zw \in \mathbf{Z}[\zeta]$.*

In other words, $\mathbf{Z}[\zeta]$ is a subring *of $\mathbf{C}$.*

Proof. The first part is clear. Let $z = a_1 + a_2\zeta$ and $w = b_1 + b_2\zeta$ with $a_1, a_2, b_1, b_2 \in \mathbf{Z}$. Then

$$z + w = (a_1 + b_1) + (a_2 + b_2)\zeta \in \mathbf{Z}[\zeta],$$

and

$$\begin{aligned} zw &= (a_1 + a_2\zeta)(b_1 + b_2\zeta) \\ &= a_1b_1 + (a_1b_2 + a_2b_1)\zeta + a_2b_2\zeta^2 \\ &= a_1b_1 + (a_1b_2 + a_2b_1)\zeta - a_2b_2(\zeta + 1) \\ &= (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1 - a_2b_2)\zeta \in \mathbf{Z}[\zeta]. \end{aligned}$$

■

2.4. The group of units and the norm. Note that one property *not* included in Proposition 2.3 is existence of reciprocals. For instance, if a is an integer with $|a| > 1$, then $a \in \mathbf{Z}[\zeta]$ but $1/a \notin \mathbf{Z}[\zeta]$. This is a good thing, since if $1/a \in \mathbf{Z}[\zeta]$ for every nonzero $a \in \mathbf{Z}[\zeta]$ then factorizing would be trivial, as

mentioned earlier. Of course, the reciprocal of an ordinary integer isn't necessarily an integer either, and we want this ring to resemble $\mathbf{Z}$ as closely as possible.

Definition 2.5. A *unit* in $\mathbf{Z}[\zeta]$ is a nonzero number $u \in \mathbf{Z}[\zeta]$ such that $1/u \in \mathbf{Z}[\zeta]$ as well. The *group of units* is the set

$$\mathbf{Z}[\zeta]^\times = \{u \in \mathbf{Z}[\zeta] \ : \ 1/u \in \mathbf{Z}[\zeta]\}.$$

Remark 2.6. The units in $\mathbf{Z}$ are just 1 and -1.

The the following proposition says that $\mathbf{Z}[\zeta]^\times$ is a *group*.

Proposition 2.7. *The set $\mathbf{Z}[\zeta]^\times$ has the following properties:*

(1) $1 \in \mathbf{Z}[\zeta]^\times$.
(2) *If $z \in \mathbf{Z}[\zeta]^\times$ then $1/z \in \mathbf{Z}[\zeta]^\times$.*
(3) *If $z, w \in \mathbf{Z}[\zeta]^\times$ then $zw \in \mathbf{Z}[\zeta]^\times$.*

In order to be able to calculate the unit group $\mathbf{Z}[\zeta]^\times$, it is useful to make the following definition.

Definition 2.8. The *norm* of an element $z \in \mathbf{Z}[\zeta]$ is defined to be the square of its complex absolute value, i.e. the norm is $|z|^2 = z\overline{z}$.

Proposition 2.9.

(1) *The norm is multiplicative, in that $|zw|^2 = |z|^2 \cdot |w|^2$ for all $z, w \in \mathbf{Z}[\zeta]$.*
(2) *For all $z \in \mathbf{Z}[\zeta]$ we have $|z|^2 \in \mathbf{Z}$.*
(3) *An element $z \in \mathbf{Z}[\zeta]$ is a unit if and only if $|z|^2 = 1$.*

Proof. The first part follows from the multiplicativity of the complex absolute value. As for the second part, observe that if $z = a + b\zeta \in \mathbf{Z}[\zeta]$ then $\overline{z} = a + b\overline{\zeta} = a + b\zeta^2 \in \mathbf{Z}[\zeta]$ as well, so that $|z|^2 \in \mathbf{Z}[\zeta]$ by Proposition 2.3. However, $|z|^2$ is also a real number, so $|z|^2 \in \mathbf{Z}[\zeta] \cap \mathbf{R} = \mathbf{Z}$.

Suppose now that z is a unit in $\mathbf{Z}[\zeta]$, with reciprocal $w = 1/z \in \mathbf{Z}[\zeta]$. Then

$$1 = |1|^2 = |zw|^2 = |z|^2|w|^2,$$

which shows that $|w|^2 = 1/|z|^2$, and hence $|z|^2$ is a unit in $\mathbf{Z}$. This implies that $|z|^2 = 1$. Conversely, if $z = a + b\zeta \in \mathbf{Z}[\zeta]^\times$ and $|z|^2 = 1$ then

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} = a + b\overline{\zeta} = a + b\zeta^2 \in \mathbf{Z}[\zeta],$$

so $z \in \mathbf{Z}[\zeta]^\times$. ∎

It is clear from Figure 1 then that

$$\mathbf{Z}[\zeta]^\times = \{\pm 1, \pm\zeta, \pm\zeta^2\},$$

which has *six* elements, not two. In fact, $\mathbf{Z}[\zeta]^\times$ is equal to $\boldsymbol{\mu}_6$, the 6th roots of unity, and is therefore a cyclic group (as you showed on yesterday's homework).

2.10. Prime factorization in $\mathbf{Z}[\zeta]$. We define divisibility in $\mathbf{Z}[\zeta]$ in the same way as in $\mathbf{Z}$:

Definition 2.11. Let $z, w \in \mathbf{Z}[\zeta]$. We say that z *divides* w, and we write $z \mid w$, provided that there exists $q \in \mathbf{Z}[\zeta]$ such that $w = qz$.

The definition of a prime element, however, is different. Even the name used in the literature is different:

Definition 2.12. A nonzero element $\pi \in \mathbf{Z}[\zeta]$ is called *irreducible* provided that π is not a unit, and for every factorization $\pi = z \cdot w$ with $z, w \in \mathbf{Z}[\zeta]$, either $z \in \mathbf{Z}[\zeta]^\times$ or $w \in \mathbf{Z}[\zeta]^\times$.

Remark 2.13. Applying this definition to ordinary integers, this says that a number p is irreducible if its only factorizations are $p = 1 \cdot p$ and $p = (-1) \cdot (-p)$. This is the same as the definition of a prime number, except we allow negative numbers to be irreducible! The reason for the new definition is that there is no notion of a "positive element" in $\mathbf{Z}[\zeta]$, so the convention of only calling positive

numbers "prime" no longer makes sense. In other words, if $\pi \in \mathbf{Z}[\zeta]$ is irreducible, then so is $u\pi$ for any $u \in \mathbf{Z}[\zeta]^\times$; no one element of $\{u\pi \,:\, u \in \mathbf{Z}[\zeta]^\times\}$ is better than any other, even though they are all somehow the "same" irreducible number. This discussion will become much more clear when we talk about ideals.

In order to show that factorizations in $\mathbf{Z}[\zeta]$ exist and are unique, we will show that it is possible to do "division with remainder" in $\mathbf{Z}[\zeta]$.

Proposition 2.14. *Let $z, w \in \mathbf{Z}[\zeta]$ with $|w| < |z|$ and $w \neq 0$. There exist $q, r \in \mathbf{Z}[\zeta]$ with $|r| < |w|$ such that*

$$z = q \cdot w + r.$$

Proof. Consider the honest quotient z/w, which is a complex number not necessarily contained in $\mathbf{Z}[\zeta]$. Let q be the point of $\mathbf{Z}[\zeta]$ closest to z/w. It is clear from Figure 2 that every point of $\mathbf{C}$ is contained in the open unit ball centered around a point of $\mathbf{Z}[\zeta]$. Therefore we have $|z/w - q| < 1$. Letting $r = z - qw \in \mathbf{Z}[\zeta]$, we have $z = qw + r$ and

$$|r| = |w| \cdot |z/w - q| < |w|.$$

■

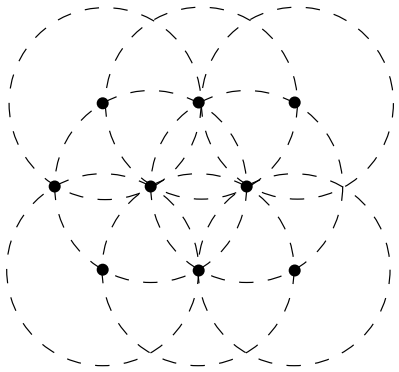

FIGURE 2. Every point in $\mathbf{C}$ is contained in the open unit ball centered around a point of $\mathbf{Z}[\zeta]$.

Now that we can do division with remainder in $\mathbf{Z}[\zeta]$, we can apply Euclid's algorthim to show that prime factorization in $\mathbf{Z}[\zeta]$ works in essentially the same way as in $\mathbf{Z}$.

Corollary 2.15. *Let $a, b \in \mathbf{Z}[\zeta]$ be nonzero elements.*

1. *There exists an element $d = \gcd(a, b) \in \mathbf{Z}[\zeta]$, called the* greatest common divisor *of a and b, such that $d \mid a$ and $d \mid b$, and any common divisor of a and b divides d. This element is unique up to multiplication by a unit.*
2. *There exist $x, y \in \mathbf{Z}[\zeta]$ such that $d = x \cdot a + y \cdot b$.*
3. *Let $\pi \in \mathbf{Z}[\zeta]$ be an irreducible element. If $\pi \mid ab$ then $\pi \mid a$ or $\pi \mid b$.*
4. *Let $a \in \mathbf{Z}[\zeta]$ be nonzero. Then there exist irreducible elements $\pi_1, \dots, \pi_n \in \mathbf{Z}[\zeta]$, not necessarily distinct, such that $a = \pi_1 \cdots \pi_n$. This irreducible decomposition is unique up to reordering of the π_i and multiplication of the π_i by units.*

Remark 2.16. An irreducible element $\pi \in \mathbf{Z}[\zeta]$ satisfying Corollary 2.15(3) for all $a, b \in \mathbf{Z}[\zeta]$ is called *prime*. The content of Corollary 2.15(3) is then that every irreducible element of $\mathbf{Z}[\zeta]$ is prime, so we will not distinguish between the two notions in this ring. We will see later that in other rings, an irreducible element need not be prime; this is essentially the statement that unique factorizations do not exist in such a ring.

Remark 2.17. Roughly, a ring with a size function $|\cdot|$ with respect to which division with remainder (Proposition 2.14) is true is called a Euclidean Domain. These are the rings in which Euclid's algorithm works; any such ring admits unique prime factorizations.

2.18. Factoring prime integers in $\mathbf{Z}[\zeta]$. Of course we can regard an ordinary integer as an integer in $\mathbf{Z}[\zeta]$, so a natural question to ask is, which prime integers are also prime elements of $\mathbf{Z}[\zeta]$? In order to answer this question, we will need the following lemma.

Lemma 2.19. *Let $\pi \in \mathbf{Z}[\zeta]$. If $|\pi|^2$ is a prime integer then π is a prime element of $\mathbf{Z}[\zeta]$.*

Proof. Suppose that $\pi = zw$ for $z, w \in \mathbf{Z}[\zeta]$, and let $p = |\pi|^2$. Then

$$p = |\pi|^2 = |zw|^2 = |z|^2 \cdot |w|^2;$$

since p is prime, this implies that either $|z|^2 = 1$ or $|w|^2 = 1$, which implies that either z or w is a unit by Proposition 2.9. ∎

Proposition 2.20. *Let p be a prime integer. Then either*

1. *p is a prime element of $\mathbf{Z}[\zeta]$, or*
2. *there exists a prime element π of $\mathbf{Z}[\zeta]$ such that $p = |\pi|^2 = \pi\overline{\pi}$, and the complex conjugate $\overline{\pi}$ is prime is well.*

Proof. Suppose that p is not prime. Then there exists a proper prime divisor π of p, say $p = \pi \cdot z$. Since π is not a unit we have $|\pi|^2 > 1$, and since z is not a unit we have $|\pi|^2 = |p|^2/|z|^2 < p^2$, so $p = |\pi|^2 = \pi\overline{\pi}$. By Lemma 2.19, $\overline{\pi}$ is also prime. ∎

The following is a useful consequence of Proposition 2.20.

Corollary 2.21. *Let p be a prime integer that is not prime in $\mathbf{Z}[\zeta]$, say $p = \pi\overline{\pi}$ for $\pi \in \mathbf{Z}[\zeta]$ prime. An ordinary integer n is divisible by p if and only if n is divisible by π.*

Proof. Clearly if n is divisible by p then n is divisible by π. Conversely, suppose that $n = z\pi$ for $z \in \mathbf{Z}[\zeta]$. Then

$$n^2 = |n|^2 = |z|^2 \cdot |\pi|^2 = p \cdot |z|^2,$$

so $p \mid n^2$, and hence $p \mid n$. ∎

The following theorem exactly characterizes which prime integers are also prime elements of $\mathbf{Z}[\zeta]$. Its proof is not difficult given some basic ring theory, but it is beyond the scope of this course.

Theorem 2.22. *A prime integer p is prime in $\mathbf{Z}[\zeta]$ if and only if the polynomial $X^2 + X + 1$ has no zeros modulo p.*

Since $1^2 + 1 + 1 \equiv 0 \pmod 3$, Theorem 2.22 says that 3 is not prime in $\mathbf{Z}[\zeta]$. This is easily verified: we calculate

$$|\zeta - 1|^2 = (\zeta - 1)(\overline{\zeta} - 1) = 1 - \zeta - \overline{\zeta} + 1 = 3$$

because $\overline{\zeta} + \zeta + 1 = \zeta^2 + \zeta + 1 = 0$. Therefore $\zeta - 1$ is prime. However, the prime 3 is unusual in that

$$\overline{\zeta} - 1 = \zeta^2 - 1 = -\zeta^2(\zeta - 1),$$

so $\overline{\zeta} - 1$ is a unit times $\zeta - 1$. In other words, 3 is a unit times $(\zeta - 1)^2$, so 3 is essentially the *square* of a prime in $\mathbf{Z}[\zeta]$. The prime $\zeta - 1$ will play a key role in the proof of Fermat's Last Theorem for $n = 3$, as covered in the homework.

3. Factorization of ideals

3.1. Imaginary quadratic integers. At this point one might be very optimistic that Kummer's approach to Fermat's Last Theorem would work for *any* odd prime exponent. And it is true that most of his proof for the exponent $n = 3$ carries over to $n = p$, using the factorization

$$z^p = x^p + y^p = (x - y)(x - \zeta_p y)(x - \zeta_p^2 y) \cdots (x - \zeta_p^{p-1} y)$$

where $\zeta_p = e^{2\pi i/p}$. The natural ring to work in is the *ring of p-cyclotomic integers*

$$\mathbf{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} \ : \ a_0, a_1, \ldots, a_{p-1} \in \mathbf{Z}\}.$$

There is a subtle, but major problem though: *this ring might not have unique factorizations*! This is likely the mistake that Fermat made in his supposed proof. Before returning to this question, we will analyze some less complicated rings in which unique factorization often fails already.

Definition 3.2. Let $D \geq 1$ be a *squarefree* integer, i.e. an integer not divisible by any squares other than 1. Let $\delta = \sqrt{-D}$, and let

$$\eta = \begin{cases} \delta & \text{if } D \equiv 1, 2 \pmod 4 \\ \frac{1}{2}(1+\delta) & \text{if } D \equiv 3 \pmod 4. \end{cases}$$

The *ring of imaginary quadratic integers for $-D$* is the set

$$\mathbf{Z}[\eta] = \{a + b\eta \ : \ a, b \in \mathbf{Z}\}.$$

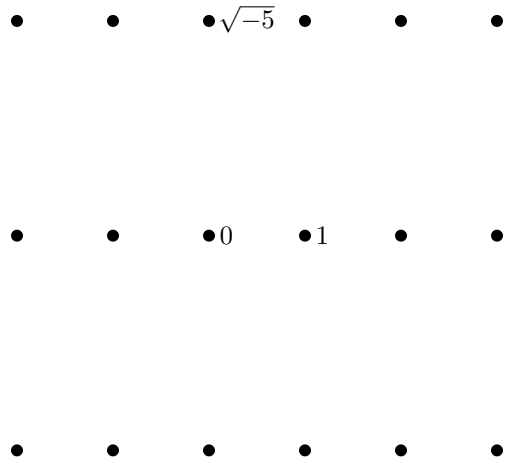

FIGURE 3. A picture of $\mathbf{Z}[\sqrt{-5}]$, the ring of imaginary quadratic integers for -5. This is a rectangular lattice since $5 \equiv 1 \pmod 4$.

If $D \not\equiv 3 \pmod 4$ then

$$\mathbf{Z}[\eta] = \mathbf{Z}[\delta] = \{a + b\sqrt{-D} \ : \ a, b \in \mathbf{Z}\},$$

and otherwise,

$$\mathbf{Z}[\eta] = \{a + b\sqrt{-D} \ : \ a, b \in \mathbf{Z} \text{ or } a, b \in \mathbf{Z} + 1/2\}.$$

In today's homework you'll see why this funny definition is the correct one. For now we note that η satisfies the polynomial equation with integer coefficients

$$\eta^2 - \eta + \frac{1}{4}(D+1) = 0$$

when $D \equiv -1 \pmod 4$. In particular, $\eta^2 \in \mathbf{Z}[\eta]$.

Since

$$\zeta = e^{2\pi i/3} = \cos(2\pi i/3) + i\sin(2\pi i/3) = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} = -1 + \frac{1}{2}(1+\sqrt{-3}),$$

the ring of 3-cyclotomic integers $\mathbf{Z}[\zeta]$ is equal to the ring of imaginary quadratic integers for -3. General rings of imaginary quadratic integers satisfy many of the properties of the ring $\mathbf{Z}[\zeta]$ *not* having to do with unique factorization. The proofs of these facts go through almost unchanged from the case of $\mathbf{Z}[\zeta]$.

Proposition 3.3. *Let $D \geq 1$ be a squarefree integer and let $R = \mathbf{Z}[\eta]$ be the ring of imaginary quadratic integers for $-D$.*

(1) *R is a subring of $\mathbf{C}$.*
(2) *If $z \in R$ then $|z|^2 \in \mathbf{Z}$. This integer is called the* norm *of z.*
(3) *The set $R^\times = \{u \in R \ : \ 1/u \in R\}$ of* units *is a group.*
(4) *An element $u \in R$ is a unit if and only if $|u|^2 = 1$.*
(5) *We have $R \cap \mathbf{R} = \mathbf{Z}$.*

Unique factorization, on the other hand, can fail horribly! In the ring $\mathbf{Z}[\sqrt{-5}]$ we have

$$6 = 2 \cdot 3 = (1+\delta)(1-\delta).$$

Clearly 2 and 3 do not divide $1 \pm \delta$. Furthermore, 2, 3, and $1 \pm \delta$ are irreducible, as you will show in the homework.

Definition 3.4. Let R be an imaginary quadratic integer ring.

(1) A nonzero element $\pi \in R$ is called *irreducible* provided that π is not a unit, and for every factorization $\pi = z \cdot w$ with $z, w \in R$, either $z \in \mathbf{Z}[\zeta]^\times$ or $w \in R^\times$.
(2) A nonzero element $\pi \in R$ is called *prime* provided that π is not a unit, and for every $z, w \in R$, if $\pi \mid zw$, then $\pi \mid z$ or $\pi \mid w$.

3.5. Ideals in imaginary quadratic integer rings. Kummer's beautiful idea was to *replace* numbers with so-called "ideal numbers" (nowadays simply called ideals) in order to recover unique factorization.

Definition 3.6. Let R be an imaginary quadratic integer ring. A subset I of R is called an *ideal* provided that

(1) I contains 0 and is closed under sums and differences (i.e. I is an additive subgroup of R), and
(2) for $r \in R$ and $z \in I$ we have $rz \in I$.

Note that $(0) = \{0\}$ is always an ideal in R, called the *zero ideal*. Likewise, $(1) = R$ is an ideal in R, called the *unit ideal*.

Definition 3.7. Let $z_1, \ldots, z_n \in R$ be any elements. The *ideal generated by* $z_1, \ldots, z_n$ is the set

$$(z_1, \ldots, z_n) \coloneqq \{r_1 z_1 + \cdots + r_n z_n \ : \ r_1, \ldots, r_n \in R\}.$$

An ideal generated by a single element $(z) = \{rz \ : \ r \in R\}$ is called *principal*.

Example 3.8. Let $\delta = \sqrt{-5}$. Consider the ideal $I = (2, 1+\delta)$ of Figure 4. We claim that

$$I = \{2a + b(1+\delta) \ : \ a, b \in \mathbf{Z}\}.$$

Let I' denote the set on the right side of the above equation. Clearly $I' \subset I$, and $2, 1+\delta \in I'$. On the other hand,

$$2\delta = -2 + 2(1+\delta) \in I' \quad \text{and} \quad \delta(1+\delta) = -5 + \delta = 2(-3) + (1+\delta) \in I'.$$

An arbitrary element z of I can be written

$$z = (a + b\delta)2 + (c + d\delta)(1+\delta) = 2a + 2\delta \cdot b + c(1+\delta) + d \cdot \delta(1+\delta),$$

which implies that $I' = I$ because I' is a subgroup of $\mathbf{Z}[\delta]$.

The ideal I is *not* a principal ideal. Indeed, if $I = (z)$ for some $z \in \mathbf{Z}[\delta]$ then $2 = wz$ and $1+\delta = w'z$ for some w, w'. But 2 and $1+\delta$ are irreducible (as noted above), so this would imply that $2 = u(1+\delta)$ for some $u \in \mathbf{Z}[\zeta]^\times = \{\pm 1\}$, which is clearly not the case.

Any nonzero ideal in an imaginary quadratic integer ring R is a *lattice* in $\mathbf{C}$: it is a discrete subgroup of $\mathbf{C}$ not contained in a line. It is known that any lattice I is of the form $I = \{az + bw \ : \ a, b \in \mathbf{Z}\}$ for some $z, w \in I$. Therefore I always can be generated by (at most) two elements.

Many notions about divisibility of numbers can be carried over to ideals.

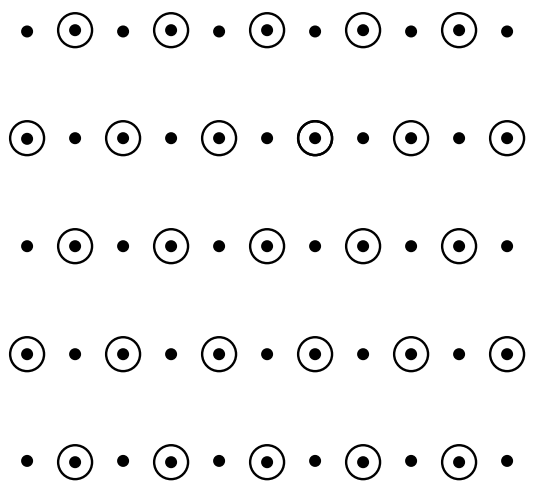

FIGURE 4. The ideal $(2, 1+\delta)$ in the ring $\mathbf{Z}[\delta]$, with $\delta = \sqrt{-5}$.

Definition 3.9. Let R be an imaginary quadratic integer ring and let $I, J \subset R$ be ideals.

(1) We say that I *divides* J provided that $J \subset I$.
(2) We say that I is *prime* provided that $I \neq R$, and for all $z, w \in R$, if $zw \in I$ then either $z \in I$ or $w \in I$.
(3) The *product ideal* IJ is the ideal generated by all elements of the form zw for $z \in I$ and $w \in J$.

The following Proposition shows that we can do "algebra" with ideals. The set of ideals form what is called a *monoid* under ideal multiplication, which is like a group without the existence of inverses.

Proposition 3.10.

(1) *If* $I = (z_1, z_2)$ *and* $J = (w_1, w_2)$ *then* $IJ = (z_1w_1, z_1w_2, z_2w_1, z_2w_2)$.
(2) *If* I *and* J *are ideals then* $IJ = JI \subset I \cap J$.
(3) *If* I, J, K *are ideals then* $(IJ)K = I(JK)$.
(4) *For any ideal* I *we have* $I(1) = I$ *and* $I(0) = (0)$.

We can associate an ideal to an element $z \in R$ by simply considering the principal ideal generated by z. The following Proposition shows that the above notions concerning ideals coincide with the analogous notions for elements of R under this association.

Proposition 3.11. (Ideal-element dictionary) *Let* R *be an imaginary quadratic integer ring and let* $z, w \in R$.

(1) z *divides* w *if and only if the ideal* (z) *divides* (w)*, which is true if and only if* $w \in (z)$.
(2) z *is prime if and only if* (z) *is prime.*
(3) *The product ideal* $(z)(w)$ *is equal to* (zw).

Proof. We will only prove (1), leaving (2) and (3) as exercises. Suppose that $z \mid w$. Then there exists $r \in R$ such that $w = rz$, so $w \in (z)$. Hence $sw \in (z)$ for all $s \in R$, so $(w) \subset (z)$. Conversely, if $(w) \subset (z)$ then $w \in (z)$, so there exists r such that $w = rz$. ■

Remark 3.12. It follows from Proposition 3.11 that if $(z) = (w)$ then $z \mid w$ and $w \mid z$, so that z and w differ by multiplication by a unit.

Definition 3.13. An imaginary quadratic integer ring R is called a *principal ideal domain* or a PID if every ideal of R is principal.

The principal ideal domains are exactly the rings in which Euclid's algorithm "works":

Proposition 3.14. *Let R be an imaginary quadratic integer ring. Then R is a principal ideal domain if and only if, for every $z, w \in R$, there exists an element $d \in R$, called the* greatest common divisor *of z and w, such that*

(1) *d divides z and w,*
(2) *if d' divides z and w then d' divides d, and*
(3) *there exist $r, s \in R$ such that $d = r \cdot z + s \cdot w$.*

Proof. Suppose that R is a PID. Then the ideal (z, w) is generated by a single element d. Since $z, w \in (d)$, we have $(z), (w) \subset (d)$, and hence $d \mid z$ and $d \mid w$. Since $d \in (z, w)$ there exist $r, s \in R$ such that $d = r \cdot z + s \cdot w$. If $d' \mid z$ and $d' \mid w$ then $z, w \in (d')$, so $d = rz + sw \in (d')$, and hence $d' \mid d$.

The proof that (1)–(3) imply that R is a PID is an exercise. ■

In particular, any Euclidean domain is a PID, so $\mathbf{Z}$ and $\mathbf{Z}[\zeta]$ are PIDs. As a formal consequence of Proposition 3.14, we get existence and uniqueness of prime factorizations.

Corollary 3.15. *Let R be an imaginary quadratic integer ring. If R is a principal ideal domain then any irreducible element of R is prime, and existence and uniqueness of prime factorizations holds in R.*

Proof. The proof of the first part is the same as the proof of Proposition 1.5, and the second part is in the homework. ■

Remark 3.16. The converse of Corollary 3.15 is also true: if R is an imaginary quadratic integer ring in which all irreducible elements are prime, then R is a PID (and hence Euclid's algorithm automatically works). The proof is beyond the scope of this class. This phenomenon is *not* a general fact about rings in which unique factorization holds, but rather has to do with the fact that an imaginary quadratic integer ring has "dimension 1". For instance, the polynomial ring $\mathbf{C}[X, Y]$, which has "dimension 2", also has unique factorizations, in that any bivariate polynomial can be expressed in a unique way (up to reordering and multiplication by nonzero scalars) as a product of irreducible polynomials. However, although the elements X and Y clearly have no common divisors, there do not exist polynomials $f(X, Y), g(X, Y) \in \mathbf{C}[X, Y]$ such that $1 = f(X, Y)\, X + g(X, Y)\, Y$ (substitute $X = Y = 0$ into the right side).

3.17. Unique factorization of ideals. In the ring $\mathbf{Z}[\sqrt{-5}]$ we had the problem that the number 6 had two distinct factorizations, namely,

$$6 = 2 \cdot 3 = (1 + \delta)(1 - \delta).$$

By passing to ideals, we can fix this problem, as follows. Let

$$I = (2, 1 + \delta) \qquad \overline{I} = (2, 1 - \delta) \qquad J = (3, 1 + \delta) \qquad \overline{J} = (3, 1 - \delta).$$

Then

$$I\overline{I} = (4,\ 2 + 2\delta,\ 2 - 2\delta,\ 6);$$

this ideal contains $2 = 6 - 4$, so $(2) \subset I\overline{I}$, and since 2 divides $4, 2 \pm 2\delta$, and 6, we have $I\overline{I} = (2)$. Similarly, $J\overline{J} = (3)$. On the other hand,

$$IJ = (6,\ 2(1 + \delta),\ 3(1 + \delta),\ (1 + \delta)^2);$$

hence $1 + \delta = 3(1 + \delta) - 2(1 + \delta) \in IJ$, so $(1 + \delta) \subset IJ$, and since $1 + \delta$ divides the generators of IJ, we in fact have $IJ = (1 + \delta)$. Similarly, $\overline{IJ} = (1 - \delta)$. Therefore our two factorizations of 6 become

$$(6) = (2)(3) = (I\overline{I})(J\overline{J}) = (IJ)(\overline{IJ}) = (1 + \delta)(1 - \delta).$$

In other words, the *ideal* generated by 6 has the factorization $I\overline{I}J\overline{J}$, which *refines* the two factorizations $6 = 2 \cdot 3$ and $6 = (1 + \delta)(1 - \delta)$. In this sense, replacing numbers with ideals has solved our unique factorization problems!

Theorem 3.18. *Let R be an imaginary quadratic integer ring. Every nonzero proper ideal $I \subsetneq R$ is equal to a product of nonzero prime ideals of R. This factorization is unique, up to reordering of the factors.*

Remark 3.19. If R is a PID, then Theorem 3.18 implies that unique factortion of elements in R holds. Indeed, if $z \in R$ is a nonzero non-unit then (z) is a nonzero proper ideal of R. Let $(z) = P_1 \cdots P_r$ be the prime factorization of (z), and let π_i be a generator of P_i. Then π_i is a prime element, and $(z) = (\pi_1 \cdots \pi_r)$, so z and $\pi_1 \cdots \pi_r$ differ by a unit. The ideal factorization theorem is much nicer to state however, since the *ideals* $P_1, \dots, P_r$ are uniquely determined up to reordering, but the *elements* $\pi_1, \dots, \pi_r$ are only determined up to reordering and multiplication by units.

In order to prove Theorem 3.18, we will need the following fact, which you will prove in the homework. First note that an imaginary quadratic integer ring R is closed under complex conjugation, and that if $I \subset R$ is an ideal then

$$\overline{I} = \{\overline{z} \ : \ z \in I\} \subset R$$

is again an ideal in R.

Lemma 3.20. (Main Lemma) *Let R be an imaginary quadratic integer ring and let $I \subset R$ be an ideal. Then there exists an integer $n \in \mathbf{Z}$ such that $I\overline{I} = (n)$. In particular, $I\overline{I}$ is* principal.

Proposition 3.21. *Let R be an imaginary quadratic integer ring and let $I, J \subset R$ be nonzero ideals.*

1. (Cancellation law) *Let $K \subset R$ be a nonzero ideal. If $IJ \supset IK$ then $J \supset K$, and if $IJ = IK$ then $J = K$.*
2. *We have $I \supset J$ (i.e. I divides J) if and only if there exists an ideal $K \subset R$ such that $J = IK$.*
3. *A nonzero prime ideal $P \subset R$ divides IJ if and only if P divides I or P divides J.*

Proof.

1. Clearly the second statement follows from the first. Suppose that $IJ \supset IK$. If $I = (z)$ is principal, then $IJ = zJ = \{zv \ : \ v \in J\}$ and $IK = zK = \{zw \ : \ w \in K\}$. Since $IK \subset IJ$, for every $w \in K$ there exists $v \in J$ such that $zw = zv$; dividing both complex numbers by z, we have $w = v$, so that $K \subset J$. If I is not principal, then
$$(n)J = \overline{I}IJ \supset \overline{I}IK = (n)K,$$
so we can apply the above argument (replacing I by (n)) to again conclude that $J \supset K$.
2. If $J = IK$ then $I \supset J$ because $I \supset IK$. Conversely, suppose that $I \supset J$. Assume for the moment that $I = (z)$ is principal. To say that I contains J means that every element of J divides z, so
$$z^{-1}J = \{z^{-1}w \ : \ w \in J\}$$
is again an ideal in R. Clearly $I(z^{-1}J) = (z)(z^{-1}J) = J$, so this proves the Proposition in this case. If I is not principal, then $(n) = \overline{I}I \supset \overline{I}J$, so by the above there exists an ideal K such that $\overline{I}IK = (n)K = \overline{I}J$; using the cancellation law, this implies that $IK = J$, as desired.
3. We only need to show that if $P \supset IJ$ then $P \supset I$ or $P \supset J$. Suppose that $P \not\supset I$, so there exists $z \in I$ such that $z \notin P$. For every $w \in J$ we have $zw \in IJ \subset P$, so $w \in P$ and hence $P \supset J$.

■

In order to prove Theorem 3.18, we will need the following basic facts from the theory of rings. (Actually, part (3) is a fact about lattices.)

Lemma 3.22. *Let R be an imaginary quadratic integer ring.*

1. *If a proper ideal $I \subsetneq R$ is* maximal *in the sense that I and R are the only ideals of R containing I, then I is prime.*
2. *Any proper ideal of R is contained in a maximal ideal of R.*
3. *If $I \subset R$ is a nonzero ideal then there are only finitely many ideals J such that $I \subsetneq J \subsetneq R$.*

Proof of Theorem 3.18**.** First we need to show that any nonzero proper ideal $I \subsetneq R$ can be factored into a product of prime ideals. Let P_1 be a maximal ideal of R containing I. If $I = P_1$ then we are done, and otherwise there exists an ideal $I_1 \subset R$ such that $I = P_1 I_1$ by Proposition 3.21(2). Note that $I_1 \supsetneq I$ since $P_1 \neq R$. If I_1 is not prime, then we can find a prime ideal P_2 and an ideal $I_2 \supsetneq I_1$

such that $I_1 = P_2 I_2$, so $I = P_1 P_2 I_2$. We can continue this procedure indefinitely; it must terminate eventually by Lemma 3.22(3). This proves the existence of prime factorizations. Uniqueness is a straightforward consequence of Proposition 3.21. ■

4. Geometry of numbers and the class group

4.1. Ideal classes. Let R be an imaginary quadratic integer ring. By Corollary 3.15 and the remark following it, unique factorization holds in R if and only if R is a principal ideal domain. The ideal class group is meant to measure to what extent R fails to be a principal ideal domain, and hence to what extent factorizations in R can fail to be unique.

Definition 4.2. Let R be an imaginary quadratic integer ring and let $I, J \subset R$ be nonzero ideals. We say that I and J are *homothetic*, and we write $I \sim J$, provided that there exist nonzero elements $z, w \in R$ such that $zI = wJ$. (Here zI is shorthand for the product ideal $(z)I$, and likewise for wJ.) Homothety is an equivalence relation; an equvalence class with respect to this relation is called an *ideal class*, and the set of all equivalence classes is the *ideal class group*. We denote the ideal class group by $\mathscr{C}(R)$, and we write $[I]$ to denote the ideal class represented by a (nonzero) ideal I.

Remark 4.3. A nonzero ideal I is homothetic to the unit ideal R if and only if there exist $z, w \in R$ such that $zI = wR = (w)$. Hence $w \mid z$, so $w/z \in R$ and $I = (w/z)$ is principal. In other words, the class of $[R]$ is exactly the set of *principal* ideals of R. In particular, R is a principal ideal domain (i.e. has unique factorizations) if and only if $\mathscr{C}(R) = \{[R]\}$.

We define a multiplication law on $\mathscr{C}(R)$ as follows: for $I, J \subset R$ nonzero ideals, set

$$[I] \cdot [J] = [IJ].$$

In order to show that this is well-defined, suppose that $I \sim I'$ and $J \sim J'$, so $[I] = [I']$ and $[J] = [J']$. Then there exist $z, z', w, w' \in R$ such that $zI = z'I'$ and $wJ = w'J'$, so $zwIJ = z'w'I'J'$, so $IJ \sim I'J'$ and hence $[IJ] = [I'J']$.

The following proposition shows that the ideal class group $\mathscr{C}(R)$ is in fact a commutative group under multiplication.

Proposition 4.4. *Let R be an imaginary quadratic integer ring and let $I, J, K \subset R$ be nonzero ideals.*

(1) $[I] \cdot [J] = [J] \cdot [I]$
(2) $([I] \cdot [J]) \cdot [K] = [I] \cdot ([J] \cdot [K])$
(3) $[I] \cdot [R] = [R] \cdot [I] = [I]$
(4) *There exists a nonzero ideal $I' \subset R$ such that $[I] \cdot [I'] = [R]$.*

Proof. Assertions (1)–(3) follow from the corresponding properties of ideal multiplication (for instance, $[I][J] = [J][I]$ because $IJ = JI$). The fourth follows from the Main Lemma 3.20: there exists $n \in \mathbf{Z}$ such that $I\overline{I} = (n)$, so $[I][\overline{I}] = [I\overline{I}] = [(n)] = [R]$. ■

4.5. Lattices and norms. The ideal class group of an imaginary quadratic integer ring R is in fact a *finite* commutative group. In order to prove this fact, and to be able to actually calculate the ideal class group, we need to analyze the geometric properties of R and its nonzero ideals as subsets of $\mathbf{C}$. To start out, it is useful to consider these subsets as lattices.

Recall that a *lattice* in $\mathbf{C}$ is a discrete subgroup $L \subset \mathbf{C}$ not contained in a line. If L is a lattice then there exist nonzero elements $z, w \in L$ such that every element of L can be uniquely written in the form $az + bw$ for $a, b \in \mathbf{Z}$; such a pair (z, w) is called a *lattice basis* for L. Let $\Delta(L)$ denote the area of the paralellogram whose vertices are $0, z, w$, and $z + w$; such a paralellogram (or any translate thereof) is called a *fundamental domain*. We will use the following facts about lattices:

Lemma 4.6. *Let $L \subset \mathbf{C}$ be a lattice.*

(1) *The number $\Delta(L)$ does not depend on the choice of lattice basis.*
(2) *Let $L' \subset \mathbf{C}$ be a lattice contained in L. The size of the quotient group L/L' is equal to $\Delta(L')/\Delta(L)$.*

The proof of part (1) is in today's homework. The size of the group L/L' in Lemma 4.6(2) is called the *index* of L' in L, and is denoted $[L : L'] = \#(L/L')$. Here is an idea of why (2) is true, if we take (1) for granted. It can be shown that one can choose a lattice basis (z, w) for L such that (az, bw) is a lattice basis for L' for some positive integers a, b. The associated fundamental domain for L' is tiled by $a \cdot b$ fundamental domains for L, so we must show that $[L : L'] = ab$. This is true because every coset in L/L' is represented by the lower-left vertex of a unique fundamental domain of L' contained in a fundamental domain for L. See Figure 5.

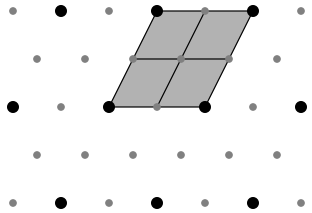

FIGURE 5. A lattice L, represented by big and small dots in the plane, and a sublattice L' consisting of only the big dots. A fundamental domain for L' is shaded in gray; this fundamental domain is tiled by four fundamental domains for L, so $\Delta(L')/\Delta(L) = 4$. Every coset in L/L' is represented by lower-left vertex of a unique fundamental domain of L contained in the fundamental domain for L'.

Let R be the imaginary quadratic integer ring for $-D$, regarded as a lattice in $\mathbf{C}$. If $D \equiv -1 \pmod 4$ then $R = \mathbf{Z}[\eta] = \{a + b\eta \,:\, a, b \in \mathbf{Z}\}$, where $\eta = (1 + \sqrt{-D})/2$. It follows that 1 and η form a lattice basis for R, so $\Delta(R) = \frac{1}{2}\sqrt{D}$ since the area of a paralellogram is equal to the length of the base times the height. If $D \equiv 1, 2 \pmod 4$ then $(1, \delta)$ is a fundamental domain for R, where $\delta = \sqrt{-D}$, so $\Delta(R) = \sqrt{D}$. To summarize:

(4.6.1)
$$\Delta(R) = \begin{cases} \frac{1}{2}\sqrt{D} & \text{if } D \equiv -1 \pmod 4 \\ \sqrt{D} & \text{if } D \equiv 1, 2 \pmod 4. \end{cases}$$

Definition 4.7. Let R be an imaginary quadratic integer ring, let $I \subset R$ be a nonzero ideal, and let $\overline{I} \subset R$ be its complex conjugate. By the Main Lemma 3.20, the product $I\overline{I}$ is generated by an integer n. The positive integer $|n|$ is called the *norm* of the ideal I, and is denoted $N(I)$.

Remark 4.8.

(1) The norm is well-defined since any other generator of $I\overline{I}$ is equal to a unit times n, and the absolute value of any unit is equal to 1.

(2) Let $I, J \subset R$ be nonzero ideals and let $n = N(I)$ and $m = N(J)$. We have $\overline{IJ} = \overline{I} \cdot \overline{J}$, so
$$(IJ)(\overline{IJ}) = IJ\overline{I}\,\overline{J} = I\overline{I}J\overline{J} = (I\overline{I})(J\overline{J}) = (n)(m) = (nm).$$
It follows that $N(IJ) = nm = N(I)N(J)$, so the norm is multiplicative.

(3) If $I = (z)$ is a principal ideal then $\overline{I} = \overline{z}$, so $I\overline{I} = (z\overline{z}) = (|z|^2)$, and therefore the norm of the ideal generated by z coincides with the norm of the element z:
$$N((z)) = |z|^2.$$

We omit the proof of the following proposition due to lack of time.

Proposition 4.9. *Let R be an imaginary quadratic integer ring and let $I \subset R$ be a nonzero ideal. Regarding I and R as lattices in $\mathbf{C}$, we have*
$$N(I) = [R : I] = \Delta(I)/\Delta(R).$$

4.10. Geometry of numbers. The central fact in this theory is a lemma of Minkowski. In order to state this lemma, we will need the following definitions:

Definition 4.11. A subset $S \subset \mathbf{C}$ is *convex* provided that for every two points $x, y \in S$, the line segment from x to y is contained in S. It is *centrally symmetric* if, for every $x \in S$, we also have $-x \in S$.

Lemma 4.12. (Minkowski's Lemma) *Let $L \subset \mathbf{C}$ be a lattice and let S be a convex, centrally symmetric subset. If the area of S is greater than $4\Delta(L)$, then S contains a lattice point of L other than zero.*

We will not give a proof Minkowski's Lemma. It is geometrically very intuitive: see Figure 6. The *geometry of numbers* is roughly the study of the applications of Minkowski's lemma (and statements of a similar flavor) to rings of algebraic integers and their ideals. The following theorems are excellent examples.

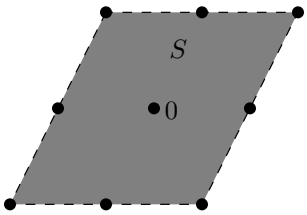

FIGURE 6. Let L be the lattice in $\mathbf{C}$ represented by the black dots, with 0 being the dot in the middle. The area of the convex, centrally symmetric shaded region S is exactly equal to $4\Delta(L)$. It is impossible to find a larger convex, centrally symmetric region that does not contain any other lattice points.

Theorem 4.13. *Let R be an imaginary quadratic integer ring and let*

$$\mu = \frac{4}{\pi}\Delta(R) = \begin{cases} \frac{2}{\pi}\sqrt{D} & \text{if } D \equiv -1 \pmod 4 \\ \frac{4}{\pi}\sqrt{D} & \text{if } D \equiv 1, 2 \pmod 4. \end{cases}$$

Every ideal class contains an ideal I such that $N(I) \leq \mu$.

Proof. Let $I \subset R$ be any nonzero ideal. Applying Lemma 4.12 to a disc of radius $r > \sqrt{4\Delta(I)/\pi}$ (which has area greater than $4\Delta(I)$), we find that for any $\varepsilon > 0$ there exists a nonzero element $z \in I$ such that $|z|^2 \leq \frac{4}{\pi}\Delta(I) + \varepsilon$. From this it is clear that there exists a nonzero element $z \in I$ such that $|z|^2 \leq \frac{4}{\pi}\Delta(I)$. Since $(z) \subset I$, by Proposition 3.21(2) there exists a nonzero ideal $J \subset R$ such that $(z) = IJ$. Taking norms of both sides, we have

$$N(I)N(J) = N(IJ) = N((z)) = |z|^2 \leq \frac{4}{\pi}\Delta(I) = \frac{4}{\pi}N(I)\Delta(R).$$

Canceling the factors of $N(I)$, this gives $N(J) \leq \mu$. Hence there exists a representative J of the ideal class $[J] = [I]^{-1}$ with $N(J) \leq \mu$. Switching the roles of I and J proves the theorem. ∎

Theorem 4.14. (Finiteness of the class group) *The ideal class group $\mathscr{C}(R)$ of an imaginary quadratic integer ring R is finite.*

Proof. By Theorem 4.13 and Proposition 4.9, it is enough to show that there are only finitely many ideals I with $N(I) = [R : I] \leq \mu$. We will show the stronger fact that there are only finitely many *lattices* $L \subset R$ with $[R : L] \leq \mu$. Let $n \leq \mu$. If $[R : L] = \#(R/L) = n$ then $nx = 0$ for all $x \in R/L$, so $nR \subset L \subset R$. There is a bijective correspondence between the set of subgroups of R/nR and the set of subgroups of R containing nR, so the theorem follows from the fact that R/nR is a finite group. ∎

4.15. Calculating the ideal class group. The following consequence of Theorem 4.13 will allow us to actually calculate some ideal class groups.

Corollary 4.16. *The ideal class group $\mathscr{C}(R)$ of an imaginary quadratic integer ring R is generated by the classes of the prime ideals P which divide the ideals generated by the prime integers $p \leq \mu$.*

Proof. Any ideal class contains a representative I with $N(I) \leq \mu$. Let $I = P_1 \cdots P_r$ be the prime factorization of I. Then $N(I) = N(P_1) \cdots N(P_r)$, so $N(P_i) \leq \mu$. In the homework you will show that there exists a prime integer $p_i \in \mathbf{Z}$ such that either $P_i\overline{P}_i = (p_i)$, in which case $p_i = N(P_i) \leq \mu$, or $P_i = (p_i)$, in which case $p_i^2 = N(P_i) \leq \mu$. In either case, P_i divides (p_i). ■

It follows from Corollary 4.16 that in order to calculate the ideal class group, all one has to do is to factor the ideals generated by integer primes p with $p \leq \mu$, and then find the relations between the prime factors.

Example 4.17. Let $D = 7$. Then $\mu = \frac{2}{\pi}\sqrt{D} \approx 1.68$, so Corollary 4.16 says that $\mathscr{C}(R)$ is generated by the *empty* set of classes of prime ideals, i.e. that $\mathscr{C}(R)$ is trivial. It follows that R is a PID, and therefore has unique factorization. Note that this method of proving that Euclid's algorithm wolks in R is *very* different than using division with remainder!

Example 4.18. Let $D = 5$. Then $\mu = \frac{4}{\pi}\sqrt{D} \approx 2.85$, so $\mathscr{C}(R)$ is generated by the classes of the prime factors of (2). We have already calculated that

$$(2) = (2, 1+\delta)(2, 1-\delta),$$

with $P = (2, 1+\delta)$ prime (as you will show on the homework). We have

$$P^2 = P \cdot P = \big(4,\, 2(1+\delta),\, (1+\delta)^2\big) = \big(4,\, 2(1+\delta),\, 2(2-\delta)\big)$$

since $(1+\delta)^2 = -2(2-\delta)$. Since every generator is divisible by 2 we have $P^2 \subset (2)$, so $P^2 \subset P\overline{P}$ and hence $P \subset \overline{P}$ by the cancellation law; since P and $\overline{P}$ are both prime we must have equality. It follows that $[P]^2 = [P]^{-1}$, so $\mathscr{C}(R)$ is isomorphic to the cyclic group of order 2.

You will do many more such calculations in the homework. There is a lot that is known about the size of the class group of an imaginary quadratic field:

Theorem 4.19. *Let R be the ring of imaginary quadratic integers for $-D$. Then R is a unique factorization domain if and only if*

$$D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

The proof of this theorem is very hard.

5. Further directions

5.1. General setup. Most of the results proved in the previous section for imaginary quadratic integer rings hold in much greater generality. For our purposes, we define a *number field* to be a subfield of $\mathbf{C}$ which is finite dimensional as a vector space over $\mathbf{Q}$. If F is a number field, its *ring of integers* is the set $\mathscr{O}_F$ of elements $z \in F$ such that there exists a monic polynomial equation $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ with *integer* coefficients $a_0, a_1, \ldots, a_{n-1}$ such that $f(z) = 0$. It is a fact that $\mathscr{O}_F$ is a subring of F.

Example 5.2. Let $D \geq 1$ be a squarefree integer and let $F = \mathbf{Q}(\sqrt{-D}) = \{a + b\sqrt{-D} \ : \ a, b \in \mathbf{Q}\}$. Then $\mathscr{O}_F$ is the imaginary quadratic integer ring for D, as you essentially showed on the homework.

Example 5.3. Let $n \geq 2$ be an integer, let $\zeta_n = e^{2\pi i/n}$, and let

$$F = \mathbf{Q}(\zeta_n) = \big\{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1} \ : \ a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}\big\}.$$

Then $\mathbf{Q}(\zeta_n)$ is a subfield of $\mathbf{C}$ of dimension n as a $\mathbf{Q}$-vector space, called the *field of n-cyclotomic numbers*. Its ring of integers is

$$\mathscr{O}_F = \mathbf{Z}[\zeta_p] = \big\{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1} \ : \ a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}\big\};$$

an element of $\mathscr{O}_F$ is called an *n-cyclotomic integer*. Note that $\mathscr{O}_F$ is "too big" to be a lattice in $\mathbf{C}$.

The theory of ideal factorization is developed in exactly the same way for the ring of integers $\mathscr{O}_F$ in a general number field F as for an imaginary quadratic integer ring. In this generality the Main Lemma is not true as stated in Lemma 3.20; what is true is the following:

Lemma 5.4. *Let F be a number field. For any nonzero ideal $I \subset \mathscr{O}_F$, there exists some nonzero ideal $I' \subset \mathscr{O}_F$ such that II' is principal.*

One deduces the existence and uniqueness of prime factorizations of ideals in much the same way as before:

Theorem 5.5. *Let F be a number field and let $I \subset \mathscr{O}_F$ be a nonzero ideal. Then there exist prime ideals $P_1, \ldots, P_r \subset \mathscr{O}_F$ such that $I = P_1 \cdots P_r$. This prime factorization is unique up to reordering of the prime factors.*

One defines ideal classes in $\mathscr{O}_F$ in exactly the same way as in imaginary quadratic integer rings; Lemma 5.4 then shows that the set of ideal classes $\mathscr{C}(\mathscr{O}_F)$ has inverses, hence is a group. One of the fundamental theorems of algebraic number theory is that the ideal class group is finite; it is proved using a more general geometry of numbers argument.

Theorem 5.6. *Let F be a number field. Then $\mathscr{C}(\mathscr{O}_F)$ is finite.*

This is only a small slice of the beautiful, rich, and deep theory of algebraic numbers.

5.7. Fermat's Last Theorem for regular primes. Finally, we come back to Kummer's proof of Fermat's Last Theorem for regular prime exponents. We will briefly give an indication of the role played by the general theory. Let p be an odd prime number, and suppose that there exist nonzero integers x, y, z such that $x^p + y^p = z^p$. Then we have the factorization

$$z^p = x^p + y^p = (x - y)(x - \zeta_p y)(x - \zeta_p^2 y) \cdots (x - \zeta_p^{p-1} y)$$

of p-cyclotomic integers, with $\zeta_p = e^{2\pi i/p}$. In the case that $p \nmid xyz$ one shows as in Homework 2 that the ideals $(x - \zeta_p^i y)$ are pairwise coprime. Since $(z)^p$ is a pth power, it follows that each ideal $(x - \zeta_p^i y)$ is a pth power as well, say $(x - \zeta_p^i y) = I_i^p$.

Definition 5.8. An integer prime number $p \in \mathbf{Z}$ is *regular* provided that p does not divide the order of the class group of the ring of p-cyclotomic integers.

Suppose now that p is regular. Since I_i^p is a principal ideal, $[I_i]^p = [(1)]$. But since p does not divide the order of $\mathscr{C}(\mathbf{Z}[\zeta_p])$, this group has no elements of order p, so I_i *must be a pricipal ideal*. Therefore $x - \zeta_p^i y$ is equal to a unit times a pth power. This ends up being the key fact in his proof of this case.

Remark 5.9. The proof in the case $p \mid xyz$ proceeds much as in Homework 2 as well, but there is one extra somewhat difficult fact that is needed. *Kummer's Lemma* states that if p is a regular prime and $e \in \mathbf{Z}[\zeta_p]^\times$ is a unit which is congruent to an integer modulo $\zeta_p - 1$, then e is in fact a pth power. The proof of Kummer's Lemma uses analytic as well as algebraic methods.