Math 356: Number Theory (Rutgers)

David Yang

Winter Break, 2023

Abstract

These notes arise from lecture videos of Math 356: Number Theory (Quadratic Forms), originally taught by Professor Alex Kontorovich, at Rutgers University. I am grateful to Professor Kontorovich for releasing the lecture videos online. I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to Professor Kontorovich and not to me. Feel free to message me with any suggestions or corrections at dyang5@swarthmore.edu.

Contents

1 Introduction to Fermat's Last Theorem

Theorem 1 (Fermat's Last Theorem, 1637)

There are no positive integers x, y, z that satisfy

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

for integer $n > 2$.

An equivalent formulation is the one discussed in lecture:

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

where $n > 2$ is an integer, has no non-trivial solutions x, y, and z in $\mathbb{Q}, \mathbb{Z}$.

Definition 2 (Diophantine Problem)

A **Diophantine problem** is a polynomial equation solved in $\mathbb{Z}$ and $\mathbb{Q}$.

Fermat's Last Theorem is an example of a Diophantine problem.

Historically, in 1993, Andrew Wiles published a proof of Fermat's Last Theorem. Later, Wiles and his student Richard Taylor rectified the 1993 proof and published the first successful proof. For these efforts, Wiles won the 2016 Abel Prize and the 2017 Copley Medal.

With some extra background, we can prove Fermat's Last Theorem for $n = 4$.

1.1 Parameterization of Pythagorean Triples

Theorem 3 (Primitive Pythagorean Triple Generation)

If (x, y, z) is a **primitive** pythagorean triple[a] ($\nexists\, d$ such that $d \mid x$, $d \mid y$ and $d \mid z$), then z is odd. Furthermore, assuming that x is odd and y is even, then there exists coprime $r, s \in \mathbb{Z}$ with such that

$$x = r^2 - s^2,\ y = 2rs,\ z = r^2 + s^2.$$

[a] if (x, y, z) is a primitive Pythagorean triple, then it follows that x, y, and z are pairwise primtiive.

Proof Sketch (Theorem 3). Since y is even, we can rewrite $y = 2y_1$ for some integer y_1. Since (x, y, z) are a Pythagorean triple, it follows that $y^2 = z^2 - x^2 = (z - x)(z + x)$. Substituting and expanding, we get that

$$4y_1^2 = (z - x)(z + x).$$

Since x, z are both odd, we can rewrite $z - x = 2a$ and $z + x = 2b$, so

$$y_1^2 = ab$$

where $(a, b) = 1$. Consequently, a, b must themselves be perfect squares. We conclude that $y_1 = rs$, where $r^2 = a$, $s^2 = b$, and so it follows that $y = 2rs$ for coprime r, s. □

1.2 Pythagorean Varieties

Definition 4 (Variety)

A **variety** is a set of solutions to a system of polynomial equations.

Consider the variety $\mathcal{V} : x^2 + y^2 - z^2$, which is a Pythagorean variety. Note that $\mathcal{V}(\mathbb{R})$ is a structure consisting of two cones which are reflections about the z-axis, and $\mathcal{V}(\mathbb{Z})$, $\mathcal{V}(\mathbb{Q})$ are subsets of $\mathcal{V}(\mathbb{R})$.

Lemma

For every $\vec{v} \in \mathcal{V}(\mathbb{Q})$, there exists a unique primitive $\vec{w} \in \mathcal{V}(\mathbb{Z})^0_+$ with $\vec{w} \sim \vec{v}$, where $\vec{u} \sim \vec{v} \iff \vec{u} = \lambda\vec{v}$, $\lambda \in \mathbb{R} \setminus \{0\}$.

Note that $\mathcal{V}(\mathbb{R})_+/\sim$ can be thought of as S^1; for a point $(x, y, z) \in \mathcal{V}(\mathbb{R})_+ \mapsto \left(\frac{x}{z}, \frac{y}{z}, 1\right)$. Furthermore, $\mathcal{V}(\mathbb{R})/\sim = S^1 \cup \{0\}$.

Furthermore, note that another set of representatives of $\mathcal{V}(\mathbb{Q})_+/\sim$ is $S^1(\mathbb{Q})$. This gives a notion for why Pythagorean triples are fundamental: they parameterize rational points on the unit circle. Formally,

$$\left(\frac{r}{u}, \frac{t}{u}\right) \in S^1(\mathbb{Q}) \iff (r, t, u) \in \mathcal{V}(\mathbb{Z})^0_+$$

1.3 Proof of Fermat's Last Theorem for $n = 4$

Statement. $x^4 + y^4 = z^4$ in $\mathbb{Z}$ implies $xyz = 0$.
Stronger Statement. $x^4 + y^4 = z^2$ in $\mathbb{Z}$ implies $xyz = 0$.

Proof. Suppose there is a solution to $x^4 + y^4 = z^2$ in $\mathbb{Z}$ with $xyz \neq 0$. Then (x^2, y^2, z) is a Pythagorean triple. Furthermore, since we can scale Pythagorean triples by their GCD to get a primitive triple, we can assume that $(x^2, y^2, z) \in \mathcal{V}(\mathbb{Z})^0_+$ is rather a primitive Pythagorean triple. By the Parameterization of primitive Pythagorean triples, there exists coprime $r, s \in \mathbb{Z}$ such that

$$x^2 = r^2 - s^2,\ y^2 = 2rs,\ z = r^2 + s^2.$$

Furthermore, since x^2 is odd and y^2 is even by assumption, r and s also have opposite parity. From the first equation, we know that

$$x^2 + s^2 = r^2,$$

where x is odd, forcing s to be even, and r to be odd. Once again, (x, s, r) is a primitive Pythagorean triple, so there exists coprime $u,\ v \in \mathbb{Z}$ such that

$$x = u^2 - v^2,\ s = 2uv,\ r = u^2 + v^2$$

where $(r, s) = 1$. We also know that $y^2 = 2rs$ from our first primitive Pythagorean triple (x^2, y^2, z). Since y is even, we can express it as $y = 2y_1$ for some $y_1 \in \mathbb{Z}$. Since $r = u^2 + v^2$, $s = 2uv$, and $y = 2y_1$, we have that

$$4y_1^2 = 2(u^2 + v^2)(2uv)$$

and so

$$y_1^2 = uv(u^2 + v^2).$$

Note however that $(u, v) = 1$. Consequently, u, v, and $u^2 + v^2$ are three pairwise coprime numbers whose product is a perfect square. Thus, u, v, and $u^2 + v^2$ must themselves be a perfect square. We now write

$$u = a^2,\ v = b^2,\ u^2 + v^2 = c^2$$

From the third equation, we have that $a^4 + b^4 = c^2$.

Note that if $xyz \neq 0$, then

$$c \leq c^2 = u^2 + v^2 \leq (u^2 + v^2)^2 = r^2 < r^2 + s^2 = z.$$

Thus, we have found a smaller, in the sense that $c < z$, primitive solution to $x^4 + y^4 = z^2$ with $abc \neq 0$.

We can continue this process of finding primitive solutions until we arive at a trivial solution. Thus, by the principle of infinite descent[1], we conclude that $x^4 + y^4 = z^2$ in $\mathbb{Z}$ implies $xyz = 0$. □

[1] or Fermat's descent

2 Modular Arithmetic

Note: Basic modular arithmetic notes skipped due to prior knowledge. Important theorems/results added for completeness.

Theorem 5 (Fermat's Little Theorem)

If p is a prime with $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Note that $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a, p \cdot a\}$ is a complete residue system modulo p. It follows that

$$(1 \cdot a)(2 \cdot a) \ldots ((p-1) \cdot a) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}.$$

Simplifying, we have that

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

Equivalently, we have that $p \mid (p-1)! \left(a^{p-1} - 1\right)$. Since $p \nmid (p-1)!$, it follows that $p \mid a^{p-1} - 1$, so

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

2.1 Linear Diophantine Equations (and Euclidean Algorithm)

Let $S = \{an + bm \mid n, m \in \mathbb{Z}\} \ldots$

Theorem 6

$S = d\mathbb{Z}$, where $d = \gcd(n, m)$.

Proof. First, note that $S \subseteq d\mathbb{Z}$. If $d \mid n$ and $d \mid m$, then $d \mid an$ and $d \mid bm$, so $d \mid an + bm$. It remains to show that $an + bm = d$ has a solution. It is possible to find such a solution by reversing the steps of the Euclidean Algorithm using n and m. □

Theorem 7 (Euclidean Algorithm)

The **Euclidean Algorithm** can be used to find the GCD of two integers $n > m > 0$ as follows:

- Apply the 'division' algorithm to rewrite $n = m \cdot q_1 + r_1$, where $0 \leq r_1 < m$.[a]
- Continue this process, finding q_j, r_j such that $r_{j-2} = r_{j-1} q_j + r_j$, with $0 \leq r_j < r_{j-1}$.
- Stop at some finite $J \leq m$ with $r_J = 0$.

It follows that $r_{J-1} = \gcd(n, m)$.

[a] for reference, we can express n as r_{-1} and m as r_0.

Proof. First, let's show that $\gcd(n,m) \mid r_{J-1}$. Note that if $l \mid n$ and $l \mid n$, $l \mid n - mq_1$, so $l \mid r_1$. Similarly, if $l \mid r_{j-2}$ and $l \mid r_{j-1}$, then $l \mid r_{j-2} - r_{j-1}q_j$, so $l \mid r_j$. Thus, it follows, that $l \mid r_{J-1}$, and so $\gcd(n,m) \mid r_{J-1}$.

It remains to show that $r_{J-1} \mid \gcd(n,m)$. Note that $r_{J-2} = r_{J-1}q_J + r_J$, and $r_J = 0$. It follows that $r_{J-1} \mid r_{J-2}$. Following our steps backwards, we will find that $r_{J-1} \mid r_j$ for all $j \in [-1, J-2]$. Recall that $r_0 = m$ and $r_{-1} = n$. Consequently, since $r_{J-1} \mid r_j$ for all j, we have that $r_{J-1} \mid n$ and $r_{J-1} \mid m$, so $r_{J-1} \mid \gcd(n,m)$.

Since $\gcd(n,m) \mid r_{J-1}$ and $r_{J-1} \mid \gcd(n,m)$, it follows that $r_{J-1} = \gcd(n,m)$, as desired. □

2.2 Connections to Algebra

When we studied Linear Diophantine Equations, we looked at sets $S = \{xn + ym \mid x, y \in \mathbb{Z}\}$. Such a set S is an example of an ideal.

Definition 8 (Ideals)

An **ideal** of the ring $\mathbb{Z}$ satisfies

- For $z \in S$, $rz \in S$ for all $r \in \mathbb{Z}$.
- For $z_1, z_2 \in S$, $z_1 \pm z_2 \in S$.

Definition 9

An ideal S of the ring $\mathbb{Z}$ is **principal** if there exists $d \in \mathbb{Z}$ such that

$$S = (d) = \{d \cdot r \mid r \in \mathbb{Z}\} = d\mathbb{Z}.$$

Theorem 10

$\mathbb{Z}$ is a **Principal Ideal Domain** (every ideal is principal).

Equivalently, suppose that $S = (n_1, \ldots, n_k)$ is an ideal. Then there exists $d \in \mathbb{Z}$ such that $S = (d)$.[a]

[a] in fact, $d = \gcd(n_1, \ldots, n_k)$.

Proof. Suppose that $S = (n_1, \ldots, n_k)$. If $l \mid n_1, \ldots, l \mid n_k$, then for all $z \in S, l \mid z$. Thus, $d = \gcd(n_1, \ldots, n_k) \mid z$ for all $z \in S$, so $S \subseteq d\mathbb{Z}$.

It remains to show that $d = \gcd(n_1, \ldots, n_k) \in S$. Let r be the smallest positive element in S. Clearly, $r\mathbb{Z} \subseteq S$. It follows, by the Euclidean Algorithm that $d \mid r$, so $d = r$. Thus, $d\mathbb{Z} \subseteq S$. □

Definition 11 ((Loose Definitions of) Groups, Rings, and Fields)

A **group** is a set S with an operation $+$, 0, and inverses.

A **ring** is a set S with operations $+, \times$ that supports addition, subtraction, and multiplication.

A **field** is a set S with operations $+, \times$ that supports addition, subtraction, multiplication, and divison[a]

[a] for all $x \in S \setminus \{0\}$, $\exists\, y \in S$ with $xy = 1$.

Theorem 12

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a field if and only if n is prime.

Proof. For prime p and $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem, so $a^{p-2} = \overline{a}$, the modular inverse of $a \pmod{p}$. Consequently, we have found an explicit inverse for each $a \not\equiv 0 \pmod{p}$.

On the other hand, suppose that n is not prime and let $a \in \mathbb{Z}/n\mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$ and $\gcd(a, n) > 1$. Then $ab + nm = 1$ has no solutions, so $ab \equiv 1 \pmod{n}$ has no solutions b. □

Definition 13 (Units)

Let u be an element of a ring R. u is a **unit** of R if and only if there exists $v \in R$ such that $uv = 1$.

The units of $\mathbb{Z}/n\mathbb{Z}$, expressed as $(\mathbb{Z}/n\mathbb{Z})^\times$, is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \pmod{n} \mid \exists\, b : ab = 1\}.$$

Exercise 1

The Gaussian Integers $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$ form a ring.

Let $R =$ linear polynomials/$\mathbb{Z}$ is not a ring (product of linear polynomials is quadratic).

Related Observation: If R is a PID, then it is a UFD.

Going back to the Gaussian integers, it turns out that we can apply the Euclidean Algorithm using the norms of the Gaussian Integers as part of the division algorithm. On the other hand, note that to avoid the issue of gcd's being unit multiples of each other, we say that two Gaussian integers are coprime if the ideal generated by them is the entire ring.

Lemma (Division Algorithm for Gaussian Integers)

For all $n, m \neq 0$ in the Gaussian integers, there exists q, r in Gaussian integers such that

$$n = qm + r \text{ and } 0 < \mathcal{N}(r) < \mathcal{N}(m)$$

where $\mathcal{N}(x + iy) = |x + iy|^2 = x^2 + y^2$.

Proof. Consider

$$\frac{n}{m} = z = \frac{n\overline{m}}{\mathcal{N}(m)}.$$

There exists a nearby close point q in $\mathbb{Z}[i]$ such that

$$\left|q - \frac{n}{m}\right| \leq \frac{\sqrt{2}}{2}$$

Multiplying both sides by $|m|$, it follows that

$$|mq - n| \leq |m|\frac{\sqrt{2}}{2}$$

We define $-r = mq - n$, so that $r = n - mq$. It follows from the above equation that

$$\mathcal{N}(r) = |r|^2 \leq \frac{1}{2}|m|^2 = \frac{1}{2}\mathcal{N}(m) < \mathcal{N}(m).$$

Thus, the division algorithm holds for Gaussian integers, as desired. □

We can also prove a number of simple division rules, using our knowledge of ideals and Linear Diophantine Equations...

2.3 Division Rules

Theorem 14

If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. The ideal $(a, b) = \mathbb{Z}$. Equivalently, the Euclidean Algorithm gives us a solution to $ax + by = 1$. Multiplying both sides of this equation by c, we get that

$$acx + bcy = c.$$

Since $a \mid bc$, $a \mid bcy$; furthermore, $a \mid acx$. Thus, a divides the left hand side and so a must also divide the right hand side, giving $a \mid c$. □

Corollary 1

If p is a prime and $p \mid bc$, then $p \mid b$ or $p \mid c$.

Proof. This follows directly from Theorem 14, with $a = p$ and $a = c$ for the two cases. □

Definition 15 (Order)

The **order of p in a**, $\text{ord}_p(a)$, is

$$\text{ord}_p(a) = \max\{k \mid (p^k \mid a)\}.$$

Corollary 2

If p is a prime and $a, b \in \mathbb{Z}$, then

$$\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b).$$

Proof. Let $\text{ord}_p(a) = \alpha$, so that $p = p^\alpha a_1$, with $p \nmid a_1$. Similarly, let $\text{ord}_p(b) = \beta$, so that $p = p^\beta b_1$, with $p \nmid b_1$.

Consider

$$ab = (p^\alpha a_1)\left(p^\beta b_1\right) = p^{\alpha+\beta} a_1 b_1.$$

By the contrapositive of Corollary 1, since $p \nmid a_1$ and $p \nmid b_1$, so $p \nmid a_1 b_1$. Thus,

$$\text{ord}_p(ab) = \alpha + \beta = \text{ord}_p(a) + \text{ord}_p(b). \qquad \square$$

Theorem 16 (Fundamental Theorem of Arithmetic)

If n is a nonzero integer, then there exists $\varepsilon(n) = 0$ or -1 such that

$$n = (-1)^{\varepsilon(n)} \prod_p p^{\text{ord}_p(n)}$$

and this decomposition is unique.

Proof. Assume for the sake of contradiction that n has a second factorization

$$n = (-1)^{\varepsilon(n)} \prod_p p^{e_p}.$$

Fix p, and apply ord_p to both sides. We have that

$$\begin{aligned}\text{ord}_p(n) &= \text{ord}_p\left((-1)^{\varepsilon(n)} \prod_q q^{e_q}\right) \\ &= \text{ord}_p\left((-1)^{\varepsilon(n)}\right) + \sum_q \text{ord}_p(q^{e_q}).\end{aligned}$$

Since $\text{ord}_p\left((-1)^{\varepsilon(n)}\right) = 0$ and $\text{ord}_p(q^{e_q}) = 0$ for $q \neq p$, it follows that $\text{ord}_p(n) = p^{e_p} = e_p$.

Thus, the second factorization must be the same as the first one, and so the decomposition is unique. $\square$

Note that the Fundamental Theorem of Arithmetic does not hold in the ring $\mathbb{Z}[\sqrt{5}i]$. For example, in this ring,

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$

2.4 Rings, Units, and Connections to Pythagorean Triples

So where does the above proof fail for this ring? Note that $\text{ord}_2(6) = 1$, $\text{ord}_{1+\sqrt{5}(i)} = \text{ord}_{1-\sqrt{5}(i)} = 0$, and so the additive property of orders for "relatively prime" numbers in the integers does not hold for the ring $\mathbb{Z}[\sqrt{5}i]$.

Exercise 2

The set of units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. The set of units of $\mathbb{Z}[\sqrt{5}i]$ are ± 1.

Thus far, we've studied the similarities between viewing Pythagorean triples as rational points on a circle. Similarly, we studied the question of which numbers appear as the hypotenuses of triples.[2] Note that this is also equivalent to finding possible norms of Gaussian integers; for example, circles centered at $(0, 0)$ with radius $\sqrt{n}$ for $n \equiv 3 \pmod 4$ pass through no lattice points. In general, we may also want to study which n arise as the values of a general binary quadratic form $Ax^2 + Bxy + Cy^2$.

Definition 17 (Irreducible)

An element r in the ring R is irreducible if, for an element b in R,

$$b \mid r \text{ implies that } b \text{ is a unit or an associate to } r.$$

Definition 18 (Associates)

Two elements r and s in the ring R are **associates** if there exists an element u in the set of non-units of R, $R^\times$, such that

$$r = us.$$

Definition 19 (Prime)

An element r in the ring R is **prime** if

$$r \mid s \cdot t \text{ implies } r \mid s \text{ or } r \mid t.$$

Remark

In $R = \mathbb{Z}[\sqrt{5}]$, 2 is irreducible but is not prime.

Definition 20 (Integral Domain)

A ring R is an **integral domain** if

$$xy = 0 \text{ implies } x = 0 \text{ or } y = 0$$

[2] numbers that are 3 (mod 4) cannot appear, due to the fact that squares are $0, 1 \pmod 4$

or equivalently, if R has no zero divisors.

Lemma (Prime implies irreducible in integral domains)
A prime element is irreducible over an integral domain R.

Proof. Let p be a prime element in R. Suppose that $s \mid p$. We want to show that s is a unit or s is an associate of p.

Since $s \mid p$, there exists some $k \in R$ such that $sk = p$. It follows that $p \mid sk$. Since p is a prime, we know by definition that $p \mid s$ or $p \mid k$.

In the former case, it follows that $s = lp$ and $p = sk$. Thus, $p = sk = (lp)k$, and so $p(lk - 1) = 0$. Since $p \neq 0$, it follows that $lk = 1$, meaning that k is a unit and s is by definition an associate of p. The latter case follows similarly, but will yield the result that s is a unit of R.

Thus, prime elements are irreducible over integral domains, as desired. □

Lemma
Let R be a PID. Then an element of R that is irreducible is also prime.

Proof. Let r be an element of R that is irreducible. Assume that $r \mid ab$, and $r \nmid a$. We want to show that $r \mid b$.

Consider the ideal (r, a). Since R is a PID, $(r, a) = (d)$, where $\gcd(r, a) = d$. Since $d \mid r$ and r is irreducible, we know that d is an associate of r or d is a unit of R.

If d is an associate of r, it follows that $d = r \cdot u$ for a unit u. Since $a \in (d)$, we must have that $d = r \cdot u \mid a$, meaning that $r \mid a$. However, by assumption, $r \nmid a$, so d cannot be an associate of r.

It follows that d is a unit of R, so $(r, a) = (d) = R$. Note that $(r \cdot b, a \cdot b) = (b)$. Furthermore, $(r \cdot b) \subset (r)$, and $(a \cdot b) \subset (r)$. It follows that $(r \cdot b, a \cdot b) \subset (r)$. Thus, $(b) \subset (r)$ and so $r \mid b$. □

Exercise 3
$R^\times$ is a group.

Remark
If R is a PID, then an element is irreducible if and only if it is prime.

2.5 Quadratic Residues and Nonresidues

Recall that we studied the question of which numbers are represented as sums of squares. From our modular arithmetic section, we know that no prime $p \equiv 3 \pmod 4$ can be expressed as a sum of squares.

Lemma

Every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

Lemma (Quadratic Residues modulo p)

Modulo any prime p, half of the numbers (excluding 0) are quadratic residues.

Equivalently, the number of numbers $n \equiv \pmod p$ where $n \neq 0$ and there exists some x such that $x^2 \equiv n \pmod p$ is $\frac{p-1}{2}$.

Proof. Note that $(x)^2 \equiv (-x)^2 \pmod p$. It follows that there must be at most half the numbers among the squares.

Furthermore, note that if $x^2 \equiv y^2 \pmod p$, then $p \mid x^2 - y^2$, so $p \mid (x-y)(x+y)$. By Corollary 1, it follows that $p \mid x - y$ or $p \mid x + y$, meaning $x \equiv y \pmod p$ or $x \equiv -y \pmod p$. Thus, all squares in the first half are distinct and there are exactly $\frac{p-1}{2}$ quadratic residues modulo p. □

Remark

$a^{\frac{p-1}{2}} = 1 \pmod p \iff a$ is a quadratic residue.

We can now find a procedure to write a prime $p \equiv 1 \pmod 4$ as a sum of two squares.

- Find quadratic non-residue a modulo p.
- Let $z = a^{\frac{p-1}{4}} \pmod p$. It follows that

$$z^2 = a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

  so $z^2 + 1 \equiv 0 \pmod p$, and $z^2 + 1 = pk$ in the integers.
- In $\mathbb{Z}[i]$, $z^2 + 1 = (z+i)(z-i)$, so $(z+i)(z-i) = pk$.
- To find the common factor, apply the Euclidean algorithm to $z + i$ and p in $\mathbb{Z}[i]$.

Put more succinctly, this procedure has two steps:

- Find quadratic non-residue a modulo p.
- Let $z = a^{\frac{p-1}{4}} \pmod p$. Find $\gcd(z+i, p)$ in $\mathbb{Z}[i]$.

Example

Let $p = 17$. Then $a = 3$ is a quadratic non-residue modulo p, and $z = 3^{\frac{17-1}{4}} \pmod{17} = 13$. Note that $13^2 + 1^2 = 170 = 17 \cdot 10$.

We apply the Euclidean Algorithm to $13 + i$ and 17 in $\mathbb{Z}[i]$:

$$17 = (13 + i) \cdot 1 + (4 - i)13 + i = (4 - i) \cdot (3 + i) + 0$$

so $\gcd(13 + i, 17) = 4 - i$.

Thus, $17 = (4 + i)(4 - i) = \boxed{4^2 + 1^2}$.

Example (Super Large Example, all calculations computed using WolframAlpha)

Take $p = 55,497,159,953$. Let $a = 21,345$ (randomly picked quadratic non-residue), so that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Let $z = a^{\frac{p-1}{4}} = 4,334,787,849$. Since $\gcd(z + i, p) = 235,532 + 4673i$, we conclude that

$$p = 235,532^2 + 4,673^2.$$

2.6 Norm Forms (and Eisenstein Integers)

Definition 21

For $\omega = e^{\frac{2\pi i}{3}}$, the ring $\mathbb{Z}[\omega]$ consists of the **Eisenstein Integers**:

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega \mid a_0, a_1 \in \mathbb{Z}\}.$$

Since ω satisfies $\omega^2 + \omega + 1 = 0$, $\omega^2 = -\omega - 1$, so $\mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2 + x + 1)$.

Remark

The Eisenstein integers form a triangular/"hexagonal" lattice in the complex plane.

Exercise 4

What is the "norm form" for $\mathbb{Z}[\omega]$?

Note that

$$\mathcal{N}(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2.$$

Definition 22

A ring R is a **Euclidean Domain** if there is a norm function $\mathcal{N} : R \setminus \{0\} \mapsto \mathbb{N}$ such that for all n, m in R with $m \neq 0$, there exists q, r in R such that

$$n = mq + r$$

with $\mathcal{N}(r) < \mathcal{N}(m)$.

Remark

The ring $R = \mathbb{R}[x]$ is a Euclidean domain, where the "norm function" is the degree of a polynomial.[a]

On the other hand, $R = \mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain, since the division algorithm does not work:

if $q = \lfloor \frac{n}{m} \rfloor$, then

$$|r|^2 = |n - mq|^2 = \left|\left(\frac{n}{m} - q\right)\right|^2 |m|^2.$$

However, note that $\left|\left(\frac{n}{m} - q\right)\right|^2 < \frac{3}{2}$, and so we can't conclude that $\mathcal{N}(r) < \mathcal{N}(m)$.

[a] we can define degree$(0) = -\infty$.

Theorem 23

If R is a Euclidean domain, it is a principal ideal domain.

Proof. Let $\mathcal{I}$ be an ideal of R. Either $\mathcal{I} = (0)$, which is principal, or $\mathcal{I}$ contains some nonzero element a. Consider the latter case. Let

$$S = \{\mathcal{N}(i) \colon i \in \mathcal{I} \setminus \{0\}\} \subseteq \mathbb{N}.$$

Let s be the least element of S and let $d \in \mathcal{I}$ satisfy $\mathcal{N}(d) = s$. By definition, $(d) \subseteq \mathcal{I}$. We want to show that, in fact, $(d) = \mathcal{I}$. Suppose that there is some nonzero element $m \in \mathcal{I} \setminus (d)$.

By the Division Algorithm, there must exist some q, r in R such that $m = dq + r$, and since $m \notin (d)$, $r \neq 0$ and $\mathcal{N}(r) < \mathcal{N}(d)$, which contradicts the fact that d has the smallest norm in S. Thus, R must be a principal ideal domain. □

2.7 Reformulating with Ideals

Let's revisit some of our definitions for units, associates, and irreducible elements of a ring R in terms of the ideals.

Definition 24

- $a \mid b$ if and only if $(b) \subseteq (a)$.
- a is an **associate** of b if and only if $(a) = (b)$.
- u is a **unit of** R if and only if $(u) = R$.
- r is **irreducible in** R if $r = s \cdot t$ for s, t in R implies s is a unit of $(s) = (r)$.
- p is a **prime in** R if and only if for $a \cdot b \in (p)$, either $a \in (p)$ or $b \in (p)$.
- a, b in R are **coprime** for R a PID if and only if $(a, b) = R$.
- d is a **gcd of** a, b **in** R if and only if $(a) \subseteq (d)$ and $(b) \subseteq (d)$ and if $(a) \subseteq (d')$ and $b \subseteq (d')$, then $(d') \subseteq (d)$.

Lemma

If R is a PID, and a and b are two elements in R, then there exists a gcd d of a and b such that $(a, b) = (d)$.

Proof. Note that there is some d such that $(d) = (a, b)$. It remains to show that d is a gcd of a and b. Note that $b \in (a, b) \subseteq (d)$. Thus, $b = d \cdot k$, and $d \mid b$. By similar logic, we know $d \mid a$.

Suppose that $d' \mid a$ and $d' \mid b$. Then $a = d' \cdot l$ and $b = d' \cdot k$, so $a \in (d')$ and $b \in (d')$. It follows that $(d) = (a, b) \subseteq (d')$, so $d \in (d')$. Thus, $d = d' \cdot r$ and $d' \mid d$. Thus, d is the gcd of a and b as desired. □

Exercise 5

Is $x^2 + 1$ irreducible in $R = (\mathbb{Z}/5)[x]$? How about in $R = (\mathbb{Z}/7)[x]$?

Answer. *$x^2 + 1$ is not irreducible in $(\mathbb{Z}/5)[x]$, as*

$$(x + 2)(x + 3) = x^2 + 5x + 6 \equiv x^2 + 1 \pmod 5.$$

Note that this is equivalent to the question of whether there exists a solution x to $x^2 \equiv -1 \pmod 5$. In general, recall that $x^2 + y^2 \equiv 0 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$ or $p = 2$.

Thus, since $7 \equiv 3 \pmod 4$, $x^2 + 1$ is irreducible in $R = (\mathbb{Z}/7)[x]$. ⊛

Definition 25 (Noetherian Ring)

A ring R is **Noetherian**[a] if

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \dots$$

is a chain of ideals, then the chain stops in finite time (there exists N such that for all $n > N$,

$I_N = I_n$).

[a]named after Emily Noether

Remark

$\mathbb{Z}$ is Noetherian (which also follows from the theorem below, as $\mathbb{Z}$ is a PID.)

Theorem 26

If R is a PID, then it is Noetherian.

Proof. Let $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \dots$ be an increasing chain of ideals in R. Let

$$\mathcal{I} = \bigcup_{k=1}^{\infty} \mathcal{I}_k.$$

$\mathcal{I}$ is an ideal, and since R is a PID, it follows that $\mathcal{I} = (a)$ for some a. There must exist a N such that $a \in \mathcal{I}_N$, so $(a) \subseteq \mathcal{I}_N$. Since for any $n > N$, $\mathcal{I}_n \subseteq \mathcal{I}_N$, and they can't add any additional elements to $\mathcal{I}_N$, all $\mathcal{I}_n = \mathcal{I}_N$. It follows that R is Noetherian. □

Lemma

If R is Noetherian, then any element r in R is a finite product of irreducibles.

Proof. If r is not irreducible, then there exists an element r_1 in R such that $r_1 \mid r$, r_1 is not a unit, $(r_1) \neq (r)$, and $(r) \subset (r_1)$.

If r_1 is itself not irreducible, then there exists some r_2 such that $r_2 \mid r_1$, r_2 is not a unit, $(r_2) \neq (r_1)$, and $(r_1) \subset (r_2)$.

Continuing this process, we arrive at an increasing chain of ideals:

$$(r) \subsetneq (r_1) \subsetneq (r_2) \dots$$

Since R is Noetherian, this process cannot go on forever. Suppose that it stops at r_j; this means that $l_1 = r_j$ is an irreducible factor of r.

We can continue this process on s_1, where $r = l_1 \cdot s_1$; we will find that there exist some l_2, an irreducible factor of s_1 and consequently, of r. Consider s_2, where $s_1 = l_2 \cdot s_2$, and so on and so forth. We once again find an increasing chain of ideals:

$$(r) \subsetneq (s_1) \subsetneq (s_2) \subsetneq \dots$$

Since R is Noetherian, this chain must stabilize, giving us an irreducible element s_J. It follows that

$$r = l_1 \cdots l_J \cdot s_J,$$

giving us a finite product of irreducible elements. □

Lemma

Let R be a Noetherian ring. Given a prime element p (equivalently, irreducible) in R and an element a in R, there exists some natural number n such that $\text{ord}_p(a) = n$.

Proof. If $p \mid a$, then $a = pa_1$. If $p \mid a_1$, then $a_1 = pa_2$, and so on and so forth. We have an increasing chain of ideals

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \dots$$

This process must stop, so there must be some n such that $p^n \mid a$ and $p^{n+1} \nmid a$. □

Lemma

If R is Noetherian and p is prime in R, then

$$\text{ord}_p(a+b) = \text{ord}_p(a) + \text{ord}_p(b).$$

Proof. Same as for $\mathbb{Z}$. □

Theorem 27 (Noetherian implies UFD)

Any element r in a Noetherian ring R is uniquely expressed as

$$r = u \prod_p p^{e_p}$$

where u is a unit, p is prime, and $e_p = \text{ord}_p(r)$.

Remark (Important Takeaway)

Note that Euclidean Domain implies PID which implies Noetherian ring which implies UFD.

Recall from earlier that $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean; this also follows from the fact that it is not a UFD:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

2.8 A Return to Norm Forms, for Eisenstein Integers

Recall that earlier in the course, we wanted to know which n could be expressed as a sum of squares: $n = x^2 + y^2$. We answered this question by studying $\mathbb{Z}[i]$, since the quadratic form $Q(x,y) = x^2 + y^2$ is the norm form for $\mathbb{Z}[i]$.

In the Eisenstein integers $\mathbb{Z}[\omega]$, the norm form is $\mathcal{N}(x + \omega y) = x^2 - xy + y^2$.

Exercise 6

Which integers n can be expressed as $n = x^2 - xy + y^2$, for integers x and y?

Answer. *We see* $n = Q(x, y) \in \{0, 1, 3, 4, 7, 9, 12, 13, \dots\}$*, and no values that are* $\equiv 2 \pmod 3$*! Additionally, for every prime* $p \equiv 1 \pmod 3$*, there exists* x, y *such that* $x^2 - xy + y^2 = p$ *(i.e. all primes equivalent to 1* $\pmod 3$ *are represented – and the* x, y *can be determined efficiently.)* ⊛

Proof. Let p be a prime equivalent to 1 $\pmod 3$. Set $z = a^{\frac{p-1}{3}} \pmod p$, for $z \not\equiv 1 \pmod p$ (there will be $\frac{2(p-1)}{3}$ possible z).

It follows by Fermat's Little Theorem that $z^3 - 1 \equiv 0 \pmod p$, so $z^3 - 1 = pk$ for some $k \in \mathbb{Z}$. Since $z^3 - 1$ factors completely into $(z-1)(z-\omega)(z-\overline{\omega})$ in $\mathbb{Z}[\omega]$, we know that

$$(z-1)(z-\omega)(z-\overline{\omega}) = pk$$

in $\mathbb{Z}[\omega]$. Since $z \not\equiv 1 \pmod p$, we know that $z - 1 \mid k$. Say that $k = (z-1)l$. Then

$$(z-\omega)(z-\overline{\omega}) = pl.$$

Note that $p \nmid z - \omega$ and $p \nmid z - \overline{\omega}$. [3] Since $p \nmid z - \omega$ and $p \nmid z - \overline{\omega}$ but $p \mid (z-\omega)(z+\overline{\omega})$, p is not prime. Suppose that $p = (x + y\omega)(x + y\overline{\omega}) = x^2 - xy + y^2$. It follows that the component $x + y\omega$ must divide at least one of $z - \omega$ or $z - \overline{\omega}$.

Take the greatest common divisor, of p and $z - \omega$ in $\mathbb{Z}[\omega]$; if this is $a + b\omega$, it follows that

$$p = a^2 - ab + b^2$$

for integers a, b. □

In the above proof, we actually find an algorithm to solve $p = \mathcal{N}(x + y\omega) = x^2 - xy + y^2$ for $p \equiv 1 \pmod 3$.

- In $\mathbb{Z}/p$, find an a such that $a^{\frac{p-1}{3}} \not\equiv 1$ and set $z = a^{\frac{p-1}{3}} \pmod p$.
- Find $\gcd_{\mathbb{Z}[\omega]}(p, z - \omega) = x + y\omega$. Then $x^2 - xy + y^2 = p$.

Example

Find integers x, y for $p = 3571$ such that

$$3571 = x^2 - xy + y^2$$

using the Eisenstein integers.

Answer. *We can check that* $p = 3571$ *is a prime equivalent to* 1 $\pmod 3$*. For ease of reference, let's define* $l = \frac{p-1}{3} = 1190$.

[3] if $p \mid z - \omega$, then $z - \omega = (c + d\omega)p$, which will only be satisfied if $pd = -1$. A similar line of reasoning can be used to show $p \nmid z - \overline{\omega}$.

- *We can find an a such that $a^l \not\equiv 1 \pmod{p}$: there are $2l$ such a, and one such a is $a = 2$, as*

$$2^{1190} \pmod{3571} = 3467 \neq 1.$$

Now, let $z = 3467$. We know that $z^3 - 1 \equiv 0 \pmod{p}$.

- *We now find* $\gcd_{\mathbb{Z}[\omega]}(3571, 3467 - \omega)$:

$$\begin{aligned} 3571 &= (3467 - \omega)(1) + (104 + \omega) \\ 3467 - \omega &= (104 + \omega)(33) + (35 - 34\omega) \\ 104 + \omega &= (35 - 34\omega)(2 + \omega) + 0. \end{aligned}$$

Thus, $\gcd_{\mathbb{Z}[\omega]}(3571, 3467 - \omega) = 35 - 34\omega$ *and so* $\mathcal{N}(35 - 34\omega) = 3571$ *and*

$$\boxed{3571 = 35^2 + 34 \cdot 35 + 34^2}.$$

⊛

Remark

Furthermore, for general $n = p_1 \cdots p_k$, where each p_j for j from 1 to k is $\equiv 1 \pmod{3}$, we can simply find a representation of each p_j and multiply the resulting Eisenstein integers to find the representation for n.

2.9 Binary Quadratic Forms

Thus far, we've studied $x^2 + y^2 = n$ and $x^2 - xy + y^2 = n$, the norm forms of the Gaussian and Eisenstein integers. We know for what values of n there are integer solutions, as well as how to efficiently find prime solutions to these equations.

However, how might we generalize this to a general binary quadratic form

$$Q(x, y) = Ax^2 + Bxy + Cy^2.$$

For ease of reference, we will use the coefficients $[A, B, C]$ to reference the above quadratic form.

Remark

$Q = [1, 2, 1]$ is degenerate since its discriminant is 0.

Similarly, $Q = [1, 3, 2]$ can be factored as $(x-2y)(x-y)$. Using the change of variables $z = x-y$ and $w = -y$, the quadratic form becomes $Q(z, w) = z(z + y)$. Note that any value n can be achieved by setting $z = 1$ and $y = n - 1$.
In general, if the quadratic form factorizes, or has discriminant zero, the values of the quadratic form can be rather uninteresting (either every integer or only perfect squares, respectively, can be achieved).

Definition 28 (Degenerate Quadratic Forms)

If a quadratic form Q has discriminant zero, it is a **degenerate** quadratic form.

If a quadratic form Q has a discriminant equal to a perfect square, it splits and is reducible (as Q is a product of two linear polynomials).

Definition 29 (Definite and Indefinite Quadratic Forms)

A quadratic form Q is **definite** if its sign never changes.

A quadratic form Q is **indefinite** if its sign does change.

Remark

In general, the **discriminant** $B^2 - 4AC$ of a quadratic form $Ax^2 + Bxy + Cy^2$ tells us whether a quadratic form is definite or indefinite:

$$\begin{cases} \text{indefinite} & \text{if } B^2 - 4AC > 0; \\ \text{definite} & \text{if } B^2 - 4AC < 0; \\ \text{definite/degenerate quadratic form (only squares)} & \text{if } B^2 - 4AC = 0 \end{cases}$$

After our brief interlude on degeneracy, discriminants, definite and indefinite quadratic forms, let's revisit the question of what n are represented in the quadratic form $Q(x, y) = Ax^2 + Bxy + Cy^2$.

Definition 30 (Primitive Quadratic Form)

A quadratic form $Q = [A, B, C]$ is **primitive** if $\gcd(A, B, C) = 1$.

A similar yet more specific question may be the following: which n are primitively represented (meaning $Q(x, y) = n$ where $\gcd(x, y) = 1$) by Q?

Answer. *For a specific quadratic Q, we can figure out all values Q takes on mod p by simply calculating p^2 values and taking them mod p. In this strategy, we keep Q constant a¿nd change values of x and y, calculating the respective modulos.*

A dual approach is to fix x and y and change Q. To illustrate this idea, consider

$$Q_1(x, y) = x^2 + y^2$$

and replace x with $x + y$ to create the new quadratic form

$$Q_2(x, y) = (x + y)^2 + y^2.$$

Note that Q_2 represents the same solutions as Q_1, any values $x = a, y = b$ in Q_1 have identical values $x = a - b, y = b$ in Q_2. The main takeaway here is that Q_1 and Q_2 differ by $\mathbb{Z}$-invertible linear change of variables.

We can work more generally using the group $GL_2(\mathbb{Z})$, the group of two-by-two invertible matrices (which must have determinant ± 1) in the integers. ⊛

Let $Q = [A, B, C]$, and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element in $GL_2(\mathbb{Z})$. Then $Q_1 = Q \circ \gamma$ represents the same n as Q. Note that

$$\begin{aligned} Q_1(x, y) &= Q\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) \\ &= Q(ax + by, cx + dy) \\ &= A(ax + by)^2 + B(ax + by)(cx + dy) + C(cx + dy)^2 \\ &= A_1x^2 + B_1xy + C_1y^2 \end{aligned}$$

where $A_1 = Aa^2 + Bac + Cc^2 = Q(a, c)$, $B_1 = A(2ab) + B(ad + bc) + C(2cd)$, and $C_1 = Ab^2 + Bbd + Cd^2 = Q(b, d)$.

Example

Suppose we start with the quadratic form $Q_0 = [7, -11, 5]$. Let us change Q_0 to a new quadratic form $Q = Q_0 \circ \gamma$ and evaluate at $(1, 0)$. Suppose we want

$$Q(1, 0) = Q_0(1, 1).$$

Then we need some matrix in $GL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Solving gives us one such solution: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Consequently, we have that

$$Q = Q_0 \circ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = [7, -11, 5] \circ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

From our above formula, we know that $Q = [A_1, B_1, C_1]$, where $A_1 = Q(a, c) = Q(1, 1) = 1$, $B_1 = 0 - 11 + 10 = -1$, and $C_1 = Q(b, d) = Q(0, 1) = 5$.

Thus, $Q(1, 0) = Q_0(1, 1)$, for $Q = [1, -1, 5]$.

We can formalize this duality process of fixing x and y and varying Q as follows.

Definition 31 (Equivalent Quadratic Forms)

The quadratic forms Q_1 and Q_2 are **equivalent**, denoted $Q_1 \sim Q_2$, if there exists some matrix $\gamma \in SL_2(\mathbb{Z})$ (2×2 matrices with determinant 1) such that $Q_1 = Q_2 \circ \gamma$.

Given a form Q, the **equivalence class** of Q, denoted $[Q]$, is the set of all forms equivalent to Q:

$$[Q] = \{Q' \mid Q' \sim Q\}.$$

Lemma (Equivalent Forms Represent Same Numbers)

If Q_1 and Q_2 are two equivalent quadratic forms, then

$$\{n \in \mathbb{Z} \mid \text{ there exists } x, y \in \mathbb{Z},\ Q_1(x,y) = n\} = \{n \in \mathbb{Z} \mid \text{ there exists } x, y \in \mathbb{Z},\ Q_2(x,y) = n\}$$

meaning that equivalent forms represent the same numbers.

Proof. If $n = Q_1(x,y)$ then $n = Q_2(x_1, y_1)$, where $\gamma \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$, so

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \gamma^{-1} \begin{pmatrix} x \\ y \end{pmatrix}.$$

□

Remark

This lemma tells us that if we started with $Q = [1, -1, 5]$ instead of $Q_0 = [7, -11, 5]$ and wrote out the values for different x and y, we would get the same values but shuffled around.

Theorem 32

If two quadratic forms Q_1 and Q_2 are equivalent, their discriminants are equal.

One proof follows directly from algebra involving the coefficients of an equivalent quadratic form, described previously. Our proof will be more elegant.

Definition 33 (Half-Hessian Matrix (Gram Matrix))

If $Q = [A, B, C]$, its **Gram Matrix** (or **Half-Hessian Matrix**) is

$$M = \frac{1}{2} \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} = \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}$$

with $\det M = -\frac{1}{4} D_Q$. Furthermore,

$$Q(x,y) = \begin{pmatrix} x & y \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix}.$$

Remark

This holds for any general quadratic form.

Proof. □