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

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

Exercise 3

$R^\times$ is a group.

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.

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

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. □

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

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