# UC Irvine Math 180B Spring 2024

## Number Theory II

Professor: Nathan Kaplan
Teaching Assistant: Tingyu Tao
Notes: Timothy Cho

June 2024
Lecture Note Series #9

# Introduction

These notes come from both the lecture and the discussion, and are roughly sorted by content. Sections are numbered chronologically using the following scheme by taking the section number modulo 10. Note that we have occasionally merged two sections for continuity reasons.

| Day | Lecture | Discussion |
|---|---|---|
| Monday | 0 | 1 |
| Tuesday | 2 | 3 |
| Wednesday | 4 | 5 |
| Thursday | 6 | 7 |
| Friday | 8 | 9 |

Additionally, the first digit (first two if the section number is three digits long) denotes the week that the lecture/discussion occurred in. It should be noted that not every lecture is recorded in these notes: some lectures were skipped, but despite this the notes should be comprehensible.

The text used was *A Friendly Introduction to Number Theory*, 4e, by Joseph Silverman. Numbers in [brackets] refer to sections in this text. The prerequisite for this course is Math 180A, taught in Winter 2024, which ended at quadratic reciprocity, so these notes merely finish my Math 180A notes, so references to Math 180A will be common.

Some material here is presented more algebraically (Math 120AB), but these will be clearly marked and presented as optional.

# 13 The Legendre Symbol

In Math 180A, we stated the Law of Quadratic Reciprocity, so our first goal in Math 180B is to prove that law. Throughout this section, let $p$ be an odd prime, and $a \in \mathbb{Z}$. First, recall the definition of the *Legendre symbol*.

**Definition 13.1.** We define the *Legendre symbol of $a$ modulo $p$* by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \in \mathsf{QR}(p) \\ -1 & a \in \mathsf{NR}(p) \\ 0 & p \mid a. \end{cases}$$

Certainly, $\left(\frac{a}{p}\right)$ is periodic with respect to $a$: if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Furthermore, we have proved in Math 180A that $\left(\frac{a}{p}\right)$ is completely multiplicative: for all $a, b \in \mathbb{Z}$, we have $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. However, the main result that has yet to be proven is the following.

**Theorem 13.2** (Law of Quadratic Reciprocity)**.** *Let $p \neq q$ be odd primes. Then we have*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}, \quad \textit{and} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{1}{4}(p-1)(q-1)}.$$

We give a more direct proof of part (2) of this theorem.

*Proof (of (2)).* Consider the product $2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{\frac{1}{2}(p-1)} \left(\frac{p-1}{2}\right)!$, and reduce each of these factors into the range $[1, \frac{1}{2}(p-1)]$, modulo $p$:

$$\begin{aligned} 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! &\equiv 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (-5) \cdot (-3) \cdot (-1) \pmod{p} \\ &\equiv (-1) \cdot 2 \cdot (-3) \cdot 4 \cdot \cdots \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right) \\ &\equiv [(-1) \cdot 1] \cdot [(-1)^2 \cdot 2] \cdot [(-1)^3 \cdot 3] \cdot [(-1)^4 \cdot 4] \cdot \cdots \cdot \left[(-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)\right] \\ &\implies 2^{\frac{p-1}{2}} \equiv (-1)^{1+2+\cdots+(p-1)/2}. \end{aligned}$$

Now $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$, which completes the proof via Euler's Criterion (Math 180A, Theorem 94.1). □

We will go on to see three proofs of the final statement of quadratic reciprocity, but for now, let us state and prove a generalization of the statement. Define the following generalization of the Legendre symbol first:

**Definition 13.3.** Let $a \in \mathbb{Z}$ and $b$ be any odd number. The *Jacobi symbol of $a$ modulo $b$* is defined as follows:

1. If $b = 1$, then $\left(\frac{a}{1}\right) := 1$.
2. If $b = p_1 p_2 \cdots p_k$ for primes $p_i$, then $\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$, where the symbols on the right are Legendre symbols.

The Jacobi symbol preserves many of the nice properties the Legendre symbol has.

**Proposition 13.4.** *The Jacobi symbol is also periodic and completely multiplicative.*

*Proof.* Let $n$ be an odd integer. If $n = 1$, then this statement is obvious, so suppose $n = p_1 p_2 \cdots p_k$ for (odd) primes $p_i$.

Periodicity: suppose $a \equiv b \pmod{n}$. Then $a \equiv b \pmod{p_i}$ for all $i \leq k$, so that it follows that expanding $\left(\frac{a}{n}\right)$ and $\left(\frac{b}{n}\right)$ into Legendre symbols and utilizing the periodicity of the Legendre symbols finishes the proof.

Multiplicativity: similar idea. □

However, the Jacobi symbol is **not** an indicator as to whether something is a quadratic residue.

**Example 13.5.** Let $p, q$ be primes.s If $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$, then $\left(\frac{a}{pq}\right) = (-1)^2 = +1$, yet $a \in \mathsf{NR}(pq)$.

Nevertheless, the Jacobi symbol can indicate whether something is a *nonresidue*.

**Proposition 13.6.** *Let $n$ be odd and $a \in \mathbb{Z}$. Then*

1. $\left(\frac{a}{n}\right) = 0$ *if and only if* $\gcd(a, n) \neq 1$, *and*
2. $\left(\frac{a}{n}\right) = -1$ *implies* $a \in \mathsf{NR}(n)$.

We will not prove this proposition, but the idea is again, expanding everything out in terms of Legendre symbols to extract the properties we want.

Quadratic Reciprocity generalizes to Jacobi symbols as well.

**Theorem 13.7** (Generalized Law of Quadratic Reciprocity)**.** *Let $a \neq b$ be distinct odd integers. Then*

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{1}{2}(b-1)}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{1}{8}(b^2-1)} \quad \textit{and} \quad \left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{1}{4}(a-1)(b-1)}.$$

*Proof.* In all three cases, note that if $b = 1$, then this follows trivially. Otherwise, we prove the three cases by expanding out everything in terms of Legendre symbols, where we know that the law of quadratic reciprocity holds. Write $b = p_1 p_2 \cdots p_k$, where the $p_i$ are prime. Then, we computes

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right) = (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_k-1}{2}},$$

where the last equality follows from Euler's Criterion. From here, it suffices to show that $\frac{1}{2}(b-1) \equiv \sum_{i=1}^{k} \frac{1}{2}(p_i - 1) \pmod 2$, so that raising $(-1)$ to both of these gives the same result. If $b \equiv 1 \pmod 4$, then the number of $p_i$ congruent to 3 modulo 4 is even, so the number of $\frac{1}{2}(p_i - 1)$ that are odd is even, so that the sum vanishes modulo 2. Now, $\frac{1}{2}(b-1)$ is even, so the two are equivalent modulo 2. A similar argument holds when $b \equiv 3 \pmod 4$, so we are done proving the first equality.

The second equality follows similarly, so we try it by induction instead. Again, suppose $b = p_1 p_2 \cdots p_k$ for primes $p_i$, so we prove by induction on the number of primes $k$. When $k = 1$, this is the regular law of quadratic reciprocity, so assume the claim holds for some $k \geq 1$. Let $b = p_1 p_2 \cdots p_k q =: mq$, where $q$ is prime. By the Jacobi symbol multiplication law, we have $\left(\frac{2}{b}\right) = \left(\frac{2}{m}\right)\left(\frac{2}{q}\right)$. Now, we consider cases.

*Case I*: $b \equiv 1 \pmod 8$. In this case, we can have $(m, q) \equiv (1,1), (3,3), (5,5), (7,7) \pmod 8$. In each of these subcases, the induction hypothesis and the law of quadratic reciprocity makes it a straightforward verification to show $\left(\frac{2}{m}\right) = \left(\frac{2}{q}\right)$, so that $\left(\frac{2}{b}\right) = 1$.

*Case II*: $b \equiv 3 \pmod 8$. In this case, we can have $(m, q) \equiv (1,3), (3,1), (5,7), (7,5) \pmod 8$. In each of these subcases, observe that $\left(\frac{2}{m}\right) = -\left(\frac{2}{q}\right)$, so that $\left(\frac{2}{b}\right) = -1$.

*Case III*: $b \equiv 5 \pmod 8$. In this case, we can have $(m, q) \equiv (1,5), (3,7), (5,1), (7,3) \pmod 8$. Again, observe $\left(\frac{2}{m}\right) = -\left(\frac{2}{q}\right)$, so $\left(\frac{2}{b}\right) = -1$.

*Case IV*: $b \equiv 7 \pmod 8$. In this case, we can have $(m, q) \equiv (1,7), (3,5), (5,3), (7,1) \pmod 8$. Hence $\left(\frac{2}{m}\right) = \left(\frac{2}{q}\right)$, so $\left(\frac{2}{b}\right) = 1$.

Thus, by induction and casework, we have established the second equality.

Finally, for the third statement, notice that if $\gcd(a, b) > 1$, it is easy to show $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = -\left(\frac{b}{a}\right) = 0$ (let $p$ be a prime dividing both $a$ and $b$, so that the expansion of both $\left(\frac{a}{b}\right)$ and $\left(\frac{b}{a}\right)$ ends up having a zero), so we suppose $\gcd(a, b) = 1$. In this case, set $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_\ell$, where $p_i \neq q_j$ for all $i \leq k$ and $j \leq \ell$. Now by expanding out and using the Jacobi symbol multiplication law, we see

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{p_i}{q_j}\right),$$

which is helpful as the symbols in the product are Legendre symbols, which we know how to manipulate. By quadratic reciprocity, we make the replacement

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left[\left(\frac{q_j}{p_i}\right)(-1)^{\frac{(p_i-1)(q_j-1)}{4}}\right] = \prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{(p_i-1)(q_j-1)}{4}}\cdot\left(\frac{b}{a}\right)$$

$$\implies \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{(p_i-1)(q_j-1)}{4}},$$

so it suffices to prove $\prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{1}{4}(p_i-1)(q_j-1)} = (-1)^{\frac{1}{4}(a-1)(b-1)}$. Now, note for any $p, q$ primes, we have by Euler's Criterion

$$(-1)^{\frac{1}{4}(p-1)(q-1)} = \left((-1)^{\frac{1}{2}(p-1)}\right)^{\frac{1}{2}(q-1)} = \left(\frac{-1}{p}\right)^{\frac{1}{2}(q-1)}.$$

Substituting this and noting $a = p_1p_2\cdots p_k$, we obtain

$$\prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{1}{4}(p_i-1)(q_j-1)} = \prod_{j=1}^{\ell}\left(\frac{-1}{a}\right)^{\frac{1}{2}(q-1)} =: A.$$

Finally, if $a \equiv 1 \pmod 4$, then $\left(\frac{-1}{a}\right) = 1$ so $A = 1 = (-1)^{\frac{1}{4}(a-1)(b-1)}$. In the case $a \equiv 3 \pmod 4$, then Euler's Criterion gives

$$A = \prod_{j=1}^{\ell}(-1)^{(q_j-1)/2} = \prod_{j=1}^{\ell}\left(\frac{-1}{q_j}\right) = \left(\frac{-1}{b}\right) = (-1)^{(b-1)/2},$$

which can be easily verified, so we are done. □

# 14 Quadratic Reciprocity: First Proof (Part 1)

We now begin a proof of the main statement of the law of quadratic reciprocity. First, we fix the following notation, in line with our proof (in Math 180A) for the case $\left(\frac{2}{p}\right)$.

**Definition 14.1.** Let $p$ be a prime, and $a \in \mathbb{Z}$ satisfy $p \nmid a$. We define $\mu(a, p)$ to be the number of integers in the range $\{1a, 2a, \ldots, \frac{1}{2}(p-1)a\}$ that have a negative remainder modulo $p$ upon reduction into the range $\left(-\frac{1}{2}(p-1), \frac{1}{2}(p-1)\right]$.

We now prove a technical lemma, which reflects our process of proof in the case $\left(\frac{2}{p}\right)$.

**Lemma 14.2.** *Let $p, a$ be as above. When the integers $a, 2a, \ldots, \frac{1}{2}(p-1)a$ are reduced modulo $p$ into the interval $\left(-\frac{1}{2}(p-1), \frac{1}{2}(p-1)\right]$, we get the numbers $\pm1, \pm2, \ldots, \pm\frac{1}{2}(p-1)$ in some order, where each number occurs once with exactly one of the $+$ or $-$ signs.*

That is, for example, $-2$ can possibly appear, but not both $-2$ and $+2$.

*Proof.* Let $u_1, u_2, \ldots, u_s$ be the number of negatives upon doing this reduction, and similarly, we set $v_1, v_2, \ldots, v_{\frac{1}{2}(p-1)-s}$ to be the number of positive residues. [Note $s = \mu(a,p)$ by definition.] It suffices to show that

$$A := \left\{-u_1, -u_2, \ldots, -u_s, v_1, v_2, \ldots, v_{\frac{1}{2}(p-1)-s}\right\} = \left\{1, 2, \ldots, \frac{1}{2}p - 1\right\}.$$

Since $a, 2a, \ldots, \frac{1}{2}(p-1)a$ are distinct modulo $p$, the elements of $A$ are distinct modulo $p$. Moreover, the $-u_i$ are distinct modulo $p$, and the $v_j$ are also distinct modulo $p$, so it suffices to show that $-u_i \not\equiv v_j$ for any $i, j$. Suppose for contradiction that there exist $u_i, v_j$ such that $-u_i \equiv v_j \pmod{p}$, so that $v_j + u_i \equiv 0 \pmod{p}$,i.e., $p \mid (v_j + u_i)$. But now there exists $k, \ell \in \mathbb{Z}$ (by definition of $u_i, v_j$) such that $ka + \ell a = (k+\ell)a \equiv 0 \pmod{p}$, where $1 \leq k, l \leq \frac{1}{2}(p-1)$. Since $p \nmid a$, we must have $p \nmid (k+\ell)$, but $2 \leq k + \ell \leq p - 1 < p$, which is absurd. Hence, the $-u_i$ and the $v_j$ are distinct modulo $p$, which establishes the lemma. □

The next result follows immediately.

**Theorem 14.3** (Gauss' Criterion)**.** *Let $p$ be a prime, and $a$ be an integer coprime to $p$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}.$$

*Proof.* Fix notation as in the proof of Lemma 14.2. Then by that same lemma,

$$a \cdot 2a \cdots \frac{1}{2}(p-1)a = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \prod u_i \prod v_j \equiv (-1)^s \left(\frac{p-1}{2}\right) \pmod{p}.$$

But now $s = \mu(a,p)$, so $\left(\frac{a}{p}\right) \equiv (-1)^s = (-1)^{\mu(a,p)}$, from which it follows that $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$. □

With this, we are ready to go into the main argument of quadratic reciprocity, though in this section, we will mainly set things up. Take $p \neq q$ as odd primes. Consider the Legendre symbol $\left(\frac{q}{p}\right)$, and take $1 \leq i \leq \frac{1}{2}(p-1)$ so that $iq$ reduces to a negative number in $\left(-\frac{1}{2}(p-1), \frac{1}{2}(p-1)\right]$. Unpacking this, there exists a unique integer $j$ such that

$$-\frac{p}{2} < iq - jp < 0 \iff 0 < jp - iq < \frac{p}{2}. \tag{1}$$

Because $0 < i < p/2$, we must have $0 < j < q/2$. By Gauss' Criterion, $\left(\frac{q}{p}\right) = (-1)^s$, where $s$ is the number of pairs $(i,j)$ satisfying $0 < i < p/2$, $0 < j < q/2$ and inequality (1).

Now, by symmetry, $\left(\frac{p}{q}\right) = (-1)^t$, where $t$ is the number of integer pairs $(i,j)$ with $0 < i < p/2$, $0 < j < q/2$, and

$$0 < iq - jp < q/2. \tag{2}$$

We will see later that all of this has a geometric interpretation: we count lattice points lying inside the rectangle $R := \left(0, \frac{p}{2}\right) \times \left(0, \frac{q}{2}\right) \subseteq \mathbb{R}^2$, such that we satisfy the two inequalities above, where we replace $i \mapsto x$ and $j \mapsto y$.

# 17 Quadratic Reciprocity: Second Proof (Part 1)

First, we give an alternate proof of Gauss' Criterion that will motivate the ideas for this proof of quadratic reciprocity.

*Proof (of Thm. 14.3).* Take $p$ to be an odd prime and $a$ coprime to $p$. Define

$$K := \{k \in \mathbb{Z} : 0 < k < p/2\},$$

and define the function $f : K \to K$ by

$$f(k) := \begin{cases} r_k & r_k < p/2 \\ p - r_k & r_k \geq p/2, \end{cases}$$

where $r_k$ is the remainder of $k \cdot a$ upon reduction modulo $p$. By design, $f$ is well-defined, so we show that $f$ is bijective, i.e., it is injective on the finite set $K$. If $k_1, k_2 \in K$ are chosen such that $f(k_1) = f(k_2)$, three cases can occur. If $r_{k_1}, r_{k_2} < p/2$ or $r_{k_1}, r_{k_2} \geq p/2$, then we simply have $k_1 = k_2$. In the third case that $r_{k_1} < p/2 \leq r_{k_2}$, we must have by definition of $f$, $r_{k_1} = p - r_{k_2}$, so that $r_{k_1} + r_{k_2} = p$. But this is impossible as $0 < r_{k_1}, r_{k_2} < p/2$. Thus, $f$ is indeed injective, so that

$$\prod_{k \in K} k = \prod_{k \in K} f(k) = \prod_{k \in K}^{r_k < p/2} r_k \cdot \prod_{k \in K}^{r_k \geq p/2} (p - r_k) \equiv (-1)^{\mu(a,p)} \prod_{k \in K} r_k \pmod{p},$$

and some basic manipulations and cancellations finishes the proof. □

We have some similar propositions. We use the notation $\mathbb{Z}/p\mathbb{Z}$ to represent the integers $0, 1, \ldots, p-1$, modulo $p$, and the notation $(\mathbb{Z}/p\mathbb{Z})^\times$ to be the integers that are invertible modulo $p$, i.e., all integers, considered modulo $p$, coprime to $p$.

**Proposition 17.1.** *Let $p$ be an odd prime and $a$ coprime to $p$. If $\beta := \sum_{k=1}^{(p-1)/2} r_{2k}$, where $r_{2k}$ is the remainder of $2k \cdot a$ modulo $p$, then $\left(\frac{a}{p}\right) = (-1)^\beta$.*

*Proof.* Define $U := \{2, 4 \ldots, p-1\} \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$, and a function $f : U \to U$ by

$$f(x) := \begin{cases} r_x & r_x \text{ is even} \\ p - r_x & r_x \text{ is odd} \end{cases}$$

This is well-defined, so we claim that $f$ is a bijection. If $x_1, x_2$ are such that $f(x_1) = f(x_2)$, it is easy to establish injectivity when $r_{x_1} \equiv r_{x_2} \pmod 2$. Now, without loss of generality, suppose $r_{x_1}$ is even and $r_{x_2}$ is odd. Then $r_{x_1} = p - r_{x_2}$, so that $r_{x_1} + r_{x_2} = p$. But we can derive a similar contradiction, so that $f$ is bijective and

$$\prod_{u \in U} au = a^{\frac{1}{2}(p-1)} \prod_{u \in U} u \equiv \prod_{u \in U}^{r_u \text{ even}} g(u) \prod_{u \in U}^{r_u \text{ odd}} (-1)^{r_u} g(u) \equiv (-1)^{\sum r_u} \prod g(u) \equiv (-1)^\beta \prod_{u \in U} u,$$

where all reductions are done modulo $p$. Hence, the result follows. □

**Proposition 17.2.** *Let $p$ be an odd prime and $p \nmid a$. If $\beta' := \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ka}{p} \right\rfloor$, then $\left(\frac{a}{p}\right) = (-1)^{\beta'}$.*

*Proof.* We know that $p\left\lfloor \frac{2ka}{p} \right\rfloor + r_{2k} = 2ka$. Reduction modulo 2 gives $p\left\lfloor \frac{2ka}{p} \right\rfloor \equiv r_{2k} \pmod 2$, so because $p$ is odd, we have $\left\lfloor \frac{2ka}{p} \right\rfloor \equiv r_{2k} \pmod 2$. The previous result thus proves the claim. □

Our next proposition will be crucial for our second proof of quadratic reciprocity.

**Proposition 17.3.** *Let $p, q$ be distinct odd primes, and set $A := \{n \in (\mathbb{Z}/pq\mathbb{Z})^\times : n < pq/2\}$. Then*

$$\prod_{n \in A} n \equiv \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod p.$$

*Proof.* We work with the slightly easier set $A' := A \cup \{\text{multiples of } p \text{ less than } pq/2\}$. More symbolically,

$$A' = \left\{ n \in \mathbb{Z} : 0 < n < \frac{1}{2}pq,\ p \nmid n \right\}.$$

Now

$$\prod_{n \in A'} n = [1 \cdot 2 \cdots (p-1)][(p+1) \cdots (2p-1)] \cdots \equiv [(p-1)!]^{\frac{1}{2}(q-1)} \cdot \left(\frac{p-1}{2}\right)! \pmod p.$$

[To see this, consider $A'$ as a grid with rows of length $p$, where we delete the rightmost element.] It follows from here that

$$\prod_{n \in A'} n = \prod_{n \in A} n \prod_{k=1}^{(p-1)/2} kq \equiv [(p-1)!]^{(q-1)/2} \left(\frac{p-1}{2}\right)!$$

$$\iff \left(\prod_{n \in A} n\right) \cdot q^{(p-1)/2} \equiv (-1)^{(q-1)/2} \pmod p,$$

where the last congruence follows from Wilson's Theorem. Hence $(-1)^{\frac{1}{2}(q-1)} \equiv q^{\frac{1}{2}(p-1)} \pmod p$, so we have $\left(\frac{-1}{q}\right) \equiv \left(\frac{q}{p}\right) \cdot \prod_{n \in A} n \pmod p$, so

$$\prod_{n \in A} n = \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod p,$$

as desired. □

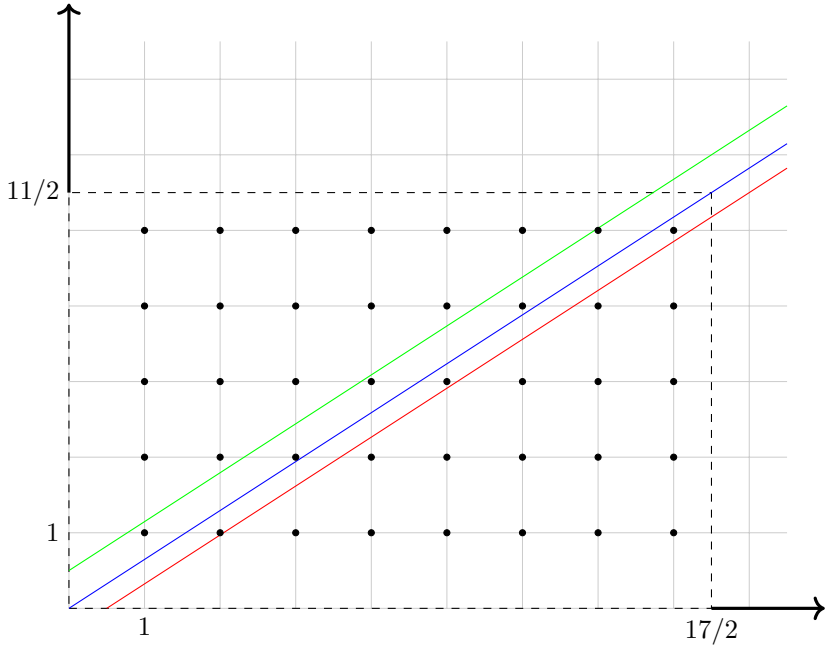
# 18 Quadratic Reciprocity, First Proof (Part 2)

[This continues from Section 14.] Let $p \neq q$ be odd primes throughout. We continue the proof of the main statement of quadratic reciprocity. In Section 14, we established a geometric interpretation, regarding the rectangle $R := (0, p/2) \times (0, q/2) \subseteq \mathbb{R}^2$. We fix the following notation.

**Definition 18.1.** We let $s$ denote the number of integer pairs $(i,j) \in R$ such that $0 < jp - iq < p/2$. Similarly, let $t$ denote the number of integer pairs $(i,j) \in R$ such that $0 < iq - jp < q/2$.

We thus have $\mu(q,p) = s$ and $\mu(p,q) = t$, by definition of $s$ and $t$.

**Example 18.2.** Let $p = 17$ and $q = 11$. Then $R = (0, 17/2) \times (0, 11/2)$. Replacing $i$ with $x$ and $j$ with $y$, our very important inequalities become regions in between the parallel lines $py - qx = 0, p/2, -q/2$:




Notice now that by construction, $s$ is the number of lattice points between the green and the blue lines, and $t$ is the number of points between the blue and the red lines. Now, no points can lie in the blue line: if $py = qx$ and $(x,y) \in \mathbb{Z}^2 \cap R$, we must have $p \mid x$ and $q \mid y$, which is impossible as $x, y$ are too small and $\gcd(p,q) = 1$. Similarly, there are no points on the two "off-diagonals," as $p/2, -q/2$ are not integers ($p, q$ are odd primes).

Now, let $U$ denote the region above the green line, and $D$ be the region below the red line. By symmetry, we can observe that the number of lattice points in $U$ and $D$ are the same, which leads us to the following proposition.

**Proposition 18.3.** *Let $U, D \subseteq R$ be defined by*

$$U := \left\{(i,j) \in R \cap \mathbb{Z}^2 : jp - iq > p/2\right\}$$
$$D := \left\{(i,j) \in R \cap \mathbb{Z}^2 : jp - iq < -q/2\right\}.$$

*Then $|U| = |D|$.*

If we can prove Prop. 18.3, then we notice that $|R \cap \mathbb{Z}^2| = \frac{p-1}{2} \cdot \frac{q-1}{2}$. So, from here, we observe

$$(-1)^{\frac{1}{4}(p-1)(q-1)} = (-1)^{|R \cap \mathbb{Z}^2|} = (-1)^{|U|}(-1)^{|D|}(-1)^s(-1)^t = (-1)^{2|U|}(-1)^s(-1)^t,$$

so that Gauss' Criterion gives

$$(-1)^{\frac{1}{4}(p-1)(q-1)} = (-1)^s(-1)^t = (-1)^{\mu}(q,p)(-1)^{\mu}(p,q) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right),$$

which would complete the proof of the main statement of quadratic reciprocity. Hence, it suffices to rigorously prove Prop. 18.3. The idea is to "flip" $U$ to lie on top of $D$, so that the integer points "line up." To do this, we make the following definition.

**Definition 18.4.** An *involution* of a finite set $A$ is a bijection $\pi : A \to A$ such that $\pi(\pi(x)) = x$.

An involution $\pi$ partitions $A$ into the set of fixed points of $\pi$, and the set of moved points. These moved points must therefore come in pairs; i.e.,

$$|A| - \#\{x \in A : \pi(x) = x\} \equiv 0 \pmod 2.$$

[Algebraically speaking, this can be seen by noting $\pi \in S_A \cong S_{|A|}$, the symmetric group on $A$, and that $\pi$, having order 2, must be a product of distinct transpositions.]

Now, we prove Prop. 18.3 by defining the involution $\varphi : U \cup D \to U \cup D$ by

$$(x,y) \mapsto \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right).$$

It is not too difficult to check that $\varphi$ is well-defined, and it is indeed an involution:

$$\varphi(\varphi(x,y)) = \varphi\left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right) = \left(\frac{p+1}{2} - \frac{p+1}{2} + x, \frac{q+1}{2} - \frac{q+1}{2} + y\right) = (x,y).$$

Now, if $(x,y) \in U$, we have $py - qx > p/2$, so that

$$p \cdot \left(\frac{q+1}{2} - y\right) - q \cdot \left(\frac{p+1}{2} - x\right) = \frac{p}{2} - \frac{q}{2} - (py + qx) < -\frac{q}{2},$$

so that $\varphi(x,y) \in D$. Similarly whenever $(x,y) \in D$, we have $\varphi(x,y) \in U$. Since $U \cap D = \varnothing$, the map $\varphi$ restricts to bijections on $U$ and $D$, so that $|U| = |D|$, completing the proof of Prop. 18.3, and thus completing the proof of the law of quadratic reciprocity. $\square$

# 20 Quadratic Reciprocity: Third Proof (Part 1)

[The prerequisites for this section are Math 120AB, which is not a prerequisite for this course, so this section may be skipped or delayed.]

We now give an alternate, algebraic proof of quadratic reciprocity. Again, fix $p \neq q$ to be odd prime, and define $F := \mathbb{F}_{q^{p-1}}$, the finite field of order $q^{p-1}$. We need the following classic fact about finite fields:

**Proposition 20.1.** *For any finite field $F$ of order $q^k$, we have $F^\times = \mathbb{Z}/(q^k - 1)\mathbb{Z}$, a cyclic group.*

Fermat's Little Theorem states that $p \mid (q^{p-1} - 1)$, so by the fact that $F^\times$ is cyclic, there exists an element of order $p$ in $F^\times$, with $F = \mathbb{F}_{q^{p-1}}$ as defined above. Call this element $\zeta$, so that $\zeta^p = 1$ but $\zeta^k \neq 1$ for all $1 \leq k < p$. Now, the $\zeta^k$ $(1 \leq k \leq p)$ are roots of $x^p - 1 \in F[x]$; now, since $F$ is a field, the $\zeta^k$ are all the roots of $x^p - 1$. Hence, $x^p - 1$ splits linearly:

$$x^p - 1 = \prod_{k=1}^{p} (x - \zeta^k).$$

Also, applying Euler's Criterion gives the following equation in $F$:

**Proposition 20.2.** *We have* $\left(\frac{p}{q}\right) = p^{\frac{1}{2}(q-1)}$*, where the symbol on the right means*

$$p^{\frac{1}{2}(q-1)} = (1 + 1 + \cdots + 1)^{\frac{1}{2}(q-1)},$$

*the sum occurring* $p$ *times.*

We also define the following:

**Definition 20.3.** Fix notation as above. The *Gauss sum* is

$$G := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta^i,$$

where everything occurs in $F$.

This completes the setup needed for this proof.

# 23 Quadratic Reciprocity: Second Proof (Part 2)

[This continues from Section 17.] Throughout, we fix the following notation: $p \neq q$ are odd primes and $A = \{n \in (\mathbb{Z}/pq\mathbb{Z})^\times : n < pq/2\}$. Proposition 17.3 tells us that

$$\prod_{n \in A} n \equiv \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \pmod{p}.$$

We also define the following:

**Definition 23.1.** Let $n \in \mathbb{Z}$. We let $r_n$ denote the remainder of $n$ modulo $p$, and $s_n$ denote the remainder of $n$ modulo $q$, as well as the sets

$$B := \left\{n \in (\mathbb{Z}/p\mathbb{Z})^\times : r_n < p/2\right\} \text{ and}$$
$$C := \left\{n \in (\mathbb{Z}/p\mathbb{Z})^\times : s_n < q/2\right\}.$$

From here, one can show

$$\prod_{n \in B} n \equiv \left[\left(\frac{p-1}{2}\right)!\right]^{q-1} \pmod{p}, \text{ and} \tag{3}$$

$$\prod_{n \in C} n \equiv [(p-1)!]^{(q-1)/2} \equiv (-1)^{\frac{1}{2}(q-1)} = \left(\frac{-1}{q}\right) \pmod{p}. \tag{4}$$

Using these, we finish our proof of quadratic reciprocity.

*Proof of Thm. 13.2(3).* Fix notation as above. Define $f : B \to A$ by

$$f(n) := \begin{cases} n & n < pq/2 \\ pq - n & n \geq pq/2. \end{cases}$$

We claim that $f$ is injective. Suppose $f(n_1) = f(n_2)$ for some $n_1, n_2 \in (\mathbb{Z}/pq\mathbb{Z})^\times$. If $n_1, n_2 < pq/2$ or $n_1, n_2 \geq pq/2$, this is obvious. If $n_1 < pq/2 \leq n_2$, observe that $f(n_1) = n$ and $f(n_2) = pq - n_2$, so $n_1 + n_2 = pq$. In particular, $p \mid (n_1 + n_2)$, so $p \mid (r_{n_1} + r_{n_2})$ upon reduction modulo $p$. But now $r_{n_1}, r_{n_2} < p/2$, a contradiction. Since $B, A$ are finite, $f : B \to A$ is in fact bijective. It follows that

$$\begin{aligned} \prod_{n \in A} n = \prod_{n \in B} f(n) &= \prod_{n \in B}^{n < pq/2} f(n) \cdot \prod_{n \in B}^{n \geq pq/2} f(n) \\ &= \prod_{n \in B}^{n < pq/2} n \cdot \prod_{n \in B}^{n \geq pq/2} (pq - n) \\ &= (-1)^\alpha \prod_{n \in B} n \pmod{pq}, \end{aligned}$$

where $\alpha$ is the number of elements $n \in B$ such that $n \geq pq/2$. But using the equations preceding this proof, we see $(-1)^\alpha = \left(\frac{p}{q}\right)$.

By a similar argument we may verify that

$$\prod_{n \in A} \equiv (-1)^\beta \prod_{n \in C} n \pmod{pq},$$

where $\beta$ is the number of elements $n \in C$ with $n \geq pq/2$, and that $(-1)^\beta = \left(\frac{q}{p}\right)$. Finally, we define the function $h : B \to C$ by

$$h(n) := \begin{cases} n & s_n < q/2 \\ pq - n & s_n \geq q/2, \end{cases}$$

which, by a similar argument, is bijective, so

$$\prod_{n \in C} n = \prod_{n \in B} h(n) = \prod_{n \in B}^{s_n < q/2} h(n) \cdot \prod_{n \in B}^{s_n \geq q/2} h(n) \equiv \prod_{n \in B}^{s_n < q/2} n \cdot \prod_{n \in B}^{s_n \geq q/2} (-n) \pmod{pq}.$$

If $n \in B$, then by definition $n < p/2$, so $r_n \in \left\{1, 2, \ldots, \frac{1}{2}(p-1)\right\}$. If in addition $s_n \geq q/2$ (which corresponds to the second product), we see $s_n \in \left\{\frac{1}{2}(p-1), \ldots, q-1\right\}$. Each $n$ in the second product is thus congruent to a pair

$$\begin{cases} n \equiv r_n \pmod{p} \\ n \equiv s_n \pmod{q}, \end{cases}$$

so by the Chinese Remainder Theorem, there are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ negative signs in the product above. It follows that

$$\prod_{n \in C} n = (-1)^{\frac{1}{4}(p-1)(q-1)} \prod_{n \in B} n,$$

hence

$$\begin{aligned}\prod_{n\in A} &\equiv (-1)^{\alpha}\prod_{n\in B} n \equiv (-1)^{\beta}\prod_{n\in C} n \\ &= (-1)^{\beta}(-1)^{\frac{1}{4}(p-1)(q-1)}\prod_{n\in B} n \\ \implies (-1)^{\alpha} &\equiv (-1)^{\beta}(-1)^{\frac{1}{4}(p-1)(q-1)} \\ \implies \left(\frac{p}{q}\right) &\equiv \left(\frac{q}{p}\right)(-1)^{\frac{1}{4}(p-1)(q-1)},\end{aligned}$$

which is exactly the statement of quadratic reciprocity. □

# 24 Quadratic Reciprocity: Third Proof (Part 2)

[This continues from Section 20, which has Math 120AB as a prerequisite, so this section may be skipped or delayed.]

We continue with the algebraic proof of quadratic reciprocity. Again, fix $p \neq q$ to be odd primes; let $F := \mathbb{F}_{q^{p-1}}$, and in $F$, define the Gauss sum

$$G := \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i \in F,$$

where $\zeta$ has order $p$ in $F^\times$. Note that because $F$ has characteristic $q$,

$$G^q = \left(\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i\right)^q = \sum_{i=1}^{q}\left(\frac{i}{p}\right)^q\zeta^{iq} = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^{iq},$$

and observe $\left(\frac{i}{p}\right) = \left(\frac{iq}{p}\right)\left(\frac{q}{p}\right)$, so that

$$G^q = \left(\frac{q}{p}\right)\sum_{i=1}^{p-1}\left(\frac{iq}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right)\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i = \left(\frac{q}{p}\right)G$$

as $i \mapsto iq$ is a bijection modulo $p$. However, we now compute $G^q$ differently using the following claim:

**Proposition 24.1.** *We have $G^2 = (-1)^{\frac{1}{2}(p-1)}p$, where $p = \underbrace{1+1+\cdots+1}_{p \text{ times}}$.*

Using the claim, we may write

$$G^q = (G^2)^{\frac{1}{2}(q-1)}G = G\left[(-1)^{\frac{1}{2}(p-1)}p\right]^{\frac{1}{2}(q-1)} = G(-1)^{\frac{1}{4}(p-1)(q-1)}\left(\frac{p}{q}\right),$$

where we have applied the claim as well as Euler's Criterion (Prop. 20.2). Since $G \in F^\times$ (note $G^2 \neq 0$ by Prop. 24.1), we obtain

$$\left(\frac{q}{p}\right)\cancel{G} = \cancel{G}(-1)^{\frac{1}{4}(p-1)(q-1)}\left(\frac{p}{q}\right) \implies \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{1}{4}(p-1)(q-1)},$$

which is quadratic reciprocity. Thus, it suffices to show Prop. 24.1 holds. We note the identity $\zeta^0 + \zeta^1 + \cdots + \zeta^{p-1} = 0$, which follows from Vieta's Formulas with $x^p - 1 \in F[x]$, so that

$$\sum_{i=1}^{p-1} \zeta^i = -1. \tag{5}$$

We also know $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$, so that

$$\sum_{i=1}^{p-2} \left(\frac{i}{p}\right) = -\left(\frac{p-1}{p}\right) = -\left(\frac{-1}{p}\right). \tag{6}$$

Thus

$$G^2 = \left(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta^i\right) \left(\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^j\right) = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \zeta^{i+j}.$$

Set $j \equiv ik \pmod{p}$ for some $k \in \mathbb{Z}$, so that $\left(\frac{ij}{p}\right) \zeta^{i+j} = \left(\frac{k}{p}\right) \zeta^{i(1+k)}$. As we sum over all pairs $(i, j)$, we get the pairs $(i, k)$ exactly once, for the map $a \mapsto ka$ is a bijection modulo $p$. Hence

$$G^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{ij}{p}\right) \zeta^{i+j} = \sum_{i=1}^{p-1} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{i(1+k)}. \tag{7}$$

Now, when $k = p + 1 \equiv -1 \pmod{p}$, we have $\zeta^{i(1+k)} = \zeta^{pi} = 1$, so fixing $k + p + 1$ and summing over $i$, we get the expression $\left(\frac{-1}{p}\right) \sum_{i=1}^{p-1} 1 = (p-1) \cdot \left(\frac{-1}{p}\right)$. Thus from equation (7), we have

$$G^2 = \left(\frac{-1}{p}\right)(p-1) + \sum_{k=1}^{p-2} \left[\left(\frac{k}{p}\right) \left(\sum_{i=1}^{p} \zeta^{i(1+k)}\right)\right]. \tag{8}$$

When $k \neq p+1$, we see that $\zeta^{i(1+k)}$ is in fact a primitive $p$th root of unity, i.e., $\left\langle \zeta^{i(1+k)} \right\rangle = \langle \zeta \rangle \leq F^\times$. Now, from equations (8) and (5), we have

$$\begin{aligned} G^2 &= \left(\frac{-1}{p}\right)(p-1) + \sum_{k=1}^{p-2} \left(\frac{k}{p}\right)(-1) \\ &= \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) \\ &= p\left(\frac{-1}{p}\right) \text{ from equation (6)} \\ &= p(-1)^{\frac{1}{2}(p-1)} \text{ by Euler's Criterion,} \end{aligned}$$

which establishes Prop 24.1 and thus quadratic reciprocity. $\square$

# 27 Quadratic Reciprocity: Worked Examples

**Example 27.1.** Suppose $p \equiv 3 \pmod 4$ is a prime $m \in \mathbb{Z}$ be such that $p \nmid m$. Show that $x^2 + y^2 = pm$ has no rational solutions.

*Proof.* Write $x = a/c$ and $y = b/c$, putting everything over a common denominator such that $\gcd(a, b, c) = 1$. Then if $x, y$ are nontrivial rational solutions, we have

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = pm \implies a^2 + b^2 = pmc^2.$$

Thus $p \mid (a^2+b^2)$ so if $p \nmid a, b$, we have $-b^2 \in \mathsf{QR}(p)$. But $\left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$ as $p \equiv 3 \pmod 4$, so we must have $p \mid a$ or $p \mid b$. In either case, this implies $p \mid a$ *and* $p \mid b$, so $p^2 \mid (a^2 + b^2)$, so that $p^2 \mid pmc^2 \implies p \mid c^2 \implies p \mid c$, so $p$ is a common factor for $a, b, c$, a contradiction. □

**Example 27.2.** Suppose $a, b \in \mathbb{Z}$ satisfy $a^2 + 3b^2 = p$, where $p$ is prime. Show that $p \equiv 1 \pmod 3$ or $p = 3$.

*Proof.* Reducing modulo 3 gives $a^2 \equiv p \pmod 3$. If $p = 3$, there is nothing to do, so suppose $p \neq 3$. Then $p$ is a quadratic residue modulo 3, so that $p \equiv 1 \pmod 3$. □

**Example 27.3.** Suppose $a, b \in \mathbb{Z}$ satisfy $2a^2 + 5b^2 = p$ for some prime $p$. Show that $p = 2$, $p = 5$, or $p \equiv 7, 13, 23, 37 \pmod{40}$.

*Proof.* If $p = 2, 5$, then nothing needs to be done, so suppose $p \neq 2, 5$. Reducing modulo 5, we obtain $2a^2 \equiv p \pmod 5$, so that $a^2 \equiv 3p \pmod 5$. Hence $3p \in \mathsf{QR}(5)$, so that

$$1 = \left(\frac{3p}{5}\right) = \left(\frac{3}{5}\right)\left(\frac{p}{5}\right) = -\left(\frac{p}{5}\right),$$

so $p \in \mathsf{NR}(5)$, i.e., $p \equiv 2, 3 \pmod 5$. Now, reduce $p$ modulo 8, and consider the cases that arise. If $p \equiv \pm 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$, so that $\left(\frac{2a^2}{p}\right) = 1$, so $\left(\frac{-5b^2}{p}\right) = 1$, so $\left(\frac{-5}{p}\right) = 1$. But $\left(\frac{p}{5}\right) = -1$ by assumption, so quadratic reciprocity gives $\left(\frac{-1}{p}\right) = -1$, i.e., $p \equiv 3 \pmod 4$. This forces $p \equiv 7 \pmod 8$. If $p \equiv 3 \pmod 8$, then $\left(\frac{2}{p}\right) = -1$, so that $\left(\frac{2a^2}{p}\right) = -1$, and thus $\left(\frac{-5b^2}{p}\right) = -1$, so $\left(\frac{-5}{p}\right) = -1$. But $\left(\frac{p}{5}\right) = -1$, so $\left(\frac{-1}{p}\right) = 1$ so that $p \equiv 1 \pmod 4$, forcing $p \equiv 5 \pmod 8$. By the Chinese Remainder Theorem, we have $p \equiv 7, 13, 27, 37 \pmod{40}$, as claimed. □

# 28 Sums of Two Squares

Let $p$ be an odd prime. Then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$, i.e., the congruence $x^2 \equiv -1 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$. [Of course, when $p = 2$, the congruence also holds as $1 \equiv -1$, but 2 is not odd.]

Suppose $p \equiv 1 \pmod 4$, so that there exist integers $0, x, y \leq p - 1$ such that $x^2 + y^2 \equiv 0 \pmod p$ (simply set $y \equiv 1 \pmod p$). However, can we show that there exists a pair such that $x^2 + y^2 = p$? The answer is in fact, affirmative.

**Theorem 28.1** (Thue, 1902)**.** *Let $p \equiv 1 \pmod 4$ be prime. Then there exist integers $0 \leq x, y \leq \sqrt{p}$ such that $x^2 + y^2 = p$.*

*Proof.* Let $p \equiv 1 \pmod 4$. There are $(1 + \lfloor p \rfloor)^2$ integer pairs $(x, y)$ with $0 \leq x \leq \sqrt{p}$. Since $\lfloor x \rfloor > x - 1$, we have

$$(\lfloor p \rfloor + 1)^2 > ((\sqrt{p} - 1) + 1)^2 = p.$$

Thus, there are *more than* $p$ such pairs $(x, y)$. Now, $\left(\frac{-1}{p}\right) = 1$, so let $s \in \mathbb{Z}$ satisfy $s^2 \equiv -1 \pmod p$. Now, applying the pigeonhole principle, there exist distinct pairs $(x', y') \neq (x'', y'')$ for which

$$x' - sy' \equiv x'' - sy'' \pmod p. \tag{9}$$

This gives $x' - x'' \equiv s(y' - y'') \pmod p$, which forces $x' \neq x''$ **and** $y' \neq y''$ (as $s \not\equiv 0 \pmod p$). Take $x := |x' - x''|$ and $y := |y' - y''|$. Squaring both sides of (9) gives $x^2 \equiv s^2 y^2 \iff x^2 \equiv -y^2 \pmod p$, so $x^2 + y^2 \equiv 0 \pmod p$. but now $x, y \in \left\{1, 2, \ldots, \lfloor \sqrt{p} \rfloor\right\}$, so that $x^2, y^2 \leq \lfloor \sqrt{p} \rfloor^2 < p$. [Note that this inequality is strict, as $\sqrt{p}$ is not an integer.] Hence $2 \leq x^2 + y^2 < p + p = 2p$, so that $x^2 + y^2 \equiv 0 \pmod p$ forces $x^2 + y^2 = p$, as desired. □

What happens if $p \equiv 3 \pmod 4$? We first prove the following statement.

**Proposition 28.2.** *Suppose $n \in \mathbb{Z}^+$ is a sum of two integer squares and $p \equiv 3 \pmod 4$ is a prime with $p \mid n$. Then $p^2 \mid n$.*

*Proof.* Write $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, so reducing modulo $p$ gives $x^2 + y^2 \equiv 0 \pmod p$. If $p \mid x$, then $p \mid y$ and thus $p^2 \mid (x^2 + y^2) = n$, so we are done. If $p \nmid x$, then $y^2 \equiv -x^2$ is a quadratic residue modulo $p$ (as $x \not\equiv 0$), but

$$1 = \left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right)\cancel{\left(\frac{x^2}{p}\right)} = \left(\frac{-1}{p}\right),$$

which is contradictory as $p \equiv 3 \pmod 4$. Thus, only the former case can hold, so $p^2 \mid n$. □

This gives a negative answer: primes congruent to 3 modulo 4 are not the sums of squares.

**Corollary 28.3.** *If $p \equiv 3 \pmod 4$, then $p$ is not a sum of two squares.*

*Proof.* If it were, then the previous proposition tells us that $p^2 \mid p$, an obvious contradiction. □

All of this is in fact enough to tell us when a general integer may be written in the form $x^2 + y^2$, for $x, y \in \mathbb{Z}$.

**Theorem 28.4.** *A positive integer $n$ can be represented as a sum of two squares if and only if any prime congruent to 3 $\pmod 4$ appears with even exponent in the prime factorization of $n$.*

*Proof.* ( $\implies$ ): Suppose $n$ is a sum of two squares. Then if $n = 1, 2$, or $n$ is a prime congruent to 1 $\pmod 4$, then we are done. Otherwise, we note the identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2,$$

which may be verified by considering the complex numbers $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$ and taking their magnitudes (or by direct expansion), so that the product of any two integers that are the sums of two squares is a sum of two squares. Now, if $k$ is a sum of two squares, then so is $z^2 k$ for any $z \in \mathbb{Z}$; writing $k = a^2 + b^2$, we have $z^2 k = (za)^2 + (zb)^2$. Since no prime congruent to 3 (mod 4) is a sum of two squares, the consequent follows.

( $\Longleftarrow$ ): If $p \equiv 3 \pmod 4$ is a prime dividing $x^2 + y^2$, then $p \mid x, y$ and $p^2 \mid n$ by Proposition 28.2. Now, if $n = x^2 + y^2$ and $p \mid n$, we have $n/p^2 = (x/p)^2 + (y/p)^2$ is a sum of two integer squares. Continuing to apply this fact gives that no prime congruent to 3 (mod 4) can divide $n$ an odd number of times, so by contraposition, we are done. $\square$

# 30 Quadratic Forms and Sums of Squares

**Definition 30.1.** Let $a, b, c \in \mathbb{Z}$. The polynomial $f(x, y) = ax^2 + bxy + cy^2$ is called a *binary quadratic form.*

We have already studied two such forms: $f(x, y) = x^2$ and $f(x, y) = x^2 + y^2$. But in general, we ask two question: whether $f(x, y) \equiv r \pmod n$ has a solution or where $f(x, y) = k$ for some $k \in \mathbb{Z}$. Another interesting question is whether two separate forms $f(x, y)$ and $g(x, y)$ represent the same set of values — this leads to a field known as the *reduction theory of binary quadratic forms.*

Alternatively, we can study quadratic forms which are not binary: for example, which integers are of the form $x_1^2 + x_2^2 + \cdots + x_n^2$? We have this well-known theorem:

**Theorem 30.2** (Lagrange's Four-Square Theorem)**.** *Every positive integer is a sum of four integer squares.*

The proof idea of Theorem 30.2 is similar to that of the 2-square case, and involves an identity that stems from taking magnitudes of *quaternions* $a + bi + cj + dk$, which we will see later.

Now, we give an alternate proof to the 2-square case, which introduces the method of *infinite descent*, which will be used later.

**Theorem 30.3** (Fermat's Two-Square Theorem)**.** *Let $p \equiv 1 \pmod 4$ be prime. Then $p = x^2 + y^2$ for some integers $x, y$.*

Though we will not prove the theorem formally in this section, we give a few examples of the proof idea. Since we assume $p \equiv 1 \pmod 4$, there is a solution to $x^2 \equiv -1 \pmod p$ (call it $A \leq p - 1$), so that we see $A^2 + 1^2 \equiv 0 \pmod p$, so write $A^2 + 1^2 = Mp$ for some $M \in \mathbb{Z}^+$. We may further assume $M < p$, as $Mp \leq (p-1)^2 + 1 < p^2$. If $M = 1$, then we are done so suppose $M \geq 2$, and that $A^2 + B^2 = Mp$ for $0 \leq A, B < p$. Here, $B$ could be 1, or it could be something else, but it does not really matter.

The idea is now to take the triple $(A, B, M)$ to find a new triple $(a, b, m)$, such that $1 \leq m < M$ and $a^2 + b^2 = mp$. If $m = 1$, this completes the proof; if not, we keep doing the *descent procedure* until we get $a^2 + b^2 = p$. We give two examples, with actual numbers, on how to do this.

**Example 30.4.** Let $p = 881$, which we can check is prime. Suppose we know that

$$387^2 + 1^2 = 170 \cdot 881,$$

so that $A = 387, B = 1$, and $M = 170$. First, the descent procedure reduces everything modulo $M = 170$ into the range $[-M/2, M/2] = [-85, 85]$ to make things as small as possible:

$$47^2 + 1^2 \equiv 0 \pmod{170}.$$

In fact, $47^2 + 1^2 = 2210 = 170 \cdot 13$, and now note the identity (this is the same identity as the one used in Theorem 28.4)

$$(47^2 + 1^2)(387^2 + 1^2) = (47 \cdot 387 + 1 \cdot 1)^2 + (1 \cdot 387 - 47 \cdot 1)^2$$

$$\implies 170^2 \cdot 13 \cdot 881 = 18190^2 + 340^2.$$

Now, we can check that $170 \mid 340$ and $170 \mid 18190$, so we may divide both sides of the above by $170^2$ to get

$$13 \cdot 881 = 107^2 + 2^2.$$

Now, we have $m = 13$, which is indeed smaller than $M = 170$. Let us do the descent procedure again: take now $A \to 107, B \to 2$, and $M \to 13$. We reduce modulo $M = 13$ into the range $[-M/2, M/2] = [-13/2, 13/2]$:

$$0 \equiv 3^2 + 2^2 \pmod{13}.$$

In fact, $3^2 + 2^2 = 13$, so we note the identity

$$(107^2 + 2^2)(3^2 + 2^2) = (107 \cdot 3 + 2 \cdot 2)^2 + (3 \cdot 2 - 107 \cdot 2)^2$$

$$\implies 13^2 \cdot 881 = 325^2 + (-208)^2 = 325^2 + 208^2,$$

and now dividing out by $13^2$ gives $\boxed{881 = 25^2 + 16^2}$, so at this point the descent procedure is complete.

**Example 30.5.** Let $p = 12049$, which we can also check is prime. Suppose we know that

$$557^2 + 55^2 = 26 \cdot 12049.$$

We follow the descent procedure again to write 12049 as a sum of squares. First, we reduce modulo $M = 26$ to obtain

$$11^2 + 3^2 \equiv 0 \pmod{26}.$$

Now, we notice that because $557 \equiv 11 \pmod{26}$ and $55 \equiv 3 \pmod{26}$, we have

$$557 \cdot 11 + 55 \cdot 3 \equiv 557 \cdot 3 - 55 \cdot 11 \equiv 0 \pmod{26}.$$

Thus, we may divide $(557 \cdot 11 + 55 \cdot 3)^2$ and $(557 \cdot 3 - 55 \cdot 11)^2$ by $26^2$ to obtain

$$\left(\frac{557 \cdot 11 + 55 \cdot 3}{26}\right)^2 + \left(\frac{557 \cdot 3 - 55 \cdot 11}{26}\right)^2 = 242^2 + 41^2 = 5 \cdot 12049.$$

Now, take $M = 5$, and continue the descent procedure by reducing modulo 5: we get $2^2 + 1^2 \equiv 0 \pmod{5}$, so that $242 \cdot 2 + 41 \cdot 1 \equiv 242 \cdot 1 - 41 \cdot 2 \equiv 0 \pmod{5}$, so b similar logic (dividing out $5^2$), we find

$$\left(\frac{242 \cdot 2 + 41 \cdot 1}{5}\right)^2 + \left(\frac{242 \cdot 1 - 41 \cdot 2}{5}\right)^2 = 105^2 + 32^2 = 11024 + 1024 = 12049,$$

which shows $\boxed{12049 = 105^2 + 32^2}$.

# 33 Quaternions

In the previous section, we mentioned Lagrange's Four-Square Theorem, and we briefly commented about its relationship to quaternions. Hence, in this section, we introduce some basic facts about quaternions.

**Definition 33.1.** We define the *quaternions* $\mathbb{H}$ as the set

$$\mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

where $i, j, k$ are symbols. We define addition componentwise, and multiplication is governed by the *quaternion relations* $ij = -ji = k$, $jk = -kj = i$, $ik = ki = j$, and $i^2 = j^2 = k^2 = ijk = -1$ then extended by distributivity over addition.

It is readily checked that $\mathbb{H}$ is a non-commutative division ring; that is, the multiplication is not commutative, but every nonzero element has a multiplicative inverse. We may demonstrate this by taking a generic quaternion $\alpha = a+bi+cj+dk$, defining the *quaternion conjugate* $\bar{\alpha} = a - bi - cj - dk$. One can check that $\alpha\bar{\alpha} = \bar{\alpha}\alpha = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$, so we define

$$|\alpha| := \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Considering $\mathbb{H}$ as a 4-dimensional inner product space over $\mathbb{R}$ (i.e., $\mathbb{R}^4$ with the dot product), we may check immediately that $|\alpha\beta| = |\alpha| \cdot |\beta|$ and $|\alpha + \beta| \leq |\alpha + \beta|$ for all $\alpha, \beta \in \mathbb{H}$. Considering this is a number theory course, we may want a notion of "distance" or "length" without the square root, so we define the following:

**Definition 33.2.** Let $\alpha = a + bi + cj + dk \in \mathbb{H}$. We define the *norm* $N : \mathbb{H} \to \mathbb{R}_{\geq 0}$ by

$$N(\alpha) := a^2 + b^2 + c^2 + d^2 = |\alpha|^2.$$

This is useful, because often we will restrict the discussion of $N$ to the set of integral quaternions:

$$L := \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\},$$

so that $N$ restricts to a map $N|_L : L \to \mathbb{Z}_{\geq 0}$. While $N$ is a norm just like how $|\cdot|$ is a norm on $\mathbb{Z}$, the set $L$ does not possess a division algorithm:

**Example 33.3.** Let $\alpha = 1 + j$ and $\beta = 1 + i$. Then there do not exist $q, r \in L$ such that $\alpha = \beta q + r$ and $N(r) < N(\beta)$.

*Proof.* Notice that $N(\beta) = 2$, so if such a pair $q, r \in L$ existed, we either have $N(r) = 0$ or $N(r) = 1$. Now, clearly $N(r) = 0$ if and only if $r = 0$, so in this case, we would have $(1 + j) = q(1 + i)$ so that $q = (1 + j)/(1 + i)$, but one can check that this choice of $q$ is not in $L$. Thus, we are forced to have $N(r) = 1$, so $r \in \{\pm 1, \pm i, \pm j, \pm k\}$. A straightforward verification of these eight cases shows that none of them produce $q$'s that are in $L$. For example, if $r = 1$, then $1 + j = q(1 + i) + 1$ implies $j = q(1 + i)$, so that $q = j \cdot (\frac{1}{2} - \frac{1}{2}i) \notin L$. Hence, no such $q, r \in L$ exist. □

However, this issue is fixed if we consider half-integer coefficients: define

$$H := \left\{ a + bi + cj + dk \;\middle|\; a, b, c, d \in \mathbb{Z} \text{ **or** } a, b, c, d \in \frac{1}{2} + \mathbb{Z} \right\}.$$

That is, all of $a, b, c, d$ are forced to be integers, or all are forced to be half-integers: $\frac{1}{2} - \frac{1}{2}i + \frac{3}{2}j - \frac{5}{2}k \in H$, but $1 - \frac{1}{2}i + 2j + \frac{3}{2}k \notin H$. Now, redoing the previous example, we can compute

$$1 + j = \left(\frac{1}{2} - \frac{1}{2}i + \frac{1}{2}j - \frac{1}{2}k\right)(1 + i) + 0.$$

From here, it could be proven that $H$ has a division algorithm with respect to the norm $N$, restricted to $H$. From the definition of $H$, it is easily checked that $N$ only assumes integer values on $H$.

Recall that a unit in a set of numbers $A$ is an element $\alpha$, such that there exists $\beta \in A$ such that $\alpha\beta = 1$. We now determine the units of $H$.

**Proposition 33.4.** *The units of $H$ are $\pm 1, \pm i, \pm j, \pm k$, and $\pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$, with each sign being picked freely.*

*Proof.* First, if $\alpha\beta = 1$, then $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $N$ assumes integer values on $H$, we must have $N(\alpha) = N(\beta) = 1$. Now, the elements of norm 1 in $H$ are exactly the list above, and we can check that they are all units using the fact that if $\alpha = 1$, then $\alpha\bar{\alpha} = N(\alpha) = 1$. □

# 34 Sums of Two Squares

In this section, we now give a formal proof of Theorem 30.3, via descent. Fix $p \equiv 1 \pmod 4$ to be prime, so there must exist integers $A, B$ such that $A^2 + B^2 = Mp$, where $1 \le M \le p-1$ and $0 \le A, B \le p - 1$.

Define $u, v \in [-\frac{M}{2}, \frac{M}{2}]$ with $u \equiv A \pmod M$ and $v \equiv B \pmod M$, so that $u^2 + v^2 = Mr$ (for some $r \in \mathbb{Z}$). Now $1 \le r \le p - 1$, for if $r = 0$, we have $u = v = 0$, so that $A \equiv B \equiv 0 \pmod M$, so that $A^2 + B^2 = Mp$ implies $M^2 \mid M \cdot p \implies M \cdot p$, so that $M = 1$, so in this case there is nothing to descend from and we are done. Hence, the assumption $r \ge 1$ is fair. Now

$$u^2 + v^2 \le \frac{M^2}{4} + \frac{M^2}{4} = M \cdot \frac{M}{2},$$

so that $r < M/2 < p$. Now, note the identity

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2 = M^2 rp. \tag{10}$$

Because $u \equiv A$ and $v \equiv B \pmod M$, we see $vA - uB \equiv 0 \pmod M$ and $uA + vB \equiv A^2 + B^2 \equiv 0 \pmod M$. Thus, dividing over by $M^2$ gives

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp,$$

which completes the descent procedure and thus the proof of the main theorem. □

Now, it follows that if $m = p_1 p_2 \cdots p_r M^2$, where the $p_i = 2$ or $p_i \equiv 1 \pmod 4$, we may write $p_i$ as sums of squares and use the multiplication identity (10) to write $p_1 \cdots p_r$ as a sum of two squares. Then $p_1 \cdots p_r = a^2 + b^2$, so $m = (Ma)^2 + (Mb)^2$. If $M > 1$, then the two squares have a common factor of $M$, but this is not always necessary, for example

$$125 = 5^2 + 10^2 = 11^2 + 2^2.$$

Thus, we might be interested as to *when* an integer can be written as a sum of two *coprime* squares. But we have the following theorem.

**Theorem 34.1.** *Let $m \in \mathbb{Z}^+$. Then $m = a^2 + b^2$, with $\gcd(a, b) = 1$, if and only if $m$ is one of the two types of integers described below:*

1. *The integer $m$ is odd and every prime divisor of $m$ is congruent to 1 modulo 4.*
2. *The integer $m$ is twice an integer of the first type.*

*Proof.* See Homework 3. □

As an interesting corollary of everything we know about sums of two squares, we refer back to an exercise we completed in Math 180A.

**Proposition 34.2.** *The equation $x^2 + y^2 = 3$ has no rational solutions.*

*Proof.* Suppose $x = a/c$ and $y = b/c$ were such a rational solution, where $\gcd(a, b, c) = 1$. Then $a^2 + b^2 = 3c^2$, so that $3c^2$ is a sum of two integer squares. But now $3c^2$ is divisible by 3 an odd number of times, which contradicts Theorem 28.4. □

# 37 Sums of Two Squares: Examples

In this section, we give sample applications of the theory we developed in the past few lectures.

**Example 37.1.** Write $m = 1189 = 29 \times 41$ as a sum of two squares.

*Solution.* First, note that $29 = 5^2 + 2^2$ and $41 = 5^2 + 4^2$, so the identity in (10) gives

$$\begin{aligned} 1189 &= (5^2 + 2^2)(5^2 + 4^2) \\ &= (5 \cdot 5 + 2 \cdot 4)^2 + (5 \cdot 4 - 2 \cdot 5)^2 \\ &= 33^2 + 10^2, \end{aligned}$$

so $1189 = \boxed{33^2 + 10^2}$. •

There is also a nice statement we can make about primitive Pythagorean triples. Recall that a *primitive Pythagorean triple* is a list of positive integers $(a, b, c)$ such that $\gcd(a, b, c) = 1$ and $a^2 + b^2 = c^2$. Hence, $c^2$ is a sum of squares, so we should expect a relationship here.

**Theorem 37.2.** *The triple of positive integers $(a, b, c)$ is a primitive Pythagorean triple if and only if $c$ is a product of primes congruent to 1 modulo 4.*

*Proof.* See the text, chapter [25]. □

**Example 37.3.** Find a primitive Pythagorean triple $(a, b, c)$ with $c = 1189$.

*Solution.* Using our classification of primitive Pythagorean triples from Math 180A (this is Theorem 14.6 in that set of notes), write $2c = 2 \cdot 29 \cdot 41 = s^2 + t^2$ for odd integers $s > t \geq 1$ with $\gcd(s, t) = 1$. Now

$$2c = (1^2 + 1^2)(33^2 + 10^2) = (33 + 10)^2 + (33 - 10)^2 = 43^2 + 23^2,$$

so let $s = 43$ and $t = 23$, so $a = 43 \cdot 23 = 989$ and $b = \frac{1}{2}(43^2 - 23^2)$. Thus, the triple we desire is $\boxed{(989, 660, 1189)}$. •

# 38 Fermat's Last Theorem for $n = 4$

In this section, we view another example of an descent argument by proving Fermat's Last Theorem for $n = 4$. In fact, we prove something stronger:

**Theorem 38.1.** *The equation $x^4 + y^4 = z^2$ has no positive integer solutions.*

*Proof.* Suppose for contradiction that $x_1^4+y_1^4 = z_1^2$ were such a solution $(x_1, y_1, z_1) \in \mathbb{Z}^+$. We show that there is a solution $(x_2, y_2, z_2)$ with $z_2 < z_1$, which is impossible as our argument will allow us to construct solutions $(x_i, y_i, z_i)$ with

$$z_1 > z_2 > \cdots > z_k > \cdots > 0,$$

which gives an infinite decreasing sequence of positive integers, which is impossible. Hence, it must be the case that the triple $(x_1, y_1, z_1)$ cannot exist in the first place.

First, we can, without loss of generality, assume that if $x_1^4+y_1^4 = z_1^2$, then $\gcd(x_1, y_1, z_1) = 1$: if $d$ is a common divisor of $x_1, y_1, z_1$, then $d^2 \mid (x_1^4 + y_1^4) = z_1^2$, so dividing out by $d$ gives a smaller positive integer solution. Hence, our assumption that $\gcd(x_1, y_1, z_1) = 1$ is valid.

Now, note that $(x_1^2, y_1^2, z_1)$ is a primitive Pythagorean triple, so without loss of generality, say $x_1$ is odd and $y_1$ is even. Thus, by our classification of primitive Pythagorean triples in Math 180A, there exist odd coprime integers $s > t \geq 1$ such that

$$x_1^2 = st, \;\; y_1^2 = \frac{1}{2}(s^2 - t^2), \text{ and } z_1 = \frac{1}{2}(s^2 + t^2).$$

Since $x_1$ is odd, observe $x_1^2 \equiv 1 \pmod 4$, so that $st \equiv 1 \pmod 4$, so $s \equiv t \pmod 4$.

Now, $2y_1^2 = s^2 - t^2 = (s - t)(s + t)$ and note $4 \mid (s - t)$, and $2 \mid (s + t)$ but $4 \nmid (s + t)$ [by the condition $s \equiv t \pmod 4$]. Hence, $2y_1^2 = 2(s - t)\left(\frac{s+t}{2}\right)$, so $y_1^2 = (s - t)\left(\frac{s+t}{2}\right)$. Now $\gcd(s - t, s + t) = 2$, which can be easily verified, so $\gcd(s - t, \frac{1}{2}(s + t)) = 1$. This implies that $(s - t)$ and $\frac{1}{2}(s + t)$ are both perfect squares, so write $2u^2 := s + t$ and $4v^2 := s - t$ — here, $u$ is odd, and recall $4 \mid (s - t)$. [Note $\gcd(u, 2v) = 1$.] This gives $s = u^2 + 2v^2$ and $t = u^2 - 2v^2$, and substituting gives

$$x_1^2 = st = (u^2 + 2v^2)(u^2 - 2v^2) = u^4 - 4v^4 \implies x_1^2 + 4v^4 = u^4.$$

Repeating this process, $(x_1, 2v^2, u^2)$ is a primitive Pythagorean triple, so there exist odd coprime integers $S > T \geq 1$ with

$$x_1 = ST, \;\; 2v^2 = \frac{1}{2}(S^2 - T^2), \text{ and } u^2 = \frac{1}{2}(S^2 + T^2),$$

so that

$$4v^2 = 2 \cdot 2v^2 = S^2 - T^2 = (S - T)(S + T).$$

Since $\gcd(S, T) = 1$ and both are odd, we see $\gcd(S - T, S + T) = 2$, so this implies $S + T = 2\alpha^2$ and $S - T = 2\beta^2$, for some $\alpha, \beta \in \mathbb{Z}^+$ with $\gcd(\alpha, \beta) = 1$. Now $S = \alpha^2 + \beta^2$ and $T = \alpha^2 - \beta^2$, so

$$u^2 = \frac{1}{2}(S^2 + T^2) = \frac{(\alpha^2 + \beta^2)^2 + (\alpha^2 - \beta^2)^2}{2} = \frac{2\alpha^4 + 2\beta^4}{2} = \alpha^4 + \beta^4.$$

Thus, we set $x_2 = \alpha$, $y_2 = \beta$, and $z_1 = u$. Certainly, $x_2, y_2, z_2 \geq 1$, and we check $z_2 < z_1$:

$$z_1 = \frac{1}{2}(s^2 + t^2) = \frac{1}{2}\left[(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2\right] = u^4 + 4v^4 > u^4 \geq u = z_2.$$

This completes the descent argument. □

We remark that we could have proceeded with the proof slightly differently, using the following version of the classification of primitive Pythagorean triples:

**Theorem 38.2.** *Every primitive Pythagorean triple $(x, y, z)$ is of the form $(r^2 - s^2, 2rs, r^2 + s^2)$, where $r > s \geq 1$, $\gcd(r, s) = 1$, and $r \not\equiv s \pmod 2$.*

Now, if $x^4 + y^4 = z^2$, we can, as before, assume $\gcd(x, y, z) = 1$, so that $(x^2, y^2, z)$ is a primitive Pythagorean triple. Again, we may suppose $x$ is odd and $y$ is even, so write

$$(x^2, y^2, z) = (r^2 - s^2, 2rs, r^2 + s^2)$$

for $r > s$ satisfying $r \not\equiv s \pmod 2$ and $\gcd(r, s) = 1$. Since $r^2 = x^2 + s^2$, it follows that $r$ is odd and $s$ is even (see this by reducing modulo 4). Since $(x, s, r)$ is also a primitive Pythagorean triple, write

$$(x, s, r) = (t^2 - u^2, 2tu, t^2 + u^2),$$

for $t > u$ satisfying $t \not\equiv u \pmod 2$ and $\gcd(t, u) = 1$. From here, this proof proceeds similarly, though there is a lot of bookkeeping involving keeping track of what is even and what is odd.

# 40 Sums of Four Squares

For yet another view of the descent argument, we prove Lagrange's Four-Square Theorem (Theorem 30.2), which states that every positive integer is a sum of 4 integer squares. To do this, we need the following identity, which is reminiscent of identity (10) and follows from multiplication in the quaternions:

**Lemma 40.1** (Euler's Four-Square Identity)**.** *We have that*

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ & + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

*holds identically.*

Proving this identity is a rote exercise in expanding everything out. Now, we state an intermediate result:

**Lemma 40.2.** *If $p$ is an odd prime, then there exist $x, y \in \mathbb{Z}$ such that $1 + x^2 + y^2 = Mp$, where $1 \leq M < p$.*

*Proof.* The integers $0, 1, \ldots, \frac{1}{2}(p-1)$, considered modulo $p$, are distinct when squared modulo $p$. Similarly, the map $y \mapsto -1 - y^2 \pmod p$ sends $0, 1, \ldots, \frac{1}{2}(p-1)$ injectively into $\mathbb{Z}/p\mathbb{Z}$. Hence, the following holds for subsets of $\mathbb{Z}/p\mathbb{Z}$:

$$\#\left\{x^2 : 0 \leq x \leq \frac{1}{2}(p-1)\right\} = \#\left\{-1 - y^2 : 0 \leq y \leq \frac{1}{2}(p-1)\right\} = \frac{1}{2}(p+1).$$

By the inclusion-exclusion principle, the two sets above have nonempty intersection, so pick some $a \in \mathbb{Z}/p\mathbb{Z}$ within this intersection. Now $a \equiv x^2 \equiv -1 - y^2 \pmod p$ for some $0 \leq x, y \leq \frac{1}{2}(p-1)$, so $x^2 + y^2 + 1 \equiv 0 \pmod p$. Finally, we note $x^2 + y^2 + 1 \geq 1$, and $x^2 + y^2 + 1 \leq \frac{1}{2}(p-1)^2 + 1 < p^2$, so that $x^2 + y^2 + 1 = Mp$ for some $1 \leq M < p$. □

It follows that (a fortiori) for an odd prime $p$, there exists some $M \in \mathbb{Z}$, $1 \leq M < p$, and some $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ with $x_1^2 + x_2^2 + x_3^2 + x_4^2 = Mp$, and from here, we give a proof of Lagrange's theorem. Let $m_0$ be the smallest positive integer such that there exist integers $x_i$ with $x_1^2 + \cdots + x_4^2 = m_0 p$. If $m_0 = 1$, there is nothing to show, so suppose otherwise; i.e., $2 \leq m_0 < p$.

Suppose $m_0$ is even. Then either all of the $x_i$'s are even, all of the $x_i$'s are odd, or exactly two of the $x_i$'s are even (in this last case, suppose $x_1, x_2$ are the even ones). But in all three cases, observe that $x_1 \pm x_2$ and $x_3 \pm x_4$ are all even, and

$$\frac{m_0}{2} \cdot p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

which contradicts the minimality of $m_0$.

Now, suppose $m_0$ is odd, so $3 \leq m_0 < p$. Write $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ as before, and choose $y_i \in [-m_0/2, m_0/2]$ with $y_1 \equiv x_i \pmod{m_0}$. This is legal because $\pm m_0/2 \notin \mathbb{Z}$ (as $m_0$ is odd), so the interval $[-\frac{(m_0-1)}{2}, \frac{m_0-1}{2}]$ is a complete set of residues modulo $m_0$. Evidently, not all of the $x_i$ are divisible by $m_0$, as otherwise $m_0^2 \mid m_0 p \implies m_0 \mid p$, which is contradictory as $3 \leq m_0 < p$. Now, $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}$, so set $y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1$ for some $m_1 \in \mathbb{Z}$. We claim $1 \leq m_1 < m_0$; since $y_i \in [-m_0/2, m_0/2]$ and $\pm m_0/2 \notin \mathbb{Z}$, we have

$$m_0 + m_1 = y_1^2 + y_2^2 + y_3^2 + y_4^2 < \frac{m_0^2}{4} + \frac{m_0^2}{4} + \frac{m_0^2}{4} + \frac{m_0^2}{4} = m_0^2,$$

so $m_1 < m_0$. Now, Euler's Four Square Identity implies that

$$(m_0 p)(m_0 m_1) = m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^2 \text{ for some } z_i \in \mathbb{Z},$$

where $m_0 \mid z_i$ via the same identity. [For example, $z_1 = x_1 y_1 + \cdots + x_4 y_4 \equiv x_1^2 + \cdots x_4^2 \equiv 0 \pmod{m_0}$.] Dividing out by $m_0^2$ gives $m_1 p = (z_1/m_0)^2 + (z_2/m_0)^2 + (z_3/m_0)^2 + (z_4/m_0)^2$, contradicting the minimality of $m_0$. This forces $m_0 = 1$, which completes the proof of the four-square theorem.

# 43 Descent: Worked Examples

**Example 43.1.** Show that $x^3 + 2y^3 + 4z^3 = 0$ only has $(0, 0, 0)$ as its only integer solution.

*Proof.* Suppose that $(x, y, z) \neq (0, 0, 0)$ were a non-trivial solution, and suppose this solution is minimal with respect to $|x| + |y| + |z|$. Then $x^3 = -2(y^3 + 2z^3)$, which implies $x^3$ is even, so $x$ is even. Write $x = (2a)^3$ for some $a \in \mathbb{Z}$, so $x^3 = 8a^3 = -2y^3 - 4z^3 \implies y^3 + 2z^3 + 4a^3 = 0$. This equation is the same as the first, except that we have shuffled the variables around and replaced something with $a$, so now completely analogous arguments show that $y, z$ are both even. Thus, dividing out the factor of 2 gives $a^3 + 2b^3 + 4c^3 = 0$, where $|a| + |b| + |c| = |x/2| + |y/2| + |z/2| < |x| + |y| + |z|$, as by supposition at least one of $x, y, z$ is nonzero. This is a contradiction. □

**Example 43.2.** Show that if $n \geq 2$, then $n \nmid (2^n - 1)$.

*Proof.* Suppose otherwise, and choose $n$ to be the smallest such $n$ such that $n \mid (2^n - 1)$, and let $p$ be its smallest prime factor, so that $p \mid (2^n - 1)$, i.e., $2^n \equiv 1 \pmod{p}$. Let $k$ be the order of 2 modulo $p$, so $k \mid (p - 1)$. But we know $k \mid n$ as $2^n \equiv 1 \pmod{p}$, and it is easy to see that $k > 1$, so pick a prime $q$ dividing $k$. Now $q \mid k$ and $k \mid n$ implies $q \mid n$, but $q \leq k < p$, a contradiction. □

# 44 Congruent Numbers

We give a final example of a theorem proven by descent. It is related to the following notion:

**Definition 44.1.** We say a rational number $D \in \mathbb{Q}$ is a *congruent number* if it is the area of a right triangle with rational side lengths.

One may ask, "which rational numbers are congruent?" — but this *congruent number problem* is a major unsolved problem in the theory of elliptic curves. However, we shall be satisfied in proving this theorem, due to Fermat, and is likely the first use of descent in modern mathematical history.

**Theorem 44.2.** *1 is not a congruent number.*

*Proof.* Suppose for contradiction that there exists a right triangle with rational side lengths with area 1, say with sides $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ with $a, b, c, d \in \mathbb{Z}$ (putting everything over a common denominator). That is, $(\frac{a}{d})^2 + (\frac{b}{d})^2 = (\frac{c}{d})^2$ and $1 = \frac{ab}{2d^2}$. This holds if and only if $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = d^2$, so that $(a, b, c)$ is a right triangle with area $d^2$, i.e., the original triangle exists if and only if there is a right triangle with *integer* side lengths and area equal to a perfect square. We show that this latter situation is impossible.

First, if $(a, b, c)$ is such an integer Pythagorean triple with area a perfect square $d^2$, we can, without loss of generality, assume that $(a, b, c)$ is primitive (just clear common factors). Now, we proceed by descent, supposing for contradiction that a primitive $(a, b, c)$ exists, with area $d^2$, and we choose such a triple where $c$ is minimized. Now, the classification of primitive Pythagorean triples gives $a = r^2 - s^2$, $b = 2rs$, and $c = r^2 + s^2$ for coprime integers satisfying $r > s \geq 1$ and $r \not\equiv s \pmod 2$. Now

$$d^2 = \frac{1}{2}ab = \frac{1}{2}(r^2 - s^2)(2rs) = rs(r - s)(r + s).$$

Since $\gcd(r, s) = 1$ and $r \not\equiv s \pmod 2$, we observe that $r \pm s$ are both odd and $\gcd(r, r \pm s) = 1$. Similarly, $\gcd(s, r \pm s) = 1$ and[1] $\gcd(r - s, r + s) = 1$. It follows that $r, s, r \pm s$ are all perfect squares, say $r =: x^2$, $s =: y^2$, $r + u =: u^2$, and $r - s =: v^2$. We now observe the following five statements:

1. $r^2 + s^2 = x^4 + y^4$.
2. $\gcd(u, v) = 1$ because $\gcd(r - s, r + s) = 1$.
3. $\gcd(u + v, u - v) = 2$ because $u \pm v$ are even.
4. $r = x^2 = \frac{1}{2}((r + s) + (r - s)) = \frac{1}{2}(u^2 + v^2)$.
5. $2s = 2y^2 = u^2 - v^2 = (u - v)(u + v)$.

From points (3) and (5), we see that one of the $u \pm v$ is congruent to 2 (mod 4) [think about this]. Without loss of generality, suppose $u + v \equiv 2 \pmod 4$; the argument is symmetric otherwise. Then $2y^2 = (u + v)(u - v) = \left(\frac{u+v}{2}\right)(u - v)$, and now the two factors are coprime, so say $u + v =: 2\alpha^2$, and since $u - v$ is even, write $4\gamma^2 := u - v$. This means $u = \frac{1}{2}(4\gamma^2 + 2\alpha^2) = \alpha^2 + 2\gamma^2$, and $v = \frac{1}{2}(2\alpha^2 - 4\gamma^2) = \alpha^2 - 2\gamma^2$. Now, by (4), we obtain $x^2 = \alpha^4 + 4\gamma^4$, so $(\alpha^2, 2\gamma^2, x)$ is a right triangle with area $A = \frac{1}{2}\alpha^2 \cdot 2\gamma^2 = (\alpha\gamma)^2$. But $x < c$, a contradiction. □

[1] Recall that if $\gcd(r, s) = 1$, then $\gcd(r - s, r + s) \mid 2$ — this was a homework problem in Math 180A.

We now shortly discuss the relationship between congruent numbers and elliptic curves, which is actually rather simple:

**Theorem 44.3.** *Let $D \in \mathbb{Q}^+$. Then there is a bijection between the two sets of ordered tuples:*

$$\left\{(a,b,c) : a^2 + b^2 = c^2 \text{ and } \frac{1}{2}ab = D\right\} \longleftrightarrow \left\{(x,y) : y^2 = x^3 - D^2x, y \neq 0\right\}.$$

*Proof.* Check that the bijection is given by $(a,b,c) \mapsto \dfrac{D}{ca}(b, 2D)$, which has the inverse $(x,y) \mapsto \dfrac{1}{y}(x^2 - D^2, 2Dx, x^2 + D^2)$. □

Furthermore, the bijection given in the proof above preserves positivity and rationality: under the map above, $a,b,c > 0$ if and only if $x,y > 0$ and $a,b,c \in \mathbb{Q}$ if and only if $x,y \in \mathbb{Q}$. From here, it follows that $D > 0$ is not a congruent number if and only if the only rational solutions to $y^2 = x^3 - D^2x$ (an elliptic curve) require $y = 0$. Thus, our proof that 1 is not a congruent number can be restated:

**Corollary 44.4.** *The only rational points on the elliptic curve $y^2 = x^3 - x$ are $(0,0)$ and $(\pm 1, 0)$.*

# 47 Quaternions and the Four-Square Theorem

We resume our work from Section 33, and we use the same notation as in that section, i.e., fix

$$H := \left\{ a + bi + cj + dk \,\middle|\, a,b,c,d \in \mathbb{Z} \text{ or } a,b,c,d \in \frac{1}{2} + \mathbb{Z} \right\}.$$

We have claimed before that $H$ possesses a division algorithm with respect to the standard norm $N$. To prove this, we state the following lemma.

**Lemma 47.1.** *For every $\alpha \in \mathbb{H}$, there exists $\beta \in H$ such that $N(\alpha - \beta) < 1$. That is, every quaternion can be "rounded" to a "close" one in $H$.*

*Proof.* Write $\alpha = a_1 + a_2 i + a_3 j + a_4 k$. Pick $b_1$ such that $|a_1 - b_1| \leq \frac{1}{4}$ (i.e., round $a_1$ to the nearest integer or half-integer $b_1 \in \frac{1}{2}\mathbb{Z}$). Now, we choose $b_2, b_3, b_4$ which are either all in $\mathbb{Z}$ (if $b_1 \in \mathbb{Z}$), or all in $\frac{1}{2} + \mathbb{Z}$ (if $b_1 \in \frac{1}{2} + \mathbb{Z}$). Then $|a_i - b_i| \leq \frac{1}{2}$ when $i \geq 2$, so that

$$N(\alpha - \beta) = \sum_{i=1}^{4} |a_i - b_i|^2 \leq \frac{1}{16} + \frac{3}{4} = \frac{13}{16} < 1,$$

which completes the proof. □

Now, if $\alpha, \beta \in H$ with $\beta \neq 0$, observe that $\beta^{-1}\alpha \in H$, so Lemma 47.1 applies and there exists $q \in H$ with $N(\beta^{-1}\alpha - q) < 1$. But now

$$N(\alpha - \beta q) = N(\beta(\beta^{-1}\alpha - q)) = N(\beta)N(\beta^{-1}\alpha - q) < N(\beta)$$

by multiplicativity, so we have proven the division algorithm:

**Theorem 47.2** (Hurwitz Quaternion Division Algorithm)**.** *Let $\alpha, \beta \in H$. Then there exists $q \in H$ such that $N(\alpha - \beta q) < N(\beta)$, and there exists $q' \in H$ such that $N(\alpha - q'\beta) < N(\beta)$.*

We remark that the set $H$ is sometimes called the set of *Hurwitz quaternions*, in honor of the German mathematician Adolf Hurwitz (1859-1919) who introduced them in his last year of life and realized they had a division algorithm.

**Lemma 47.3** (Bézout's Lemma for Hurwitz Quaternions)**.** *For all $\alpha, \beta \in H$, there exists $\gamma \in H$ such that $I := \{\alpha x + \beta y : x, y \in H\}$ and $J := \{\gamma z : z \in H\}$ are equal. That is, $\gamma$ functions like a "greatest common divisor" of $\alpha$ and $\beta$.*

*Proof.* Essentially, the proof is just doing the Euclidean algorithm on $H$; we remark that for those with experience in ring theory this is very similar to the the result that every Euclidean domain is a PID — here, $I, J$ are right ideals of $H$, and $H$ contains a left- and right-division algorithm. □

With this, we are on our way to prove Lagrange's Four-Square Theorem using divisibility properties of Hurwitz quaternions.

**Proposition 47.4.** *For every odd prime, there exists $\alpha, \beta \in H$, non-units, such that $p = \alpha\beta$.*

*Proof.* By Lemma 40.2, find $m, n \in \mathbb{Z}$ such that $p \mid (m^2 + n^2 + 1)$. We note the factorization over $H$

$$m^2 + n^2 + 1 = (1 + mi + nj)(1 - mi - nj), \tag{11}$$

and we define $I := \{px + (1 - mi - nj)y : x, y \in H\}$ and by Lemma 47.3, there exists $\alpha$ such that $J := \{\alpha z : z \in H\} = I$. In the definition of $I$ above, take $x = 1$ and $y = 0$, so $p = \alpha\beta$ for some $\beta \in H$. If $\beta$ is a unit, then $\alpha = p\beta^{-1}$, and take $x = 0, y = 1$, so there exists $z$ such that $1 - mi - nj = \alpha z = p\beta^{-1}z$, so[2] $p \mid_H (1 - mi - nj)$, but because $p \in \mathbb{Z}$ is central in $H$, $\beta^{-1}z = \frac{1}{p} - \frac{m}{p}i - \frac{n}{p}j \notin H$ (as $p > 2$), which is contradictory, so $\beta$ cannot exist.

Now, if $\alpha$ is a unit, then there exists $x, y \in H$ such that $px + (1 - mi - nj)y = \alpha z = 1$. But now

$$(1 + mi + nj)px + (1 + mi + nj)(1 - mi - nj)y = 1 + mi + nj,$$

so by (11), $p \mid (1 + mi + nj)$, which gives a similar contradiction. Hence $p = \alpha\beta$, and neither $\alpha$ nor $\beta$ are units in $H$. □

From here, we finish off the proof of the four-square theorem. If $p = \alpha\beta$ for non-units $\alpha, \beta$, then $N(\alpha) = N(\beta) = p$ by comparing norms. Now, we must have $\bar{\alpha} = \beta$, so there exists $a, b, c, d \in \mathbb{Z}$, **or** $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, such that $p = a^2 + b^2 + c^2 + d^2$. If $a, b, c, d \in \mathbb{Z}$, we are done, so suppose otherwise. Now, there exists a unit $u \in H$ such that $\alpha + u$ has even coefficients (take a unit of the form $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$). Now, $p = \alpha\bar{\alpha}$, so

$$p = \alpha\bar{\alpha} = (\alpha + u - u)(\overline{\alpha + u} - \overline{u}) = \left((\alpha + u)\bar{u} - 1\right)\left(\overline{\alpha + u} \cdot u - 1\right).$$

The first of these terms, $(\alpha + u)\bar{u} - 1$, has integer coefficients, so we are done — use Euler's Four-Square Identity to build all other integers as sums of four squares.

[2] The subscript $H$ just means we are discussing divisibility in $H$, not $\mathbb{Z}$.

# 50 Primitive Roots (I)

We first prove a preliminary result which will be used later.

**Theorem 50.1.** *Let $n \in \mathbb{Z}^+$. Then $n = \sum_{d|n} \varphi(d)$, where $\varphi$ is Euler's $\varphi$-function.*

We remark that this has a nice group-theoretic interpretation.

*Proof 1.* Consider the cyclic group $C_n$, which has a unique cyclic subgroup of order $d$ for all $d \mid n$. Let $\langle x \rangle \leq C_n$ have order $d$; we see $|x^k| = d$ if and only if $\gcd(d,k) = 1$ as we know $|x^k| = d/\gcd(d,k)$. Hence, $\langle x \rangle$ has $\varphi(d)$ elements of order $d$, so $C_n$ has $\varphi(d)$ elements of order $d$ (why?). Now, the formula $n = \sum_{d|n} \varphi(d)$ follows immediately, as the order of an element divides the order of $C_n$, which is $n$. □

*Proof 2.* We prove this statement for prime powers first. We know $\varphi(p^k) = p^k - p^{k-1}$, and we know that the divisors of $p^k$ are the $p^j$, for $0 \leq j \leq k$. Hence

$$\sum_{d|p^k} \varphi(d) = \sum_{j=0}^{k} \varphi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k,$$

so the theorem holds for prime powers. Now, recall that $\varphi$ is multiplicative; i.e., if $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. Define the function $F(n) := \sum_{d|n} \varphi(d)$. We have shown that $F(p^k) = p^k$ for all prime powers $p^k$; we claim $F(n) = n$ in general. To do this, we notice that the fundamental theorem of arithmetic tells us that it suffices to show that $F$ is multiplicative. Take $m, n$ to be coprime and let $\{d_1, \ldots, d_r\}$, $\{e_1, \ldots, e_s\}$ be the divisors of $m$ and $n$ respectively. Since $\gcd(m,n) = 1$, the divisors of $mn$ are $\{d_i e_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ and we know that $\varphi(d_i e_j) = \varphi(d_i)\varphi(e_j)$ as $\gcd(d_i, e_j) = 1$. Now

$$F(mn) = \sum_{i=1}^{r}\sum_{j=1}^{s} \varphi(d_i e_j) = \sum_{i=1}^{r}\sum_{j=1}^{s} \varphi(d_i)\varphi(e_j) = \sum_{i=1}^{r} \varphi(d_i) \sum_{j=1}^{s} \varphi(e_j) = F(m)F(n),$$

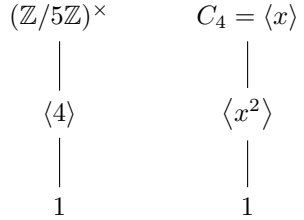
which completes the proof. □

We have made a comment about the previous theorem's relation to groups, and in particular, cyclic groups. Hence, we make the following definition, pertaining to the *multiplicative group* $(\mathbb{Z}/p\mathbb{Z})^\times$:

**Definition 50.2.** Let $p$ be a prime and $p \nmid a$. We define the *order of $a$ modulo $p$*, denoted $e_p(a)$ or $|a|_p$, to be the smallest positive integer $k$ such that $a^k \equiv 1 \pmod{p}$.

That is, $|a|_p$ is simply the order of $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

**Example 50.3.** We have $|1|_5 = 1$, $|2|_5 = |3|_5 = 4$, and $|4|_5 = 2$. This corresponds to the following subgroup diagram, with an isomorphic group to the right:



We also notice $|(\mathbb{Z}/5\mathbb{Z})|^\times = 4$, and that $|a|_5$ divides 4 for all $\bar{a} \in (\mathbb{Z}/5\mathbb{Z})^\times$. This is something that is true about the orders of elements in any group in general, but for our purposes, we only state it for the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.

**Proposition 50.4.** *Let $p$ be a prime and $p \nmid a$. Then if $a^n \equiv 1 \pmod{p}$, then $|a|_p$ divides $n$.*

We remark that the above tells us that $|a|_p$ always divides $p - 1 = |(\mathbb{Z}/p\mathbb{Z})|^\times$.

*Proof.* By the division algorithm, we have[3] $n = q|a| + r$, for $0 \leq r < |a|$. Now

$$1 \equiv a^n = a^{q|a|+r} = (a^{|a|})^q a^r \equiv a^r.$$

If $r \neq 0$, this contradicts the minimality of $|a|$, so $r = 0$ and $n = q|a|$. □

**Definition 50.5.** An integer $g$ with $|g|_p = p - 1$ for some prime $p$ is called a *primitive root modulo $p$*.

That is, primitive roots modulo $p$ are precisely generators of the group $(\mathbb{Z}/p\mathbb{Z})^\times$. If such a thing exists for a prime $p$, this tells us that $(\mathbb{Z}/p\mathbb{Z})^\times$ is in fact *cyclic*, which will be very helpful in understanding the multiplicative structure modulo a prime.

# 53 Descent: Worked Examples (I)

**Theorem 53.1** (Legendre's Three-Square Theorem)**.** *Let $n \in \mathbb{Z}^+$. Then $x^2 + y^2 + z^2 = n$ has an integer solution if and only if $n \neq 4^a(8b + 7)$ for any integers $a, b \geq 0$.*

As an exercise, we will prove the "only if" direction of this theorem.

*Proof.* ($\implies$): By contraposition, let $n = 4^a(8b+7)$. We show that $x^2+y^2+z^2 = 4^a(8b+7)$ has no solution by proceeding by induction on $a$. When $a = 0$, we see $n \equiv 7 \pmod{8}$. Then reducing modulo 8, we obtain $x^2+y^2+z^2 \equiv 7 \pmod{8}$. Now, the squares modulo 8 are $0, 1$, and 4, and no combination of these gives 7 modulo 8, so no solution exists. Now, suppose for some $a \geq 0$, $x^2 + y^2 + z^2 = 4^a(8b + 7)$ has no integer solutions. Consider the equation $x^2 + y^2 + z^2 = 4^{a+1}(8b + 7)$, so now suppose for contradiction that a solution exists. Then exactly 0 or 2 of $x, y, z$ are odd; the contradiction is obvious if none are odd. Otherwise, without loss of generality, suppose $x, y \equiv 1 \pmod{2}$ and $z$ is even, which implies $x^2+y^2 \equiv 2 \pmod{8}$. But now $z^2 \equiv 0, 4 \pmod{8}$, so $x^2+y^2+z^2 \equiv 2, 6 \pmod{8}$, yet $4^{a+1}(8b+7) \equiv 0, 4 \pmod{8}$, a contradiction. This completes the induction. □

**Example 53.2.** Show that $x^2 + y^2 + z^2 = 7$ has no rational solutions.

*Proof.* For contradiction, let $(a/d)^2 + (b/d)^2 + (c/d)^2 = 7$ be a rational solution, so that $a^2 + b^2 + c^2 = 7d^2$ is an equation in integers. Also, suppose $a, b, c, d$ are chosen so that $\gcd(a, b, c, d) = 1$ (a common factor can be divided out otherwise). Now, reduce modulo 8 to obtain $a^2 + b^2 + c^2 \equiv 0, 4, 7 \pmod{8}$. If $7d^2 \equiv 7$, the contradiction follows from a similar argument given above. If $7d^2 \equiv 0, 4$, then $d^2 \equiv 0, 4$ so that $d$ is even. Again, this implies that either exactly 0 or 2 of $a, b, c$ are odd; if the former holds, this violates minimality, so without loss of generality, suppose $a, b \equiv 1 \pmod{2}$ and $c \equiv 0 \pmod{2}$. Then $a^2 + b^2 \equiv 2 \pmod{8}$, but now $a^2 + b^2 + c^2 \equiv 2, 6 \pmod{8}$ which is contradictory. □

[3] We will often write $|a| = |a|_p$ when the prime $p$ is clear from context.

# 57 Descent: Worked Examples (II)

**Example 57.1.** Show that $x^2 + 3y^2 = p$ has integer solutions for a prime $p$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

*Proof.* ( $\implies$ ): Suppose $x^2 + 3y^2 = p$ has an integer solution. Clearly, $p = 3$ works, so suppose $p \neq 3$. Reducing modulo $p$, we obtain $x^2 \equiv -3y^2 \pmod p$, so that $-3 \in \mathsf{QR}(p)$. This implies $p \equiv 1 \pmod 3$.

( $\impliedby$ ): Suppose $p = 3$. Then $0^2 + 3 \cdot 1^2 = 3$, so there is nothing to do. Hence, suppose $p \equiv 1 \pmod 3$. Then $-3 \in \mathsf{QR}(p)$, so the congruence $a^2 + 3 \equiv 0 \pmod p$ has a solution. Thus, take $A, B \in \mathbb{Z}$ such that $A^2 + 3B^2 = Mp$ for some $M > 0$; we may assume $0 \leq A, B \leq \frac{1}{2}(p-1)$, so that

$$A^2 + 3B^2 \leq \left(\frac{p-1}{2}\right)^2 + 3\left(\frac{p-1}{2}\right)^2 = 4 \cdot \frac{(p-1)^2}{4} = (p-1)^2 < p^2,$$

so that $1 \leq M < p$. Now, take $a, b \in \mathbb{Z}$ such that $a \equiv A \pmod M$ and $b \equiv B \pmod M$, and $|a|, |b| \leq M/2$. Then $a^2 + 3b^2 \equiv A^2 + 3B^2 \equiv 0 \pmod M$. In fact, we may write $a^2 + 3b^2 = Mr$ for some $1 \leq r < M$; if $r = 0$, then $a = b = 0$, so $A \equiv B \equiv 0 \pmod M$, so that $M^2 | Mp \implies M | p$, so $M = 1$, so there would be nothing to do. Now, $|a|, |b| \leq M/2$, so $a^2 + 3b^2 \leq \frac{1}{4}M^2 + \frac{3}{4}M^2 \leq M^2$, so $r \leq M$; note $r \neq M$ as otherwise $a, b = \pm M/2$, so that $M$ is even, but this is contradictory as $M/2 \in \mathbb{Z}$, so that $a, b = M/2$, so that $A^2 + 3B^2$ s a multiple of $M^2$, giving $M = 1$ as before, so we can take $1 \leq r < M$. Now

$$(a^2 + 3b^2)(A^2 + 3B^2) = Mp \cdot Mr = M^2 rp,$$

but now

$$(a^2 + 3b^2)(A^2 + 3B^2) = (aA + 3bB)^2 + 3(aB - bA)^2,$$

and by assumption, $aA + 3bB$ and $aB - bA$ are multiples of $M$, so dividing out by $M^2$ gives

$$rp = \left(\frac{aA + 3bB}{M}\right)^2 + 3\left(\frac{aB - bA}{M}\right)^2,$$

which completes the descent. □

**Example 57.2.** Let $n \in \mathbb{Z}^+$. Show that $n$ is a congruent number if and only if the system $x^2 + ny^2 = z^2, x^2 - ny^2 = w^2$ has a nonzero integer solution.

*Proof.* Suppose $n$ is congruent. Then there exists $r, s, t \in \mathbb{Q}^+$ with $r^2 + s^2 = t^2$ and $\frac{1}{2}rs = n$, so $2rs = 4n$.. Now, $(r \pm s)^2 = t^2 \pm 4n$, so $\left(\frac{1}{2}(r \pm s)\right)^2 = \left(\frac{t}{2}\right)^2 \pm n$. Making the transformation $t/2 = x/y$, $\frac{1}{2}(r + s) = z/y$, and $\frac{1}{2}(r - s) = w/y$ and multiplying appropriately solves the system. This transformation is invertible, so the other direction also holds. □

# 60 Primitive Roots (II)

Recall that a primitive root modulo $p$ (a prime) is any integer $a$ with $|a| = p - 1$, i.e., it is a generator for the group $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $\left\{g, g^2, \ldots, g^{p-1}\right\} \equiv \{1, 2, \ldots, p-1\} \pmod p$. In this section, we show that primitive roots modulo a prime always exist.

**Theorem 60.1.** *Let $p$ be a prime, and suppose $d \mid p-1$. The number of integers $a \in \{1, 2, \ldots, p-1\}$ with order $|a| = d$ is $\varphi(d)$. In particular, there are exactly $\varphi(p-1)$ primitive roots modulo $p$.*

*Proof.* Define the function $\psi(d) := \#\{a \in (\mathbb{Z}/p\mathbb{Z})^\times : |a| = d\}$, i.e., $\psi$ counts the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order exactly $d$. We must show that $\psi(d) = \varphi(d)$ for all $d \mid p-1$.

Suppose $n \mid p-1$. Then $p-1 = nk$ for some $k \in \mathbb{Z}$. Now, consider the polynomial $x^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$, whose roots are $\{1, 2, \ldots, p-1\}$. Now, we note

$$x^{p-1} = x^{nk} - 1 = (x^n - 1)(1 + x^n + x^{2n} + \cdots + x^{(k-1)n}).$$

Now, $x^n - 1$ has at most $n$ roots, and $(1 + x^n + \cdots + x^{(k-1)n})$ has at most $(k-1)n$ roots. Hence, both must have the maximal number of roots (as $x^{p-1} - 1$ has $p-1$ roots), i.e., there are $n$ integers with order dividing $n$. Hence $n = \sum_{d \mid n} \psi(d)$, but we know that $n = \sum_{d \mid n} \varphi(d)$. Now, we proceed by induction to show $\psi(d) = \varphi(d)$ for all $d \mid p-1$. First, $\varphi(1) = \psi(1) = 1$, so suppose $n \mid p-1$ and that we have shown $\psi(d) = \varphi(d)$ for any $d \mid p-1$ with $d < n$. Let $d_1, d_2, \ldots, d_r$ be the divisors of $n$, and without loss of generality, assume $d_1 = n$. We have that $\varphi(n) + \sum_{i=2}^{r} \varphi(d_i) = n$, and similarly, we see $\psi(n) + \sum_{i=2}^{r} \psi(d_i) = n$. Since the $d_i$ (with $i \geq 2$) are proper divisors of $n$, we have $\psi(d_i) = \varphi(d_i)$ (whenever $i \geq 2$) by the induction hypothesis, so that we have $\varphi(n) = \psi(n)$, as claimed. This completes the proof of the theorem. □

We end with two questions to consider. First, what about primitive roots modulo $m$, for an arbitrary integer $m$?

**Example 60.2.** Take $m = 9$. Then $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$, and we can check that 2 is a primitive root modulo 9, but when $m = 8$, $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ lacks a primitive root.

Alternatively, given a number $n$, for which primes $p$ is $n$ a primitive root modulo $p$? This gives the following (yet) unsolved conjecture:

**Conjecture 60.3** (Artin)**.** *There are infinitely many primes $p$ for which 2 is a primitive root modulo $p$.*

# 63 Primitive Roots Modulo $n$

We know that all primes have primitive roots. Hence, we state the generalization of this fact:

**Theorem 63.1.** *Let $n \geq 2$. Then a primitive root modulo $n$ exists if and only if $n = 2, 4$, or $n = p^k, 2p^k$ where $p$ is an odd prime and $k \in \mathbb{Z}^+$.*

*Proof.* We consider four cases: $n = 2^m$, $n = p^k$, $n = 2^m p^k$, and the case where $n$ has more than one odd prime in its factorization. These cases cover all $n \geq 2$.

*Case I*: $n = 2^m$ for some $m \in \mathbb{Z}^+$. We show that $n$ has a primitive root if and only if $m \geq 2$. When $n = 2^1, 2^2$, this is trivial: 1 is a primitive root when $n = 2$, and 3 is a primitive root when $n = 4$. Now, let $m \geq 3$. When $m = 3$, we check that $1, 3, 5, 7$ are all not primitive roots modulo 8, so we proceed by induction on all $m \geq 3$. Suppose $2^m$ has no primitive roots, so that the orders of $a$ modulo $2^m$ divide $\varphi(2^m) = 2^{m-1}$, but is not equal to $2^{m-1}$; i.e., $|a| \leq 2^{m-2}$ for all $a \in (\mathbb{Z}/2^m\mathbb{Z})^\times$. Take any element $a \in (\mathbb{Z}/2^{m+1}\mathbb{Z})^\times$, and

set $|a| =: k$. We know $a^{2^{m-2}} \equiv 1 \pmod{2^m}$, so that $a^{2^{m-2}} \equiv 1, 2^m + 1 \pmod{2^{m+1}}$. In the first case, we are done, but in the second, note

$$(2^m + 1)^2 = 2^{2m} + 2^m + 1 \equiv 0 + 0 + 1 \equiv 1 \pmod{2^{m+1}},$$

so $a^{2^{m-1}} \equiv 1 \pmod{m}$. Hence $|a| \leq 2^{m-1} < 2^m = \varphi(2^{m+1})$, so $2^{m+1}$ has no primitive roots as claimed.

*Case II:* $n = p^k$ for some odd prime $p$ and $k \in \mathbb{Z}^+$. We know that when $k = 1$, we have a primitive root. Define, for some fixed $p^k$ and a primitive root $g \in (\mathbb{Z}/p\mathbb{Z})^\times$, $h := g$ if $g^{p-1} \not\equiv 1 \pmod{p^2}$, and $h := g + p$ otherwise. We claim that $h \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ is a primitive root modulo $p^k$. To prove this, we show that $h^{\varphi(p^{k-1})} \not\equiv 1 \pmod{p^k}$, and we do so by induction. When $k = 2$, the definition of $h$ gives the base case as follows: if $g^{p-1} \not\equiv 1 \pmod{p^2}$, then $h = g$, so $h^{p-1} \not\equiv 1 \pmod{p^2}$. If $g^{p-1} \equiv 1 \pmod{p^2}$, then $h = g + p$, so

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} pg^{p-2} + \binom{p-1}{2} p^2 g^{p-3} + \cdots + p^{p-1} \\ &\equiv g^{p-1} + (p^2 - p)g^{p-2} \pmod{p^2} \\ &\equiv g^{p-1} + \cancel{p^2 g^{p-2}} - pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}.\end{aligned}$$

Now, $p \nmid g$, so $pg^{p-2} \equiv 0 \pmod{p}$, so we are done. Now, we induct on our claim. Suppose the claim holds when $n = p^k$, i.e., $h^{\varphi(p^{k-1})} \not\equiv 1 \pmod{p^k}$. By Euler's Theorem, write $h^{\varphi(p^{k-1})} = cp^{k-1} + 1$ for some $c \in \mathbb{Z}$, so that $\varphi(p^k) = p \cdot \varphi(p^{k-1})$ implies $h^{\varphi(p^k)} = \left(cp^{k-1} + 1\right)^p$. Expanding this yields

$$\begin{aligned}\left(cp^{k-1} + 1\right)^p &= 1 + \binom{p}{1} cp^{k-1} + \binom{p}{2} c^2 p^{2(k-1)} + \cdots + \binom{p}{p} c^p c^{p(k-1)} \\ &\equiv 1 + cp^k + 0 + 0 + \cdots + 0 \pmod{p^2} \\ &\equiv 1 + cp^k \pmod{p^2}.\end{aligned}$$

Now, we claim $p \nmid c$, which will complete the induction — if $p \mid c$, then $h^{\varphi(p^{k-1})} = p^k m + 1$, which contradicts our assumption that $h^{\varphi(p^{k-1})} \not\equiv 1 \pmod{p^k}$. Hence, we are done.

*Case III*: $n = 2^m p^k$ for an odd prime $p$. If $m = 1$, let $g$ be a primitive root modulo $p^k$ (which exists by Case II), and define $h := g$ if $g$ is odd, and $h := p^k + g$ if $g$ is even. This ensures that $\gcd(h, n) = 1$, so that $|h| = |g| = \varphi(p^k) = \varphi(2p^k)$ as $p$ is odd.

*Case IV:* $n = rp^k$ for an odd prime $p$, and some *integer* $r \geq 3$ with $p \nmid r$. Here, we have $\varphi(n) = \varphi(r)\varphi(p^k)$, and since $r \geq 3$, $\varphi(r)$ is even. We know that for any $a$, we have $a^e \equiv 1 \pmod{n}$ if and only if $a^e \equiv 1 \pmod{p^k}$ and $a^e \equiv 1 \pmod{r}$. But this happens when $\varphi(r) \mid e$ and $\varphi(p^k) \mid e$. This holds in particular when $e = \frac{1}{2}\varphi(n) < \varphi(n)$, so no primitive roots exist in this case. □

The proof above gives us a technique to find primitive roots.

**Example 63.2.** Find a primitive root of 54.

*Solution.* We note that $54 = 2 \cdot 3^3$, so we find a primitive root of 27 first. Clearly, 2 is a primitive root modulo 3, and we check that $2^2 = 4 \pmod{3^2 = 9}$, so pick $h = 2$. The proof of Theorem 63.1 tells us that 2 is a primitive root modulo 27. Applying the proof again, we let $\bar{h} := 27 + 2 = \boxed{29}$, which is a primitive root modulo 54. •

**Example 63.3.** Find a primitive root of 250.

*Solution.* We factor $250 = 2 \cdot 5^3$. Again, 2 is a primitive root modulo 5, and $2^4 = 16 \not\equiv 1 \pmod{25 = 5^2}$, so pick 2 as a primitive root modulo 125. Now, we have $h = 125 + 2 = \boxed{127}$. •

# 64 Indices

**Definition 64.1.** Let $p$ be a prime, and $g$ be a primitive root modulo $p$. If $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, the *index* modulo $p$ for the *base* $g$ is the number $k$, where $1 \le k \le p-1$, such that $g^k \equiv a$, and is denoted $I_g(a)$.

We will often suppress the $g$ in the notation "$I_g(a)$" for brevity.

**Proposition 64.2.** *Let $p$ be a prime, and $g$ be a primitive root modulo $p$. Then for all $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have*

1. $I(ab) \equiv I(a) + I(b) \pmod{p-1}$,
2. $I(a^k) \equiv k \cdot I(a) \pmod{p-1}$.

We compare the rules for logarithms: we have $\ln ab = \ln a + \ln b$ and $\ln a^k = k \cdot \ln a$. Hence, for this reason the index is called the *discrete logarithm*, and should be a very natural notion.

*Proof.* For (1), write $a = g^k$ and $b = g^\ell$. Now $ab = g^k g^\ell = g^{k+\ell}$, so $I(ab) \equiv k + \ell \equiv I(a) + I(b) \pmod{p-1}$. Similarly, for (2), we have $a = g^m$. Then $a^k = g^{mk} = (g^m)^k$, so $I(a^k) \equiv mk \equiv k \cdot I(a) \pmod{p-1}$. □

Indices are useful for computation, as follows.

**Example 64.3.** Find the solutions to the congruence $3x^{30} \equiv 4 \pmod{37}$.

*Solution.* First, note that $g = 2$ is a primitive root modulo 37. Now, we take indices of both sides of the congruence above:

$$I(3x^{30}) \equiv I(4) \pmod{37 - 1 = 36}$$

$$\iff 30I(x) \equiv I(4) - I(3) \pmod{36}.$$

Now, we may check that $I(4) = 2$ and $I(3) = 26$, so we have the **linear** congruence $30I(x) \equiv 12 \pmod{36}$. Since $\gcd(30, 36) = 6$ and $6 \mid 12$, we have 6 incongruent solutions: $I(x) \equiv 4, 10, 16, 22, 28, 34 \pmod{36}$. Hence, the solutions to the original congruence are $x \equiv 2^4, 2^{10}, 2^{16}, 2^{22}, 2^{28}, 2^{34} \pmod{37}$, which can be computed via successive squaring or other means. •

# 68 Square-Triangular Numbers

Let us examine a familiar sequence.

**Definition 68.1.** We define the sequence of *triangular numbers* by $T_n := 1 + 2 + \cdots + n$.

By induction, it follows that $T_n = \frac{1}{2}n(n+1)$. We also notice that some triangular numbers are also squares, like 1 or 36. Our goal is to find all of such numbers: write $n^2 = \frac{1}{2}m(m+1)$, so that $8n^2 = 4m^2+4m$. Completing the square yields $8n^2 = (2m+1)^2-1$, which suggests substituting $x := 2m+1$ and $y := 2n$:

$$x^2 - 2y^2 = 1. \tag{12}$$

We are concerned with finding positive integer solutions: certainly $(3,2)$ is a solution; $(17,12)$ is another. Conversely, given $x$ and $y$, we may find $m, n$ by $m = \frac{1}{2}(x-1)$ and $n = \frac{y}{2}$, so in order to find all square-triangular numbers, it suffices to solve equation (12). For example, if $x = 17$ and $y = 12$, we get $m = 8$ and $n = 6$, which gives $36 = 6^2 = \frac{1}{2} \cdot 8 \cdot 9$. Hence, we state the following theorem.

**Theorem 68.2.** *Every positive integer solution to $x^2-2y^2 = 1$ is obtained by raising $3+2\sqrt{2}$ to powers; i.e., the solutions are exactly the $(x_k, y_k)$ given by $x_k + y_k\sqrt{2} := (3+2\sqrt{2})^k$.*

*Proof.* First, notice that $(3+2\sqrt{2})(3-2\sqrt{2}) = 9-8 = 1$, so $1^k = (3+2\sqrt{2})^k(3-2\sqrt{2})^k$, so write $x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k$. Then we can check that $x_k - y_k\sqrt{2} = (3-2\sqrt{2})^k$, so that $x_k^2 - 2y_k^2 = 1$.

Conversely, suppose $(u,v)$ is a positive integer solution to $x^2-2y^2 = 1$. Clearly, $u \neq 1, 2$. If $u = 3$, then $v = 2$, so $(u,v) = (x_1, y_1) = (3,2)$. Suppose $u \geq 4$; we will prove that there exist $s, t \in \mathbb{Z}^+$ with $s < u$ such that $s^2 - 2t^2 = 1$ and $u + v\sqrt{2} = (s+t\sqrt{2})(3+2\sqrt{2})$. By descent, we will eventually find $s = 3$, forcing $t = 2$, so that $u + v\sqrt{2}$ is a power of $3+2\sqrt{2}$. Hence, it is actually sufficient to show such $s, t$ exist.

If such $s, t$ existed, then $u + v\sqrt{2} = (3s+4t) + (3t+2s)\sqrt{2}$, so $s, t$ must satisfy the linear equations $3s + 4t = u$ and $2s + 3t = v$. Solving gives $s = 3u - 4v$ and $t = 3v - 2u$, so such numbers actually exist. Now, we check that $s < u$, $s^2 - 2t = 1$, and $s, t > 0$. First, since $u^2 - 2v^2 = 1$, we have

$$\begin{aligned} s^2 - 2t^2 = (3u-4v)^2 - 2(3v-2u)^2 + 9u^2 + 16v^2 - \cancel{24uv} - 18v^2 - 8u^2 + \cancel{24uv} \\ = 9(u^2-2v^2) - 8(u^2-2v^2) = 9 \cdot 1 - 8 \cdot 1 = 1. \end{aligned}$$

Next, we check $s, t > 0$, so that $u + 3s + 4t$ implies $s < u$. Since $s = 3u - 4v$, we claim $v < \frac{3}{4}u$. To see this, we recall $u^2 = 2v^2 + 1 > 2v^2$, so $\frac{1}{2}u^2 > v^2$, i.e, $\frac{\sqrt{2}}{2}u > v$. Since $\frac{\sqrt{2}}{2} < \frac{3}{4}$, we are done. Now, since $t = 3v - 2u$, we claim $u < \frac{3}{2}v$. For contradiction, suppose otherwise that $u \geq \frac{3}{2}v$. Then

$$u^2 - 2v^2 \geq \left(\frac{3}{2}v\right)^2 - 2v^2 = \frac{9}{4}v^2 - 2v^2 = \frac{1}{4}v^2.$$

Because we assumed $u \geq 4$, a simple manipulation with inequalities shows $v > 2$ and thus $\frac{1}{4}v^2 > 1$. But then $1 = u^2 - 2v^2 > 1$, a contradiction, so $u < \frac{3}{2}v$ and $t > 0$. By descent, we are done. □

From the above theorem, we know that $x_k \pm y_k\sqrt{2} = (3 \pm 2\sqrt{2})^k$, so that

$$x_k = \frac{1}{2}\left((3+2\sqrt{2})^k + (3-2\sqrt{2})^k\right) \overset{k\to\infty}{\longrightarrow} \frac{1}{2}\left(3+2\sqrt{2}\right)^k.$$

This fact shows that our solutions grow (roughly) exponentially, especially when we raise to higher powers. Similarly, we may verify $y_k \approx \frac{\sqrt{2}}{2}(3+2\sqrt{2})^k$, with the approximation becoming better when $k$ gets large. This allows us to quickly determine large values of $x_k$ and $y_k$.

**Example 68.3.** A calculator shows that $\frac{1}{2}(3+2\sqrt{2})^{10} \approx 22619536.999$. Since $x_{10} > \frac{1}{2}(3+2\sqrt{2})^{10}$, but only marginally so (i.e., it is larger by only $\frac{1}{2}(3-2\sqrt{2})^k$, which is a very small number), we can immediately "eyeball" $x_{10} = \boxed{22619537}$.

We also generalize the equation $x^2 - 2y^2 = 1$.

**Definition 68.4.** Let $D \in \mathbb{Z}^+$ be not a perfect square. The equation $x^2 - Dy^2 = 1$ is called a *Pell equation*.

Notice that if $(x_1, y_1)$ is a positive integer solution to $x^2 - Dy^2 = 1$, factoring over $\mathbb{Z}[\sqrt{D}]$ gives

$$1 = x_1^2 - Dy_1^2 = (x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}).$$

Taking $k$th powers yields $1 = (x_1 + y_1\sqrt{D})^k(x_1 - y_1\sqrt{D})^k$, and writing $x_k \pm y_k\sqrt{D} := (x_1 \pm y_1\sqrt{D})^k$ gives the solution $(x_k, y_k)$ to the Pell equation. However, are these all the solutions? And does the initial solution $(x_1, y_1)$, which we just supposed into existence, actually exist?

# 70 Pell's Equation (I)

We answer the questions we posed in the previous section. As to the types of solutions we get, the following theorem explains:

**Theorem 70.1.** *Consider the equation $x^2 - Dy^2 = 1$. If $(x_1, y_1)$ is the solution with the smallest $x$-coordinate (if it exists), then all the solutions $(x_k, y_k)$ of $x^2 - Dy^2 = 1$ are given by*

$$x_k + y_k\sqrt{D} := (x_1 + y_1\sqrt{D})^k.$$

*Proof.* The proof of this is basically the same as when $D = 2$ (that is, Theorem 68.2), but we replace the 2's with $D$'s. Again, it is easy to check that if $(x_1, y_1)$ is a solution to $x^2 - Dy^2 = 1$, then $(x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}) = x_1^2 - Dy_1^2 = 1$, so raising $(x_1 + y_1\sqrt{D})$ to powers does indeed give integer solutions $(x_k, y_k)$, where $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$.

Conversely, suppose $(u, v)$ is a positive integer solution to the equation $x^2 - Dy^2 = 1$. We copy the argument we gave above, which proceeds by descent. If $u = x_1$, then again there is nothing to do, so suppose $u > x_1$. We claim that there is a positive integer solution $(s, t)$ satisfying

$$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})(s + t\sqrt{D}) = (sx_1 + Dty_1) + (tx_1 + sy_1)\sqrt{D},$$

i.e., such solutions must satisfy the relations $u = sx_1 + Dty_1$ and $v = tx_1 + sy_1$. Indeed, we have

$$s = \frac{ux_1 - Dvy_1}{x_1^2 - Dy_1^2} = ux_1 - Dvy_1 \text{ and } t = \frac{vx_1 - uy_1}{x_1^2 - Dy_1^2} = vx_1 - uy_1,$$

and these are indeed solutions, as

$$\begin{aligned} s^2 - Dt^2 &= (ux_1 - Dvy_1)^2 - D(vx_1 - uy_1)^2 \\ &= u^2x_1^2 - \cancel{2Duvx_1y_1} + D^2v^2y_1^2 - Dv^2x_1^2 + \cancel{2Duvx_1y_1} - Du^2y_1^2 \\ &= x_1^2(u^2 - Dv^2) - y_1^2D(u^2 - Dv^2) \\ &= x_1^2 \cdot 1 - Dy_1^2 \cdot 1 = x_1^2 - Dy_1^2 = 1. \end{aligned}$$

Now, we need to check that $s, t$ are both positive, and that $s < u$, in order to complete the descent argument — eventually, if we continue this process, we will find a solution with a first-coordinate of $x_1$, from which we get the first power of $x_1 + y_1\sqrt{D}$.

That $s$ is positive is relatively easy to see, as we have $u^2 = 1 + Dv^2 > Dv^2$, so that $u > \sqrt{D}v$ by positivity of $u$ and $v$. Now $s = ux_1 - Dvy_1 > \sqrt{D}vx_1 - Dvy_1 = \sqrt{D}v(x_1 - y_1\sqrt{D})$. We recall that $(x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}) = 1 > 0$, and since $x_1 + y_1\sqrt{D}$ is positive, we see $x_1 - y_1\sqrt{D}$ is positive and thus $s > \sqrt{D}v(x_1 - y_1\sqrt{D}) > 0$ by positivity of $v$.

Finally, we check the positivity of $t$. We see that $t > 0$ if and only if $vx_1 > uy_1$, i.e., $u < \frac{x_1}{y_1}v$. Suppose for contradiction otherwise; i.e., that $u \geq \frac{x_1}{y_1}v$, so then

$$u^2 - Dv^2 \geq \left(\frac{x_1}{y_1}v\right)^2 - Dv^2 = \frac{x_1^2}{y_1^2}v^2 - Dv^2 = \frac{x_1^2 - \cancel{Dy_1^2}^{\,1}}{y_1^2}v^2 = \frac{v^2}{y_1^2}.$$

Because we assumed $u > x_1$ at the beginning of this argument, we observe $1 = u^2 - Dv^2 > x_1^2 - Dv^2$, so that $1 - x_1^2 > -Dv^2$ which implies $v^2 > (x_1^2 - 1)/D$. But now $x_1^2 - Dy_1^2 = 1$, so that $x_1^2 - 1 = Dy_2$, so we have indeed $v^2 > y_1^2$, so by positivity of $v$ and $y_1$, $v > y_1$, so that $1 = u^2 - Dv^2 \geq v^2/y_1^2 > 1$, which is a contradiction. Hence, we must have $u < \frac{x_1}{y_1}v$, i.e., $t$ is positive. From here, our descent is complete as $u = sx_1 + Dty_1 > sx_1 > s$ by positivity of $t$, so indeed $s < u$ as claimed. □

That is, supposing one solution exists, we know what the rest of the solutions look like. However, to guarentee that a smallest solution actually exists, we need a completely different idea. In general, the "size" of the smallest solution can be highly variable: $(3, 2)$ solves $x^2 - 2y^2 = 1$, yet $(1766319049, 226153980)$ is the smallest solution of $x^2 - 61y^2 = 1$. [This is reflecting something interesting in the arithmetic of the quadratic number field $\mathbb{Q}(\sqrt{61})$, and the bound on the smallest solution is related to the *class number* of $\mathbb{Q}(\sqrt{D})$ in general.]

Now, note that if $1 = x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D})$, then $(x - y\sqrt{D}) = (x + y\sqrt{D})^{-1}$. If $x, y > 0$ and are significantly large, then $x - y\sqrt{D} \to 0$. How *small*, exactly, can we make $x - y\sqrt{D}$? If so, then perhaps $x^2 - Dy^2 = 1$, which solves the problem of having the smallest solution actually exist.

A naïve idea to do this is to fix some $y \in \mathbb{Z}^+$, and round $y\sqrt{D}$ to a closest integer $x$. Then certainly $|x - y\sqrt{D}| \leq \frac{1}{2}$. Occasionally, $|x - y\sqrt{D}| \ll \frac{1}{2}$, and in these cases, we may observe $x^2 - Dy^2 =: M$ to be "decently small" (in terms of absolute value) — in fact, such $M$ is provably small, as follows.

**Theorem 70.2** (Dirichlet's Diophantine Approximation Theorem)**.** *Let $\alpha > 0$ be an irrational number. Then there are infinitely many pairs of integers $(x, y)$, with $x \geq 0$ and $y > 0$, such that $|x - y\alpha| < \frac{1}{y}$. Equivalently, $\left|\frac{x}{y} - \alpha\right| < \frac{1}{y^2}$, so $\alpha$ is "well-approximated" by $\frac{x}{y}$.*

*Proof.* Pick $Y \in \mathbb{Z}^+$, and partition the real interval $[0, 1)$ into $Y$ pieces of equal size:

$$[0, 1) = \left[0, \frac{1}{Y}\right) \cup \left[\frac{1}{Y}, \frac{2}{Y}\right) \cup \cdots \cup \left[\frac{Y-1}{Y}, 1\right).$$

Consider the first $Y + 1$ multiples of $\alpha$, including zero: $0\alpha, 1\alpha, 2\alpha, \ldots, (Y-1)\alpha, Y\alpha$, and write $n\alpha = N_n + F_n$, where $N_n = \lfloor n\alpha \rfloor$. Then clearly $F_n \in [0, 1)$, so by the pigeonhole principle, there exist $F_m, F_n$, with $m < n$, such that $F_m, F_n \in \left[\frac{k}{Y}, \frac{k+1}{Y}\right)$, i.e., $|F_m - F_n| < \frac{1}{Y}$. Now $F_m = m\alpha - N_m$ and $F_n = n\alpha - N_n$, so $|(N_n - N_m) - \alpha(n - m)| < \frac{1}{Y}$. Now, let

$x := N_n - N_m \geq 0$ and $y := n - m > 0$, so $|x - \alpha y| < \frac{1}{y} \leq \frac{1}{Y}$ (as $y \leq Y$), which finishes the proof — since $Y$ was arbitrary and the quantity $|x - \alpha y|$ is fixed with respect to $Y$, we an keep picking larger $Y$'s if necessary. □

Now, we are on our way to prove the existence of the solution to Pell's Equation.

# 74 Pell's Equation (II)

We assemble the tools from the previous section to prove the following.

**Theorem 74.1.** *Let $D$ be a positive integer that is not a square. Then $x^2 - Dy^2 = 1$ has a positive integer solution.*

*Proof.* Suppose $x, y$ are positive integers[4] satisfying $|x - y\sqrt{D}| < \frac{1}{y}$, by Theorem 70.2. Now

$$\left|x^2 - Dy^2\right| = \left|x + y\sqrt{D}\right| \left|x - y\sqrt{D}\right| < \left|x + y\sqrt{D}\right| \cdot \frac{1}{y}.$$

Since $\left|x - y\sqrt{D}\right| < \frac{1}{y}$, we have $x < \frac{1}{y} + y\sqrt{D}$, so that $\left|x + y\sqrt{D}\right| = x + y\sqrt{D} < \frac{1}{2} + 2y\sqrt{D}$. Obviously, $\frac{1}{y} < 1 < y\sqrt{D}$, so $x + y\sqrt{D} < 3y\sqrt{D}$, so $\left|x^2 - Dy^2\right| < 3y\sqrt{D} \cdot \frac{1}{y} = 3\sqrt{D}$. Since $x, y$ were arbitrary, Theorem 70.2 tells us that there are infinitely many pairs of positive integers $(x, y)$ with $|x - y\sqrt{D}| < \frac{1}{y}$, with each satisfying $x^2 - Dy^2 = M \in \mathbb{Z}$ for $|M| < 3\sqrt{D}$. The possible values of $M$ are thus $M = \pm 1, \pm 2, \ldots, \pm \left\lfloor 3\sqrt{D} \right\rfloor$; by the pigeonhole principle, there exists a choice of $M$ such that there exist infinitely many positive integer pairs $(x, y)$ with $|x - y\sqrt{D}| < \frac{1}{y}$ and thus $x^2 - Dy^2 = M$. Call these pairs $(x_1, y_1), (x_2, y_2), \ldots$, for brevity, assume[5] $M > 0$ and reduce each solution $(x_i, y_i)$ modulo $M$. By the pigeonhole principle again, there exist distinct solutions, without loss of generality call them $(x_1, y_1) \neq (x_2, y_2)$, with $x_1 \equiv x_2 \pmod{M}$ and $y_1 \equiv y_2 \pmod{M}$. Consider

$$x + y\sqrt{D} := \frac{x_1 - y_1\sqrt{D}}{x_2 - y_2\sqrt{D}} = \frac{x_1x_2 - Dy_1y_2 + (x_1y_2 - x_2y_1)\sqrt{D}}{M},$$

so that $x = \frac{1}{M}(x_1x_2 - Dy_1y_2)$ and $y = \frac{1}{M}(x_1y_2 - x_2y_1)$. We claim $x, y \in \mathbb{Z}$ and $x^2 - Dy^2 = 1$. For the latter, we have

$$x^2 - Dy^2 = \left(\frac{x_1x_2 - Dy_1y_2}{M}\right)^2 - D\left(\frac{x_1y_2 - x_2y_1}{M}\right)^2 = \frac{(x_1 - Dy_1)^2(x_2 - Dy_2)^2}{M^2} = \frac{M^2}{M^2} = 1.$$

Now, we just check $x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 \equiv 0 \pmod{M}$ and $x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{M}$, so both $x$ and $y$ are integers. Finally, since $x^2 - Dy^2 = 1$, simply replace $x$ with $-x$ and $y$ with $-y$ if necessary, so that $x, y \geq 0$. We must show that $x, y > 0$. Clearly, $x \geq 1$; for contradiction, assume $y = 0$. This implies $x_1y_2 = x_2y_1$ by definition of $y$, so consider

$$y_2^2M = y_2^2(x_1^2 - Dy_1^2) = x_1^2y_2^2 - Dy_1^2y_2^2 = x_2^2y_1^2 - Dy_1^2y_2^2 = y_1^2(x_2^2 - Dy_2^2) = y_1^2M.$$

This implies $y_1^2 = y_2^2$; by positivity we have $y_1 = y_2$, so that $x_1 = x_2$, contradicting distinctness of $(x_1, y_1)$ and $(x_2, y_2)$. Hence $y \neq 0$, which completes the proof. □

[4] Why can we suppose $x$ is positive here?

[5] The proof runs the same when $M < 0$.

# 78 Pell's Equation (III)

In this section, we give an alternate proof to Theorem 70.1, which we restate below:

**Theorem 70.1.** *If $(x_1, y_1)$ is the solution to $x^2 - Dy^2 = 1$ with the smallest $x$-coordinate, then all the solutions $(x_k, y_k)$ of $x^2 - Dy^2 = 1$ are given by $x_k + y_k\sqrt{D} := (x_1 + y_1\sqrt{D})^k$.*

*Proof.* Clearly, such $(x_k, y_k)$ are solutions, so conversely suppose $(u, v)$ is a positive integer solution to $x^2 - Dy^2 = 1$. Define $z := x_1 + y_1\sqrt{D} > 1$ and $r := u + v\sqrt{D} > 1$. By minimality of $z$, there exists a positive integer $k := \lfloor \log_z r \rfloor$ such that $z^k \leq r < z^{k+1}$. Hence $1 \leq rz^{-k} < z$. It suffices to show $rz^{-k} = 1$, so that $u + v\sqrt{D} = z^k = (x_1 + y_1\sqrt{D})^k$. Again, we may verify that $z^{-k} = x_k - y_k\sqrt{D}$, so

$$\begin{aligned} rz^{-k} = (u + v\sqrt{D})(x_k - y_k\sqrt{D}) &= (ux_k - vy_kD) + (vx_k - uy_k)\sqrt{D} \\ &=: s + t\sqrt{D}. \end{aligned}$$

Note that $s - t\sqrt{D} = (x_k + y_k\sqrt{D})(u - v\sqrt{D})$. Then $s^2 - Dt^2 = (x_k^2 - Dy_k^2)(u^2 - Dv^2) = 1 \cdot 1 = 1$, so $(s, t)$ is an integer solution to $x^2 - Dy^2 = 1$. Now, we have $1 \leq s + t\sqrt{D} < z$; we claim $s, t \geq 0$. Suppose for contradiction otherwise; we consider 3 cases. If $s, t < 0$, then $s + t\sqrt{D} < 0$, a contradiction. If $s \geq 0$ and $t < 0$, then observe $s - t\sqrt{D} > s + t\sqrt{D} \geq 1$, implying $s^2 - Dt^2 > 1$, a contradiction. Finally, if $s < 0$ and $t \geq 0$, then $-s + t\sqrt{D} > s + t\sqrt{D} \geq 1$. Then $(-s + t\sqrt{D})(s + t\sqrt{D}) = -s^2 + Dt^2 = -1$, a contradiction. Hence, we must have $s, t \geq 0$. We show that at least one of $s, t$ must be zero; from here, we are forced to have $t = 0$, which shows $1 = rz^{-k}$. Again, suppose for contradiction that $s, t > 0$. Since $(x_1, y_1)$ is the minimal solution to $x^2 - Dy^2 = 1$, we see $s \geq x_1$. From here, it is not hard to see $t^2 = \frac{s^2-1}{D} \geq \frac{x_1^2-1}{D} = y_1^2$, so $t > y_1$ by positivity. But now $s + t\sqrt{D} \geq x_1 = y_1\sqrt{D} = z$, but we know $s + t\sqrt{D} < z$, a contradiction. This completes the proof. □

# 80 Continued Fractions

We know that if $x \in \mathbb{R}$, then $x = n + u$, for some $n \in \mathbb{Z}$ and $u \in [0, 1)$. Now, suppose $x = n_1 + u_1$, taking $n_1 \in \mathbb{Z}$ and $u_1 \in [0, 1)$. If $u_1 = 0$, then $x \in \mathbb{Z}$. Otherwise, $\frac{1}{u_1} > 1$, so we may write $\frac{1}{u_1} = n_2 + u_2$, where $n_2 \in \mathbb{Z}^+$ and $u_2 \in [0, 1)$. If $u_2 = 0$, then $x = n_1 + \frac{1}{n_2}$; in general, we have $x = n_1 + \frac{1}{n_2+u_2}$. Continuing this inductively, if $u_2 > 0$, then write

$$x = n_1 + \frac{1}{n_2 + u_2} = n_1 + \cfrac{1}{n_2 + \cfrac{1}{n_3 + u_3}}, \text{ for some } n_3 \in \mathbb{Z}^+, u_3 \in [0, 1).$$

This process either terminates, or it continues indefinitely by setting $\frac{1}{u_k} = n_{k+1} + u_{k+1}$ for $n_{k+1} \in \mathbb{Z}^+$ and $u_{k+1} \in [0, 1)$. For a shorthand to the following inductive procedure, we define the following.

**Definition 80.1.** Let $a_0, a_1, \ldots, a_n \in \mathbb{R}$, where $a_i > 0$ for $i \geq 1$. We define the *finite simple continued fraction* by

$$[a_0; a_1, a_2, \ldots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

The numbers $a_0, a_1, \ldots, a_n$ are called the *partial quotients* of the continued fraction.

**Example 80.2.** Let us compute $[2; 1, 1, 2]$:

$$[2; 1, 1, 2] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3/2}} = 2 + \cfrac{1}{1 + \frac{2}{3}} = 2 + \frac{1}{5/3} = 2 + \frac{3}{5} = \boxed{\frac{13}{5}}.$$

Incidentally, notice that applying the Euclidean algorithm to 13 and 5 yields

$$\begin{aligned} 13 &= \mathbf{2} \cdot 5 + 3 \\ 5 &= \mathbf{1} \cdot 3 + 2 \\ 3 &= \mathbf{1} \cdot 2 + 1 \\ 2 &= \mathbf{2} \cdot 1 + 0. \end{aligned}$$

This is in fact not incidental.

**Example 80.3.** One can check that $\frac{85}{48} = [1; 1, 3, 2, 1, 3]$. We run the Euclidean algorithm on 85 and 48 to obtain

$$\begin{aligned} 85 &= \mathbf{1} \cdot 48 + 37 \\ 48 &= \mathbf{1} \cdot 37 + 11 \\ 37 &= \mathbf{3} \cdot 11 + 4 \\ 11 &= \mathbf{2} \cdot 4 + 3 \\ 4 &= \mathbf{1} \cdot 3 + 1 \\ 3 &= \mathbf{3} \cdot 1 + 0. \end{aligned}$$

To explain this, we try computing the continued fraction expansion as claimed:

$$\frac{85}{48} = \mathbf{1} + \frac{37}{48} = \mathbf{1} + \cfrac{1}{\mathbf{1} + \cfrac{11}{37}} = \mathbf{1} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{3} + \cfrac{4}{11}}} = \cdots = [1; 1, 3, 2, 1, 3].$$

Indeed, we notice that in computing the continued fraction expansion, we are really applying the Euclidean algorithm when we write a number as an integer part plus a fractional part. We now proceed to prove the general idea, but we introduce the following preliminaries first.

The first of these is an easy proposition:

**Proposition 80.4.** *If $m \geq 1$, then* $[a_0; a_1, a_2, \ldots, a_m] = a_0 + \cfrac{1}{[a_1; a_2, a_3, \ldots, a_m]}$.

This can be verified by expanding out what the continued fraction on the left actually means. Second, we need a new piece of notation:

**Definition 80.5.** If $a/b = [a_0; a_1, a_2, \ldots, a_m]$ is a rational number, then we define the *jth convergent* by

$$\frac{p_j}{q_j} := [a_0; a_1, a_2, \ldots, a_j].$$

**Example 80.6.** We saw that $\frac{13}{5} = [2; 1, 1, 2]$. The convergents are $[2] = 2$, $[2; 1] = 2 + \frac{1}{1} = 3$, $[2; 1, 1, ] = \frac{5}{2}$, and $[2; 1, 1, 2] = \frac{13}{5}$. Notice that $2 < 3 > \frac{5}{2} < \frac{13}{5}$. Similarly, the convergents of $\frac{85}{48}$ are

$$1 < 2 > \frac{7}{4} < \frac{16}{9} > \frac{23}{13} < \frac{85}{48}.$$

The fact that the convergents "alternate" between over- and under-estimates is true in general, and can be proven as an exercise.

We now state the main result.

**Theorem 80.7.** *Let $a, b \in \mathbb{Z}$ with $b \geq 1$. If the Euclidean algorithm for $a, b$ has length $n$ with partial quotients $q_0, q_1, \ldots, q_{n-1}$, then $a/b = [q_0; q_1, \ldots, q_{n-1}]$.*

*Proof.* Let $r_0 = 0$ and $r_1 = b$. We proceed by induction on the length of the Euclidean algorithm, $n$. For $n = 1$, then $b \mid a$, so $a = q_0 b + 0$, then $a/b = q_0 = [q_0]$. Now, assume the inductive hypothesis for some length-$n$ Euclidean algorithm. Let $a, b \in \mathbb{Z}$, $b \geq 1$ be chosen so that the Euclidean algorithm on $a, b$ has length exactly $n+1$. Writing $r_0 = a$ and $r_1 = b$, the algorithm starts $r_0 = q_0 r_1 + r_2$, $r_1 = q_1 r_2 + r_3$. Past this point, the Euclidean algorithm for $r_1, r_2$ has length $n$, so that $r_1/r_2 = [q_1; q_2, \ldots, q_n]$ by the inductive hypothesis. Now

$$\begin{aligned}
\frac{a}{b} = \frac{q_0 r_1 + r_2}{r_1} &= q_0 + \frac{r_2}{r_1} \\
&= q_0 + \frac{1}{r_1/r_2} \\
&= q_0 + \frac{1}{[q_1; q_2, \ldots, q_n]} \\
&= [q_0; q_1, q_2, \ldots, q_n],
\end{aligned}$$

where the last step follows from Proposition 80.4. This completes the induction. □

# 83 Infinite Continued Fractions

For an irrational number, some interesting things happen with the continued fraction expansions, as they do not terminate. For example, consider

$$\begin{aligned}
\pi &= [3; 7, 15, 1, 292, 1, 1, \ldots], \\
\sqrt[3]{2} &= [1; 3, 1, 5, 1, 1, 4, 1, 1, 8, \ldots], \\
\sqrt{2} &= [1; 2, 2, 2, 2, 2, 2, \ldots], \\
e &= [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].
\end{aligned}$$

Some of these have patterns, such as clearly the one for $\sqrt{2}$ — we say that it is *periodic* as it contains a repeating part. We will define periodicity more carefully later, but for the sake of notation, we write $x = [a_0; a_1, a_2 \ldots, a_k, \overline{b_1, b_2, \ldots, b_n}]$ to mean that the part under the overline repeats forever. Here are some example computations:

**Example 83.1.** Continued fraction expansions for rational numbers are not periodic, because they are terminating. For example, we may compute $\frac{312}{47} = 6 + \frac{30}{47}$, $\frac{47}{30} = 1 + \frac{17}{30}$, $\frac{30}{17} = 1 + \frac{13}{17}$, $\frac{17}{13} = 1 + \frac{4}{13}$, $\frac{13}{4} = 3 + \frac{1}{4}$, and $\frac{4}{1} = 4$. Hence $\frac{312}{47} = \boxed{[6; 1, 1, 1, 3, 4]}$.

**Example 83.2.** Let us find $[\overline{1; 2}]$. We first write $[\overline{1; 2}] = [1; 2, 1, 2, \ldots] = [1, 2, \overline{1; 2}]$, so

$$x := [\overline{1, 2}] = 1 + \frac{1}{2 + \frac{1}{[\overline{1, 2}]}} = 1 + \frac{1}{2 + \frac{1}{x}}, \text{ so solving gives}$$

$$\begin{aligned}
x - 1 = \frac{1}{2 + \frac{1}{x}} &\implies \frac{1}{x - 1} = 2 + \frac{1}{x} \\
&\implies \frac{1}{x - 1} = \frac{2x + 1}{x} \\
&\implies x = (2x + 1)(x - 1) \\
&\implies \cancel{x} = 2x^2 - 1 + \cancel{x} - 2x \\
&\implies 0 = 2x^2 - 2x - 1 \\
&\implies x = \frac{2 + \sqrt{2^2 - 4(2)(-1)}}{2(2)} = \boxed{\frac{1 + \sqrt{3}}{2}},
\end{aligned}$$

where we take the + sign in the quadratic formula because all of our quantities here are positive.

**Example 83.3.** Find the simple continued fraction expansion for $\sqrt{5}$.

*Solution.* First, we have $\lfloor \sqrt{5} \rfloor = 2$, so we write $\sqrt{5} = 2 + (\sqrt{5} - 2)$. Now $\frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2$, so that

$$\sqrt{5} = 2 + (\sqrt{5} - 2) = 2 + \frac{1}{\sqrt{5} + 2} = 2 + \frac{1}{4 + (\sqrt{5} - 2)},$$

but we already know that

$$\sqrt{5} - 2 = \frac{1}{4 + (\sqrt{5} - 2)},$$

so replacing this in the denominator gives

$$\sqrt{5} = 2 + \frac{1}{4 + (\sqrt{5} - 2)} = 2 + \frac{1}{4 + \frac{1}{4 + (\sqrt{5} - 2)}},$$

from which we see $\sqrt{5} - 2$ again, so continuing this *ad infinitum* gives $\sqrt{5} = \boxed{[2; \overline{4}]}$. •

**Example 83.4.** Find the continued fraction expansion of $\sqrt{3}$.

*Solution.* First, write $\sqrt{3} = 1 + (\sqrt{3} - 1)$. Now $\dfrac{1}{\sqrt{3}-1} = \dfrac{1+\sqrt{3}}{2}$, so

$$\sqrt{3} = 1 + \frac{1}{\left(\dfrac{1+\sqrt{3}}{2}\right)} = 1 + \frac{1}{1 + \dfrac{\sqrt{3}-1}{2}} = 1 + \frac{1}{1 + \dfrac{1}{2 + (\sqrt{3}-1)}},$$

from which we see $\sqrt{3} - 1$ again. Replacing this *ad infinitum* gives $\sqrt{3} = \boxed{[1; \overline{1, 2}]}$. •

# 84 Convergents of a Continued Fraction

In this section, we study the relationships among the convergents, given any continued fraction. Since continued fractions are inductive by nature, we might expect a recursive relationship between the convergents, which we actually do get — this is the main theorem we state below.

**Theorem 84.1.** *Let $p_n/q_n = [a_0; a_1, \ldots, a_n]$, where everything is a formal expression. Then the numerators $p_i$ are given by*

$$p_0 = a_0,\ p_1 = a_0a_1 + 1 \ \text{ and } p_n = a_np_{n-1} + p_{n-2} \text{ for } n \geq 2,$$

*and the denominators $q_i$ are given by*

$$q_0 = 1, q_1 = a_1, \ \text{ and } q_n = a_nq_{n-1} + q_{n-2} \text{ for } n \geq 2.$$

*Proof.* We proceed by induction on $k = 0, 1, \ldots, n$. First, we check $p_0/q_0 = [a_0] = a_0/1$ and $p_1/q_1 = [a_0; a_1] = (a_0a_1 + 1)/a_1$. Now, assume that the claim holds for all integers $j \leq k$, where $k \geq 0$. Then

$$\begin{aligned}
\frac{p_{n+1}}{q_{n+1}} = [a_0; a_1, a_2, \ldots, a_{n+1}] &= \left[a_0; a_1, a_2, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right] \\
&\overset{*}{=} \frac{\left(a_n + \frac{1}{a_{n+1}}\right)p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right)q_{n-1} + q_{n-2}} \\
&= \frac{a_np_{n-1} + \frac{p_{n-1}}{a_{n+1}} + p_{n-2}}{a_nq_{n-1} + \frac{q_{n-1}}{a_{n+1}} + q_{n-2}} \\
&= \frac{a_na_{n+1}p_{n-1} + p_{n-1} + a_{n+1}p_{n-2}}{a_na_{n+1}q_{n-1} + q_{n-1} + a_{n+1}q_{n-2}} \\
&= \frac{a_{n+1}(a_np_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_nq_{n-1} + q_{n-2}) + q_{n-1}} \\
\implies \frac{p_{n+1}}{q_{n+1}} &\overset{*}{=} \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}},
\end{aligned}$$

where the equalities marked with an asterisk $*$ signify the use of the inductive hypothesis. This completes the proof. □

Our second theorem allows us to compare convergents.

**Theorem 84.2.** *Let $p_0/q_0, p_1/q_1, \ldots$ be the convergents of the continued fraction $[a_0; a_1, a_2, \ldots]$. Then $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$ for all $n \in \mathbb{Z}^+$.*

*Proof.* We proceed by induction on $n$. When $n = 1$, we have $p_0q_1 - q_0p_1 = \cancel{a_0a_1} - 1(\cancel{a_0a_1} + 1) = -1 = (-1)^1$. Assume the inductive hypothesis holds for some $n \in \mathbb{Z}^+$, so we compute, by virtue of the previous theorem,

$$\begin{aligned} p_nq_{n+1} - p_{n+1}q_n &= p_n(a_{n+1}q_n + q_{n-1}) - (a_{n+1}p_n + p_{n-1})q_n \\ &= \cancel{a_{n+1}p_nq_n} + p_nq_{n-1} - \cancel{a_{n+1}p_nq_n} - p_{n-1}q_n \\ &= p_nq_{n-1} - p_{n-1}q_n \\ &= -(p_{n-1}q_n - p_nq_{n-1}) = -(-1)^n = (-1)^{n+1}, \end{aligned}$$

where the last line follows the inductive hypothesis. This completes the proof. □

There is an alternative view of Theorem 84.2 in terms of $2 \times 2$ matrices. Let

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; M_1 = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot M_0 = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and}$$

$$M_j = \begin{pmatrix} a_{j-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot M_{j-1} \text{ for } j \geq 2.$$

Then it turns out (if one is willing to work through the matrix multiplication) that

$$M_j = \begin{pmatrix} p_{j-1} & q_{j-1} \\ p_{j-2} & q_{j-2} \end{pmatrix}.$$

Taking determinants gives an alternate proof of Theorem 84.2.

# 88 Periodic Continued Fraction Expansions

In this section, we consider periodic continued fraction expansions more carefully.

**Example 88.1.** Let $b \in \mathbb{Z}^+$, and $B := [b; b, b, b, \ldots]$. Then $B = b + \frac{1}{B}$, so solving for $B$ yields $B^2 - bB - 1 = 0$, which we may solve using the quadratic formula:

$$B = \frac{b \pm \sqrt{b^2 - 4(1)(-1)}}{2(1)} = \frac{b \pm \sqrt{b^2+4}}{2}.$$

Since $B > 0$, we see $B = \dfrac{b + \sqrt{b^2+4}}{2}$.

**Example 88.2.** Let $a, b \in \mathbb{Z}^+$, and let $x := [a; b, b, b, b, \ldots]$. Then $x = a + \dfrac{1}{[b; b, b, \ldots]} = a + \dfrac{2}{b + \sqrt{b^2+4}}$, which we simplify:

$$\begin{aligned} x = a + \frac{2}{b+\sqrt{b^2+4}} &= \frac{ab + a\sqrt{b^2+4}+2}{b+\sqrt{b^2+4}} \\ &= \frac{(ab + a\sqrt{b^2+4}+2)(b-\sqrt{b^2-4}}{b^2-(b^2+4)} \\ &= \frac{ab^2 + \cancel{ab\sqrt{b^2+4}} + 2b - \cancel{ab\sqrt{b^2+4}} - a(b^2+4) - 2\sqrt{b^2+4}}{-4} \\ &= \frac{\cancel{ab^2} + 2b - \cancel{ab^2} - 4a - 2\sqrt{b^2+4}}{-4} \\ &= a - \frac{b}{2} + \frac{\sqrt{b^2+4}}{2}. \end{aligned}$$

Indeed, $[1;\bar{2}] = 1 - \frac{2}{2} + \frac{\sqrt{2^2+4}}{2} = \cancel{1} - \cancel{1} + \frac{\sqrt{8}}{2} = \sqrt{2}$, so this checks out.

Now, we give a formal definition of a periodic continued fraction.

**Definition 88.3.** A *periodic* continued fraction takes the form

$$[a_1; a_2, \ldots a_\ell, b_1, b_2, \ldots, b_m, b_1, b_2, \ldots, b_m, \ldots],$$

where the part $b_1, b_2, \ldots, b_m$ repeats indefinitely. We say that $a_1, a_2, \ldots, a_\ell$ is the *initial part* and $b_1, b_2, \ldots, b_m$ is the *periodic part*. The *period* is the minimum number $m$ such that we get a clear repeating pattern. If $\ell = 0$, we say that the fraction is *purely periodic*.

Our work in the first two examples of this section shows that we understand (roughly) periodic fractions of period 1. What about period 2?

**Example 88.4.** Let $b, c \in \mathbb{Z}^+$, and $x = [\overline{b, c}]$. Then

$$x = b + \frac{1}{[c, b, c, b, \ldots]} = b + \frac{1}{c + \frac{1}{[\overline{b, c}]}} = b + \frac{1}{c + \frac{1}{x}}.$$

Now, solving for $x$ yields $\cancel{x} = c(x-b)x + \cancel{x} - b$, which gives us a quadratic equation with the solution

$$x = \frac{bc + \sqrt{b^2c^2 - 4(c)(-b)}}{2c} = \frac{bc + \sqrt{b^2c^2 + 4bc}}{2c}.$$

Indeed, if $b = c$, then $x = \frac{b^2 + \sqrt{b^4 + 4b^2}}{2b} = \frac{b + \sqrt{b^2+4}}{2}$, so this checks out.

All of this, or course, generalizes inductively.

**Theorem 88.5.** *Let $\beta := [\overline{b_1, b_2, \ldots, b_m}]$, where $b_i \in \mathbb{Z}^+$. Then $\beta$ is a quadratic irrationality, i.e., it takes the form*

$$\beta = \frac{I + J\sqrt{D}}{K},$$

*where $I, J, K, D \in \mathbb{Z}$ with $D, K > 0$. Similarly, if $\alpha = [a_1, \ldots, a_\ell, \overline{b_1, \ldots, b_m}]$, then $\alpha$ is also a quadratic irrationality.*

*Proof.* The proof essentially proceeds inductively after writing

$$\beta = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{b_4 + \cfrac{1}{\ddots + \cfrac{1}{\beta}}}}}$$

and then simplifying to get an expression of the form

$$\beta = \frac{u\beta + v}{w\beta + z},$$

where $u, v, w, z$ are polynomial expressions in the $b_i$. As integers, clearly $u, v, w, z > 0$. Now, solving the above is a quadratic equation, from which the claim follows. The case for $\alpha$ is similar. □

We can also go the other way: the quadratic irrationalities are precisely the numbers with periodic continued fraction expansions. But this is a lot harder to prove.

**Theorem 88.6.** *Let $r, s, t, D \in \mathbb{Z}$ with $D, t > 0$ and $D$ not a perfect square. Then the continued fraction expansion of $\dfrac{r + s\sqrt{D}}{t}$ is periodic.*

*Proof.* Hard. □

# 94 Continued Fractions and Pell's Equation

As a continued fraction, we know that if $\frac{p}{q}$ is a convergent to $\sqrt{D}$ for some non-square $D$, then $\frac{p}{q} \approx \sqrt{D}$ and thus $\frac{p^2}{q^2} \approx D$. This idea is vague, but it is somewhat similar to the idea we used to solve Pell's equation. Hence, in this section, we give two theorems that explain this connection, but we will not prove them.

**Theorem 94.1.** *Let $D \in \mathbb{Z}^+$ be an integer that is not a square, and write*[6]

$$\sqrt{D} =: [a_1; \overline{b_1, \ldots, b_n}].$$

*Let $p/q := [a_1; b_1, \ldots, b_{n-1}]$. Then $(p, q)$ is the smallest positive integer solution to $x^2 - Dy^2 = (-1)^m$.*

Note that if $m$ is even, then we have a solution to Pell's equation $x^2 - Dy^2 = \pm 1$. Else, if $m$ is odd, consider

$$(p + q\sqrt{D})^2 = (p^2 + q^2 D) + 2pq\sqrt{D}$$

so that by the relation $p^2 - Dq^2 = (p + q\sqrt{D})(p - q\sqrt{D}) = -1$, we have

$$(p + q\sqrt{D})^2 (p - q\sqrt{D})^2 = (-1)^2 = 1.$$

In fact, this solution is also the smallest one to $x^2 - Dy^2 = +1s$, though, as we have mentioned, we will not prove this.

[6] That the initial part is only one term is not immediately obvious; see Exercise 48.9 in the text.

**Theorem 94.2.** *Fix notation as on the previous page. The smallest positive integer solution to* $x^2 - Dy^2 = 1$ *is*

$$\begin{cases} (p, q) & \text{if } m \text{ is even} \\ (p^2 + q^2 D, 2pq) & \text{if } m \text{ is odd.} \end{cases}$$

**Example 94.3.** Let $D = 2$. Then $\sqrt{2} = [1; \overline{2}]$, with a period of $m = 1$. Then $p/q = [1] = 1/1$, and we observe $1^2 - 2 \cdot 1^2 = -1$, exactly as the theorems predict. Hence $(1^2 + 1^2 \cdot 2, 2 \cdot 1 \cdot 1) = (3, 2)$ is the smallest solution to the Pell equation $x^2 - 2y^2 = 1$.

# 98 Perfect Numbers

Now, let us return back to the familiar domain of integers $\mathbb{Z}$. A lot of our work has been determining how divisors of a number relate to each other, especially from a multiplicative standpoint. However, now let us view things additively. We start with the following definition.

**Definition 98.1.** A positive integer is a *perfect number* if it is equal to the sum of its positive divisors.

This is fairly straightforward, so we view some examples.

**Example 98.2.** We claim that $6, 28$, and $496$ are perfect numbers. To see this, write

$$\begin{aligned} 6 &= \mathbf{1} + \mathbf{2} + 3 \\ 7 &= \mathbf{1} + \mathbf{2} + \mathbf{4} + 7 + 14 \\ 496 &= \mathbf{1} + \mathbf{2} + \mathbf{4} + \mathbf{8} + \mathbf{16} + 31 + 62 + 124 + 248. \end{aligned}$$

Pay attention to the factors of powers of 2 that occur. Indeed, we notice a pattern here, especially after taking out all the powers of two: $6 = 2 \cdot 3 = 2(2^2 - 1)$, $28 = 4 \cdot 7 = 2^2(2^3 - 1)$, and $496 = 16 \cdot 31 = 2^4(2^5 - 1)$. To illustrate this, the number 68 is not of this form, for $68 = 4 \cdot 17$. We can check that 68 is not a perfect number:

$$68 \neq 1 + 2 + 4 + 17 + 34 = 58.$$

Seemingly, we have a pattern on our hands, but it might be easier to define a function that is obviously helpful here.

**Definition 98.3.** Let $n \in \mathbb{Z}^+$. We define the *sum-of-divisors function* (or the *sigma function*) to be the sum of all positive divisors of $n$:

$$\sigma(n) := \sum_{d|n} d.$$

Then, it follows that $n$ is perfect if and only if $\sigma(n) = 2n$ (we must remember to count the non-proper divisor $n$). We also have some fun terms that we will never use: we say $n$ is *abundant* if $\sigma(n) > 2n$ and $n$ is *deficient* if $\sigma(n) < 2n$. The etymology of these terms should be clear.

Now, let us prove some results about the sigma function.

**Proposition 98.4.** *Let $p$ be a prime and $m, n$ be integers.*

1. *If $p^k$ is a prime power, then $\sigma(p^k) = \dfrac{p^{k+1}-1}{p-1}$.*
2. *If $\gcd(m,n) = 1$, then $\sigma(mn) = \sigma(m)\sigma(n)$. That is, $\sigma$ is multiplicative.*

*Proof.* (1) is trivial. For (2), note that the function $f(n) = n$ is obviously multiplicative. By a similar argument to Theorem 50.1, we can show that $\sigma$ is multiplicative — see Lemma 204.1 in Homework 4 for details. □

With this, we are ready to establish one of our conjectures as a theorem.

**Theorem 98.5** (Euclid's Perfect Number Formula)**.** *If $2^p - 1$ is prime, then $2^{p-1}(2^p-1)$ is a perfect number.*

*Proof.* The proof goes by direct verification. Since $2^p-1$ is prime, the divisors of $2^{p-1}(2^p-1)$ are

$$1, 2, 4, \ldots, 2^{p-1}, (2^p-1), 2(2^p-1), 4(2^p-1), \ldots, 2^{p-1}(2^p-1).$$

Now, just add everything up:

$$\begin{aligned}\sigma(2^{p-1}(2^p-1)) &= \sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-1} 2^k(2^p-1) \\ &= (2^p - \cancel{1} + \cancel{1})\sum_{k=0}^{p-1} 2^k \\ &= 2^p(2^p-1),\end{aligned}$$

which completes the proof. □

Now, we discuss even perfect numbers in general. To do this, we note the following proposition:

**Proposition 98.6.** *If $a^n - 1$ is prime for integers $a, n \geq 2$, then $a = 2$ and $n$ is prime.*

*Proof.* Exercise. □

Primes of the form $2^p - 1$ have a special name.

**Definition 98.7.** A prime of the form $2^p - 1$ is called a *Mersenne prime*.

Using this, we prove the following.

**Theorem 98.8** (Euler's Perfect Number Theorem)**.** *Suppose $n \in \mathbb{Z}^+$ is an even perfect number. Then $n = 2^{p-1}(2^p-1)$, where $2^p - 1$ is a Mersenne prime.*

That is to say, after proving this theorem, we will have established that even perfect numbers are exactly the numbers of the form $2^{p-1}(2^p-1)$, where $2^p - 1$ is prime.

*Proof.* Suppose $n$ is an even perfect number, and write $n = 2^k m$ where $k \geq 1$ and $m$ is odd. Then $\sigma(n) = 2n = 2 \cdot 2^k m = 2^{k+1}m$, and since $\gcd(2, m) = 1$, write

$$\sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^k - 1)\sigma(m),$$

implying $2^{k+1}m = (2^k-1)\sigma(m)$. Since $2^k - 1$ is odd, we are forced to have $2^{k+1} \mid \sigma(m)$, so write $\sigma(m) = 2^{k+1}c$ for some $c \in \mathbb{Z}$. Cancelling $2^{k+1}$'s, we have $m = (2^{k+1}-1)c$ and $\sigma(m) = 2^{k+1}c$.

We claim that $c = 1$, so suppose for contradiction $c \geq 2$. Then $1, c, m = (2^{k+1} - 1)c$ are all divisors of $m$, so now $\sigma(m) \geq 1 + c + (2^{k+1} - 1)c = 1 + 2^{k+1}c = 1 + \sigma(m)$, implying $0 \geq 1$, a contradiction. Hence $c = 1$, so it follows that $m = 2^{k+1} - 1$ and $\sigma(m) = 2^{k+1} = m + 1$. But this is only possible if $m$ is prime, so $n = 2^k(2^{k+1} - 1)$ where $2^{k+1}$ is a Mersenne prime. $\square$

Notice that we have only proved a result about even perfect numbers; what about odd ones? For odd perfect numbers, no one knows if they even exist yet — we are still unable to find examples of them. There *probably* are not any odd perfect numbers, but no one has proven this for certain yet.

# 100 Carmichael Numbers

Recall that Fermat's Little Theorem tells us that $a^p \equiv a \pmod{p}$ for any prime $p$. Hence, if given a number $n$, it may be easy to check that $n$ is not a prime if we find $a^n \not\equiv a \pmod{n}$. Thus, we make the following definition:

**Definition 100.1.** If $n \in \mathbb{Z}^+$ and $a^n \not\equiv a \pmod{n}$, then we say $a$ is a *witness* for $n$.

It follows that if $n$ has at least one witness, then $n$ is not prime.

**Example 100.2.** We check $2^6 \equiv 4 \not\equiv 2 \pmod{6}$, so 2 is a witness for 6. Hence, we have proven that 6 is not prime.

The natural question is: do witnesses always exist? Compiling some data, it is not hard to see that there are usually "a lot" of witnesses if $n$ is not prime:

| Non-prime $n$ | $287 = 7 \cdot 41$ | $314 = 2 \cdot 157$ | $190 = 2 \cdot 5 \cdot 19$ |
|---|---|---|---|
| Number of Witnesses | 278 | 310 | 150 |
| Witness Rate | 96.9% | 98.7% | 78.9% |

However, this is not always the case — some composite numbers have no witnesses at all.

**Definition 100.3.** A *Carmichael number* $n \in \mathbb{Z}^+$ is a composite number such that $a^n \equiv a \pmod{n}$ for every integer $a$.

**Example 100.4.** Let $n = 561 = 51 \cdot 11 = 3 \cdot 11 \cdot 17$. We claim that 561 is a Carmichael number, i.e., $a^{561} \equiv a \pmod{561}$ for all $a \in \mathbb{Z}$, i.e., $561 \mid a^{561} - a$. To show this (without directly computing 561 modulo problems), we just check that $3, 11, 17 \mid a^{561} - a$. But now this is routine: if $3 \mid a$, then $a^{561} \equiv 0 \equiv a \pmod{3}$, and if $3 \nmid a$, then $a^2 \equiv 1 \pmod{3}$, so $a^{561} = a^{2 \cdot 280 + 1} \equiv a \pmod{3}$. Doing similar arguments for 11 and 17, we will have proved our claim.

Notice that 561 is a product of distinct odd primes; this is in fact true of Carmichael numbers in general. Furthermore, for each prime $p \mid 561$, we have $561 \equiv 1 \pmod{p - 1}$ (or, $p - 1 \mid 560$), which is what causes our calculations to fall through. We now prove these things in general.

**Theorem 100.5** (Korselt's Criterion)**.** *Let $n \in \mathbb{Z}^+$ be a composite number. Then $n$ is a Carmichael number if and only if $n$ is an odd number such that every prime $p \mid n$ satisfies $p^2 \nmid n$ and $(p - 1) \mid (n - 1)$.*

It follows that it is easy to check whether a number is a Carmichael number if we are given its factorization, but this is hard in general.

**Example 100.6.** Let $n = 1105 = 5 \cdot 13 \cdot 17$. Certainly, 1105 is odd and squarefree, and it is routine to check $1105 - 1 = 1104 = 16 \cdot 69 = 2^4 \cdot 3 \cdot 23$, so $4, 12, 16 \mid 1104$. Hence, by Korselt's Criterion, 1105 is a Carmichael number.

Similarly, let $n = 2465 = 5 \cdot 17 \cdot 29$. Then 2465 is odd and squarefree, and $2465 - 1 = 2464 = 32 \cdot 77 = 2^5 \cdot 7 \cdot 11$, and certainly $4, 16, 28 \mid 2464$. Hence, 2465 is a Carmichael number by Korselt's Criterion.

We now prove Korselt's Criterion.

*Proof of Theorem 100.5.* First, we establish that every Carmichael number is odd. Suppose that $n \geq 3$ is even, and let $a = n - 1$. Then $a^n \equiv (-1)^n \equiv 1 \pmod{n}$ because $n$ is even, so $n$ has a witness. It thus follows that all Carmichael numbers are odd.

Next, we show that every Carmichael number is squarefree. Suppose $p^2 \mid n$, for some prime $p$. If (for contradiction) $p^n \equiv p \pmod{n}$, then $n \mid p^n - p = p(p^{n-1} - 1)$, but now $p^2 \mid n \mid p(p^{n-1} - 1)$, but this is impossible as $p^{n-1} - 1$ is not a multiple of $p$. This implies that $p^n \not\equiv p \pmod{n}$, so $p$ is a witness for $n$.

Finally, suppose $n = p_1 p_2 \cdots p_r$, where the $p_i$ are distinct odd primes. To finish the proof, it suffices to check that $n$ is a Carmichael number if and only if $p_i - 1 \mid n - 1$ for each $i \leq r$. If $n$ is a Carmichael number, then by definition $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$, if and only if $a^n \equiv a \pmod{p_i}$ for all $i \leq r$, splitting the congruence into prime factors. If $p_i \mid a$, then $a^n \equiv 0 \equiv a \pmod{p_i}$, and if $p_i \nmid a$, then Fermat's Little Theorem implies $a^{p_i - 1} \equiv 1 \pmod{p_i}$. Apply the division algorithm to write $n = q(p_i - 1) + r$ where $0 \leq r < p_i - 1$, so $a \equiv a^n = a^{q(p_i-1)} a^r \equiv a^r \pmod{p_i}$. Now, the congruence above holds for all integers $a$, so in particular, pick $a$ to be be a primitive root modulo $p_i$. By size, this forces $r = 1$ as $|a|_{p_i} = p_i - 1$, so $n = q(p_i - 1) + 1$, which proves the claim since $i$ was arbitrary.

Conversely, let $n = p_1 p_2 \cdots p_r$ be odd and squarefree, where $p_i - 1 \mid n - 1$ for all $i \leq r$. We show that $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. Now, it suffices to show $a^n \equiv a \pmod{p_i}$, but this is routine: if $p_i \mid a$, then the result follows immediately, and if $p_i \nmid a$, we know $a^{p_i - 1} \equiv 1 \pmod{p_i}$. Now $p_i - 1 \mid n - 1$, so that $a^{n-1} \equiv 1 \pmod{p_i}$, so that $a^n = a^{n-1} a \equiv 1 \cdot a = a \pmod{p_i}$. This proves the claim. □

We might ask are there infinitely many Carmichael numbers? The answer is affirmative, though the proof is difficult and uses quite a bit of analytic number theory:

**Theorem 100.7** (Alford, Granville, Pomerance 1994)**.** *There are infinitely many Carmichael numbers.*

Of course, we can verify the following easier statement, by direct computation, which seems like a way we can generate infinitely Carmichael numbers, but then we need to see if there are infinitely many $k$ such that $6k + 1, 12k + 1, 18k + 1$ are all prime — this is hard.

**Proposition 100.8.** *Suppose $k \in \mathbb{Z}^+$ such that $6k + 1$, $12k + 1$, and $18k + 1$ are all prime. Then $n := (6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number.*

# 104 The Rabin-Miller Primality Test

Carmichael numbers exclude Fermat's Little Theorem for being a possible *primality test*, or a method to see if a number if prime. Hence, it would seem like we are stuck with trial division: given a number $n$, check all the primes $p \leq \sqrt{n}$ to see if they divide $n$; if no such primes divide $n$, then $n$ is prime. Clearly, this works with 100% accuracy, but it is very slow: its time complexity is $O(\sqrt{n})$, which is fairly large.

Hence, we present a new primality test which may be faster, based on the idea of Fermat's Little Theorem. Pick a positive integer $k$, and repeat the following steps $k$ times:

1. Choose some random integer $a \in [2, n-2]$.
2. Compute $a^n \bmod n$. If $a^n \equiv a \pmod{n}$, then $n$ is not prime.
3. If not, continue.

If $a^n \equiv a \pmod{n}$ for every one of these random $k$'s, then $n$ is *probably* prime. This algorithm is fast, as computing $a^n \bmod n$ using successive squaring is fast, but the problem is that this has a chance of failing due to Carmichael numbers. Additionally, with our random choices of $a$, we could have missed all of the witnesses and returned a false positive: what is the probably that we miss all of a number's witnesses, given that $n$ is not a Carmichael number? The Rabin-Miller test is a test that gives answers to these questions, and is based on the following fact:

**Proposition 104.1.** *Let $p$ be an odd prime and write $p - 1 = 2^k q$, where $q$ is odd. Pick $a \in \mathbb{Z}$ with $p \nmid a$. Then one of the following two conditions holds:*

1. *We have $a^q \equiv 1 \pmod{p}$.*
2. *We have that one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^k q}$ is congruent to $-1$ modulo $p$.*

*Proof.* By Fermat's Little Theorem, $a^{2^k q} = a^{p-1} \equiv 1 \pmod{p}$. Now, every integer in the list $a^q, a^{2q}, \ldots, a^{2^k q}$ is the square of the previous integer, considered modulo $p$. We know $a^{2^k} q \equiv 1 \pmod{p}$, so either all entries are 1 modulo $p$, giving us condition (1), or not, forcing one of the integers $a^{2^i} q$, to be congruent to $-1$ modulo $p$, as $-1$ is the unique element of multiplicative order 2 modulo $p$. This gives condition (2). □

Now, we describe the test.

**Corollary 104.2** (Rabin-Miller Primality Test)**.** *Let $n$ be an odd positive integer and write $n - 1 = 2^k q$, where $q$ is odd. Let $a \in \mathbb{Z}$ with $n \nmid a$. If $a^q \not\equiv 1 \pmod{n}$ and $a^{2^i q} \not\equiv -1 \pmod{n}$ for any $i \in \{0, 1, 2, \ldots, k-1\}$, then $n$ is not prime.*

*Proof.* This is merely the contrapositive of Proposition 104.1. □

The test is just about finding the $a$ such that the two conditions in the above corollary are satisfied. For bookkeeping, we make the following definition:

**Definition 104.3.** Let $n \in \mathbb{Z}^+$ be odd. If $a \in \mathbb{Z}$ satisfies the two conditions of compositeness in Corollary 104.2, then $a$ is a *Rabin-Miller witness* for the compositeness of $n$.

Hence, the test proceeds again as follows. Pick a positive integer $m$, and repeat the following steps $m$ times:

1. Choose a random integer $a \in [2, n-2]$.
2. Compute $a^q, a^{2q}, \ldots, a^{2^k q} \pmod{n}$. If $a$ is a Rabin-Miller witness, then $n$ is not prime.
3. If not, continue.

This seems like it suffers from the same issues, but we have the following theorem which guarantees success — assuming we do enough trials.

**Theorem 104.4.** *If $n$ is an odd composite number, then at least $\frac{3}{4}$ of $a \in \{1, 2, \ldots, n-1\}$ are Rabin-Miller witnesses for $n$.*

*Proof.* See these notes,[7] Section 5. □

Now, some basic probability shows that given $m$ trials and a composite number $n$, the probability that we did not find a witness for $n$ in $m$ trials is at most $\left(\frac{1}{4}\right)^m$ (binomial distribution). Hence, if we end up never finding a witness for some given $n$, it is *very, very* likely that $n$ is prime. Though this is not as satisfying as a test that definitively states whether a number is prime or not, it is "good enough" and it is *fast* — successive squaring is $O(\log n)$, which is much faster than the $O(\sqrt{n})$ time complexity we had by trial division.

In fact, we can streamline our testing. What if we check $a = 2, 3, 4, \ldots$, until we hit a witness? At worst, we check $a = \frac{n}{4} + 1$, from which Theorem 104.4 tells us that $n$ is *definitively* prime. But we have the following theorem:

**Theorem 104.5.** *If some Extended Riemann Hypothesis holds, then every composite odd $n$ has a Rabin-Miller witness $a$, with $a \leq 2 \cdot (\ln n)^2$.*

Unfortunately, this theorem hinges on something that is not proven yet, but the Extended Riemann Hypothesis is probably(?) true, and most mathematicians (generally?) believe it to be true. This sort of statement is fairly common in analytic number theory. Hence, Rabin-Miller is probabilistic, for now, here is a theorem that gives a deterministic test:

**Theorem 104.6** (Agrawal–Kayal–Saxena, 2002)**.** *For every $\varepsilon > 0$, there exists an algorithm that conclusively determines whether a positive integer $n$ is prime in no more than $O((\ln n)^{6+\varepsilon})$ steps.*

If we believe the theorem, then the *AKS test* works (i.e., it is deterministic). Unfortunately, it is much slower than the Rabin-Miller test, so it is usually not practical. A primality test that is both deterministic and fast is still open.

[7] That is, `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf`.

# Homework Exercises

What follows are my attempted problem set solutions this quarter. I believe most of these were graded on completion, so there is no guarentee of accuracy here. Also, I have omitted some exercises out of taste, and have revised some for clarity.

## 201 Homework 1: Quadratic Reciprocity

**Silverman 20.3: Cubic Residues**

A number[8] $a \not\equiv 0 \pmod{p}$ is called a *cubic residue modulo* $p$ if it is congruent to a cube modulo $p$; that is, if there is a number $b$ such that $a \equiv b^3 \pmod{p}$.

Parts (a) and (b) are omitted.

(c) If $p \equiv 2 \pmod{3}$, make a conjecture as to which $a$'s are cubic residues. Prove that your conjecture is correct.

We claim that if $p \equiv 2 \pmod{3}$, then *every* $a$ with $p \nmid a$ is a cubic residue.

*Proof.* Suppose $p \equiv 2 \pmod{3}$. It suffices to show that the mapping $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ by $x \mapsto x^3$ is bijective, where $\mathbb{Z}/p\mathbb{Z}$ is the set of residue classes modulo $p$. Since $\mathbb{Z}/p\mathbb{Z}$ is a finite set, we show that $f$ is injective. Suppose $a^3 \equiv b^3 \pmod{p}$. Notice that the congruence $x^3 \equiv 0 \pmod{p}$ has exactly one solution, namely $x \equiv 0 \pmod{p}$, so whenever $a^3 \equiv b^3 \equiv 0$, we have $a \equiv b \equiv 0$.

Hence, suppose $a \not\equiv 0$ and $b \not\equiv 0$, so that $a^3 \equiv b^3 \not\equiv 0 \pmod{p}$. In this case, we have $\gcd(p, b) = 1$, so we may find some $c$ such that $bc \equiv 1 \pmod{p}$. Thus $a^3 \equiv b^3 \implies a^3c^3 = (ac)^3 \equiv 1 \pmod{p}$, which suggests the substitution $x := ac$, so we obtain $x^3 \equiv 1 \pmod{p}$. From here, it suffices to show $x \equiv 1 \pmod{p}$, from which it follows $a \equiv b$. We factor

$$x^3 \equiv 1 \iff x^3 - 1 \equiv 0 \iff (x-1)(x^2 + x + 1) \equiv 0 \pmod{p}.$$

Now, $x \equiv 1$ is clearly a root of this polynomial. When $p = 2$, the polynomial congruence $x^2 + x + 1 \equiv 0$ has the solution $x \equiv 1$ as well, which can be easily verified. Hence, suppose $p \neq 2$. Then 2 has an inverse modulo $p$, which we denote by the symbol "1/2," and 4 has the inverse 1/4, so we may write

$$x^2 + x + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} \equiv 0 \pmod{p},$$

where the formal symbol 3/4 means $3 \cdot 4^{-1} \pmod{p}$. Hence, if $x^2 + x + 1$ has any roots modulo $p$, they must satisfy

$$\left(x + \frac{1}{2}\right)^2 \equiv -\frac{3}{4} \iff (2x+1)^2 \equiv -3,$$

i.e., $-3$ is a quadratic residue modulo $p$. However, $p \equiv 2 \pmod{3}$, so we claim that $-3$ is not a quadratic residue modulo $p$. Write $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. If $\left(\frac{-1}{p}\right) = 1$, then quadratic

[8] The condition $a \not\equiv 0$ is not given in the original text, but kept here to keep consistency with quadratic residues.

reciprocity tells us $p \equiv 1 \pmod 4$, so that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$, as $p \equiv 2 \pmod 3$. Similarly, if $\left(\frac{-1}{p}\right) = -1$, then quadratic reciprocity gives $p \equiv 3 \pmod 4$, so $\left(\frac{3}{p}\right) \equiv -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = +1$. Hence, $x^2 + x + 1 \equiv 0 \pmod p$ has no roots, so that the only solution to $x^3 \equiv 1 \pmod p$ is $x \equiv 1$. This proves that $f$ is bijective. □

**Silverman 22.6: Jacobi Symbols**

In this exercise, we prove two parts of the Generalized Law of Quadratic Reciprocity. Let $\left(\frac{a}{b}\right)$ denote the *Jacobi symbol* of $a$ modulo $b$, where $b$ is odd.

(a) Prove that $\left(\frac{2}{b}\right) = 1$ whenever $b \equiv 1, 7 \pmod 8$ and $\left(\frac{2}{b}\right) = -1$ otherwise.

*Proof.* If $b = 1$, there is nothing to do. Hence, suppose $b = p_1 p_2 \cdots p_k$ for primes $p_i$, so we prove by induction on the number of primes $k$. When $k = 1$, this is the regular law of quadratic reciprocity, so assume the claim holds for some $k \geq 1$. Let $b = p_1 p_2 \cdots p_k q =: mq$, where $q$ is prime. By the Jacobi symbol multiplication law, we have $\left(\frac{2}{b}\right) = \left(\frac{2}{m}\right)\left(\frac{2}{q}\right)$. Now, we consider cases.

*Case I*: $b \equiv 1 \pmod 8$. In this case, we can have $(m, q) \equiv (1,1), (3,3), (5,5), (7,7) \pmod 8$. In each of these subcases, the induction hypothesis and the law of quadratic reciprocity makes it a straightforward verification to show $\left(\frac{2}{m}\right) = \left(\frac{2}{q}\right)$, so that $\left(\frac{2}{b}\right) = 1$.

*Case II*: $b \equiv 3 \pmod 8$. In this case, we can have $(m, q) \equiv (1,3), (3,1), (5,7), (7,5) \pmod 8$. In each of these subcases, observe that $\left(\frac{2}{m}\right) = -\left(\frac{2}{q}\right)$, so that $\left(\frac{2}{b}\right) = -1$.

*Case III*: $b \equiv 5 \pmod 8$. In this case, we can have $(m, q) \equiv (1,5), (3,7), (5,1), (7,3) \pmod 8$. Again, observe $\left(\frac{2}{m}\right) = -\left(\frac{2}{q}\right)$, so $\left(\frac{2}{b}\right) = -1$.

*Case IV*: $b \equiv 7 \pmod 8$. In this case, we can have $(m, q) \equiv (1,7), (3,5), (5,3), (7,1) \pmod 8$. Hence $\left(\frac{2}{m}\right) = \left(\frac{2}{q}\right)$, so $\left(\frac{2}{b}\right) = 1$.

Thus, by induction and casework, we have established the claim. □

(b) Let $a, b$ be odd numbers. Prove that $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ if $a$ or $b$ is congruent to 1 modulo 4, and $\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ if $a \equiv b \equiv 3 \pmod 4$.

*Proof.* Notice that if $\gcd(a, b) > 1$, it is easy to show $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = -\left(\frac{b}{a}\right) = 0$ (let $p$ be a prime dividing both $a$ and $b$, so that the expansion of both $\left(\frac{a}{b}\right)$ and $\left(\frac{b}{a}\right)$ ends up having a zero), so we suppose $\gcd(a, b) = 1$. In this case, set $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_\ell$, where $p_i \neq q_j$ for all $i \leq k$ and $j \leq \ell$. Now by expanding out and using the Jacobi symbol multiplication law, we see

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k} \prod_{j=1}^{\ell} \left(\frac{p_i}{q_j}\right),$$

which is helpful as the symbols in the product are Legendre symbols, which we know how to manipulate. By quadratic reciprocity, we make the replacement

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k} \prod_{j=1}^{\ell} \left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{k} \prod_{j=1}^{\ell} \left[\left(\frac{q_j}{p_i}\right)(-1)^{\frac{(p_i-1)(q_j-1)}{4}}\right] = \prod_{i=1}^{k} \prod_{j=1}^{\ell} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} \cdot \left(\frac{b}{a}\right)$$

$$\implies \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{(p_i-1)(q_j-1)}{4}},$$

so it suffices to prove $\prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{1}{4}(p_i-1)(q_j-1)} = (-1)^{\frac{1}{4}(a-1)(b-1)}$. Now, note for any $p, q$ primes, we have by Euler's Criterion

$$(-1)^{\frac{1}{4}(p-1)(q-1)} = \left((-1)^{\frac{1}{2}(p-1)}\right)^{\frac{1}{2}(q-1)} = \left(\frac{-1}{p}\right)^{\frac{1}{2}(q-1)}.$$

Substituting this and noting $a = p_1 p_2 \cdots p_k$, we obtain

$$\prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{\frac{1}{4}(p_i-1)(q_j-1)} = \prod_{j=1}^{\ell}\left(\frac{-1}{a}\right)^{\frac{1}{2}(q-1)} =: A.$$

Finally, if $a \equiv 1 \pmod 4$, then $\left(\frac{-1}{a}\right) = 1$ so $A = 1 = (-1)^{\frac{1}{4}(a-1)(b-1)}$. In the case $a \equiv 3 \pmod 4$, then Euler's Criterion gives

$$A = \prod_{j=1}^{\ell}(-1)^{(q_j-1)/2} = \prod_{j=1}^{\ell}\left(\frac{-1}{q_j}\right) = \left(\frac{-1}{b}\right) = (-1)^{(b-1)/2},$$

which can be easily verified, so we are done. □

**Silverman 23.4: The Second Supplement to Quadratic Reciprocity**

Let $p$ be an odd prime, $P = \frac{1}{2}(p-1)$, and $a$ be an even integer not divisible by $p$.

(a) Show that $\displaystyle\sum_{k=1}^{P}\left\lfloor\frac{ka}{p}\right\rfloor \equiv \frac{1}{8}(p^2-1) + \mu(a,p) \pmod 2$.

*Proof.* For $1 \le k \le P$, write $ka = q_k p + r_k$ for $-P < r_k < P$. Thus $\frac{ka}{p} = q_k + \frac{r_k}{p}$, so that

$$\left\lfloor\frac{ka}{p}\right\rfloor = \begin{cases} q_k & r_k > 0 \\ q_k - 1 & r_k < 0. \end{cases}$$

Thus, it follows that

$$\sum_{k=1}^{P}\left\lfloor\frac{ka}{p}\right\rfloor = \sum_{k=1}^{P} q_k - \mu(a,p)$$

$$\implies \sum_{k=1}^{P}\left\lfloor\frac{ka}{p}\right\rfloor \equiv \sum_{k=1}^{P} q_k + \mu(a,p) \pmod 2,$$

so it suffices to show $q_1 + q_2 + \cdots + q_P \equiv \frac{1}{8}(p^2-1) \pmod 2$. Now, we know because $a$ is even and $p$ is odd, we have $0 \equiv q_k + r_k \iff r_k \equiv q_k \pmod 2$. But a lemma we established in lecture shows that the $r_i$ are exactly the numbers $\pm 1, \pm 2, \ldots, \pm P$ in some order, with

one choice of sign per number. Because we work modulo 2, we may disregard the signs and write

$$q_1 + \cdots + q_P \equiv r_1 + \cdots + r_P \equiv 1 + \cdots + P = \frac{P(P+1)}{2} = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} = \frac{p^2-1}{8},$$

which completes the proof. □

(b) Take $a = 2$ and use (a) and Gauss' Criterion to show $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$.

*Proof.* From part (a), we have

$$\sum_{k=1}^{P} \left\lfloor \frac{2k}{p} \right\rfloor \equiv \frac{1}{8}(p^2-1) + \mu(2,p) \pmod 2.$$

However, notice for all $1 \leq k \leq P$, we have

$$\frac{2k}{p} \leq \frac{2P}{p} = \frac{2(p-1)}{2p} = \frac{p-1}{p} < 1,$$

so the sum on the left completely vanishes. Hence $\frac{1}{8}(p^2-1) \equiv \mu(2,p) \pmod 2$ (signs are irrelevant in characteristic 2), so by Gauss' Criterion, we have

$$\left(\frac{2}{p}\right) = (-1)^{\mu(2,p)} = (-1)^{\frac{1}{8}(p^2-1)},$$

exactly as claimed. □

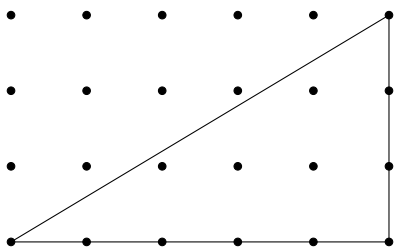
**Silverman 23.5: They Did Counting on a Triangle**

Let $a, b \in \mathbb{Z}^+$ and let $T$ be the triangle whose vertices are $(0,0)$, $(a,0)$ and $(a,b)$. Consider the following three quantities:

$$\begin{aligned} A &= \text{area of } T, \\ N &= \text{number of integer points strictly inside } T, \\ B &= \text{number of integer points on the edges of } T. \end{aligned}$$

(a) Draw a picture for the case $a = 5$ and $b = 3$, and use it to compute $A, N, B$, and $A - N - \frac{1}{2}B$.

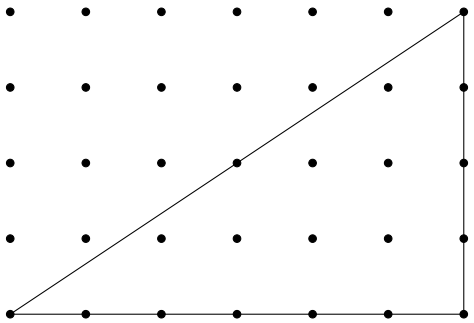
*Solution.* In this case, $T$ is the triangle with vertices $(0,0)$, $(5,0)$, and $(5,3)$, which we can sketch below.



The area of the triangle is $A = \frac{1}{2}(5)(3) = \frac{15}{2}$, and by looking at the diagram, $N = 4$ and $B = 9$. Thus, $A - N - \frac{1}{2}B = \frac{15}{2} - 4 - \frac{9}{2} = \boxed{-1}$. •

(b) Repeat (a) with $a = 6$ and $b = 4$.

*Solution.* In this case, $T$ is the triangle with vertices $(0, 0), (6, 0)$, and $(6, 4)$, which we can sketch below.



The area of the triangle is $A = \frac{1}{2}(6)(4) = 12$, and by looking at the diagram, we count $N = 7$ and $B = 12$. Thus $A - N - \frac{1}{2}B = 12 - 7 - 6 = \boxed{-1}$. •

(c) Make a conjecture relation $A, N$, and $B$.

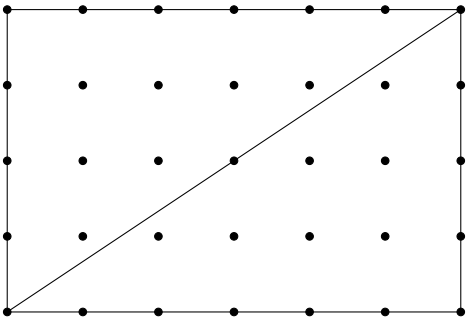
We state our conjecture as a proposition, as the next part tells us to prove the conjecture.

**Proposition 201.1.** *Let $A, N, B$ be defined as above. Then*

$$A - N - \frac{1}{2}B = -1.$$

(d) Prove that your conjecture is correct.

*Proof.* We consider the rectangle $R := [0, a] \times [0, b] \subseteq \mathbb{R}^2$, which can be viewed as two copies of the triangle $T$. For example, in part (b), $R$ looks like



We know that $A = \frac{1}{2}ab$. Let $L$ denote the number of points which lie on the line $y = \frac{b}{a}x$ and are not the "endpoints" $(0, a)$ and $(a, b)$, $E$ denote the number of points on the edge of $R$, and $I$ denote the number of points strictly interior to $R$. Then $(a + 1)(b + 1) = E + I$, and we can count $E = 2B - 2 - 2L$ and $I = 2N + L$. Hence

$$(a + 1)(b + 1) = E + I = 2N + 2B - 2 - L, \text{ but}$$

$$(a+1)(b+1) = ab + a + b + 1 = 2A + a + b + 1.$$

But now notice $a + b + 1$ is precisely $B - L$, so that

$$2N + 2B - 2 - L = 2A + B - L \iff 2N + B - 2 = 2A$$
$$\iff -2 = 2A - B - 2N \iff -1 = A - N - \frac{1}{2}B,$$

as claimed. □

**Kaplan 1.1: Linear Transformations**

Show that if $p \nmid m$, then $\displaystyle\sum_{a=1}^{p-1} \left(\frac{ma}{p}\right) = 0$.

*Proof.* Recall that the map $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ by $a \mapsto ma$ is a bijection modulo $p$ if and only if $p \nmid m$. Hence,

$$\sum_{a=1}^{p-1} \left(\frac{ma}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right).$$

From here, it follows that exactly half of the $a$'s are quadratic residues modulo $p$, and the other half are non-residues, so the sum is 0 as claimed. □

**Kaplan 1.2: A Pell-Like Equation**

Let $a \in \mathbb{Z}$, and suppose $n = x^2 - ay^2$ for some $x, y \in \mathbb{Z}$. Prove that for every odd divisor $p$ of $n$, either $p \mid x$ or $\left(\frac{a}{p}\right) = 1$.

*Proof.* Suppose $n = x^2 - ay^2$. Reduce modulo $p$ (where $p \mid n$) to obtain $0 \equiv x^2 - ay^2 \iff ay^2 \equiv x^2 \pmod{p}$. If $p \mid x$, there is nothing to do. Otherwise, notice that because $x^2 \not\equiv 0 \pmod{p}$, we must have $a \not\equiv 0 \pmod{p}$ and $y^2 \not\equiv 0 \pmod{p}$. Hence $y$ is invertible; i.e., there exists $z$ such that $yz \equiv 1 \pmod{p}$. It follows that $a \equiv (xz)^2 \pmod{p}$, so $\left(\frac{a}{p}\right) = 1$. □

# 202 Homework 2: Quadratic Forms

**Kaplan 2.1: Binary Quadratic Forms and Discriminants**

A *binary quadratic form* is a polynomial $f(x, y) = ax^2 + bxy + cy^2$, for $a, b, c \in \mathbb{Z}$. The *discriminant* of this form is the integer $d := b^2 - 4ac$. Show that

$$4a \cdot f(x, y) = (2ax + by)^2 - dy^2.$$

*Proof.* This identity may be verified by expanding everything out. If $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form, then

$$\begin{aligned}(2ax + by)^2 - dy^2 &= (2ax + by)^2 - (b^2 - 4ac)y^2 \\ &= 4(ax)^2 + 4axby + (by)^2 - b^2y^2 - 4acy^2 \\ &= 4(ax)^2 + 4axby - 4acy^2 = 4a(ax^2 + bxy - cy^2),\end{aligned}$$

as claimed. □

**Kaplan 2.2: Non-trivial Solutions Modulo $p$**

Let $p$ be an odd prime, and let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with $a \not\equiv 0 \pmod{p}$. We say that $f(x,y)$ has a *nontrivial solution* modulo $p$ if there exist integers $(x,y) \not\equiv (0,0) \pmod{p}$ such that $f(x,y) \equiv 0 \pmod{p}$. Prove that $f(x,y)$ has a nontrivial solution modulo $p$ if and only if $d \equiv 0 \pmod{p}$ or $d$ is a quadratic residue modulo $p$.

*Proof.* Suppose $f(x,y) = ax^2 + bxy + cy^2$, with $a \not\equiv 0 \pmod{p}$, has a nontrivial solution $(x,y) \not\equiv (0,0) \pmod{p}$. Then the identity above gives

$$4a \cdot 0 \equiv (2ax + by)^2 - dy^2 \implies dy^2 \equiv (2ax + by)^2 \pmod{p}.$$

It follows that $dy^2$ is a quadratic residue modulo $p$, so that if $y \not\equiv 0$, then $d$ is a quadratic residue modulo $p$, or $d \equiv 0 \pmod{p}$. In the case that $y \equiv 0 \pmod{p}$, then our congruence simplifies to $0 \equiv (2ax)^2 = 4ax^2 \pmod{p}$, and since $x \not\equiv 0$ as the solution is nontrivial, we must have $0 \equiv a \pmod{p}$, which is contradictory. Hence, it follows that $d$ is a quadratic residue modulo $p$, or $d \equiv 0 \pmod{p}$.

Conversely, suppose $d \equiv 0 \pmod{p}$ or $d$ is a quadratic residue modulo $p$. If $d \equiv 0 \pmod{p}$, then we know that $4a \cdot f(x,y) = (2ax+by)^2$ holds identically, so that by inspection, setting $x \equiv -b$ and $y \equiv 2a$ gives a solution:

$$4a \cdot f(-b, 2a) = \left(2a(-b) + b(2a)\right)^2 \equiv 0^2 = 0 \pmod{p},$$

so that $f(-b, 2a) \equiv 0$. This solution is nontrivial as $y \equiv 2a \not\equiv 0 \pmod{p}$.

Now, if $d \not\equiv 0 \pmod{p}$ is a quadratic residue modulo $p$. We want to solve the congruence $0 \equiv (2ax+by)^2 - dy^2 \pmod{p}$, which, if non-trivially solvable, will give us a solution to the quadratic form. We compute

$$\begin{aligned} 0 &\equiv (2ax + by)^2 - dy^2 \\ dy^2 &\equiv (2ax + by)^2 \\ \sqrt{d}y &\equiv 2ax + by \\ 0 &\equiv 2ax + (b - \sqrt{d})y, \end{aligned}$$

where the symbol $\sqrt{d}$ represents a solution to the congruence $x^2 \equiv d \pmod{p}$. From here, it is clear that setting $x \equiv (b - \sqrt{d})$ and $y \equiv -2a$ gives a solution:

$$\begin{aligned} 4a \cdot f\left(b - \sqrt{d}, -2a\right) &= \left(2a(b - \sqrt{d}) + b(-2a)\right)^2 - d(-2a)^2 \\ &\equiv \left(2ab - 2a\sqrt{d} - 2ab\right)^2 - 4a^2 d \\ &\equiv 4a^2 d - 4a^2 d \equiv 0 \pmod{p}, \end{aligned}$$

So that $f(b - \sqrt{d}, -2a) \equiv 0 \pmod{p}$. This solution is nontrivial as $y = -2a \not\equiv 0 \pmod{p}$, so this completes the proof. □

**Kaplan 2.3: The Form $x^2 + xy + y^2$**

Find all primes $p$ for which the binary quadratic form $f(x, y) = x^2 + xy + y^2$ has a nontrivial solution modulo $p$.

*Solution.* Arguing by the previous two exercises, $f(x, y)$ has a non-trivial solution modulo a prime $p$ if and only if the discriminant $d = 1^2 - 4(1)(1) = -3$ is either divisible by $p$, or is a quadratic residue modulo $p$. In the first case, we have $p \mid (-3)$, implying that $f(x, y)$ has a nontrivial solution when $\boxed{p = 3}$, namely the solution $(1, 1)$. In the second case, we have $-3 \not\equiv 0 \pmod{p}$ and $\left(\frac{-3}{p}\right) = 1$, but now $1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$, so that $p \equiv 1 \pmod 3$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1$, so that again $p \equiv 1 \pmod 3$. Thus, the second case tells us that $f(x, y)$ has a nontrivial solution when $\boxed{p \equiv 1 \pmod 3}$. •

**Kaplan 2.4: Affine Transformations**

Let $p$ be a prime and $a \in \mathbb{Z}$ satisfy $p \nmid a$. Prove that $\displaystyle\sum_{x=0}^{p-1} \left(\frac{ax + b}{p}\right) = 0$.

*Proof.* Since $p \nmid a$, recall that the map $x \mapsto ax$ is a bijection modulo $p$ (i.e., it is a group automorphism $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$), so that shifting by some $b \in \mathbb{Z}$ preserves bijectivity. Thus, it follows that

$$\sum_{x=0}^{p-1} \left(\frac{ax + b}{p}\right) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) = \left(\frac{0}{p}\right) + \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right).$$

Now, we know that there are exactly $\frac{1}{2}(p-1)$ quadratic residues in the range $\{1, 2, \ldots, p-1\}$, and exactly $\frac{1}{2}(p-1)$ quadratic residues in that same range. It follows that these cancel in the summation, so we do indeed obtain a result of 0 as desired. □

**Kaplan 2.5: The Congruence $x^2 - y^2 \equiv a$**

Let $p$ be an odd prime.

(a) Show that the number of solutions to $x^2 - y^2 \equiv a \pmod p$ is given by

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p}\right)\right).$$

*Proof.* Rearrange and write $x^2 \equiv y^2 + a \pmod p$. If $y^2 + a$ is a quadratic residue modulo $p$, then we have the two solutions $x_{1,2} \equiv \pm\sqrt{y^2 + a}$, where the square root is considered modulo $p$. If $y^2 + a \equiv 0 \pmod p$, we have the solution $x \equiv 0$, and if $y^2 + a$ is a quadratic non-residue modulo $p$, we get no solutions. Taking into account the value of the Legendre symbol, we observe that the number of solutions is given by

$$\sum_{y : y^2 + a \in \mathsf{QR}(p)} 2 + \sum_{y : y^2 + a \in \mathsf{NR}(p)} 0 + \sum_{y : y^2 + a \equiv 0} 1$$

$$= \sum_{y:y^2+a\in \mathsf{QR}(p)} \left(1+\left(\frac{y^2+a}{p}\right)\right) + \sum_{y:y^2+a\in \mathsf{NR}(p)} \left(1+\left(\frac{y^2+a}{p}\right)\right) + \sum_{y:y^2+a\equiv 0} \left(1+\left(\frac{y^2+a}{p}\right)\right),$$

which covers all the possible cases for $y$, running from 0 to $p-1$, so the sum claimed does hold. □

(b) By calculating directly, show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is $p-1$ if $p \nmid a$ and $2p-1$ if $p \mid a$.

*Proof.* As per the hint, define $u := x+y$ and $v := x-y$. Then $x^2 - y^2 \equiv a$ is equivalent to

$$x^2 - y^2 = (x+y)(x-y) = uv \equiv a \pmod{p}.$$

Because this is an invertible linear change of variables over the finite field $\mathbb{Z}/p\mathbb{Z}$, we do not change the number of solutions we get, so it suffices to count the number of solutions $(u, v)$. In the case $a \equiv 0 \pmod{p}$, the solutions take the form $(0,0)$, $(u,0)$, and $(0,v)$ for $u, v \in \{1, 2, \ldots, p-1\}$. Counting these, we indeed get $2p-1$ solutions when $p \mid a$.

Now, when $a \not\equiv 0 \pmod{p}$, we observe that $u, v \not\equiv 0 \pmod{p}$, so that we get the relation $u \equiv av^{-1}$. In this case, the solutions are of the form $(av^{-1}, v)$, where $v \in \{1, 2, \ldots, p-1\}$, so there are $p-1$ solutions when $p \nmid a$. □

(c) Combining parts (a) and (b), show $\displaystyle\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = \begin{cases} -1 & p \nmid a \\ p-1 & p \mid a. \end{cases}$

*Proof.* From part (a), we know that the number of solutions to the congruence $x^2 - y^2 \equiv a \pmod{p}$ is given by

$$\sum_{y=0}^{p-1} \left(1+\left(\frac{y^2+a}{p}\right)\right) = p + \sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right).$$

In the case $p \nmid a$, we know that from part (b), there are $p-1$ solutions to $x^2 - y^2 \equiv a$, so that solving for the sum from above gives $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = -1$. Similarly, when $p \mid a$, part (b) tells us that there are $2p-1$ solutions, so solving again gives $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = p-1$. □

**Kaplan 2.6: Quadratic Polynomials and Legendre Symbols**

Let $p$ be an odd prime. Suppose $x^2 + ax + b$ is not the square of a linear polynomial modulo $p$. Compute $\displaystyle\sum_{n=0}^{p-1} \left(\frac{n^2+an+b}{p}\right)$.

*Solution.* We complete the square and write

$$n^2 + an + b \equiv \left(n + \frac{a}{2}\right)^2 + \left(b - \frac{a^2}{4}\right) \pmod{p},$$

where the formal "fractions" represent inversion modulo $p$. Now, take the linear change (over $\mathbb{Z}/p\mathbb{Z}$) of variables $y := n + a/2$ and $a' := b - a^2/4$ (reducing modulo $p$ into the range $[0, p)$ if necessary), so that

$$\sum_{n=0}^{p-1} \left(\frac{n^2+an+b}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y^2+a'}{p}\right),$$

which we can evaluate by Exercise 5(c) to obtain $\boxed{-1}$ whenever $p \nmid a'$, and $\boxed{p-1}$ whenever $p \mid a'$. •

# 203 Homework 3: Sums of Squares

### Silverman 24.4/5: Computations Involving Sums of Squares

**Exercise 1.** Start from $261^2 + 947^2 = 10 \cdot 96493$ and use the Descent Procedure to write the prime 96493 as a sum of two squares.

*Solution.* First, note $96493 \equiv 1 \pmod 4$, so this is actually possible to do. First, we reduce modulo 10 to get the congruence $1^2 + 7^2 \equiv 0 \pmod{10}$, so we have that

$$(261 \cdot 1 + 947 \cdot 7)^2 + (261 \cdot 7 - 947 \cdot 1)^2 \equiv 0 \pmod{10}.$$

In fact, simplifying this gives

$$6890^2 + 880^2 = 5 \cdot 100 \cdot 96493,$$

so dividing out by 100 yields $689^2 + 88^2 = 5 \cdot 96493$. Now, we do the descent procedure again: reduce modulo 5 to obtain $(-1)^2 + (-2)^2 \equiv 0 \pmod 5$, so we have that

$$(689 \cdot (-1) + 88 \cdot (-2))^2 + (689 \cdot (-2) - 88 \cdot (-1))^2 \equiv 0 \pmod 5,$$

or $(-865)^2 + (-1290)^2 = 5^2 \cdot 96493$. Dividing out by 25 gives $\boxed{96493 = 173^2 + 258^2}$. •

**Exercise 2.** This exercise relates to sums of squares and Pythagorean triples.

(a) Write 1885 as a sum of two squares, or explain why it is not possible to do so.

*Solution.* We factor $1885 = 5 \times 13 \times 29$. All of the primes in this factorization are congruent to 1 modulo 4, so that writing 1885 as a sum of two squares is possible. Note that $5 \times 13 = 65 = 8^2 + 1^2$, and that $29 = 5^2 + 2^2$, so that $1885 = 65 \cdot 29 = (8^2 + 1^2)(5^2 + 2^2) = (8 \cdot 5 + 1 \cdot 2)^2 + (8 \cdot 2 - 1 \cdot 5)^2 = \boxed{42^2 + 11^2}$. •

(b) Write 3185 as a sum of two squares, or explain why it is not possible to do so.

*Solution.* We factor $3185 = 5 \times 7^2 \times 13$. Here, the only prime congruent to 3 modulo 4 is squared, so that it is possible to write 3185 as a sum of two squares: just note $3185 = 65 \times 49 = 7^2(8^2 + 1^2) = \boxed{56^2 + 7^2}$. •

(c) Find a primitive Pythagorean triple with $c = 1885$, if possible.

*Solution.* This amounts to finding odd coprime integers $s > t \geq 1$ such that $a = st$, $b = \frac{1}{2}(s^2 - t^2)$, and $c = \frac{1}{2}(s^2 + t^2)$. Write

$$1885 = 42^2 + 11^2 = \frac{1}{2}(s^2 + t^2),$$

so that

$$\begin{aligned} 3770 = s^2 + t^2 &= (42^2 + 11^2) \cdot 2 = (42^2 + 11^2)(1^2 + 1^2) \\ &= (42 \cdot 1 + 11 \cdot 1)^2 + (42 \cdot 1 - 11 \cdot 1)^2 \\ &= 53^2 + 31^2, \end{aligned}$$

so take $s = 53$ and $t = 31$. Clearly, $\gcd(s, t) = 1$, so this gives a primitive Pythagorean triple. Now, it is easy to compute $a = st = 1643$, $b = \frac{1}{2}(s^2 - t^2) = 924$, and $c = 1885$, so the triple is $\boxed{(1643, 924, 1885)}$. •

(d) Find a primitive Pythagorean triple with $c = 3185$, if possible.

*Solution.* This is **impossible** by Theorem 25.2 in the text; we saw the factorization $3185 = 5 \times 7^2 \times 13$, which contains a prime not congruent to 1 modulo 4. •

**Silverman 25.5: A Proof of Theorem 34.1**

In this exercise we prove Theorem 34.1. Let $m$ be a positive integer.

(a) If $m$ is odd and if every prime dividing $m$ is congruent to 1 (mod 4), prove that $m$ can be written as a sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$.

*Proof.* We proceed by induction on the number of prime factors of $m$. If $m = p$, where $p \equiv 1 \pmod 4$, then if $p = a^2 + b^2$, observe that if $d \mid a, b$, we must have $d^2 \mid p$. That $d = p$ is absurd, so $d = 1$, so $\gcd(a, b) = 1$.

Now, assume that the theorem holds when $m$ is the product of $k$ primes congruent to 1 (mod 4). Let $m = p_1 p_2 \cdots p_k q$, where $p_i, q \equiv 1 \pmod 4$ are prime. By the induction hypothesis, we may write

$$p_1 p_2 \cdots p_k = a^2 + b^2 \text{ with } \gcd(a, b) = 1, \text{ and}$$

the base case gives $q = c^2 + d^2$ with $\gcd(c, d) = 1$. Now

$$m = (a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2;$$

we claim that either $\gcd(ac + bd, ad - bc) = 1$ or $\gcd(ac - bd, ad + bc) = 1$. Suppose that $\gcd(ac + bd, ad - bc) \neq 1$; we show that $\gcd(ac - bd, ad + bc) = 1$. Then, there exists a prime $r$ such that $r \mid (ac + bd)$ and $r \mid (ad - bc)$, so that

$$r \mid c(ac + bd) - d(ad - bc) = a(c^2 + d^2) \text{ and}$$

$$r \mid d(ac + bd) - c(ad - bc) = b(c^2 + d^2).$$

Since $\gcd(a, b) = 1$, we have $r \mid c^2 + d^2 = q$, so $r = q$. Now, if $\gcd(ac - bd, ad + bc) \neq 1$, observe

$$m = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

implies that $r \mid ac - bd$ and $r \mid ad + bc$, so $r \mid 2ac$ and $r \mid 2bd$. Since $r = c^2 + d^2$ is odd, we have $r \mid ac$ and $r \mid bd$, but clearly $c^2 + d^2 \nmid c, d$, so $r \mid a, b$, which is contradictory as $\gcd(a, b) = 1$. This completes the proof. □

(b) If $m$ is even and $m/2$ is odd and if every prime dividing $m/2$ is congruent to 1 (mod 4), prove that $m$ can be written as the sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$.

*Proof.* Suppose $m$ is even and $m/2$ is odd, and every prime dividing $m/2$ is congruent to 1 (mod 4). Write $m/2 = x^2 + y^2$, where $\gcd(x, y) = 1$, as per part (a). Now

$$m = \frac{m}{2} \cdot 2 = (x^2 + y^2)(1^2 + 1^2) = (x + y)^2 + (x - y)^2.$$

We claim that $d := \gcd(x + y, x - y) = 1$. First, note that by Bezout's Lemma, there exist $u, v \in \mathbb{Z}$ such that $ux - vy = 1$. It follows that

$$\begin{aligned}(u - v)(x + y) + (u + v)(x - y) &= (ux - vx + uy - vy) + (ux - uy + vx - vy) \\ &= 2ux - 2vy = 2(ux - vy) = 2,\end{aligned}$$

so that $d \mid 2$. If $d = 2$, this implies that $u$ and $v$ have the same parity. But this is absurd as that implies $u^2 + v^2 = m/2$ is even, a contradiction, so we must have $d = 1$. Hence $\gcd(x + y, x - y) = 1$, so take $a := x + y$ and $b := x - y$, so $m = a^2 + b^2$. □

(c) If $m$ can be written as the sum of two squares $m = a^2 + b^2$ with $\gcd(a, b) = 1$, prove that $m$ is one of the numbers described in parts (a) or (b).

*Proof.* Suppose $m = a^2 + b^2$, with $\gcd(a, b) = 1$. If $m$ is odd, take any prime $p$ dividing $m$. Since $\gcd(a, b) = 1$, $p$ does not divide at least one of $a$ and $b$. In fact, $p \nmid a, b$, as without loss of generality if $p \mid a$, then $p \mid (m - a^2) = b^2$ implying $p \mid b$, contradicting the fact that $\gcd(a, b) = 1$. Now, reduce modulo $p$ to obtain $-b^2 \equiv a^2 \pmod{p}$. This implies $-b^2$ is a quadratic residue modulo $p$, so we must have

$$1 = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\cancel{\left(\frac{b^2}{p}\right)} = \left(\frac{-1}{p}\right),$$

so by quadratic reciprocity, $p \equiv 1 \pmod{4}$. Since $p$ was arbitrary, every prime $p \mid m$ is congruent to 1 (mod 4), which is the case described in part (a).

Now, suppose $m = a^2 + b^2$ (with $\gcd(a, b) = 1$) is even. If we have that $4 \mid m$, this implies $0 \equiv a^2 + b^2 \pmod{4}$. However, we know that $a^2, b^2 \equiv 0, 1 \pmod{4}$, so that $a^2 + b^2 \equiv 0 \pmod{4}$ if and only if $a^2 \equiv b^2 \equiv 0 \pmod{4}$. But this exactly means $2 \mid a, b$, so that $\gcd(a, b) > 2$, a contradiction, so we must have $4 \nmid m$, i.e., $m/2$ is odd. It suffices to show that $m/2 = x^2 + y^2$ for integers $x, y$ with $\gcd(x, y) = 1$, as then we can just repeat the first case of this argument on $m/2$ to finish the proof. Hence, we must solve

$$a^2 + b^2 = (x^2 + y^2)(1^2 + 1^2) = (x + y)^2 + (x - y)^2,$$

i.e., we must find coprime $x, y \in \mathbb{Z}$ such that $a = x + y$ and $b = x - y$. We claim that $x = \frac{1}{2}(a + b)$ and $y = \frac{1}{2}(a - b)$; notice these are actually integers because $m$ is even, so $a^2$ and $b^2$ are forced to have the same parity (in fact, they are both forced to be odd, but we do not need this fact). Now, because $\gcd(a, b) = 1$, we can find (by Bezout's Lemma) some $u, v \in \mathbb{Z}$ such that $au - bv = 1$. Now

$$(u - v)x + (u + v)y = \frac{1}{2}\left((u - v)(a + b) + (u + v)(a - b)\right)$$

$$= \frac{1}{2}((ua - va + ub - vb) + (ua + va - ub - vb)) = \frac{1}{2}(2ua - 2vb) = ua - vb = 1,$$

so by Bezout's Lemma we have $\gcd(x, y) = 1$. Thus, $m/2 = x^2 + y^2$, with $\gcd(x, y) = 1$ so applying the first part of this argument finishes the proof, as $m/2$ is odd by assumption. □

**Silverman 30.1: The Equation $y^2 = x^3 + xz^4$**

Show that the equation $y^2 = x^3 + xz^4$ has no solutions in nonzero integers $x, y, z$.

*Proof.* Assume for contradiction that $(x, y, z)$ were a non-trivial solution. Notice that without loss of generality, we may assume $\gcd(x, z) = 1$, as if $p$ is a common prime factor of $x$ and $z$, we may write $x = ap$ and $y = bp$, so that

$$y^2 = ap(a^2p^2 + b^4p^4) = a^3p^3 + ab^4p^5 = p^3(a^3 + ab^4p^2),$$

from which it follows $p^3 \mid y^2 \implies p^3 \mid y$, as $p$ is prime (the exponent 3 is odd). Now write $y = cp^3$, so that

$$y^2 = c^2p^6 = p^3(a^3 + ab^4p^2) \implies c^2p^3 = a^3 + ab^4p^2 = a(a^2 + b^4p^2),$$

so that $p^3 \mid a \implies p \mid a$, and writing $a = mp$ for $m \in \mathbb{Z}$ gives

$$c^2p^3 = mp(m^2p^2 + b^4p^2) \implies c^2 = m^3 + b^4,$$

which is a reduced solution, which shows that our without-loss-of-generality assumption that $\gcd(x, z) = 1$ is legitimate. Now, note that $y^2 = x(x^2 + z^4)$, so the right-hand side is a perfect square. If $x$ is a perfect square, then $x = \alpha^2$ for some $\alpha \in \mathbb{Z}$. But now this means

$$y^2 = x(x^2 + z^4) = \alpha^2(\alpha^4 + z^4),$$

so that because $y^2$ is a perfect square, $\alpha^4 + z^4$ is also a perfect square. Hence, there exists $c \in \mathbb{Z}$ such that $\alpha^4 + z^2 = c^2$, which contradicts Theorem 30.1 in the text. Hence, $x$ must take the form $x = \alpha^2\beta$, where $\alpha, \beta \in \mathbb{Z}$ are such that $\beta$ is squarefree. In this case, we have

$$y^2 = x(x^2 + z^4) = \alpha^2\beta(\alpha^4\beta^2 + z^4) \iff \left(\frac{y}{\alpha}\right)^2 = \beta(\alpha^4\beta^2 + z^4).$$

Because the right-hand side is an integer, so is $(y/\alpha)^2$, and because $\beta$ is square-free, the factor $\alpha^4\beta^2 + z^4$ must have an odd number of $\beta$ factors in order to make $(y/\alpha)^2$ a perfect square. In particular, this implies $\beta \mid (\alpha^4\beta^2 + z^4) \implies \beta \mid z^4$, and because $\beta$ is squarefree, we have $\beta \mid z$. But now $\gcd(x, z) = 1$, and since $\beta \mid x$, we must have $\beta = 1$. Bu this implies $x = \alpha^2\beta = \alpha^2$ is a perfect square, but we have shown this to be impossible. Thus, the equation $y^2 = x^3 + xz^2$ has no non-trivial solutions. □

**Silverman 30.2-3: An Exploration of Markoff Triples**

**Exercise 1.** A *Markoff triple* is a triple of positive integers $(x, y, z)$ such that $x^2+y^2+z^2 = 3xyz$. There is one obvious Markoff triple, namely $(1, 1, 1)$.

(a) Find all Markoff triples that satisfy $x = y$.

*Solution.* When $x = y$, the Markoff equation simplifies to $3x^2z = 2x^2+z^2$, or $x^2(3z-2) = z^2$. This is a quadratic in $z$, which we write as

$$0 = z^2 - (3x^2)z + (2x^2).$$

This has rational roots precisely when $(3x^2)^2 - 4(1)(2x^2) = 9x^4 - 8x^2 = x^2(9x^2 - 8)$ is a perfect square, i.e., whenever $9x^2 - 8$ is a perfect square. Notice $9x^2$ is always a perfect

square, but the only two perfect squares with a distance of $8 = 3 + 5$ apart are $1 = 1^2$ and $9 = 3^2$, after noting the identity

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Hence, we are forced to have $9x^2 - 8 = 1$, i.e., $x = 1$ (as $x$ is positive). Hence, we get the relation $0 = z^2 - 3z + 2$, or $z = 1, 2$. Hence, the only Markoff triples with $x = y$ are $\boxed{(1, 1, 1)}$ and $\boxed{(1, 1, 2)}$. •

(b) Let $(x_0, y_0, z_0)$ be a Markoff triple. Show that the following are also Markoff triples:

$$F(x_0, y_0, z_0) = (x_0, z_0, 3x_0z_0 - y_0)$$
$$G(x_0, y_0, z_0) = (y_0, z_0, 3y_0z_0 - x_0)$$
$$H(x_0, y_0, z_0) = (x_0, y_0, 3x_0y_0 - z_0).$$

This gives a way to create new Markoff triples from old ones.

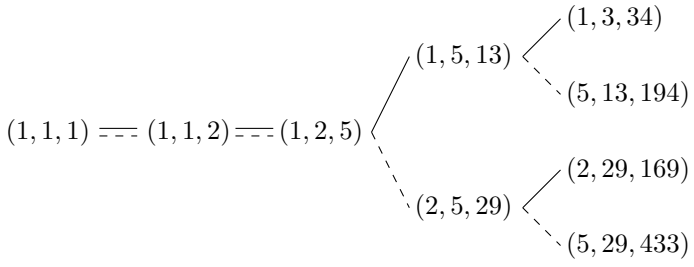
*Proof.* This is a straightforward verification. [For brevity, we suppress the subscript 0's.] Note that $x^2 + y^2 + z^2 = 3xyz$, so we compute

$$\begin{aligned} x^2 + z^2 + (3xz - y)^2 &= x^2 + z^2 + 9x^2z^2 - 6xyz + y^2 \\ &= 3xyz + 9x^2z^2 - 6xyz \\ &= 3(xyz + 3x^2z^2 - 2xyz) \\ &= 3(3x^2z^2 - xyz) \\ &= 3xz(3z - y). \end{aligned}$$

This shows that $F(x, y, z)$ is a Markoff triple. Note that by commutativity if $(x, y, z)$ is a Markoff triple, then any permutation of the integers $x, y, z$ is trivially a Markoff triple. Clearly, $G(x, y, z) = F(y, x, z)$ and $H(x, y, z) = F(x, z, y)$, so the computation above completes the proof. □

(c) Starting with the Markoff triple $(1, 1, 1)$, repeatedly apply the functions $F$ and $G$ described in (b) to create at least eight more Markoff triples. Arrange them in a picture with two Markoff triples connected by a line segment if one is obtained from the other by using $F$ or $G$.

*Solution.* We suppress our calculations and give the graph below. Solid lines indicate an application of $F$, while dashed lines indicate an application of $G$. This is read left to right.



•

**Exercise 2.** This exercise continues the study of the Markoff equation from the previous exercise.

(a) We say that a Markoff triple $(x_0, y_0, z_0)$ s normalized if its coordinates are arranged in increasing order of magnitude. Prove that if $(x_0, y_0, z_0)$ is a normalized Markoff triple, then both $F(x_0, y_0, z_0)$ and $G(x_0, y_0, z_0)$ are normalized Markoff triples.

*Proof.* Again, for brevity we suppress the subscript 0's. Let $(x, y, z)$ be a normalized Markoff triple. Given that $1 \leq x \leq y \leq z$, it suffices to show $z \leq 3xz - y$ and $z \leq 3yz - x$. Observe $y + z \leq z + z = 2z < 3z \leq (3x)z$, so the first inequality follows, and that $x + z \leq z + z = 2z < 3z \leq (3y)z$, so the second inequality follows. In fact, the third coordinates of $F(x, y, z)$ and $G(x, y, z)$ are both strictly greater than $z$. □

(b) The *size* of a Markoff triple $(x_0, y_0, z_0)$ is defined to be the sum of its coordinates:

$$\mathsf{size}(x_0, y_0, z_0) := x_0 + y_0 + z_0.$$

Prove that if $(x_0, y_0, z_0)$ is a normalized Markoff triple, then

$$\begin{aligned}
\mathsf{size}(x_0, y_0, z_0) &< \mathsf{size}\, F(x_0, y_0, z_0), \\
\mathsf{size}(x_0, y_0, z_0) &< \mathsf{size}\, G(x_0, y_0, z_0), \\
\mathsf{size}(x_0, y_0, z_0) &> \mathsf{size}\, H(x_0, y_0, z_0).
\end{aligned}$$

*Proof.* Again, for brevity, we suppress the subscript 0's. The first two inequalities are obvious: we have, by virtue of (the strict version of) part (a),

$$\begin{aligned}
\mathsf{size}(x, y, z) = x + y + z < x + y + (3xz - y) = \mathsf{size}\, F(x, y, z); \\
\mathsf{size}(x, y, z) = x + y + z < x + y + (3yz - x) = \mathsf{size}\, G(x, y, z).
\end{aligned}$$

For the last inequality, we must show $x + y + z > x + y + (3xy - z)$, which is equivalent to showing $2z > 3xy$. In the case $x = y = 1$, this is easy to verify by hand, so we take $y \geq x \geq 2$. Because we know $x^2 + y^2 + z^2 = 3xyz$, we may rearrange this and write this as a quadratic in $z$, namely $z^2 - (3xy)z + (x^2 + y^2) = 0$. Solving for $z$ by the quadratic formula, we have

$$z = \frac{3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}}{2}.$$

Now, some rearranging yields

$$z = \frac{3xy \pm \sqrt{x^2y^2 + 4(x^2y^2 - x^2) + 4(x^2y^2 - y^2)}}{2},$$

and since we know $0 \leq x \leq y$, we have $4(x^2y^2 - x^2), 4(x^2y^2 - y^2) \geq 0$ [in fact, it is easily verified that at least one of these must be positive], so that

$$\sqrt{x^2y^2 + 4(x^2y^2 - x^2) + 4(x^2y^2 - y^2)} > \sqrt{x^2y^2} = xy.$$

Now, if we were to take the negative sign in the expression for $z$ above, we then observe

$$z = \frac{3xy - \sqrt{9x^2y^2 - 4(x^2 + y^2)}}{2} < \frac{3xy - xy}{2} = xy.$$

Now, because $x^2+y^2+z^2 = 3xyz$, we observe $x^2+y^2+z^2 > 3z^2$, which implies

$$x^2+y^2 > 2z^2 = z^2+z^2 \geq x^2+y^2,$$

which is an absurdity. Hence, we must have

$$z = \frac{3xy + \sqrt{x^2y^2+4(x^2y^2-x^2)+4(x^2y^2-y^2)}}{2} > \frac{3xy}{2},$$

from which it follows that $2z > 3xy$, which is what we wanted to show. □

(c) Prove that every Markoff triple can be obtained by starting with the Markoff triple $(1,1,1)$ and repeatedly applying the functions $F$ and $G$.

*Proof.* Suppose for contradiction that there exist Markoff triples not obtainable from $(1,1,1)$ and iteratively applying $F$ and $G$. If this is a case, by well-ordering, there must be a normalized triple of minimal size; call it $(x_0,y_0,z_0)$ [where of course, $x_0 \leq y_0 \leq z_0$]. By virtue of part (b), the triple $H(x_0,y_0,z_0) = (x_0,y_0,3x_0y_0-z_0)$ is of smaller size than $(x_0,y_0,z_0)$; however, $H(x_0,y_0,z_0)$ is not necessarily normalized. However, since $x_0 \leq y_0$, at least one of these rearrangements must be normalized:

$$(x_0,y_0,3x_0y_0-z_0) \text{ or } (x_0,3x_0y_0-z_0,y_0) \text{ or } (3x_0y_0-z_0,x_0,y_0).$$

We claim that the first of these is not normalized: notice that

$$H(x_0,y_0,3x_0y_0-z_0) = (x_0,y_0,3x_0y_0-(3x_0y_0-z_0)) = (x_0,y_0,z_0),$$

but we know $\mathsf{size}(x_0,y_0,3x_0y_0-z_0) < \mathsf{size}(x_0,y_0,z_0)$ by part (b). This would be contradictory unless $(x_0,y_0,3x_0y_0-z_0)$ were not normalized, so that it follows that either $(x_0,3x_0y_0-z_0,y_0)$ or $(3x_0y_0-z_0,x_0,y_0)$ are normalized. But

$$F(x_0,3x_0y_0-z_0,y_0) = (x_0,y_0,z_0) \text{ and } G(3x_0y_0-z_0,x_0,y_0) = (x_0,y_0,z_0),$$

and both $(x_0,3x_0y_0-z_0,y_0)$ and $(3x_0y_0-z_0,x_0,y_0)$ are of smaller size than $(x_0,y_0,z_0)$, which is a contradiction of the minimality of $(x_0,y_0,z_0)$: both of the smaller triples are by assumption constructed from $(1,1,1)$ and applying $F$ and $G$, and thus we have just shown $(x_0,y_0,z_0)$ is constructed in the same way. □

# 204 Homework 4: Primitive Roots

### Silverman 27.1: A Result about Divisor Sums

A function $f(n)$ that satisfies $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$ is called a *multiplicative function*. Suppose $f$ is multiplicative and $g(n) = f(d_1)+f(d_2)+\cdots+f(d_r)$, where the $d_i$ are the divisors of $n$. Prove that $g$ is multiplicative.

*Proof.* Essentially, the proof proceeds by counting the divisors. Let $m$ have the divisors $d_1 < d_2 < \cdots < d_r = m$, and $n$ have the divisors $e_1 < e_2 < \cdots < e_s = n$. If $\gcd(m,n) = 1$, then the divisors of $mn$ are the products $d_ie_j$, for $1 \leq i \leq r$ and $1 \leq j \leq s$. Furthermore, $f(d_ie_j) = f(d_i)f(e_j)$ as $\gcd(d_i,e_j) = 1$. Then

$$g(mn) = \sum_{i=1}^{r}\sum_{j=1}^{s} f(d_ie_j) = \sum_{i=1}^{r}\sum_{j=1}^{s} f(d_i)f(e_j) = \sum_{i=1}^{r} f(d_i)\sum_{j=1}^{s} f(e_j) = g(m)g(n),$$

which completes the proof. □

We actually used the result in the main notes (for example to prove a proposition about the sum of divisors function), so we state it separately here:

**Lemma 204.1.** *Suppose $f$ is multiplicative, and $g(n) = \sum_{d|n} f(n)$. Then $g$ is multiplicative.*

**Silverman 27.2: Liouville's Lambda Function**

Liouville's *lambda function* $\lambda(n)$ is defined by $\lambda(1) = 1$, and otherwise, factoring $n$ into a product of primes, $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, where the $p_i$ are all distinct, then setting $\lambda(n) = (-1)^{k_1+k_2+\cdots+k_t}$.

(a) Compute $\lambda(30), \lambda(504)$, and $\lambda(60750)$.

*Solution.* We have $30 = 2^1 \cdot 3^1 \cdot 5^1$, $504 = 2^3 \cdot 3^2 \cdot 7^1$, and $60750 = 2^1 \cdot 3^5 \cdot 5^3$. Hence, $\lambda(30) = (-1)^{1+1+1} = \boxed{-1}$, $\lambda(504) = (-1)^{3+2+1} = \boxed{+1}$, and $\lambda(60750) = (-1)^{1+5+3} = \boxed{-1}$. •

(b) Prove that $\lambda(n)$ is multiplicative.

*Proof.* Let $m, n$ be integers with $\gcd(m, n) = 1$. Write $m = p_1^{a_1} \cdots p_r^{a_r}$ for distinct primes $p_i$, and $n = q_1^{b_1} \cdots q_s^{b_s}$ for distinct primes $q_j$. Since $\gcd(m, n) = 1$, we see that $p_i \neq q_j$ for all $i, j$. Now $mn = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$ is the prime factorization for $mn$, so

$$\lambda(mn) = (-1)^{a_1+\cdots+a_r+b_1+\cdots+b_s} = (-1)^{a_1+\cdots+a_r}(-1)^{b_1+\cdots+b_s} = \lambda(m)\lambda(n),$$

which completes the proof. □

(c) Define $G(n) = \sum_{d|n} \lambda(n)$. Compute $G(n)$ for $1 \leq n \leq 18$.

*Solution.* Notice that when $p$ is prime, we have $G(p) = \lambda(1)+\lambda(p) = 1-1 = 0$, and for prime powers, we have $G(p^k) = \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^k) = 1 + (-1) + 1 + \cdots + (-1)^k = 0$ if $k$ is odd, and 1 if $k$ is even. Using this and the fact that $G$ is multiplicative by Lemma 204.1 (as $\lambda$ is multiplicative), we obtain

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $G(n)$ | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

•

(d) Using the computations in (c), guess the value of $G(n)$ and compute $G(62141689)$ and $G(60119483)$.

*Solution.* We claim that $G(n) = 1$ whenever $n$ is a perfect square, and 0 otherwise. Now, we know that the perfect squares, reduced modulo 10, are $0, 1, 4, 9, 6, 5$. Hence 60119483 is not a perfect square, and thus $G(60119483) = \boxed{0}$. Using a calculator, we can check that $7883^2 = 62141689$, so $G(62141689) = 1$. •

(e) Prove that your guess in (d) is correct.

*Proof.* We have shown in part (c) that for prime powers, $G(p^k) = 1$ if $k$ is even and $G(p^k) = 0$ if $k$ is odd, and $G$ is multiplicative by Exercises 1 and 2(b). Certainly, $G(1) = 1$, and 1 is a perfect square. Now, write, for $n \geq 2$, $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where the $p_i$ are distinct primes. Then $n$ is a perfect square if and only if the $a_i$ are all even, if and only if

$$G(n) = G(p_1^{a_1} \cdots p_r^{a_r}) = G(p_1^{a_1}) \cdots G(p_r^{a_r}) = 1 \cdot 1 \cdots 1 = 1.$$

Otherwise, one of the $a_i$ must be odd so that $G(p_i^{a_i}) = 0$, so $G(n) = 0$. □

**Silverman 28.5: Finding Primitive Roots**

This exercise concerns determining other primitive roots from a given primitive root.

(a) If $g$ is a primitive root modulo 37, which of the numbers $g^2, g^3, \ldots, g^8$ are primitive roots modulo 37?

*Solution.* Suppose $g^\ell$ is a primitive root modulo 36. Then $g^{36\ell} \equiv 1 \pmod{37}$, but $g^{k\ell} \not\equiv 1$ for all $1 \le k < 36$. Because $g$ is a primitive root, this implies $36 \nmid k\ell$ for all $1 \le k < 36$, so this means $\operatorname{lcm}(36, \ell) = 36\ell$, i.e., $\gcd(36, \ell) = 1$. Hence, only $\boxed{g^5}$ and $\boxed{g^7}$ are primitive roots modulo 37 on that list. •

(b) If $g$ is a primitive root modulo $p$, determine with proof when $g^k$ is a primitive root modulo $p$.

We claim that $g^k$ is a primitive root modulo $p$ if and only if $\gcd(k, p-1) = 1$.

*Proof.* We will actually prove a more general statement: if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order $n$, then $a^k$ has order $n/\gcd(n,k)$. Let $d := \gcd(n,k)$, so that $(a^k)^{n/d} = (a^n)^{k/d} \equiv 1^{k/d} \equiv 1 \pmod{p}$. This implies that $|a^k| \le n/d$. We claim that $|a^k| = n/d$; suppose otherwise, so that there exists $1 \le \ell < n/d$ (if and only if $1 \le \ell d < n$) with $(a^k)^\ell \equiv 1$. Writing $d = xn + yk$ for integers $x, y$ (which is possible by Bezout's Lemma), we have

$$a^{d\ell} = a^{(xn+yk)\ell} = a^{xn\ell} a^{yk\ell} = (a^n)^{x\ell} (a^{k\ell})^y \equiv 1 \cdot 1 = 1,$$

but this is illegal as $d\ell < n$, and $n$ is the order of $a$. Hence $|a^k| = n/d$, so our result follows as a corollary. □

(c) Suppose $g$ is a primitive root modulo the prime $p = 21169$. Use (b) to determine which of the numbers $g^2, g^3, \ldots, g^{20}$ are primitive roots modulo 21169.

*Solution.* We have $p - 1 = 21168 = 2^4 \cdot 3^3 \cdot 7^2$. The numbers in the range $2, 3, \ldots, 20$ coprime to 21168 are thus $5, 11, 13, 17, 19$, so $\boxed{g^5, g^{11}, g^{13}, g^{17}, g^{19}}$ are primitive roots. •

**Silverman 28.8: Primitive Roots and Quadratic Residues**

Let $p$ be an odd prime and $g$ be a primitive root modulo $p$.

(a) Prove that $g^k$ is a quadratic residue modulo $p$ if and only if $k$ is even.

*Proof.* Clearly, when $k$ is even, $g^k$ is a perfect square, so it is a quadratic residue. That is, $g^2, g^4, g^6, \ldots, g^{p-1}$ are all quadratic residues modulo $p$. This is a list of $\frac{1}{2}(p-1)$ quadratic residues, but there are only $\frac{1}{2}(p-1)$ quadratic residues, so the rest of the powers $g^k$ must be quadratic nonresidues — these are exactly the odd powers of $g$. □

(b) Use (a) to prove that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

*Proof.* If either $p \mid a$ or $p \mid b$, there is nothing to do, so suppose $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Pick a primitive root $g$ modulo $p$, and write $a = g^k$ and $b = g^\ell$. Then $ab = g^{k+\ell}$, and part (a) shows that for any $x = g^m$, we have $\left(\frac{x}{p}\right) = (-1)^m$. Hence $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^k(-1)^\ell = (-1)^{k+\ell} = \left(\frac{ab}{p}\right)$ as claimed. In particular, the product of two nonresidues is a residue. □

(c) Use (a) to give a quick proof of Euler's Criterion $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

*Proof.* If $p \mid a$, there is nothing to do; otherwise, write $a = g^k$ for some primitive root $g$. If $k$ is even, then $\left(\frac{a}{p}\right) = (-1)^k = 1$ by part (a), but now $k = 2m$ (for some $m \in \mathbb{Z}$) so that $a^{(p-1)/2} \equiv (g^{2m})^{(p-1)/2} = g^{m(p-1)} = (g^{p-1})^m \equiv 1 = \left(\frac{a}{p}\right)$.

On the contrary, if $k$ is odd, then $\left(\frac{a}{p}\right) = (-1)^k = -1$ by part (a), but now writing $k = 2j+1$ and reusing our work from part (a)

$$a^{\frac{1}{2}(p-1)} \equiv (g^{2j+1})^{\frac{1}{2}(p-1)} \equiv g^{\frac{1}{2}(2jp-2j+p-1)} \equiv g^{\frac{1}{2}(p-1)} \pmod{p}.$$

Clearly, $(g^{\frac{1}{2}(p-1)})^2 \equiv 1$ by Fermat's Little Theorem, so $g^{\frac{1}{2}(p-1)} \equiv \pm 1$. Since $g$ is a primitive root, we must pick the $-$ sign, so it follows that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$. □

**Silverman 29.3: Indices**

This exercise concerns relations among indices.

(a) If $a, b$ satisfy the relation $ab \equiv 1 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related to each other?

*Solution.* We have $I(1) = 0$. Thus taking indices of both sides yields $I(ab) \equiv I(1) \equiv 0 \pmod{p-1}$, which implies $\boxed{I(a) \equiv -I(b) \pmod{p-1}}$. •

(b) If $a, b$ satisfy the relation $a + b \equiv 0 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related to each other?

*Solution.* We have $a \equiv -b \pmod{p}$, so taking indices of both sides yields $I(a) \equiv I(-b) \pmod{p-1}$, but now $I(-b) = I(-1 \cdot b) = I(-1) + I(b)$. To compute $I(-1)$, notice that $0 = I(1) \equiv I(-1 \cdot -1) = 2I(-1) \pmod{p-1}$, so $I(-1) = \frac{p-1}{2}$. Hence our relation is $\boxed{I(a) \equiv \frac{p-1}{2} + I(b) \pmod{p-1}}$. •

**Silverman 29.4: The Congruence $x^k \equiv a$**

This exercise concerns solutions to $x^k \equiv a \pmod{p}$.

(a) If $k \mid p-1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exact $k$ distinct solutions modulo $p$.

*Proof.* Just take indices of both sides with respect to some primitive root $g$ to obtain $kI(x) \equiv 0 \pmod{p-1}$. Since $k \mid p-1$, we see $\gcd(k, p-1) = k$, so there are $k$ distinct solutions to this linear congruence, say $y_1, y_2, \ldots, y_k$; we may arrange $0 \le y_i < p-1$ for each solution. Since $g$ is a primitive root, the numbers $g^{y_i}$ are all distinct modulo $p$, which completes the proof. □

(b) More generally, consider the congruence $x^k \equiv a \pmod{p}$. Find a simple way to use the values $k, p, I(a)$ to determine how many solutions this congruence has.

*Solution.* Taking indices again, we have $kI(x) \equiv I(a) \pmod{p-1}$. This linear congruence has solutions if and only if $\gcd(k, p-1) \mid I(a)$. In this case, there are $\gcd(k, p-1)$ solutions, and otherwise, there are 0 solutions. •

(c) The number 3 is a primitive root modulo $p = 1987$. How many solutions are there to $x^{111} \equiv 729 \pmod{1987}$?

*Solution.* Taking indices with respect to 3 and noting $729 = 27^2 = 3^6$, we have $111I(x) \equiv 6 \pmod{1986}$. Now, $111 = 3 \times 37$ and 1986 is divisible by 3 but not 37, so $\gcd(111, 1986) = 3$, which divides 6. Hence, there are $\boxed{3}$ solutions. •

# 205 Homework 5: Pell's Equation

### Silverman 32.1: A Trivial "Pell" Equation

What are the positive integer solutions to the equation $x^2 - A^2y^2 = 1$, where $A$ is an integer?

*Solution.* In this case, we may write $(x - Ay)(x + Ay) = 1$, but since $x$ and $y$ are positive integers, we are forced to have $x + Ay = 1$, so that $x - Ay = 1$. Now $x + Ay = x - Ay$, so $Ay = -Ay$, which implies $y = 0$ because $A \neq 0$. This means $1 = x + Ay = x + 0$, so $x = 1$. Hence, the only non-negative integer solution is $(1, 0)$, but then this implies there are no *positive* integer solutions. •

[Here, we omitted two exercises because we placed them in the main notes as the first proof of Theorem 70.1.]

### Silverman 33.4: There Was an Attempt to Approximate $\sqrt{2}$

Dirichlet's Diophantine Approximation Theorem tells us that there are infinitely many pairs of positive integers $(x, y)$ with $|x - y\sqrt{2}| < 1/y$. This exercise sees if we can do better.

(a.i) For each of the following $y$'s given, find and $x$ such that $|x - y\sqrt{2}| < \frac{1}{y}$.

*Solution.* We make our table below. Computations are done by Wolfram-Alpha — we type in the equation $|x - y^*\sqrt{2}| < \frac{1}{y^*}$ for the value of $y$ we are interested in.

| $y$ | 12 | 17 | 29 | 41 | 70 | 99 | 169 | 239 | 408 | 577 | 985 | 1393 | 2378 | 3363 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | 17 | 24 | 41 | 58 | 99 | 140 | 239 | 338 | 577 | 816 | 1393 | 1970 | 3363 | 4756 |

•

(a.ii) For each of the $y$'s above, compute the quantities $y|x - y\sqrt{2}|$ and $y^2|x - y\sqrt{2}|$. Can you make a guess as to the smallest possible value of $y|x - \sqrt{2}|$?

*Solution.* We make our table below, with the help of Desmos.

| $y$ | 12 | 17 | 29 | 41 | 70 | 99 | 169 |
|---|---|---|---|---|---|---|---|
| $y\left\|x - y\sqrt{2}\right\|$ | 0.3532 | 0.7077 | 0.3536 | 0.7070 | 0.3535 | 0.7071 | 0.3536 |
| $y^2\left\|x - y\sqrt{2}\right\|$ | 4.2390 | 12.031 | 10.255 | 28.987 | 24.748 | 70.005 | 59.751 |

| $y$ | 239 | 408 | 577 | 985 | 1393 | 2378 | 3363 |
|---|---|---|---|---|---|---|---|
| $y\left\|x-y\sqrt{2}\right\|$ | 0.7071 | 0.3536 | 0.7071 | 0.3536 | 0.7071 | 0.3536 | 0.7071 |
| $y^2\left\|x-y\sqrt{2}\right\|$ | 169.00 | 144.25 | 408.00 | 348.25 | 985.00 | 840.75 | 2378.00 |

The number 0.7071 looks suspiciously close to $\dfrac{\sqrt{2}}{2} \approx 0.70710678118$, so the smallest possible value of $y|x-y\sqrt{2}|$ seems to "converge" towards $\dfrac{\sqrt{2}}{2}$, as well as half of that value, $\dfrac{\sqrt{2}}{4}$. •

(b) Prove that the following two statements are true for every pair of positive integers $(x, y)$: (1) that $|x^2 - 2y^2| \geq 1$ and (2) if $|x - y\sqrt{2}| < \frac{1}{y}$, then $x + y\sqrt{2} < 2y\sqrt{2} + \frac{1}{y}$. Does this explain your computations in (a)?

*Proof.* For (1), we know that $|x^2 - 2y^2| \geq 1$ as long as $x^2 \neq 2y^2$, as both $x, y$ are positive integers. If for contradiction we have that $x^2 = 2y^2$, then $(x/y)^2 = 2$ so that $\sqrt{2} = x/y$ is rational, which is a contradiction. This establishes (1).

For (2), suppose that $\left|x - y\sqrt{2}\right| < \frac{1}{y}$. Then certainly $x - y\sqrt{2} < \frac{1}{y}$, so that adding $2y\sqrt{2}$ to both sides yields $x + y\sqrt{2} < 2y\sqrt{2} + \frac{1}{y}$ as claimed. □

To explain the computations of part (a), we write

$$1 \leq \left|x^2 - 2y^2\right| = \left|x - y\sqrt{2}\right| \left|x + y\sqrt{2}\right| = \left|x - y\sqrt{2}\right| \left(2y\sqrt{2} + \frac{1}{y}\right).$$

This implies that

$$\left|x - y\sqrt{2}\right| \geq \frac{1}{2y\sqrt{2} + \frac{1}{y}} \overset{y\to\infty}{\approx} \frac{1}{2y\sqrt{2}} = \frac{1}{y} \cdot \frac{\sqrt{2}}{4},$$

so that $y\left|x - y\sqrt{2}\right|$ stays *roughly* above $\sqrt{2}/4 \approx 0.35355339059$, as we saw in part (a).

**Silverman 34.1: The Negative Pell Equation**

In this chapter we have shown that the Pell's Equation $x^2 - Dy^2 = 1$ always has a solution in positive integers. This exercise explores what happens if the 1 on the right-hand side is replaced by some other number.

(a) For each $2 \leq D \leq 15$ that is not a perfect square, determine whether the equation $x^2 - Dy^2 = -1$ has a solution in positive integers. Can you determine a pattern that lets you predict for which $D$'s it has a solution?

*Solution.* For $D = 2$, we have the solution $1^2 - 2(1)^2 = -1$.

When $D = 3$, we have $x^2 - 3y^2 = -1$, so that $x^2 + 1 = 3y^2$. Reducing modulo 3, we have $x^2 + 1 \equiv 0 \pmod 3$, but we know that this is irreducible, so there are no solutions.

When $D = 5$, we have $x^2 + 1 = 5y^2$. Reducing modulo 5, we have $x^2 + 1 \equiv 0 \pmod 5$, so we try $x = 2$: indeed, this gives us the solution $(2, 1)$.

When $D = 6$, we have $x^2 + 1 = 6y^2$. Reducing modulo 3, observe that we get $x^2 + 1 \equiv 0 \pmod 3$ again, which has no solution. By the same argument, we conclude that when $D = 3n$, we have no solutions, so there is no need to check these.

When $D = 7$, we have $x^2 + 1 = 7y^2$. Reducing modulo 7, we have $x^2 + 1 \equiv 0 \pmod 7$, which by quadratic reciprocity has no solutions. In general, if $D = 4k + 3$ is prime, then quadratic reciprocity tells us we have no solutions.

When $D = 8$, we have $x^2 + 1 = 8y^2$. Reducing modulo 8, we have $x^2 + 1 \equiv 0 \pmod 8$, which has no solutions.

When $D = 10$, we have $x^2 + 1 = 10y^2$. From here, it is not too hard to see that $(3, 1)$ is a solution.

When $D = 13$, we have $x^2 + 1 = 13y^2$. Reducing modulo 13, we get $x^2 \equiv -1 \pmod{13}$, which has a solution by quadratic reciprocity, namely $x \equiv 5, 8 \pmod{13}$. However, neither of these give solutions until we try $x = 13 + 5 = 18$, so that $18^2 + 1 = 325 = 13(5)^2$.

When $D = 14$, there are no solutions after reducing modulo 7.

When $D = 17$, we have $x^2 + 1 = 17y^2$. Reducing modulo 17, we have $x^2 \equiv -1 \pmod{17}$, which has solutions by quadratic reciprocity, namely $x = 4, 13$. We observe that $(4, 1)$ is thus a solution.

Finally, when $D = 20$, we have $x^2 + 1 = 20y^2$. But looking at this modulo 4, we have $x^2 + 1 \equiv 0$, which has no solutions.

In summary, our table of solutions is given below.

| $D$ | 2 | 3 | 5 | 6 | 7 | 8 | 10 | 11 | 12 | 13 | 14 | 15 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Solution? | Y | N | Y | N | N | N | Y | N | N | Y | N | N | Y | N | N | N |

It seems like whether we have a solution is intimately related with quadratic reciprocity, so it might be easier to determine when $x^2 + 1 = Dy^2$ *does not* have a solution. First, if $D$ is divisible by any prime $p$ congruent to 3 (mod 4), then reducing modulo $p$ gives $x^2 + 1 \equiv 0 \pmod p$, which has no solutions by quadratic reciprocity. Second, if $D$ is divisible by $2^\alpha$ for any $\alpha \geq 2$, looking at the equation modulo 4 gives $x^2 + 1 \equiv 0 \pmod 4$, which has no solutions. However, for anything else (i.e., for $D$ of the form $2^k p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $p_i \equiv 1 \pmod 4$ and $k = 0, 1$), the pattern seems to be much less predictable. For example, it is not always the case that if $x^2+1 = D_1y^2$ and $x^2+1 = D_2y^2$ have solutions, then $x^2+1 = D_1D_2y^2$ has a solution; this works when $(D_1, D_2) = (2, 5)$ but not when $(D_1, D_2) = (2, 17)$, which we can check by querying Wolfram-Alpha for integer solutions of $x^2 + 1 = 34y^2$. •

(b) If $(x_0, y_0)$ is a solution to $x^2 - Dy^2 = -1$ in positive integers, show that $(x_0^2 + Dy_0^2, 2x_0y_0)$ is a solution to Pell's equation $x^2 - Dy^2 = 1$.

*Proof.* We just plug in and note the relation $x_0^2 - Dy_0^2 = -1$:

$$\begin{aligned}(x_0^2 + Dy_0^2)^2 - D(2x_0y_0)^2 &= x_0^4 + D^2y_0^4 + 2Dx_0^2y_0^2 - 4Dx_0^2y_0^2 \\ &= x_0^4 - 2Dx_0^2y_0^2 + D^2y_0^4 \\ &= (x_0^2 - Dy_0^2)^2 = (-1)^2 = 1,\end{aligned}$$

so we are done. □

(c) Find a solution to $x^2 - 41y^2 = -1$ by brute force, and use it to find a solution to the Pell's equation $x^2 - 41y^2 = 1$.

*Solution.* We consider the quantities $41y^2 - 1$. By calculator, we plug in $y = 1, 2, \ldots$, we see $41(5)^2 - 1 = 1024 = 32^2$. Hence, a solution is $(32, 5)$. Using part (b), we have that $(32^2 + 41 \cdot 5^2, 2 \cdot 32 \cdot 5) = \boxed{(2049, 320)}$ is a solution to $x^2 - 41y^2 = 1$. •

(d.i) If $(x_0, y_0)$ solves $x^2 - Dy^2 = M$, and if $(x_1, y_1)$ solves $x^2 - Dy^2 = 1$, show that $(x_0x_1 + Dy_0y_1, x_0y_1 + y_0x_1)$ is a solution to the equation $x^2 - Dy^2 = M$.

*Proof.* Again, we prove by plugging in, and noting that $x_0^2 - Dy_0^2 = M$ and $x_1^2 - Dy_1^2 = 1$.

$$\begin{aligned}(x_0x_1 + Dy_0y_1)^2 - D(x_0y_1 + y_0x_1)^2 &= D^2y_0^2y_1^2 - Dx_1^2y_0^2 - Dx_0^2y_1^2 + x_0^2x_1^2 \\ &= Dy_0^2(Dy_1^2 - x_1^2) + x_0^2(-Dy_1^2 + x_1^2) \\ &= -Dy_0^2(x_1^2 - Dy_1^2) + x_0^2(x_1^2 - Dy_1^2) \\ &= (x_0^2 - Dy_0^2)(x_1^2 - Dy_1^2) \\ &= M \cdot 1 = M,\end{aligned}$$

which completes the proof. □

(d.ii) Use (d.i) to find five different solutions in positive integers to the equation $x^2 - 2y^2 = 7$.

*Solution.* First, notice that $(x_0, y_0) = (3, 1)$ satisfies $3^2 - 2(1)^2 = 3 - 2 = 7$, and we know the solutions to $x^2 - 2y^2 = 1$ are given by raising $(3 + 2\sqrt{2})$ to powers. We take the first 5 solutions: $(3, 2), (17, 12), (99, 70), (577, 408), (3363, 2378)$, and do the computation as described in (d.i) to obtain the solutions

$$\boxed{(13, 9), (75, 53), (437, 309), (2547, 1801), (14845, 10497)}.$$

•

**Silverman 34.2: Some "Pell-like" Equations**

Find a solution to the following equations, or show that none exist.

(a) $x^2 - 11y^2 = 7$.

*Solution.* We look at the equation modulo 11 to obtain $x^2 \equiv 7 \pmod{11}$. Then by quadratic reciprocity, we have $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1$, so this equation has no solutions, because the related congruence has no solutions. •

(b) $x^2 - 11y^2 = 433$.

*Solution.* Again, reduce modulo 11 to obtain $x^2 = 4 \pmod{11}$. Clearly, we observe $x \equiv 2, 9 \pmod{11}$, so this tells us what values of $x$ to try. We must have $x^2 = 11y^2 + 433$, which implies $x \geq 21$. This means we check $(x^2 - 433)/11$ for $x = 24, 31, 35, 42, 46, 53, \ldots$ and hope one of them gives a perfect square. Luckily, 42 gives a solution, so we have $\boxed{(42, 11)}$. •

(c) $x^2 - 11y^2 = 3$.

*Solution.* Again, reduce modulo 11 to obtain $x^2 = 3 \pmod{11}$, and quadratic reciprocity tells us that $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = +1$, so if we have a solution $(x, y)$, we must have $x \equiv 5, 6$. If we try to search for solutions, we get stuck, so we try reducing modulo the other sensible thing: 3, to obtain $x^2 - 2y^2 \equiv 0 \pmod{3}$. This means $x^2 \equiv 2y^2 \pmod{3}$, but 2 is not a quadratic residue modulo 3, so $x$ and $y$ are multiples of 3. But this is impossible as then $9 \mid (x^2 - 11y^2) = 3$, so not solutions can exist. •

# 206 Homework 6: Continued Fractions

### Nathanson 1.3.13: Convergents Spaced 2 Apart

Let $[a_0; a_1, a_2, \ldots, a_N]$ be a finite simple continued fraction, and let $p_n/q_n$ be the convergents. Prove that $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ for $n = 2, 3, \ldots, N$.

*Proof.* This seems like an induction exercise, but induction is actually unnecessary here, because we have already done the induction to prove the recursion formula. We compute

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n p_{n-1} q_{n-2} + \cancel{p_{n-2} q_{n-2}} - a_n p_{n-2} q_{n-1} - \cancel{p_{n-2} q_{n-2}} \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= -a_n (p_{n-2} q_{n-1} - p_{n-1} q_{n-2}) \\ &= -a_n (-1)^{n-1} \\ &= a_n (-1)^n, \end{aligned}$$

where the last step follows from a theorem proven in lecture. This completes the proof. □

### Nathanson 1.3.14: Successive Convergents Alternate

Let $x := [a_0; a_1, \ldots, a_N]$ be a finite simple continued fraction. Prove that the even convergents are strictly increasing, the odd convergents are strictly decreasing, and that the odd convergents are always greater than the even convergents, i.e.,

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots \leq x \leq \cdots \leq \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

*Proof.* By virtue of the previous exercise, write

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}} \neq 0. \tag{13}$$

Now, because we are working with a finite simple continued fraction, the $a_i$ are all positive; it follows from the recursion formula that the $q_i$ are all positive. Hence the difference in (13) is positive whenever $n$ is even, and negative whenever $n$ is odd, giving us that the odd convergents are strictly decreasing and the even convergents are strictly increasing.

Now, to show that the odd convergents are always greater than the even convergents, it suffices to show that if $j$ is odd, then $p_j/q_j > p_{j+1}/q_{j+1}$. We compute

$$\frac{p_j}{q_j} - \frac{p_{j+1}}{q_{j+1}} = \frac{p_j q_{j+1} - p_{j+1} q_j}{q_j q_{j+1}} = \frac{(-1)^{j+1}}{q_j q_{j+1}} = \frac{1}{q_j q_{j+1}} > 0$$

by evenness of $j + 1$. Hence, the claim follows. □

### Silverman 47.6: Convergents Are Already Reduced

Prove that, given a convergent $p_n/q_n$, that $\gcd(p_n, q_n) = 1$, i.e., that whatever convergent we get is already in lowest terms.

*Proof.* By Theorem 47.2 in the text, we see that $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$ for all $n \geq 0$. But the $p_i$ and $q_i$ are all integers, but this exactly means that we have found integers $x, y$ such that $p_n x + q_n y = \pm 1$; just take $x = q_{n+1}$ and $y = -p_{n+1}$. By Bézout's Lemma, we have $\gcd(p_n, q_n) = 1$, which establishes the claim. □

**Silverman 47.9: Reversing the Partial Quotients**

In this exercise, we consider reversing the partial quotients.

(a) How are the numerators of $[a;b]$ and $[b;a]$ related to each other?

*Solution.* We have $[a;b] = a + \dfrac{1}{b} = \dfrac{ab+1}{b}$ and $[b;a] = b + \dfrac{1}{a} = \dfrac{ab+1}{a}$. We see that the numerators are **equal**. •

(b) How are the numerators of $[a;b,c]$ and $[c;b,a]$ related to each other?

*Solution.* A slightly longer computation reveals that

$$[a;b,c] = a + \frac{1}{[b,c]} = a + \frac{c}{bc+1} = \frac{a(bc+1)+c}{bc+1} = \frac{abc+a+c}{bc+1} \text{ and}$$
$$[c;b,a] = c + \frac{1}{[b,a]} = c + \frac{a}{ab+1} = \frac{c(ab+1)+a}{ab+1} = \frac{abc+c+a}{ab+1},$$

and again, the numerators are the **same**. •

(c) More generally, how do the numerators of $[a_0,\ldots,a_n]$ and $[a_n,\ldots,a_0]$ relate to each other?

*Solution.* We claim that the numerators are $\boxed{\text{equal}}$. •

(d) Prove that your conjecture in (c) is correct.

*Proof.* We proceed by induction on $n \geq 0$. The base case $n = 0$ is trivial to check, so suppose the inductive hypothesis holds for some $n$, i.e., the numerators of $[a_0;\ldots,a_n]$ and $[a_n;\ldots,a_0]$ match; call this numerator $p$. Call the denominator of $[a_0;a_1,\ldots,a_n]$ by $q_1$ and the denominator of $[a_n;a_{n-1},\ldots,a_0]$ by $q_2$. That is, write $[a_0;a_1,\ldots,a_n] = p/q_1$ and $[a_n;a_{n-1},\ldots,a_0] = p/q_2$. Then

$$[a_0;a_1,\ldots,a_n,a_{n+1}] = \left[a_0;a_1,\ldots,a_n + \frac{1}{a_{n+1}}\right]$$

has the same numerator as $\left[a_n + \dfrac{1}{a_{n+1}};a_{n-1},\ldots,a_1,a_0\right]$ (by the induction hypothesis); call it $p'$. But now

$$\left[a_n + \frac{1}{a_{n+1}};a_{n-1},\ldots,a_1,a_0\right] = \frac{1}{a_{n+1}} + [a_n;a_{n-1},\ldots,a_1,a_0] = \frac{1}{a_{n+1}} + \frac{p}{q_2} = \frac{q_2+pa_{n+1}}{q_2}$$

has numerator $p' = q_1 + pa_{n+1}$. Now applying the inductive hypothesis again, observe that we have

$$[a_{n+1};a_n,\ldots,a_1,a_0] = a_{n+1} + \frac{1}{[a_n;a_{n-1},\ldots,a_1,a_0]} = a_{n+1} + \frac{q_2}{p} = \frac{a_{n+1}p+q_2}{a_{n+1}p} = \frac{p'}{p}.$$

This completes the induction and thus the proof. □

**Silverman 48.3: The Continued Fraction** $[b_1; b_2, \ldots, b_n, B]$

We have seen before that

$$[b_1; b_2, B] = \frac{(b_1 b_2 + 1)B + b_1}{b_2 B + 1}.$$

(a) Simplify $[b_1; b_2, b_3, B]$.

*Solution.* Using the above, write

$$\begin{aligned}
[b_1; b_2, b_3, B] &= b_1 + \frac{1}{[b_2; b_3, B]} \\
&= b_1 + \frac{b_3 B + 1}{(b_2 b_3 + 1)B + b_2} \\
&= \frac{b_1[(b_2 b_3 + 1)B + b_2] + b_3 B + 1}{(b_2 b_3 + 1)B + b_2} \\
&= \frac{b_1 b_2 b_3 B + b_1 B + b_1 b_2 + b_3 B + 1}{(b_2 b_3 + 1)B + b_2} \\
&= \frac{(b_1 b_2 b_3 + b_1 + b_3)B + b_1 b_2 + 1}{(b_2 b_3 + 1)B + b_2}.
\end{aligned}$$

•

(b) Simplify $[b_1; b_2, b_3, b_4, B]$.

*Solution.* Using the above, write

$$\begin{aligned}
[b_1; b_2, b_3, b_4, B] &= b_1 + \frac{1}{[b_2; b_3, b_4, B]} \\
&= b_1 + \frac{(b_3 b_4 + 1)B + b_3}{(b_2 b_3 b_4 + b_2 + b_4)B + b_2 b_3 + 1} \\
&= \frac{b_1[(b_2 b_3 b_4 + b_2 + b_4)B + b_2 b_3 + 1] + (b_3 b_4 + 1)B + b_3}{(b_2 b_3 b_4 + b_2 + b_4)B + b_2 b_3 + 1} \\
&= \frac{(b_1 b_2 b_3 b_4 + b_1 b_2 + b_1 b_4 + b_3 b_4 + 1)B + b_1 b_2 b_3 + b_1 + b_3}{(b_2 b_3 b_4 + b_2 + b_4)B + b_2 b_3 + 1}.
\end{aligned}$$

•

(c) Look at your answers in (a) and (b), and compare them to $[b_1, b_2]$, $[b_1, b_2, b_3]$, and $[b_1, b_2, b_3, b_4]$.

*Solution.* Let $p_n$ denote the numerator of the convergent $[b_1, \ldots, b_n]$, and $q_n$ denote its denominator. [Annoyingly, the indices are shifted by 1 from the text.] Then we notice

$$\begin{aligned}
[b_1; b_2, B] &= \frac{p_2 B + p_1}{q_2 B + q_1} \\
[b_1; b_2, b_3, B] &= \frac{p_3 B + p_2}{q_3 B + q_2} \\
[b_1; b_2, b_3, b_4, B] &= \frac{p_4 B + p_3}{q_4 B + q_3}.
\end{aligned}$$

•

(d) More generally, when the continued fraction $[b_1, b_2, \ldots, b_m, B]$ is simplified as

$$[b_1, b_2, \ldots, b_m, B] = \frac{u_m B + v_m}{w_m B + z_m},$$

explain how the numbers $u_m, v_m, w_m, z_m$ can be described in terms of the convergents $[b_1, b_2, \ldots, b_{m-1}]$ and $[b_1, b_2, \ldots, b_m]$. Prove that your description is correct.

We claim that $[b_1; b_2, \ldots, b_m, B] = \dfrac{p_m B + p_{m-1}}{q_m B + q_{m-1}}$.

*Proof.* The proof is a straightforward induction exercise. We have already shown that the base case holds. Now assume the inductive hypothesis, so that the claim holds for some $m \geq 1$. Then

$$\begin{aligned}
[b_1; b_2, \ldots, b_m, b_{m+1}, B] &= \left[b_1; b_2, \ldots, b_m, b_{m+1} + \frac{1}{B}\right] \\
&= \frac{p_m\left(b_{m+1} + \frac{1}{B}\right) + p_{m-1}}{q_m\left(b_{m+1} + \frac{1}{B}\right) + q_{m-1}} \\
&= \frac{p_m b_{m+1} + \frac{p_m}{B} + p_{m-1}}{q_m b_{m+1} + \frac{q_m}{B} + q_{m-1}} \\
&= \frac{B p_m b_{m+1} + B p_{m-1} + p_m}{B q_m b_{m+1} + B q_{m-1} + q_m} \\
&= \frac{B p_{m+1} + p_m}{B q_{m+1} + q_m},
\end{aligned}$$

where the second equality follows from the induction hypothesis and the last equality follows from the recurrence rule. This completes the induction. □