UC Irvine Math 180A Winter 2024

Number Theory I

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

March 2024
Lecture Note Series #**6**

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.

Date	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. A prerequisite to this course is Math 13, which covers some basic number theory, so these notes might frequently gloss over the basics, or invoke concepts before they have been formally introduced in lecture.

13 Basic Properties of Numbers

If we want to study numbers, then we should understand the basic building blocks of the numbers we are studying, which in this course, is the natural numbers $\mathbb{N} := \{0, 1, 2, \ldots\}$. A very natural thing about the natural numbers is their order, for example

$$0 < 1 < 2 < 3 < \cdots .$$

This is not the only type of order we can define (later, we will see an important type of order that is not $<$), so we make the following definition.

Definition 13.1. Let A be a nonempty set. A relation $\preceq$ on A is called a *partial order* on A if it is reflexive, antisymmetric, and transitive. If we have further that for all $a, b \in A$, we have $a \preceq b$ or $b \preceq a$, we call $\preceq$ a *total order* on A.

For example, we can verify that $\leq$, the standard "less-than-or-equal-to," is a total order on all of $\mathbb{N}$. Total orders have nice properties.

Proposition 13.2. *Let A be a nonempty set, and let $\preceq$ be a total order on A. Then any finite, non-empty subset $S \subseteq A$ has a maximum and minimum with respect to $\preceq$.*

Proof. Induction. □

In particular, when $A = \mathbb{N}$, we get this property, which we use implicitly in proofs:

Theorem 13.3 (Well-Ordering Property of $\mathbb{N}$)**.** *Every nonempty subset of $\mathbb{N}$ has a minimum.*

Example 13.4. Show that every integer at least 2 has a prime factor.

Proof. Suppose otherwise, so that there is a *minimal* $n \in \mathbb{N}_{\geq 2}$ lacking a prime factor. If $k \mid n$ for all $2 \leq k \leq n - 1$, then n is prime and thus is its own prime factor, a contradiction. Otherwise, $n = jm$ for $2 \leq j, m \leq n - 1$. But now, by minimality of n, both j and m have prime factors, which is a contradiction as now n has prime factors. □

Example 13.5. Show that there are infinitely many ordered pairs $(x, y) \in \mathbb{N}^2$ such that $x^2 - 2y^2 = \pm 1$.

Proof. First of all, these pairs exist, and the first few smallest examples are $(1, 0), (1, 1), (3, 2)$, $(7, 5)$, and $(17, 12)$. Suppose there exist finitely many such (x, y), so take

$$S := \{x \in \mathbb{N} : \text{there exists } y \in \mathbb{N} \text{ with } x^2 - 2y^2 = \pm 1\},$$

which most also be finite. Hence, S has a maximum, so take $X := \max S$, and find some Y such that $X^2 - 2Y^2 = \pm 1$. But now take $Y_1 := X + Y$ and $X_1 := X + 2Y$, so that

$$\begin{aligned} X_1^2 - 2Y_1^2 &= (X + 2Y)^2 - 2(X + Y)^2 \\ &= X^2 + 4XY + 4Y^2 - 2X^2 - 4XY - 2Y^2 \\ &= -X^2 + 2Y^2 = \mp 1, \end{aligned}$$

which means $X_1 \in S$. But now $X_1 > X$, which is a contradiction. □

14 Pythagorean Triples

Recall that the side lengths $a < b < c$ of a right triangle satisfy the equation $a^2 + b^2 = c^2$ by the Pythagorean Theorem. As a motivating example of number theory, we will study these special triangles; in particular, we want to find all right triangles with integer side lengths. We make the following definition.

Definition 14.1. A *Pythagorean triple* is a triple of positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$.

Example 14.2. We know that $(3, 4, 5)$ is a Pythagorean triple, as $3^2 + 4^2 = 5^2$. Notice that this one triple generates an infinite set of triples, namely $(3n, 4n, 5n)$ for all $n \in \mathbb{Z}^+$. Hence, Pythagorean triples are abundant, but not all of them are "interesting," in the way we shall quantify below.

Definition 14.3. A *primitive Pythagorean triple* (a PPT) is a Pythagorean triple (a, b, c) such that $\gcd(a, b, c) = 1$.

By dividing out common factors, say out of $(6, 8, 10)$, we can always arrive back at a PPT, in this case $(3, 4, 5)$. Hence, to understand all Pythagorean triples, it suffices to understand PPTs. We get the following preliminary facts about PPTs, which will later allow us to find all of them.

Lemma 14.4. *If (a, b, c) is a primitive Pythagrean triple, then exactly one of a, b is odd.*

Proof. If a, b are both even, then $c^2 = a^2 + b^2$ is even, but this is only possible if c is even. Hence $\gcd(a, b, c) \geq 2$, a contradiction. Now, assume for contradiction that both a and b are odd. Then we may write $a = 2x + 1$ and $b = 2y + 1$, for $x, y \in \mathbb{Z}$. Now a computation shows

$$c^2 = a^2 + b^2 = 4(x^2 + y^2) + 4(x + y) + 2,$$

so this forces c^2 to be even, and hence c to be even. But if c is even, then c^2 must be divisible by 4, a contradiction to the above. □

The above lemma narrows down a lot of possible PPTs already. Hence, let (a, b, c) be a PPT, and suppose without loss of generality that a is odd and b is even. We know $a^2 + b^2 = c^2$, so that $c^2 - b^2 = a^2$, i.e.,

$$a^2 = (c - b)(c + b).$$

Clearly, the factors $c \pm b$ are important, and testing numbers will reveal that it seems like $\gcd(c - b, c + b) = 1$. This is in fact the case.

Lemma 14.5. *Let (a, b, c) be a primitive Pythagorean triple. Then $\gcd(c - b, c + b) = 1$.*

Proof. Suppose d is a common divisor of the $c \pm b$. Then[1] $d \mid (c - b + c + b) \iff d \mid 2c$, and a similar argument shows $d \mid 2b$. If $\gcd(b, c) \neq 1$, then it is easy to see $\gcd(a, b, c) \neq 1$, a contradiction the fact that (a, b, c) is a PPT, so we have $\gcd(b, c) = 1$. Since c is odd and b is even (notice that we assumed without loss of generality b is even, and thus $a^2 + b^2 = c^2$ is odd), both $c \pm b$ are odd, implying d is odd. Hence $d \mid b$ and $d \mid c$ (as $\gcd(2, d) = 1$), and so $d \mid 1$, so $d = 1$. □

We know $a^2 = (c - b)(c + b)$, so because of this, the Fundamental Theorem of Arithmetic[2] tells us that $c \pm b$ are both perfect squares (count the primes in their prime factorizations). Hence, set $s^2 := c + b$ and $t^2 := c - b$. From the above proof, we can conclude that s, t are both odd, and this proves (after some algebra) the first half of the following theorem.

Theorem 14.6. *Every PPT (a, b, c), with a odd and b even has the form*

$$a = st, b = \frac{1}{2}(s^2 - t^2), c = \frac{1}{2}(s^2 + t^2),$$

where $s > t \geq 1$ are odd integers with $\gcd(s, t) = 1$, and every pair of such integers s, t gives a PPT.

Proof. All that is left is to show that any valid choices of s, t gives us a PPT, so let $s > t \geq 1$ be odd coprime integers. Define $a = st$, $b = \frac{1}{2}(s^2 - t^2)$, $c = \frac{1}{2}(s^2 + t^2)$ as in the theorem statement. It is easy to verify that a is odd and b is even, and that $a^2 + b^2 = c^2$. We are left to check $\gcd(a, b, c) = 1$, so assume for contradiction that p is a prime factor dividing a, b, and c. Then $p \mid a = st$, so that by Euclid's Lemma[3] $p \mid s$ or $p \mid t$. Doing other manipulations past this point will lead to a contradiction, so we are done. □

18 Pythagorean Triples and the Unit Circle

In this section, we take a second view at Pythagorean triples, which will be more geometric. If (a, b, c) is a Pythagorean triple, then $a^2 + b^2 = c^2$. But this also implies $(a/c)^2 + (b/c)^2 = 1$, so making the obvious change of variables $x := a/c$ and $y := b/c$, we get $x^2 + y^2 = 1$, which we recognize as the equation of the unit circle. Hence, it is evident to us that Pythagorean triples are intimately related to rational points on the unit circle, so it may be important to classify the rational points on the unit circle.

Theorem 18.1. *Every rational point (x, y) on the unit circle, except for $(-1, 0)$ takes the form*

$$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right),$$

[1] Recall from Math 13 that $a \mid b$ means "a divides b." We will discuss this in more depth later.

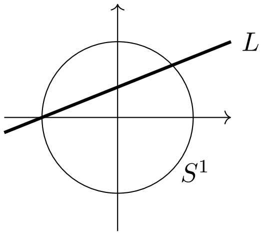
[2] We will cover this later, but this should have been covered in Math 13.

[3] Again, Math 13.

where $m \in \mathbb{Q}$, and every $m \in \mathbb{Q}$ gives such a point. That is, there is a bijection

$$\mathbb{Q} \leftrightarrow (S^1 \cap \mathbb{Q}^2) \setminus \{(-1,0)\}.$$

Proof. Clearly, $(-1,0)$ is a rational point on the unit circle. Draw a line L through $(-1,0)$ with rational slope m:



We claim that the intersection $L \cap S^1$ is a rational point. The equation of the line L is $y = m(x+1)$, so $L \cap S^1$ is the solution to the system of equations $y = m(x+1)$ and $x^2+y^2=1$. Substituting gives us the quadratic equation

$$(1+m^2)x^2 + 2m^2x + (m^2-1) = 0,$$

which is a quadratic we can solve by Vieta: we know $x = -1$ is already a root, as the line intersects the circle at the point we want to find **and** $(-1,0)$. We leave it for the reader to verify that the other root is $x = (1-m^2)/(1+m^2)$, from which our formula follows.

Conversely, let $(\alpha, \beta) \in S^1 \setminus \{(-1,0)\}$ be a rational point. Then, the line connecting $(-1,0)$ and (α,β) has rational slope, so it corresponds to one of the lines we have drawn in the first part of the proof. □

Now, using this, we may classify the Pythagorean triples again. Let $m = v/u$, where $v, u \in \mathbb{Z}$ with $u \neq 0$, so substituting into the formula given in the theorem above yields

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

so clearing denominators gives $x^2+y^2=1 \iff (u^2-v^2)^2+(2uv)^2=(u^2+v^2)^2$. This gives us a Pythagorean triple $(a,b,c) = (u^2-v^2, 2uv, u^2+v^2)$, which likely is not primitive, but can be reduced to a PPT if necessary.

This section concludes our brief, introductory study of the equation $x^2+y^2=z^2$. However, as mathematicians, we are obliged to generalize and consider the equation $x^n+y^n=z^n$, for $n \geq 3$. Suddenly, the problem becomes far more difficult (for reasons outside the scope of this course), and it was one of the triumphs of 20th century mathematics that finally solved this equation. We state this famous theorem below, and will obviously not prove it.

Theorem 18.2 (Fermat's Last Theorem)**.** *Let $n \geq 3$. Then $a^n+b^n=c^n$ has no positive integer solutions (a,b,c).*

23 Rational Points on Algebraic Curves

In the previous section, we considered the rational points on the unit circle $x^2+y^2=1$. Let us extend our viewpoint by seeing examples of rational points on other, similar curves.

Example 23.1. Let us find all of the rational points on the ellipse $C := \{(x,y) : 3x^2+4y^2 = 7\}$. Clearly, $(1,1)$ is such a rational point, so draw a line L through $(1,1)$. If L is a vertical line, then it intersects C at $(1,-1)$ only, so suppose L has rational slope m. Then L has the equation $y = m(x-1)+1$. Substituting this into the equation of the ellipse yields

$$3x^2 + 4\left(m(x-1)+1\right)^2 = 7 \iff (3+4m^2)x^2 + 8(1-m)mx + c = 0,$$

for some constant c, which is irrelevant by Vieta's Formulas: we know $x = 1$ is a root, and if r_2 is the other root, we have

$$1 + r_2 = -\frac{8(1-m)m}{3+4m^2} = \frac{8(m-1)m}{4m^2+3}, \text{so } r_2 = \frac{4m^2-8m-3}{4m^2+3}.$$

The corresponding y-value can be calculated from this, so the set of rational points on C is

$$C \cap \mathbb{Q}^2 = \boxed{\{(1,\pm 1)\} \cup \left\{\left(\frac{4m^2-8m-3}{4m^2+3}, \frac{-4m^2-6m+3}{4m^2+3}\right) : m \in \mathbb{Q}\right\}}.$$

Example 23.2. We prove that there is no rational point on the curve $x^2 + y^2 = 3$.

Proof. This argument uses some modular arithmetic, which one should review from Math 13. Suppose for contradiction that $(a/b, c/d)$ is a rational point on the circle $x^2+y^2 = 3$, where $\gcd(a,b) = 1 = \gcd(c,d)$. Then

$$3 = x^2 + y^2 = \frac{a^2}{b^2} + \frac{c^2}{d^2} = \frac{a^2d^2+b^2c^2}{b^2d^2} \iff 3(bd)^2 = (ad)^2 + (bc)^2,$$

in which the latter is an equation in all integers. Reducing it modulo 3, we obtain $0 \equiv (ad)^2 + (bc)^2 \pmod 3$, and now we notice by computation that for all $n \in \mathbb{Z}$, either $n^2 \equiv 0$ or $n^2 \equiv 1 \pmod 3$. This forces $(ad)^2 \equiv (bc)^2 \equiv 0 \pmod 3$, which is problematic in view of the original integer equation, as we can divide out a common factor of 3. □

We now examine an example of a cubic curve.

Example 23.3. We attempt to find all rational points on $C = \{(x,y) : y^2 = x^3 + 17\}$. We can verify that $(-2,3) \in C$, and we try drawing a line L through $(-2,3)$. In the case that L is vertical, we pass through the intersection point $(-2,-3) \in C$. Now, if L has rational slope, then L has equation $y = m(x+2)+3$, for some $m \in \mathbb{Q}$. Substituting into the equation of the curve C, we get a quadratic polynomial: however, this is problematic, as we cannot guarantee the rationality of the roots.

The above example demonstrates the difficulties in determining rational points for algebraic curves where the highest power is 3 or more — it turns out that cubic curves are at the very boundary of what modern mathematics is able to do. However, if we are given more points, we can at least reliably generate some rational points.

Example 23.4. Take the curve C as above in the given example. We already saw that $(-2,3) \in C$, and we can also verify that $(2,5) \in C$. Now, draw a line L through $(-2,3)$ and $(2,5)$, which has the equation $y = \frac{1}{2}x + 4$. Substituting this into the equation of C, we get

$$\left(\frac{1}{2}x + 4\right)^2 = x^3 + 17 \iff \frac{1}{4}(x+8)^2 = x^3 + 17$$

$$\iff x^2 + 16x + 64 = 4x^3 + 68 \iff 4x^3 - x^2 + 16x + 4 = 0.$$

We know two roots of this polynomial, namely $r_1 = -2$ and $r_2 = 2$. By Vieta, we see that if r_3 is the missing root,

$$r_1 + r_2 + r_3 = \frac{1}{4}, \text{ so } r_3 = \frac{1}{4}.$$

Substituting this into the equation of C gives the rational point $\boxed{\left(\frac{1}{4}, \frac{33}{8}\right)}$.

24 Divisibility

Recall the following facts about integers from Math 13. These definitions and theorems will form much of our discussion throughout the rest of the course.

Definition 24.1. Let $m, n \in \mathbb{Z}$. We say that m *divides* n if there exists some $k \in \mathbb{Z}$ sch that $n = k \cdot m$, and we write $m \mid n$.

To determine whether an integer divides another, we are accustomed to doing long division, which we rigorize as the division algorithm.

Theorem 24.2 (Division Algorithm). *For all $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.*

That is, "division with remainder" is something sane we can do over the integers.

Proof. [4] We first prove the existence of q and r. Fix $b > 0$, and we apply induction on non-negative $n \in \mathbb{Z}$. [Of course, we flip everything around as necessary when $a < 0$ or $b < 0$.] For $a = 0$, we simply set $q = r = 0$. Now, assume the inductive hypothesis, and $a = bq + r$ for $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, k-1\}$. We then see that $n + 1 = kq + r + 1$, and we consider 2 cases.

Case I: $r < b - 1$. In this case, there is nothing to do, simply set $q' = q$ and $r' = r + 1$. Notice that $r' \in \{0, 1, \ldots, k-1\}$ in this case, so this is legal. Hence $a + 1 = q'b + r'$.

Case II: $r = b - 1$. Then $a + 1 = bq + r + 1 = bq + (b - 1) + 1 = b(q + 1)$. Hence, set $r' = 0$ and $q' = q + 1$, so $a + 1 = q'b + r'$.

Now, we prove uniqueness. Fixing $b > 0$ (again, the proof for $b < 0$ is similar) and some $a \in \mathbb{Z}$, suppose $a = qb + r = q'b + r'$ for $q, q' \in \mathbb{Z}$ and $r, r' \in \{0, 1, \ldots, k-1\}$. It suffices to show $q = q'$ and $r = r'$.

First, we have $a = qb + r = q'b + r'$. By some algebra, we write this as $b(q - q') = r' - r$. Since $q - q'$ is an integer, we see by the definition of divisibility that $b \mid (r' - r)$. Without loss of generality, assume $r' \geq r$. But then $r', r \in \{0, 1, \ldots, k-1\}$ implies $r' - r \in \{0, 1, \ldots, k-1\}$, so the divisibility condition is impossible unless $r' = r$.

From the fact that $r' = r$, we simply have $qb + r = q'b + r' \implies qb = q'b \implies q = q'$, so we are done. □

Definition 24.3. Let $m, n \in \mathbb{Z} \backslash \{0\}$. The *greatest common divisor* (GCD) of m and n, denoted $\gcd(m, n)$, is the largest positive integer dividing both m and n. If $\gcd(m, n) = 1$, we say that m and n are *coprime* (or *relatively prime*).

To compute the GCD of two numbers, recall that we use the Euclidean algorithm, which is simply many iterations of the division algorithm that eventually terminates.

[4] This is an alternate proof that I learned in Math 13.

Example 24.4. We compute $\gcd(57970, 10353)$, by doing the division algorithm as follows:

$$\begin{aligned}
57970 &= 5 \cdot 10353 + 6205 \\
10353 &= 1 \cdot 6205 + 4148 \\
6295 &= 1 \cdot 4148 + 2057 \\
4148 &= 2 \cdot 2057 + 34 \\
2057 &= 60 \cdot 34 + 17 \\
34 &= 2 \cdot 17 + 0.
\end{aligned}$$

We read off the last non-zero remainder to get the GCD: $\gcd(57970, 10353) = \boxed{17}$.

The GCD also behaves nicely with respect to multiplication. We will see more examples of this later, but we prove one of these now.

Proposition 24.5. *Let a, b, c be nonzero integers. Then $\gcd(ka, kb) = k \gcd(a, b)$.*

Proof. Write $d := \gcd(a, b)$, and set $g := \gcd(ka, kb)$. It suffices to show $g \mid dk$ and $dk \mid g$. Obviously, $k \mid ka$ and $k \mid kb$, so $k \mid \gcd(ka, kb) \iff k \mid g$, by definition of GCD. This implies $g = kx$ for some $x \in \mathbb{Z}$. Now, $kx \mid ka$ and $kx \mid kb$, as $g = kx$, so that $x \mid a, b$, which implies $x \mid d$, so $kx \mid kd \iff g \mid dk$. Finally, note $d \mid a$ and $d \mid b$, so $kd \mid ka$ and $kd \mid kb$. By definition of GCD, $kd \mid g$, so $kd = g$. □

While the above proof is logically sound, it is rather confusing and obviously very convoluted. In the next few sections, we will develop ways to simply GCD proofs.

28 The Euclidean Algorithm and Bezout's Lemma

We have already seen how to use the Euclidean algorithm to quickly compute the greatest common divisor of two numbers. In this section, we prove that the algorithm works, and give some immediate, but very important consequences.

Theorem 28.1 (Euclidean Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$, and define $r_{-1} := a$, $r_0 = b$, and recursively $r_{i-1} = q_{i+1}r_i + r_{i+1}$, where q_{i+1}, r_{i+1} satisfy the conditions of the division algorithm. Then the last nonzero r_i is the greatest common divisor of a and b.*

Proof. We prove this theorem for the case where $a, b > 0$; it is similar if any of these are negative. We notice $r_1 > r_2 > r_3 > \cdots \geq 0$, so that well-ordering tells us that there must be a minimal r_i such that $r_i > 0$ but $r_j = 0$ for all $j > i$. Call $r_n > 0$ the last non-zero remainder. Now, we know $r_{n-1} = q_{n+1}r_n + 0$, so that $r_n \mid rn - 1$. Continuing inductively, we see $r_n \mid r_{n-1} \mid r_{n-2} \mid \cdots \mid r_1 \mid b \mid a$, so that $r_n \mid a$ and $r_n \mid b$. Hence, $r_n \mid \gcd(a, b)$.

Viewing this the other way, let d be the greatest common divisor of a and b. It thus follows that since $r_1 = a - q_1 b$, we have $d \mid r_1$. Continuing inductively, we observe $d \mid r_n$, so that $r_n = d = \gcd(a, b)$ as claimed. □

The fact that the Euclidean algorithm can be "reversed" as in the proof above gives the following consequences.

Corollary 28.2 (Bézout's Lemma)**.** *Let a, b be nonzero integers, and let $d := \gcd(a, b)$. Then the equation $ax + by = n$ has integer solutions (x, y) if and only if $d \mid n$.*

Theorem 28.3 (Linear Equation Theorem)**.** *Let a, b be nonzero integers, and let $d := \gcd(a, b)$. If $(x_1, y_1) \in \mathbb{Z}^2$ is an integer solution to $ax + by = d$, then all integer solutions to this equation are given by*

$$\left(x_1 + k \cdot \frac{b}{d}, y_1 - k \cdot \frac{a}{d}\right)$$

for any $k \in \mathbb{Z}$.

Proof. By Bézout's Lemma, this equation does indeed have integer solutions, so we suppose (x_1, y_1) is an integer solution. That $(x_1 + kb/d, y_1 - ka/d)$ is a solution for some $k \in \mathbb{Z}$ is obvious by substituting, so we just need to check that all solutions take this form. Notice that the equation $ax + by = d$ is equivalent to $\frac{a}{d}x + \frac{b}{d}y = 1$, so it just suffices to check integers a, b with $\gcd(a, b) = 1$.

Hence, suppose $\gcd(a, b) = 1$, and that (x_1, y_1) is an integer solution to $ax + by = 1$. If (x_2, y_2) is another solution, we get the system of equations

$$\begin{cases} ax_1 + by_1 = 1 \\ ax_2 + by_2 = 1, \end{cases}$$

which gives us $ax_1y_2 - ax_2y_1 = y_2 - y_1$. Set $k = x_2y_1 - x_1y_2 \in \mathbb{Z}$, so that $-ak = y_2 - y_1$, which implies $y_1 - ak = y_2$. A similar argument shows $x_2 = x_1 + bk$, so we are done. □

We now view an example of a linear equation.

Example 28.4. Let us solve $105x+121y = 1$ over the integers. First, this equation has solutions if and only if $\gcd(105, 121) \mid 1$, so we compute the GCD via the Euclidean algorithm:

$$\begin{aligned} 121 &= 1 \cdot 105 + 16 \\ 105 &= 6 \cdot 16 + 9 \\ 16 &= 1 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

so we have $\gcd(105, 121) = 1$, which does indeed divide 1. Now, back-substituting (that is, solving for $16, 9, 7, 2, 1$ in the equations above) will give us the relation $1 = -53 \cdot 105 + 46 \cdot 121$, so a solution is $(x_1, y_1) = (-53, 46)$. Now, the linear equation theorem tells us all other solutions, which are $(x, y) = \boxed{(-53 + 121t, 46 - 105t)}$ for $t \in \mathbb{Z}$.

Example 28.5. Let us solve $3x + 5y = 2$ over the integers. Notice that clearly $\gcd(3, 5) = 1$, so this equation has integer solutions by Bézout's Lemma. We can see that $3(7) + 5(-4) = 1$, so $(7, -4)$ solves $3x + 5y = 1$. Hence, the solutions to this simpler equation are $(7 - 5t, -4 + 3t)$ for $t \in \mathbb{Z}$. Doubling these solutions gives $(14 - 10t, -8 + 6t)$, which solve the original equation. However, the linear equation theorem **does not** tell us that these are all of the solutions, as while $1 \mid 2$, $\gcd(3, 5) = 1 \neq 2$; in fact, we observe $(x_1, y_1) = (-1, 1)$ is a solution to $3x + 5y = 2$. Now, if $(x, y) \in \mathbb{Z}^2$ is a solution, we must have $3x + 5y = 2 = 3x_1 + 5y_2$, so solving gives $\boxed{(-1 + 5n, 1 - 3n)}$, $n \in \mathbb{Z}$, as the general solution.

Example 28.6. Suppose $ad - bc = \pm 1$. We prove $\gcd(a+b, c+d) = 1$.

Proof. Notice that $d(a+b) - b(c+d) = ad + bd - bc - bd = ad - bc = \pm 1$, so Bézout's Lemma gives $\gcd(a+b, c+d) = 1$. □

34 The Fundamental Theorem of Arithmetic

We will now shift our focus onto prime numbers, and in this section, we will prove a fundamental result which demonstrates that the primes are the "building blocks" of the integers. First, we present the following lemma, which we have seen already in Math 13.

Lemma 34.1 (Euclid's Lemma)**.** *Let p be a prime, and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Suppose $p \mid ab$. If $p \mid a$, there is nothing to do, so suppose $p \nmid a$. Of course, it follows that $\gcd(a, p) = 1$, so by Bézout's Lemma, there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. Multiplying though by b, we get $pbx + aby = b$, and since $p \mid ab$ by assumption, $p \mid (pbx + aby) = b$. □

This generalizes by induction:

Corollary 34.2. *Let p be a prime, and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.*

Using this, we are ready to state and prove the Fundamental Theorem of Arithmetic.

Theorem 34.3 (Fundamental Theorem of Arithmetic — FTA)**.** *Every integer $n \geq 2$ has a representation as a product of primes $n = p_1 p_2 \cdots p_r$, where the p_i are prime, and this representation is unique up to permuting the primes.*

Proof. First, we prove that such a representation exists by induction on $n \geq 2$. If $n = 2$, then $2 = 2$ is a representation as a product of primes, so suppose the theorem holds for all numbers $2 \leq k < n$, for some $n \geq 2$. Now, if n is prime, we are done. If n is not prime, then there exists some a, b such that $n = ab$, and we know without loss of generality $2 \leq a < n$. Now, the size of b is bounded:

$$\frac{n}{n-1} < b < \frac{n}{2} < n,$$

and since b is an integer $b \geq 2$. Hence, the induction hypothesis applies to a and b, so write $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_s$. Then $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ is a representation as a product of primes.

Now, we prove uniqueness. Suppose $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where the p_i, q_j are primes. Certainly $p_1 \mid n = q_1 q_2 \cdots q_s$, so by Corollary 34.2, $p_1 \mid q_j$ for some $1 \leq j \leq s$. Without loss of generality, set $j = 1$, so that $p_1 \mid q_1$, and since q_1 is prime, $p_1 = q_1$. Now, cancel and continue inductively to see $r = s$ and $p_i = q_i$ for all i, and we are done. □

38 Consequences of the FTA

We start with the following definition.

Definition 38.1. Let $n \geq 2$ be an integer. A representation $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where the p_i are **distinct** primes and $\alpha_i \geq 1$ are integers, is called a *prime factorization* of n.

In reality, we should be saying **the** prime factorization of n, as the FTA guarantees that this representation is unique. From this, we deduce useful propositions relying on the existence of prime factorizations.

Throughout these next few propositions, write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$, where the p_i are distinct primes, and the $\alpha_i, \beta_i \geq 0$. Notice that this is a slight weakening of prime factorization that is not necessarily unique, but it is useful, as it allows us to write two integers in terms of the same primes.

Proposition 38.2. *We have $m \mid n$ if and only if $\alpha_i \geq \beta_i$ for all $i \leq r$.*

Proof. Exercise. □

Proposition 38.3. *We have* $\gcd(m, n) = \displaystyle\prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$.

Proof. The largest power of p_i dividing both m and n is $\min(\alpha_i, \beta_i)$. Now, apply Proposition 38.2. □

The below can be occasionally useful.

Proposition 38.4. *The integer n is a perfect square if and only if the α_i's are all even.*

Proof. Suppose n is a perfect square. Then $n = u^2$ for some $u \in \mathbb{Z}$, so by FTA, we have $u = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$. Hence $n = p_1^{2\lambda_1} p_2^{2\lambda_2} \cdots p_r^{2\lambda_r}$, so we have $\alpha_i = 2\lambda_i$ for all i. The converse direction is similar. □

The following two propositions allow us to complete the proof of our classifications of PPTs in Section 14.

Proposition 38.5. *We have $m^2 \mid n^2$ if and only if $m \mid n$.*

Proof. Notice that $m^2 \mid n^2$ implies $2\alpha_i \geq 2\beta_i$, so cancelling the 2 gives $\alpha_i \geq \beta_i$ so that $m \mid n$ by Propositions 38.2. □

Proposition 38.6. *If mn is a perfect square and $\gcd(m, n) = 1$, then m and n are both perfect squares.*

Proof. Write $m = \prod {p_i}^{\gamma_i}$, where the γ_i must all be even. Since $\gcd(m, n) = 1$, the prime factorizations of m and n have no primes in common, so each of the p_i divides exactly one of m and n. The result now follows from the fact that the γ_i are all even. □

Dually, we can consider least common multiples.

Definition 38.7. The *least common multiple* (LCM) of two integers $m, n \in \mathbb{Z}$, denoted $\operatorname{lcm}(m, n)$, is the smallest $k \in \mathbb{Z}^+$ such that $m \mid k$ and $n \mid k$.

Without knowing prime factorizations, finding least common multiples is an annoying task, but with them, an analogous formula to GCDs holds.

Proposition 38.8. *We have* $\operatorname{lcm}(m, n) = \displaystyle\prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.

Proof. The proof is essentially the same as that of GCDs. □

40 Modular Arithmetic

We now revisit the idea of divisibility, using the point of view of remainders. Recall that the division algorithm, when given two integers a, m, allows us to write $a = qm + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < m$. Now, suppose $b = q'm + r$, for the same remainder r. It follows that $a - b = qm + r - q'm - r = m(q - q')$, which is a multiple of m. We make the following definition.

Definition 40.1. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is *congruent* to b *modulo* m, denoted $a \equiv b \pmod{m}$, if $m \mid (a-b)$. The integer m is called the *modulus* of the congruence.

This next result should be quite natural.

Proposition 40.2. *If $a \in \mathbb{Z}$ has remainder $0 \leq r < m$ when divided by some modulus $m > 0$, then $a \equiv r \pmod{m}$.*

Proof. Write $a = qm + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < m$. Then $a - r = qm$, which is a multiple of m, so $a \equiv r \pmod{m}$. □

From here, it follows that every integer is congruent to one in the set $\{0, 1, \ldots, m-1\}$.

Our next proposition tells us how to effectively manipulate congruences.

Proposition 40.3. *Suppose $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Then $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ and $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.*

Proof. We know $m \mid (a_1 - b_1)$ and $m \mid (a_2 - b_2)$. Certainly $m \mid (a_1 + a_2) - (b_1 + b_2)$, so $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$. Setting $a_2 \mapsto -a_2$ and $b_2 \mapsto -b_2$ gives $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$.

For multiplication, write $a_1 = q_1 m + r_1$, $a_2 = q_2 m + r_2$, and since b_1, b_2 share the same remainder as a_1 resp. r_2, write $b_1 = q_3 m + r_1$, $b_2 = q_4 m + r_2$. Now, expanding out the product $a_1 a_2 - b_1 b_2$ in terms of the q_i, r_j, and m will finish the proof. □

That is, addition, subtraction, and multiplication behave nicely even when done modulo m. However, this is not the case for division:

Example 40.4. We see $1 \cdot 2 \equiv 3 \cdot 2 \pmod{4}$ yet $1 \not\equiv 3 \pmod{4}$. The reason for this is because $\gcd(c, m) \neq 1$.

However, inversion is legal whenever $\gcd(c, m) = 1$.

Proposition 40.5. *Suppose $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$. Then $a \equiv b \pmod{m}$.*

Proof 1. Suppose $\gcd(c, m) = 1$. Now, we are given that $m \mid (ac - bc) = c(a - b)$. But $m \nmid c$, so we are forced to have $m \mid (a - b)$. □

Proof 2. Alternatively, we argue by Bezout's Lemma. Suppose $\gcd(c, m) = 1$, so there exist integers x, y such that $cx + my = 1$. Certainly, $acx \equiv bcx \pmod{m}$, so that $m \mid (acx - bcx) = cx(a - b) = (1 - my)(a - b) = (a - b) + my(a - b)$. The second term is clearly divisible by m, so we must have $m \mid (a - b)$. □

We should also recall this fact.

Proposition 40.6. *Let $m \geq 2$. Then $\equiv \pmod{m}$ is an equivalence relation.*

Proof. Certainly $a \equiv a$ as $m \mid (a-a) = 0$. Similarly, $a \equiv b$ if and only if $b \equiv a$, so $\equiv$ is both symmetric and reflexive. Finally, suppose $a \equiv b$ and $b \equiv c$. Then $m \mid (a-b)$ and $m \mid (b-c)$. This implies that m divides $(a-b)+(b-c) = a-c$, so $a \equiv c$. □

This is helpful in abstract algebra, where we are interested in defining quotient groups. We will leave this alone for now.

Linear Congruences

In this subsection, we are interested in congruences of the form $ax + b \equiv c \pmod{m}$, which simplifies to congruences of the form $ax \equiv b \pmod{m}$. We will later classify the solutions to these, but we view an easy example.

Example 40.7. Solve $x + 7 \equiv 3 \pmod{10}$.

Solution. Subtracting 7 yields $x \equiv 3 - 7 \equiv 6 \pmod{10}$, so the solutions are $x \in 6 + 10\mathbb{Z}$. •

Example 40.8. Solve $11x \equiv 3 \pmod{13}$.

Solution. We want to "invert" 11, so we note that $11 \times 6 = 66 = 65 + 1$. Then

$$11x \equiv 3 \implies (6 \cdot 11)x \equiv 6 \cdot 3 \implies x \equiv 18 \equiv 5 \pmod{13},$$

so the solutions are $x \in 5 + 13\mathbb{Z}$. •

However, solutions of linear equations involving congruences are more complex in general. In fact, we do not always get one solution (up to congruence mod m):

Example 40.9. Solve $2x \equiv 2 \pmod{4}$ and $2x \equiv 1 \pmod{4}$.

Solution. It is tempting to cancel the 2 to get $x \equiv 1 \pmod{4}$, but we note that $x \equiv 3$ is also a solution, as $2 \cdot 3 \equiv 2 \pmod{4}$. Here, we have two incongruent solutions to a linear congruence. Worse, $2x \equiv 1$ has no solutions, as $2x - 1$ is always odd, yet we must have $4 \mid (2x-1)$. This is because $\gcd(2,4) = 2 > 1$, which causes problems. •

In general, the number of solutions to a linear congruence $ax \equiv b \pmod{m}$ is dependent on $\gcd(a,m)$, as we see in the theorem below.

Theorem 40.10 (Linear Congruence Theorem)**.** *Let $a, c, m \in \mathbb{Z}$ with $m \geq 2$, and let $g := \gcd(a,m)$. Then:*

(1) *The congruence $ax \equiv c \pmod{m}$ has solutions if and only if $g \mid c$.*

(2) *In the case where $g \mid c$, there are exactly g distinct solutions to $ax \equiv c \pmod{m}$, up to congruence modulo m. In fact, if $(u_0, v_0) \in \mathbb{Z}^2$ is a solution to the linear equation $au + bv = g$, then $x_0 = cu_0/g$ is a solution to the congruence $ax \equiv c$, and the complete set of g incongruent solutions is given by*

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m},$$

where $k \in \{0, 1, \ldots, g-1\}$.

Proof. We start by supposing $ax \equiv c \pmod{m}$, which means $m \mid (ax - c)$. This implies $g \mid (ax - c)$; yet $g \mid a$, so $g \mid ax$. This gives $g \mid c$. Conversely, suppose $g \mid c$, so that there exist integers x_1, y_1 such that $ax_1 + my_1 = c$. Reducing modulo m, we have $ax_1 \equiv c \pmod{m}$, so $x = x_1$ is a solution.

Suppose $\gcd(a, m) =: g \mid c$, and let (u_0, v_0) be a solution to the linear equation $au + mv = g$. Let $x_0 := cu_0/g$. Now, suppose x_1 is a solution to $ax \equiv c \pmod{m}$. Then certainly $ax_1 \equiv ax_0 \pmod{m}$, which implies $m \mid a(x_1 - x_0)$, i.e., there exists $y \in \mathbb{Z}$ such that $my = a(x_1 - x_0)$. Dividing by g, we see that

$$\frac{m}{g} \cdot y = \frac{a}{g}(x_1 - x_0),$$

implying m/g divides $a(x_1 - x_0)/g$. Because $g = \gcd(a, m)$, we observe that $\gcd(a/g, m/g) = 1$, so that m/g divides $x_1 - x_0$; i.e., there exists some integer k with $km/g = x_1 - x_0$; i.e., $x_1 = x_0 + k \cdot \frac{m}{g}$. Now, any two solutions that differ by a multiple of m are congruent, so we get the solutions

$$x_0, x_0 + 1 \cdot \frac{m}{g}, x_0 + 2 \cdot \frac{m}{g}, \ldots, x_0 + (g - 1)\frac{m}{g},$$

which are all of the solutions up to congruence modulo m. □

48 Polynomial Congruences

We now consider congruences of the form $f(x) \equiv 0 \pmod{m}$, where $m \in \mathbb{Z}^+$ is some modulus and $f(x)$ is a polynomial. The linear congruence theorem tells us what happens when $f(x)$ has degree 1, and at the end of this course, we will be able to say some things about quadratic polynomials, but in general, this is a difficult question and is a primary topic of study in abstract algebra. However, we prove this basic result about polynomial congruences, modulo a prime.

Theorem 48.1. *Let p be a prime number, and let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $p \nmid a_d$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most d solutions, up to congruence modulo m.*

The above proof, for the more algebraically minded, is the same as proving that a polynomial residing in $R[x]$, where R is an integral domain, as at most as many roots as its degree.

Proof. Suppose for contradiction that $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is a polynomial of **minimal** degree d, such that $r_1, \ldots, r_{d+1}$ are distinct roots of $f(x) \equiv 0$, up to congruence modulo p. First, we notice that for any r, $f(x) - f(r)$ has a factor of $x - r$, as

$$f(x) - f(r) = a_d(x^d - r^d) + a_{d-1}(x^{d-1} - r^{d-1}) + \cdots + \cancel{(a_0 - a_0)},$$

from which we can factor out an $(x - r)$ using the polynomial identity

$$(x^k - r^k) = (x - r)(x^{k-1} + rx^{k-2} + \cdots + r^{k-2}x + r^{k-1}).$$

In particular, if $r = r_1$ is a root of $f(x)$ modulo p, we may write $f(x) - f(r_1) = (x - r_1)g(x)$, where $g(x)$ has degree $d - 1$, and has leading coefficient a_1. Thus

$$f(x) = f(r_1) + (x - r_1)g(x) \equiv (x - r_1) \pmod{p},$$

as $f(r_1) \equiv 0 \pmod{p}$ by assumption. Now, for $i \geq 2$, we observe

$$0 \equiv f(r_i) = (r_i - r_1)g(x) \pmod{p},$$

so that $p \mid (r_i - r_1)g(r_1)$. By assumption, $p \nmid (r_i - r_1)$ (otherwise r_i, r_1 are congruent modulo p), so $p \mid g(r_i)$, i.e., $g(r_i) \equiv 0 \pmod{p}$. But this implies $r_2, r_3, \ldots, r_{d+1}$ are d possible roots of g, contradicting the minimality of the degree of f. □

Notice that the primality of p is used in the very last part of the proof, where we needed to conclude $p \mid g(r_i)$. This is usually untrue if p were not prime, as demonstrated in the example below.

Example 48.2. The polynomial congruence $x^2 - 1 \equiv 0 \pmod{8}$ has 4 incongruent solutions, namely $x \equiv \boxed{1, 3, 5, 7}$.

50 Fermat's Little Theorem

A focus in number theory is considering the the remainders of the numbers $a^k \pmod{p}$, where p is some prime number, where a and k could both be large. For example, consider the computation below:

Example 50.1. Find the remainder of 6^{22} when divided by 23.

Notice that this is equivalent to finding an integer $a \in \{0, 1, \ldots, 22\}$ such that $6^{22} \equiv a \pmod{23}$, but this is very difficult if we cannot compute 6^{22} efficiently. While it takes a computer less than a second to give

$$6^{22} = 131621703842267136, \text{ so that}$$
$$131621703842267136 = 5722682775750745 \cdot 23 + 1,$$

so that $6^{22} \equiv 1 \pmod{23}$, computing high powers is likely infeasible for numbers like $27^{45^{63}}$, say, we want to find the remainder modulo 47. However, needing to do these calculations is fundamental to applications of number theory, but we have the following theorem.

Theorem 50.2 (Fermat's Little Theorem)**.** *Let p be a prime number and let $a \in \mathbb{Z}$ satisfy $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

We remark from the above that $\gcd(6, 23) = 1$, so immediately we can deduce $6^{22} \equiv 1 \pmod{23}$ without any calculations. We give two proofs of this theorem, one that uses abstract algebra, and one that is elementary. Both proofs are equally enlightening.

Proof 1. We represent the integers modulo p using the group $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$, which consists of every residue class besides $\bar{0}$ (which are all of the multiples of p). Now, this group has order $p - 1$, so the order of any element $\bar{a}$ in the group must divide $p - 1$, so that it follows $\bar{a}^{p-1} = \bar{1}$. Said in modular arithmetic, $a^{p-1} \equiv 1 \pmod{p}$. □

For our second proof, we need the following lemma.

Lemma 50.3. *Let p be prime and let $a \in \mathbb{Z}$ satisfy $\gcd(a, p) = 1$. Then the numbers $1a, 2a, 3a, \ldots, (p-1)a \pmod{p}$ are exactly the numbers $1, 2, 3, \ldots, (p-1)$, but in a different order. That is, the map $x \mapsto xa$ (where the multiplication happens modulo p) is a bijection modulo p.*

Proof. The list $1a, 2a, 3a, \ldots, (p-1)a$ are $p - 1$ numbers, and none of them are divisible by p. Hence, we just check that this multiplication map is injective. Without loss of generality, suppose $1 \le j \le i \le p - 1$ satisfy $ai \equiv aj \pmod{p}$. Then

$$p \mid (ai - aj) = a(i - j),$$

but since $\gcd(p, a) = 1$, we have $p \nmid a$. Hence $p \mid (i - j)$, but now $0 \leq i - j \leq p - 1$, so this forces $i - j = 0$ and thus $i = j$. This completes the proof. □

From here, we prove Fermat's Little Theorem again.

Proof 2 of Theorem 50.2. By the lemma above, we see

$$a^{p-1}(p-1)! = (1a)(2a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) = (p-1)! \pmod p,$$

but now we notice $\gcd(p, (p-1)!) = 1$ (by construction of the factorial), so we may cancel it from our congruence to obtain $a^{p-1} \equiv 1 \pmod p$. □

63 The Euler Totient Function

In this section, we introduce an important arithmetic function that relates to counting coprime numbers.

Definition 63.1. The *Euler totient function* (or the Euler φ-function) is the function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}$ given by

$$\varphi(n) := \# \{1 \leq a \leq n : \gcd(a, n) = 1\}.$$

This is an arithmetic function, so we will be interested on its value on prime powers, as we can then use the information we know about a number's prime factorization to calculate φ effectively.

Proposition 63.2. *Let p be a prime. Then $\varphi(p^k) = p^k - p^{k-1}$, and if $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.*

A function, in general, satisfying $f(ab) = f(a)f(b)$ whenever $\gcd(a, b) = 1$ is called *(weakly) multiplicative*, and the proposition above tells us that φ is multiplicative.

Proof. First, the numbers *not* coprime to p^k are exactly the multiples of p, and there are p^{k-1} of them from 1 to p^k. Hence, counting gives $\varphi(p^k) = p^k - p^{k-1}$. For the second part, it suffices to prove this for a number of the form $p^a q^b$, where $p \neq q$ are primes, then induction finishes the proof. Again, counting finishes this argument. □

Proposition 63.3. *For any $n \in \mathbb{Z}^+$, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is its prime factorization, then*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Proof. This is a simple exercise in rearranging the above proposition. □

Now, we give other important properties of the values of the φ-function.

Proposition 63.4. *Let $n \geq 3$. Then $\varphi(n)$ is even.*

Proof. Write the prime factorization of n: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, so that the above propositions give

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}).$$

Now, if any of the p_i's are odd, then $p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ is even, so we are done. In the case that none of the p_i's are odd, then $n = 2^k$ is a power of two, and we can simply compute $\varphi(2^k) = 2^{k-1}$, which is at least 2 (and hence even) if $n \geq 3$ as assumed. □

Proposition 63.5. *If $n \in \mathbb{Z}^+$ is odd, then $\varphi(n) = \varphi(2n)$.*

Proof. This follows immediately from the fact that $\gcd(2, n) = 1$. □

Using the Euler φ-function, we get the following generalization of Fermat's Little Theorem.

Theorem 63.6 (Euler's Theorem)**.** *Suppose $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

We give two proofs: one using group theory and one that is elementary.

Proof 1. Recall that the multiplicative group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of all residue classes of elements coprime to n. In particular, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and by definition of the Euler φ-function, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Now, the order of an element divides the order of the group; i.e., $(\bar{a})^{\varphi(n)} = \bar{1}$ when viewed in $(\mathbb{Z}/n\mathbb{Z})^\times$. In other words, $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Proof 2. Let $1 = b_1 < b_2 < \cdots < b_{\varphi(n)}$ be the $\varphi(n)$ numbers between 0 and n that are coprime with n, and set $B = \{b_i\}_{i=1}^{\varphi(n)}$. Now, the map $B \to B$ by $b_i \mapsto b_i a$ is a bijection modulo n since $\gcd(a, n) = 1$, and we can check this via a similar argument to (link the other lemma for FLT). Using this, we now compute

$$b_1 b_2 \cdots b_{\varphi(n)} \equiv (b_1 a)(b_2 a) \cdots (b_{\varphi(n)} a) \pmod{n}$$

$$\implies b_1 b_2 \cdots b_{\varphi(n)} \equiv a^{\varphi(n)} b_1 b_2 \cdots b_{\varphi(n)} \pmod{n},$$

and now cancelling the $b_1 b_2 \cdots b_{\varphi(n)}$ (which is legal) gives us $a^{\varphi(n)} \equiv 1 \pmod{n}$ as desired. □

This next proposition allows us to restate our first proof of Euler's Theorem, without abstract algebra.

Proposition 63.7. *Suppose $\gcd(a, n) = 1$, and suppose $b \in \mathbb{Z}^+$ is the smallest possible integer solution to the congruence $a^x \equiv 1 \pmod{n}$. Then $b \mid \varphi(n)$.*

Such a number b is called the *order* of a modulo n.

Proof. By the Division Algorithm, write $\varphi(n) = qb + r$, where $0 \leq r < b$. Now, we know $1 \equiv a^{\varphi(n)} = a^{qb+r} = (a^b)^q a^r \equiv a^r$. Now, if $r > 0$, this violates the minimality of b, so $r = 0$. Hence $b \mid \varphi(n)$. □

Example 63.8. Show that $n \mid \varphi(a^n - 1)$ whenever $a > 2$.

Proof. We want to write this in a way so that we can use the previous proposition. Notice that $\gcd(x, x+1) = 1$ for all $x \in \mathbb{Z}^+$, and notice that $a^n \equiv 1 \pmod{a^n - 1}$. Now, this n is the minimal solution to $a^x \equiv 1 \pmod{a^n - 1}$, as we observe $0 < a^j < a^n - 1$ for all $1 \leq j \leq n-1$ (as $a > 2$). Hence, the previous proposition applies and $n \mid \varphi(a^n - 1)$. □

Finally, we observe another important property of the Euler φ-function — namely, that it preserves divisibility.

Proposition 63.9. *Suppose $a \mid b$. Then $\varphi(a) \mid \varphi(b)$.*

Proof. Write $a = \prod p_i^{\alpha_i}$ and $b = \prod q_i^{\beta_i}$ over the same set of primes p_i, and suppose $a \mid b$. Then $\alpha_i \le \beta_i$ for all i. Now, we know $\varphi(a) = \prod(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ and $\varphi(b) = \prod(p_i^{\beta_i} - p_i^{\beta_i - 1})$, so it just suffices to show that $p^{\alpha_i} - p^{\alpha_i - 1}$ divides $p_i^{\beta_i} - p_i^{\beta_i - 1}$, but we can quickly compute

$$\frac{p_i^{\beta_i} - p_i^{\beta_i - 1}}{p^{\alpha_i} - p^{\alpha_i - 1}} = \frac{p^{\beta_i - 1}(p-1)}{p^{\alpha_i - 1}(p-1)} = p^{\beta_i - \alpha_i},$$

which is an integer as $\alpha_i \le \beta_i$, so we are done. □

64 The Chinese Remainder Theorem

Our next cornerstone theorem will give us a way to solve various problems, where we have a list of simultaneous congruences we need to solve.

Theorem 64.1 (Chinese Remainder Theorem — CRT)**.** *Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise coprime, and let $a_1, \ldots, a_k \in \mathbb{Z}$ be any integers. Then the simultaneous congruences $x \equiv a_i \pmod{n_i}$, $1 \le i \le k$, has a unique solution up to congruence modulo $N := n_1 n_2 \cdots n_k$.*

Proof. It suffices to prove this statement for $k = 2$, and we can extend by induction. Consider the integers $a_2 + n_2 t$, for $0 \le t \le n_1 - 1$. We claim that these integers are distinct modulo n_1: suppose that $0 \le i \le j \le n_1 - 1$ and $a_2 + n_2 i \equiv a_2 + n_2 j \pmod{n_1}$. Then $n_2(i - j) \equiv 0 \pmod{n_1}$, i.e., $n_1 \mid n_2(i-j)$. Since $\gcd(n_1, n_2) = 1$, we must have $n_2 \mid (i - j)$, but by the sizes of i and j, we have $i = j$. Hence, one of the $a_2 + n_2 t$'s must be congruent to $a_1 \pmod{n_1}$, as we have a list of n_1 distinct integers modulo n_1, and clearly, $a_2 + n_2 t \equiv a_2 \pmod{n_2}$. Take $x \equiv a_2 + n_2 t_0 \pmod{n_1 n_2}$ to be this solution, which is unique as claimed. □

Example 64.2. Let us find x such that $x \equiv 1 \pmod 4$ and $x \equiv 6 \pmod 9$. The Chinese Remainder Theorem tells us that there exists a unique solution modulo $4 \times 9 = 36$, and the second congruence gives $x \equiv 6, 15, 24, 33 \pmod{36}$. As the proof of the theorem states, exactly one of these numbers is congruent to $1 \pmod 4$, and it is $x \equiv \boxed{33} \pmod{36}$.

Example 64.3. In a similar fashion, we find x such that $x \equiv 5 \pmod 7$ and $x \equiv 6 \pmod 8$. The CRT tells us there exists a unique solution modulo $7 \times 8 = 56$, so we write $x - 5 \equiv 0 \pmod 7$, so that $x - 5 = 7k$ for some $k \in \mathbb{Z}$. Now, $x - 6 \equiv 0 \pmod 8$ implies $x - 5 = 7k \equiv 1 \pmod 8$, so this is now a single congruence we can solve: $k \equiv 7 \pmod 8$. Substituting, we see $x = 7k + 5 = 7 \cdot 7 + 5 = \boxed{54}$, which is our unique solution.

More generally, suppose $x \equiv a_1 \mod n_1$ and $x \equiv a_2 \pmod{n_2}$. Then $x - a_i = kn_1$, so we have

$$kn_1 = x - a_1 \equiv a_2 - a_1 \pmod{n_2}.$$

This is now a congruence in one variable, which has a solution whenever $\gcd(n_1, n_2) \mid (a_1 - a_2)$. Alternatively, in the case $\gcd(n_1, n_2) = 1$, there exist $m_2, m_1 \in \mathbb{Z}$ such that $n_2 m_1 \equiv 1 \pmod{n_1}$ and $n_1 m_2 \equiv 1 \pmod{n_2}$, so that the unique solution given by CRT is

$$x \equiv a_1 n_2 m_1 + a_2 n_1 m_2 \pmod{n_1 n_2}.$$

The same idea works "by induction" when we have a system of three or more congruences.

Example 64.4. Find x such that $x \equiv 1 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 2 \pmod 7$.

Solution. We solve the last two congruences first, where we can observe $x \equiv 23 \pmod{35}$. We are thus left with solving $x \equiv 1 \pmod 3$ and $x \equiv 23 \pmod{35}$, so we check $x = 23, 58$ and note that $x \equiv \boxed{58} \pmod{105}$ works. •

In proofs, the CRT often guarantees the existence of an integer crucial to the problem.

Example 64.5. Show that if $\gcd(a,b) = 1$, then for all $c \neq 0$, there exists $n \in \mathbb{Z}$ with $\gcd(a+bn, c) = 1$.

Proof. Notice that $p \mid a$ and $p \mid (a+b)$ cannot be both true. Now, let $c \neq 0$ be arbitrary. Then if $\gcd(a,c) = 1$, notice that $n = 0$ works. Hence, assume $\gcd(a,c) > 1$. Let p be any prime dividing c. We want to have an n such that $\gcd(a+bn, p) = 1$. If $p \mid a$, pick $n \equiv 1 \pmod p$, otherwise pick $n \equiv 0 \pmod p$. Run this through every prime dividing c, and so CRT gives a unique n satisfying the system of congruences we generated. □

Example 64.6. Show that for distinct primes $p_1, \ldots, p_k$, there exists some $n \in \mathbb{N}$ such that $p_i \mid (n+i)$ for all $i \leq n$.

Proof. This is equivalent to finding n such that $n \equiv ** -i \pmod{p_i}$. The CRT tells us that this is possible. □

67 The Binomial Theorem

In this section, we give an alternate proof to Fermat's Little Theorem using a quasi-combinatorial technique.

Definition 67.1. Let $n, k \in \mathbb{Z}$ with $n \geq k \geq 0$. We define the *binomial coefficient* $\binom{n}{k}$ by

$$\binom{n}{k} := \frac{n!}{k!(n-k!)}.$$

Immediately, we notice the symmetry $\binom{n}{k} = \binom{n}{n-k}$, and that $\binom{n}{0} = \binom{n}{n} = 1$ for all $n \geq 0$. We should also be familiar with *Pascal's identity*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}, \tag{1}$$

which can be verified by direct computation. This gives us the following proposition, which is not too obvious from the definition alone.

Proposition 67.2. *For all $n, k \in \mathbb{Z}$ with $n \geq k \geq 0$, $\binom{n}{k}$ is an integer.*

Proof. Notice $\binom{0}{0} = \binom{1}{1} = \binom{1}{0} = 1 \in \mathbb{Z}$. Now, by induction assume that $\binom{n}{k}$ is an integer for any $k \leq n$. Then Pascal's identity gives $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \in \mathbb{Z}$. If $k = n$, then $\binom{n+1}{n+1} = 1 \in \mathbb{Z}$, so we are done. □

This gives us the following identity relating polynomials.

Theorem 67.3 (Binomial Theorem). *Suppose $a, b \in \mathbb{C}$. Then $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ for all $n \in \mathbb{Z}^+$.*

Proof. We prove by induction on n. If $n = 1$, this is obvious, so suppose the theorem holds for some $n \in \mathbb{Z}^+$. We expand

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)\left[\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n\right]\end{aligned}$$

$$= \left[\binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{n}ab^n\right] + \left[\binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n}b^{n+1}\right].$$

Now, combining like terms gives

$$\binom{n}{0}a^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]a^n b + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]ab^n + \binom{n}{n}b^{n+1},$$

and noting Pascal's identity and the fact that $\binom{n}{0} = \binom{n+1}{0} = \binom{n}{n} = \binom{n+1}{n+1} = 1$, we see

$$(a+b)^{n+1} = \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n+1}b^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{(n+1)-k},$$

which is exactly what we need to finish the proof by induction. □

By reducing modulo p for prime p, we gain a useful corollary.

Corollary 67.4. *For any $a, b \in \mathbb{Z}$ and prime p, we have $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

Proof. The Binomial Theorem gives $(a+b)^p = \displaystyle\sum_{k=0}^{p}\binom{p}{k}a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k b^{p-k}$. Now, notice that $p \mid \binom{p}{k}$ whenever $1 \leq k \leq p-1$, as

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \iff p! = \binom{p}{k}k!(p-k)!.$$

Since p is prime and clearly $p \mid \binom{p}{k}k!(p-k)!$, we observe $p \nmid k!(p-k)!$, so indeed $p \mid \binom{p}{k}$ as claimed, which, after reducing modulo p, finishes the proof. □

This gives a proof of an alternate form of Fermat's Little Theorem.

Theorem 67.5. *For all $a \in \mathbb{Z}_{\geq 0}$, we have $a^p \equiv a \pmod{p}$ for some prime p.*

Proof. We proceed by induction on a. When $a = 0$, this is obvious, so suppose the theorem holds for some $a \geq 0$. Now $(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}$ by the induction hypothesis and the preceding corollary. □

68 Prime Numbers

In this section, we examine two proofs about prime numbers.

Theorem 68.1 (Euclid's Theorem)**.** *There are infinitely many prime numbers.*

Proof. Assume for contradiction that $\mathbb{P} = \{p_1, \ldots, p_n\}$ is the finite list of all primes (where the p_i are pairwise distinct). Now, consider the number $N := p_1 p_2 \cdots p_n + 1$. If N is prime, then $N > p_i$ for all $i \leq n$, so $N \notin \mathbb{P}$, a contradiction. Otherwise, if N is composite, N splits into prime factors by FTA; call one of them $q \in \mathbb{P}$. Then $q = p_i$ for some $i \leq n$, so $p_i \mid N = p_1 p_2 \cdots p_n + 1$, so that $p_i \mid 1$, a contradiction. □

A very similar argument is used to show that there are infinitely many primes of a specific type: $3 \bmod 4$.

Theorem 68.2. *There are infinitely many prime numbers congruent to* 3 *modulo* 4.

Proof. Assume for contradiction that $\mathbb{P} = \{3, p_1, \ldots, p_r\}$, a list of $r + 1$ distinct primes, is the set of all primes congruent to 3 modulo 4. Define $A := 4p_1 p_2 \cdots p_r + 3$. Note $A \equiv 3 \pmod 4$. if A is prime, then certainly $A > 3$ and $A > p_i$ for all $i \leq n$, so $A \notin \mathbb{P}$, a contradiction. If A is composite, note that A is odd, so that it is a product of primes, either congruent to $1 \pmod 4$ or $3 \pmod 4$. There must exist a prime congruent to $3 \pmod 4$, as otherwise $A = 1 \cdot 1 \cdots 1 = 1 \pmod 4$, a contradiction. Let $q \mid A$ be a prime congruent to 3, so that $q \in \mathbb{P}$. If $q \mid 3$, then $3 \mid 4p_1 p_2 \cdots p_r$, a contradiction as $\gcd(3, p_i) = 1$ for all i, but if $q = p_i$, then $p_i \mid 3$, also a contradiction. □

78 Successive Squaring

We start by completing the following task.

Example 78.1. Compute $2^{32} \pmod{32749}$.

Solution. Notice that 32749 is a number that is very hard to factor, so Fermat's and Euler's Theorems are very much not applicable. While we can compute (or memorize) the 32-bit integer limit $2^{32} = 4294967296$, then long-divide by 32749, a better way to do this is to note $2^{16} = 63356 = 2 \cdot 32749 + 38$, so that $2^{16} \equiv 38 \pmod{32749}$. Now, $2^{32} = (2^{16})^2 \equiv 38^2 = \boxed{1444} \pmod{32749}$. •

Above, we found it too impractical to multiply 2^{32} out directly, so we instead found 2^{16}, reduced it modulo 32749 and squared it, which costs less as 38^2 is easy to calculate. We will develop this into an efficient computational method in this section, but first we introduce the following proposition, which we will not prove (usually, a result like this is seen in Math 13).

Proposition 78.2. *Every positive integer has a binary expansion, i.e., if $k \in \mathbb{Z}^+$, then k has a unique representation $k = u_0 + u_1 2^1 + u_2 2^2 + \cdots + u_r 2^r$, where $r \in \mathbb{Z}_{\geq 0}$ and $u_i \in \{0, 1\}$, with $u_r = 1$.*

This gives us the following algorithm for computing $a^k \pmod m$, even if k might be large.

Theorem 78.3 (Successive Squaring Algorithm)**.** *Let $a, m \in \mathbb{Z}$, and $k \in \mathbb{Z}^+$. Write $k = u_0 + u_1 2^1 + \cdots + u_r 2^r$ where r, u_i satisfy the conditions of the proposition above. Now, we compute $a, a^2, a^4, \ldots, a^{(2^r)} \pmod m$ by writing $a^{2^j} = (a^{2^{j-1}})^2$. Then*

$$a^k \equiv \prod_{k=0}^{r} a^{u_i 2^i} \pmod m.$$

The proof of this theorem follows immediately from exponent laws, so we view an example.

Example 78.4. Compute $5^{13} \pmod{23}$.

Solution. We compute $5^1 = 5, 5^2 \equiv 2, 5^4 \equiv 2^2 = 4$, and $5^8 \equiv 16 \pmod{23}$. Thus

$$5^{13} = 5^8 5^4 5^1 \equiv 16 \cdot 4 \cdot 5 \equiv 320 \pmod{23}.$$

Now, notice $23 \times 13 = 299$, so $320 \equiv \boxed{21} \pmod{23}$. •

80 Roots Modulo m

In this section, we consider congruences of the form $x^k \equiv b \pmod{m}$, for a fixed $k, b \in \mathbb{Z}$. Of course, we know that these congruences may sometimes have no solutions: we can easily verify that $x^2 \equiv 2 \pmod{3}$ has no solutions. However, if we suppose that there exists $u \in \mathbb{Z}^+$ with $ku \equiv 1 \pmod{\varphi(m)}$, then the number $x = b^u$ is a solution by Euler's Theorem, *if indeed* $\gcd(b, m) = 1$:

$$x^k = (b^u)^k = b^{uk} = b^1 \cdot b^{\ell\varphi(m)} \equiv b \pmod{m}.$$

We have thus proven the following:

Theorem 80.1. *Let $b, k, m \in \mathbb{Z}$ be such that $k, m \geq 1$ and $\gcd(b, m) = \gcd(k, \varphi(m)) = 1$. Then if $u \in \mathbb{Z}^+$ satisfies $uk \equiv 1 \pmod{\varphi(m)}$, then $x := b^u$ satisfies $x^k \equiv b \pmod{m}$.*

We view the following example.

Example 80.2. Find a solution to the congruence $x^7 \equiv 2 \pmod{33}$.

Solution. Notice $k = 7, b = 2, m = 33$. Now $\gcd(2, 33) = 1$, and $\gcd(7, \varphi(33)) = \gcd(7, 20) = 1$, so a solution exists. Write $7 \times 3 = 21 \equiv 1 \pmod{20}$, so that we take $u = 3$. Hence $2^u = 2^3 = \boxed{8}$ is a solution. •

We note that a key step into computing a root modulo m is needing to find the value of $\varphi(m)$. However, we know that this relies on knowing the prime factors of m; however, finding prime factorizations is in general a very hard problem for most computers. This may seem like a problem, but it is actually a *feature* to build simple yet secure codes. Say we have a message we would like to send, like "number theory." The first thing we can do is apply a substitution cipher to it, say by sending

$$a \mapsto 11, b \mapsto 12, c \mapsto 13, \ldots, z \mapsto 36,$$

so we get the string $24312312152830181525283$5. This initial step of encoding is clearly not secure, so we need to encode this further. Choose two <u>large</u> prime numbers p, q (usually, this is on the order of 10^{100} or even more), and let $m := pq$. We can easily compute $\varphi(m) = (p-1)(q-1)$, and so pick some $k \in \mathbb{Z}^+$ with $\gcd(k, \varphi(m)) = 1$. We note two important things:

- The tuple (m, k) is made *public* for all to see: this is so that messages could be sent and received.
- However, p and q, the two large primes, must be kept secret — as we shall see, if anyone can compute $\varphi(m) = (p-1)(q-1)$, they can decrypt any message that is sent.

To send and encode a message, we follow these steps:

1. Use a substitution cipher to convert the message into a string of numbers.
2. Break the string of digits into blocks, where each block is a number less than m. [Usually, we take a look at the number ℓ of digits m has, and break the string of digits into blocks of length $\ell - 1$]. This gives us a string of numbers $0 \leq a_1, a_2, \ldots, a_r < m$.
3. Use successive squaring to quickly compute $a_i^k \pmod{m}$ for all $1 \leq i \leq r$. This gives a new string of numbers $b_i := a_i^k \pmod{m}$, still less than m.
4. Send the string $b_1, b_2, \ldots, b_r$.

Now, a receiver decodes the string $b_1, b_2, \ldots, b_r$, following these steps:

1. Find $u \in \mathbb{Z}^+$ such that $uk \equiv 1 \pmod{\varphi(m)}$.
2. Compute $b^u = a^{ku} \equiv a$ by Euler's Theorem.
3. Undo the substitution cipher to read the message.

We stress that the security of this system, called the *RSA cryptosystem*, lies in the fact that p, q are kept secret, so that $\varphi(m)$ is virtually unknown despite m being known. Hence, the first step in decrypting is exceedingly difficult for eavesdroppers who do not know $\varphi(m)$, as this amounts to needing to factor $m = pq$, which, as we have mentioned before, is very difficult.

To finish this section, we end with one final example.

Example 80.3. Solve $x^{509} \equiv 3 \pmod{91}$.

Solution. We compute $\varphi(91) = \varphi(13)\varphi(7) = 12 \times 6 = 72$. Then $x^{509} = x^{504}x^5 \equiv x^5 \pmod{91}$ by Euler's Theorem, so now we just need to solve $x^5 \equiv 3 \pmod{91}$. Notice that the inverse of 5 modulo $\varphi(91) = 72$ is 29, as $29 \times 5 = 145 = 144 + 1$, so our solution is $x \equiv 3^{29}$. By successive squaring, compute $3^2 = 9, 3^4 = 81 \equiv -10, 3^8 \equiv 100 \equiv 9, 3^{16} \equiv 81 \pmod{91}$, so

$$\begin{aligned} 3^{29} \equiv 3^{16}3^8 3^4 3^1 &\equiv 81 \cdot 9 \cdot 81 \cdot 3 \pmod{91} \\ &\equiv (-10)^2 \cdot 9 \cdot 3 \pmod{91} \\ &\equiv 9 \cdot 9 \cdot 3 \equiv (-10) \cdot 3 \equiv \boxed{61} \pmod{91}, \end{aligned}$$

so we are done. •

90 Quadratic Residues

Now, we turn our attention to congruences of the form $x^2 \equiv b \pmod{p}$, where $p \geq 3$ is a prime. We know that $\varphi(p) = p - 1$, so attempting to solve this using the theory from the previous section, we must find $u \in \mathbb{Z}$ such that $2 \cdot u \equiv 1 \pmod{p-1}$. However, this is impossible as $p - 1$ is even, thus $\gcd(2, p-1) = 2$. Hence, we are stuck to no better than guessing; however, we note $k^2 \equiv (-k)^2 \pmod{n}$. Using this, and observing that

$$(km + r)^2 \equiv r^2 \pmod{m},$$

we can build lists of squares modulo m quickly by checking the residue classes $0, 1, \ldots, \lfloor m/2 \rfloor$.

Example 90.1. The squares modulo 7 are $0^2, 1^2, 2^2$, and 3^2, or simplifying: $0, 1, 4,$ and 2. It follows that any number outside of these is *not* a square modulo 7.

In particular, if $m = p$ is and odd prime, there are at most $(p-1)/2$ distinct non-zero squares modulo p. In fact, we have equality, but we first introduce terminology.

Definition 90.2. An integer a with $p \nmid a$ is called a *quadratic residue modulo* p whenever $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}$. Otherwise, we say a is a *quadratic nonresidue modulo* p.

In particular, the multiples of p: $0, \pm p, \pm 2p, \ldots$, are neither residues nor nonresidues.

Theorem 90.3. *Let p be an odd prime. Then there are exactly $\frac{1}{2}(p-1)$ distinct quadratic residues up to congruence modulo p, and exactly $\frac{1}{2}(p-1)$ distinct nonresidues modulo p.*

Proof. We have already seen that there are at most $\frac{1}{2}(p-1)$ distinct residues modulo p, so it suffices to show that the integers $1^2, 2^2, \ldots, \left[\frac{1}{2}(p-1)\right]^2$ are distinct modulo p. Suppose $i^2 \equiv j^2 \pmod{p}$. Then $p \mid (i^2 - j^2) = (i-j)(i+j)$, but now $2 \leq i + j \leq p - 1$ so $p \nmid (i+j)$. This forces $p \mid (i+j)$, but because $|i - j| < p$, we have $i = j$ and we are done. The rest of the integers left (that are not $0 \bmod p$) must be quadratic nonresidues. □

Notationally, we will now denote the set of quadratic residues modulo p by $\mathrm{QR}(p)$, and the set of nonresidues by $\mathrm{NR}(p)$.

Proposition 90.4. *Let p be a prime. If $a, b \in \mathrm{QR}(p)$, then $ab \in \mathrm{QR}(p)$.*

Proof. Suppose $a, b \in \mathrm{QR}(p)$. Then there exists $x, y \in \mathbb{Z}$ such that $a \equiv x^2, b \equiv y^2 \pmod{p}$. In particular, x, y are not multiples of p. Now $ab \equiv x^2y^2 = (xy)^2 \pmod{p}$, and we know $ab \not\equiv 0 \pmod{p}$, so indeed $ab \in \mathrm{QR}(p)$. □

Algebraically speaking, noting that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a finite group and $1 \in \mathrm{QR}(p)$, we see we have the inclusion of groups $\mathrm{QR}(p) \leq (\mathbb{Z}/p\mathbb{Z})^\times$. From here, Theorem 90.3 tells us that this subgroup has index 2, so we have the isomorphism

$$\frac{(\mathbb{Z}/p\mathbb{Z})^\times}{\mathrm{QR}(p)} \cong \mathbb{Z}/2\mathbb{Z}$$

where the elements of the quotients are necessarily the cosets $\mathrm{QR}(p)$ and $\mathrm{NR}(p)$. Using this isomorphism, it is easy to observe that

- If $a \in \mathrm{QR}(p)$ and $b \in \mathrm{NR}(p)$, then $ab \in \mathrm{NR}(p)$;
- If $a, b \in \mathrm{NR}(p)$, then $ab \in \mathrm{QR}(p)$.

We have thus just proven this following theorem, but we will provide a non-algebraic proof as well.

Theorem 90.5. *Let p be an odd prime. Then:*

1. *The product of two quadratic residues modulo p is a quadratic residue modulo p;*
2. *The product of a quadratic residue with a nonresidue is a nonresidue modulo p;*
3. *The product of two quadratic nonresidues is a residue modulo p.*

Proof. We already seen (1) as the proposition above. For (2), suppose for contradiction that $a_1 \in \mathrm{QR}(p)$ and $a_2 \in \mathrm{NR}(p)$ are such that $a_1a_2 \in \mathrm{QR}(p)$. Then $a_1a_2 \equiv x^2 \pmod p$ for some $x \in \mathbb{Z}$. Since $a_1 \in \mathrm{QR}(p)$, there exists $y \in \mathbb{Z}$ with $y^2 \equiv a_1 \pmod p$. Hence $y^2a_2 \equiv x^2 \pmod p$; in particular, $y \not\equiv 0 \pmod p$, so there exists z with $yz \equiv 1$. Multiplying by z^2 yields $a_2 \equiv x^2z^2 = (xz)^2 \pmod p$, a contradiction.

Finally, for (3), let $a \in \mathrm{NR}(p)$. Since $a \not\equiv 0 \pmod p$, the map $x \mapsto ax \pmod p$ is a bijection modulo p. Using (2) and counting by Theorem 90.3 finishes the proof. □

This suggests the following notation.

Definition 90.6. The *Legendre symbol* of an integer a modulo p, denoted $\left(\frac{a}{p}\right)$, is

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

This gives us an equivalent form of the "multiplication" law we proved above:

Corollary 90.7 (Multiplication Law). *For an odd prime p and any $a, b \in \mathbb{Z}$, we have*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

94 Quadratic Reciprocity I

We have developed quite a bit of theory surrounding quadratic residues modulo p and even introduced some notation (namely the Legendre symbol), but we do not yet know *how* to calculate a Legendre symbol other than by guessing, or using the multiplication law if we are lucky. Thus, in the next two sections, we will develop a better way to compute quadratic residues, which relies less on guessing and checking.

Consider the Legendre symbol $\left(\frac{-1}{p}\right)$, which is 1 precisely when $x^2 \equiv -1 \pmod p$ and -1 otherwise. Now, if $p = 2$, then $\left(\frac{-1}{2}\right) = 1$, so there is nothing to do. We can verify the following data for odd primes however:

$$\left(\frac{-1}{p}\right) = -1 \text{ when } p = 3, 7, 11, 19, 23, 31;$$
$$\left(\frac{-1}{p}\right) = +1 \text{ when } p = 5, 13, 17, 29, 37.$$

Notice that the primes in the first line are congruent to $3 \pmod 4$, while the primes in the second are congruent to $1 \pmod 4$. This is in fact the case in general, but first, we prove the following theorem, from which our conjecture will fall out as a corollary.

Theorem 94.1 (Euler's Criterion). *Let p be an odd prime. Then for any $a \in \mathbb{Z}$,*

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

Proof. If $p \mid a$, there is nothing to check, so assume $p \nmid a$. If $a \in \mathrm{QR}(p)$, then there exists b such that $a \equiv b^2 \pmod{p}$. Hence $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem (notice $p \nmid b$), and indeed, $\left(\frac{a}{p}\right) = 1$ by assumption. Now,, suppose $a \in \mathrm{NR}(p)$. Again, by Fermat's Little Theorem, $a^{p-1} \equiv 1$, so that $a^{(p-1)/2}$ is a solution to the congruence $x^2 - 1 \equiv 0 \pmod{p}$. We can read off the two roots of this congruence, so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, which is half of what we need. It suffices to show $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, which is equivalent to showing that a is not a root of the congruence $x^{(p-1)/2} - 1 \equiv 0$. For this second congruence, we know that the elements of $\mathrm{QR}(p)$ are roots of it, but we also know $|\mathrm{QR}(p)| = (p-1)/2$, and thus the elements of $\mathrm{QR}(p)$ are the only solutions to this congruence. This thus forces $a^{(p-1)/2} - 1 \not\equiv 0$, so that $a^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}$. □

Corollary 94.2 (Quadratic Reciprocity, First Supplement)**.** *Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = +1$ if $p \equiv 1 \pmod{4}$, and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \pmod{4}$.*

Proof. By Euler's Criterion, we have $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Now, $\frac{1}{2}(p-1)$ is odd precisely when $p \equiv 3 \pmod{4}$, and $\frac{1}{2}(p-1)$ is even when $p \equiv 1 \pmod{4}$. From here, the result follows. □

A fun application is the following.

Theorem 94.3. *There are infinitely many primes congruent to 1 modulo 4.*

Proof. Suppose $\mathbb{L} := \{p_1, p_2, \ldots, p_r\}$ is a list of r distinct primes congruent to 1 modulo 4. We find a prime congruent to 1 modulo 4 that is not in $\mathbb{L}$. Consider $A := (2p_1p_2\cdots p_r)^2 + 1$. Clearly, $A \equiv 1 \pmod{4}$. Now, let q be a prime dividing A. Notice that q is odd as A is odd, and $q \notin \mathbb{L}$, as otherwise $p_i \mid 1$. Now, since we assumed $q \mid A$, we have $A \equiv 0 \pmod{q}$, so $(2p_1p_2\cdots p_r)^2 \equiv -1 \pmod{q}$. Hence, -1 is a quadratic residue modulo q, which occurs precisely when $q \equiv 1 \pmod{4}$. This means that $q \notin \mathbb{L}$, and q is congruent to 1 modulo 4, so there must be infinitely many primes congruent to 1 modulo 4. □

Now, we turn our attention to the Legendre symbol $\left(\frac{2}{p}\right)$. When $p = 2$, there is again nothing to do as $\left(\frac{2}{2}\right) = 0$, and again we can verify the following for odd primes p:

$$\left(\frac{2}{p}\right) = +1 \text{ when } p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89;$$
$$\left(\frac{2}{p}\right) = -1 \text{ when } p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59.$$

Reducing the lists modulo 8, we see that the primes in the first row are congruent to $1, 7 \pmod{8}$, while those in the second row are congruent to $3, 5 \pmod{8}$. This is in fact true in general.

Theorem 94.4 (Quadratic Reciprocity, Second Supplement)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8}. \end{cases}$$

Proof. We consider the cases $p \equiv 3, 7 \pmod 8$; the other two are similar. When $p \equiv 3 \pmod 8$, write $p = 8k + 3$. Consider the even numbers $2, 4, \ldots, p - 1 = 8k + 2$:

$$2, 4, 6, \ldots, 4k, 4k + 2, 4k + 4, \ldots, 8k + 2.$$

Note that $\frac{1}{2}(p - 1) = 4k + 1$, so if we reduce these numbers into the range $(-(4k + 1), 4k + 1]$, we would get $2k + 1$ negative signs, corresponding to the even numbers from $4k + 2$ to $8k + 2$. This now allows us to use Euler's Criterion:

$$2^{(p-1)/2} \cdot P! = 2 \cdot 4 \cdot 6 \cdots (8k - 2) \equiv (-1)^{2k+1} P! \pmod p,$$

so that $2^{(p-1)/2} \equiv -1 \pmod p$, so $\left(\frac{2}{p}\right) = -1$.

Now, if $p \equiv 7 \pmod 8$, we write $p = 8k + 7$ and consider the even numbers $2, 4, \ldots, p - 1 = 8k + 6$. Note that $\frac{1}{2}(p - 1) = 4k + 3$, so if we reduce these numbers into the range $(-(4k+3), 4k+3]$, we get $2k+2$ negative signs, corresponding to the even numbers from $4k+4$ up to $8k + 6$. By a similar argument using Euler's Criterion, we observe $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) = 1 \pmod p$. □

104 Quadratic Reciprocity II

In the previous section, we have proven results about $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, and we can prove analogous results, in a similar fashion, about $\left(\frac{a}{p}\right)$ for a specifically chosen a. However, this is tedious past a certain point, where we would simply prefer to have one theorem which proves a result about $\left(\frac{p}{q}\right)$ instead, where p, q are primes. We certainly know $\left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right)$, but it would be beneficial to know when the sign actually changes. Again, we can verify data for tuples of primes (p, q) to obtain some relationships, but eventually, we will come to this rule, which we will not prove in this course (but in Math 180B).

Theorem 104.1 (Law of Quadratic Reciprocity)**.** *Let p, q be odd primes. Then*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & p, q \equiv 3 \pmod 4. \end{cases}$$

Alternatively stated, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{(p-1)(q-1)/4}$.

Using this, we can efficiently compute Legendre symbols.

Example 104.2. Using the multiplication law and what we know about $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, we compute

$$\begin{aligned} \left(\frac{105}{179}\right) &= \left(\frac{3}{179}\right)\left(\frac{5}{179}\right)\left(\frac{7}{179}\right) \\ &= \left[-\left(\frac{179}{3}\right)\right]\left(\frac{179}{5}\right)\left[-\left(\frac{179}{7}\right)\right] \\ &= \left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{4}{7}\right) = -1 \cdot 1 \cdot 1 = \boxed{-1}. \end{aligned}$$

Example 104.3. Given that both 1783 and 7523 are prime, we compute

$$\begin{aligned}\left(\frac{1783}{7523}\right) = -\left(\frac{7523}{1783}\right) &= -\left(\frac{391}{1783}\right) \\ &= -\left(\frac{17}{1783}\right)\left(\frac{23}{1783}\right) \\ &= \left(\frac{1783}{17}\right)\left(\frac{1783}{23}\right) = \left(\frac{15}{17}\right)\left(\frac{12}{23}\right) \\ &= \left(\frac{3}{17}\right)\left(\frac{5}{17}\right)\left(\frac{4}{23}\right)\left(\frac{3}{23}\right) \\ &= -\left(\frac{17}{3}\right)\left(\frac{17}{5}\right)\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{3}\right) = (-1)(-1) = \boxed{+1}.\end{aligned}$$

Homework Exercises

What follows are my attempted solutions to every homework exercise that has been assigned this quarter. Most of these assignments received full marks, but I cannot guarentee the correctness of the work here. I have revised a few of these in these notes for clarity.

Homework 1: Rational Points

Exercise 1 (Chapter 2 #1)**.** In lecture we showed that in any primitive Pythagorean triple (PPT) (a, b, c), exactly one of a and b is even. Try the same for the primes 3 and 5.

(a) Use a similar argument to show that either a or b is a multiple of 3.

We first establish the following claim: if n is not a multiple of 3, then n^2 is always one more than a multiple of 3. To see this, note that if $3 \nmid n$, then we either have $n = 3x + 1$ or $n = 3x + 2$ for some appropriate $x \in \mathbb{Z}$. Then

$$n^2 = (3x + 1)^2 = 9x^2 + 6x + 1 = 3(3x^2 + 2x) + 1,$$

which is one more than a multiple of 3, or

$$n^2 = (3x + 2)^2 = 9x^2 + 12x + 4 = 3(3x^2 + 4x + 1) + 1,$$

which is still one more than a multiple of 3. Hence n^2 is 1 more than a multiple of 3. With this, we complete the following proof of the main statement.

Proof. Let (a, b, c) be a PPT, so that $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$. If both a and b are multiples of 3, then $a = 3x$ and $b = 3y$ for some $x, y \in \mathbb{Z}$. Hence

$$c^2 = a^2 + b^2 = 9x^2 + 9y^2 = 9(x^2 + y^2),$$

which implies that $9 \mid c^2$, so that $3 \mid c$, as c^2 is a perfect square. This would imply (a, b, c) is not primitive, so a and b cannot be both multiples of 3.

Similarly, assume that neither a nor b are multiples of 3. Then we know from the fact above that $a^2 = 3m + 1$ and $b^2 = 3n + 1$ for $m, n \in \mathbb{Z}$, so that

$$c^2 = a^2 + b^2 = 3(m + n) + 2,$$

which is impossible, as c^2 is a perfect square and must be one more than a multiple of 3. Hence, exactly one of a and b must be a multiple of 3. □

(b) What about multiples of 5?

We claim that **exactly one of** a, b, c **must be a multiple of** 5, where (a, b, c) is a PPT.

Proof. Let (a, b, c) be a PPT. It is impossible for all 3 of a, b, c to be a multiple of 5, otherwise they have a common factor of 5. Similarly, if exactly two of a, b, c are a multiple of 5, we consider 3 cases:

Case I: $5 \mid a, b$. In this case, we see $5 \mid (a^2 + b^2) \iff 5 \mid c^2$, but because 5 is prime, this must mean $5 \mid c$, which causes (a, b, c) to not be primitive.

Case II: $5 \mid a, c$. In this case, we see $5 \mid (c^2 - a^2) \iff 5 \mid b^2$, but similarly, this implies $5 \mid b$, again a contradiction with primitivity.

Case III: $5 \mid b, c$. This case causes the same contradiction.

Hence, it is impossible for exactly two of a, b, c to be a multiple of 5. Now, suppose none of a, b, c are multiples of 5. *Reducing modulo* 5, this means that $a, b, c \equiv 1, 2, 3, 4 \pmod 5$. But we can verify the squares modulo 5 are

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 4 \pmod 5,$$

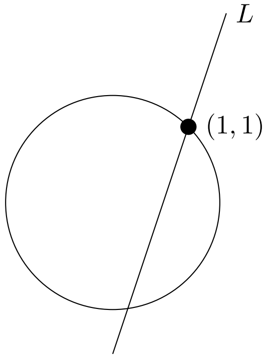
so that $a^2, b^2 \equiv 1, 4 \pmod 5$. In either case, we see that $c^2 = a^2 + b^2$ can only take on the values $4+1, 1+4, 1+1$, or $4+4$ modulo 5, i.e., $c^2 \equiv 0, 2, 3 \pmod 5$. The case $c^2 \equiv 0 \pmod 5$ implies $5 \mid c^2$, so that by primality of 5 we have $5 \mid c$. The cases $c^2 \equiv 2, 3$ are impossible, as a perfect square must be congruent to $0, 1$, or 4 modulo 5. Hence, it is impossible for none of a, b, c to be divisible by 5, so we have shown that **exactly one** of a, b, c must be divisible by 5. □

Exercise 2 (Chapter 2 #2)**.** A nonzero integer d is said to *divide* an integer m if $m = dk$ for some integer k. Show that if d divides both m and n, then d also divides $m - n$ and $m + n$.

Proof. Suppose d divides both m and n. Then $m = dk$ and $n = dj$ for $j, k \in \mathbb{Z}$. Now we compute $m + n = dk + dj = d(k + j)$. Since $k + j$ is an integer, we have shown that d divides $m + n$. Similarly, we compute $m - n = dk - dj = d(k - j)$. Since $k - j$ is also an integer, we have shown that d divides $m - n$. □

Exercise 3 (Chapter 3 #2a)**.** Use lines through the point $(1, 1)$ to describe all the rational points on the circle $x^2 + y^2 = 2$.

Solution. Certainly, $(1, 1)$ is a rational point on the circle $x^2 + y^2 = 2$ (we call the circle C). Draw a line L through $(1, 1)$ with rational slope m:



By this picture, we see that L intersects C at two points: at $(1, 1)$ and at some other point (x, y). The equation of line L is given by point-slope form:

$$y - 1 = m(x - 1) \iff y = 1 + m(x - 1).$$

Finding the intersection gives us a system of equations, which reduces to solving a quadratic:

$$\begin{aligned}
x^2 + [1 + m(x-1)]^2 &= 2 \\
x^2 + m^2(x-1)^2 + 2m(x-1) + 1 &= 2 \\
x^2 + m^2(x-1)^2 + 2m(x-1) - 1 &= 0 \\
(x^2 - 1) + m^2(x-1)^2 + 2m(x-1) &= 0 \\
(x-1)(x+1) + m^2(x-1)^2 + 2m(x-1) &= 0 \\
(x-1)\left[(x+1) + m^2(x-1) + 2m\right] &= 0.
\end{aligned}$$

Of course, the solution $x = 1$ is not very interesting, as this yields $y = 1 + m(1-1) = 1$, and we already knew that L intersects C at $(1,1)$ by construction. The other solution yields

$$x + 1 + m^2x - m^2 + 2m = 0 \iff (m^2+1)x + (1 + 2m - m^2) = 0 \iff x = \frac{m^2 - 2m - 1}{m^2+1},$$

so the corresponding y-value is

$$\begin{aligned}
y = 1 + m(x-1) &= 1 + m\left(\frac{m^2-2m-1}{m^2+1} - 1\right) \\
&= 1 + m\left(\frac{m^2 - 2m - 1 - m^2 - 1}{m^2+1}\right) \\
&= 1 + m\left(\frac{-2m-2}{m^2+1}\right) = 1 - \frac{2m(m+1)}{m^2+1} \\
y &= \frac{m^2 + 1 - 2m^2 - 2m}{m^2+1} = \frac{1 - 2m - m^2}{m^2+1}.
\end{aligned}$$

At this point, we are almost done — we note that $(1,1)$ can be found using these formulas by setting $m = -1$ (here, the line L is tangent to C), but we are still missing one point. Namely, we can draw a vertical line (with infinite slope) through $(1,1)$, which has equation $x = 1$. By inspection, this vertical line intersects the circle at $(1,-1)$, so that is the missing point. Hence, the set of rational points on the circle $x^2 + y^2 = 2$ is

$$C \cap \mathbb{Q}^2 = \{(1,-1)\} \cup \left\{\left(\frac{m^2-2m-1}{m^2+1}, \frac{1-2m-m^2}{m^2+1}\right) : m \in \mathbb{Q}\right\}.$$

The other direction we need to show is trivial: if (α, β) is a rational point that is not $(1,-1)$, then the line connecting (α,β) and $(1,1)$ has rational slope.

Here is an interactive graph[5] I made for this problem. •

Exercise 4 (Chapter 3 #3)**.** Find a formula for all of the rational points on the hyperbola $x^2 - y^2 = 1$.

Solution. Call the given hyperbola C. Certainly, $(-1,0) \in C$ is a rational point, so we draw a line L of rational slope m through C. The equation of the line is given by point-slope form:

$$y - 0 = m(x - (-1)) \iff y = m(x+1).$$

To prove that L intersects C at exactly two points, we just solve a system of equations:

[5] `https://www.desmos.com/calculator/poi6hexshw`

$$\begin{cases} y = m(x+1) \\ x^2 - y^2 = 1 \end{cases} \implies x^2 - [m(x+1)]^2 = 1.$$

This is a quadratic we can solve:

$$\begin{aligned} x^2 - m^2(x+1)^2 &= 1 \\ x^2 - m^2(x^2+2x+1) &= 1 \\ (1-m^2)x^2 - 2m^2x - (m^2+1) &= 0. \end{aligned}$$

We know one root of the polynomial on the left, namely -1. By Vieta's Formulas, if x is the other root of the equation, we have that the product of the roots -1 and x is

$$-1 \cdot x = \frac{-(m^2+1)}{(1-m^2)} \implies x = \frac{1+m^2}{1-m^2}.$$

Hence

$$\begin{aligned} y = m(x+1) = m\left(\frac{1+m^2}{1-m^2}+1\right) &= m \cdot \frac{1+m^2+1-m^2}{1-m^2} \\ \implies y = \frac{2m}{1-m^2}, \end{aligned}$$

so we are almost done. The case where we draw a vertical line through $(-1,0)$ does not matter, as the line $x=-1$ only intersects C at $(-1,0)$, as it is tangent to C there. Hence, the set of rational points on the hyperbola $x^2-y^2=1$ is

$$C \cap \mathbb{Q}^2 = \{(-1,0)\} \cup \left\{\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right) : m \in \mathbb{Q}\right\}.$$

As usual, the other way around is trivial. Here is an interactive graph[6] I made for this problem. •

Exercise 5. This exercise concerns a rational point on an elliptic curve.

(a) Consider a general cubic equation

$$(x-a)(x-b)(x-c) = x^3 + p_2x^2 + p_1x + p_0 = 0,$$

where a, b, c are the roots. Prove that if the coefficients p_i are rational and that two of the roots are rational, then so is the third root.

Proof. Suppose p_0, p_1, p_2 above are rational. Without loss of generality, suppose a and b are rational. We quickly see that[7] expanding the product on the left gives

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+bc+ac)x - abc,$$

so equating coefficients gives, in particular, $p_2 = -(a+b+c)$. Hence $c = -(p_2+a+b)$, which is a rational quantity, as p_2, a, and b are all rational. Thus, if two roots of a cubic polynomial with rational coefficients are rational, then all three roots are rational. □

[6] https://www.desmos.com/calculator/gu4kfs3b1s

[7] The coefficients of the x^i are the *symmetric polynomials* in a, b, c of degree $3-i$.

(b) (Chapter 3 #4). The curve $y^2 = x^3 + 8$ contains the points $(1, -3)$ and $(-7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

For obvious reasons, we used a calculator for the solution below.

Solution. Let C be the curve $y^2 = x^3+8$, and let L be the line through $(1, -3)$ and $(-7/4, 13/8)$. This line has slope

$$m = \frac{(13/8) - (-3)}{(-7/4) - 1} = -\frac{37}{22},$$

so the equation of the line is given by point-slope form:

$$y + 3 = -\frac{37}{22}(x - 1) \iff y = -\frac{1}{22}(37x + 29).$$

To find the solutions, we substitute the equation of L into the equation of C to obtain the following cubic:

$$\begin{aligned} y^2 = x^3 + 8 \implies & \left[-\frac{1}{22}(37x + 29)\right]^2 = x^3 + 8 \\ \iff & \frac{1}{484}(1369x^2 + 2146x + 841) = x^3 + 8 \\ \iff & x^3 - \frac{1369}{484}x^2 - \frac{1073}{242}x + \frac{3031}{484} = 0. \end{aligned}$$

We know two roots of this equation already: 1 and $-7/4$. To find the third root x_3, we know by the previous part, the sum of the three roots is the negative of the quadratic coefficient:

$$1 - \frac{7}{4} + x_3 = \frac{1369}{484} \implies x_3 = \frac{433}{121}.$$

The associated y-coordinate y_3 is thus

$$y_3 = -\frac{1}{22}(37x_3 + 29) = -\frac{9765}{1331},$$

so the third point is $\boxed{\left(\frac{433}{121}, -\frac{9765}{1331}\right)} \approx (3.579, -7.337)$. Of course, part (a) predicts that this point would be rational, as the cubic we found had rational coefficients. This explains why the x-coordinate is rational. That the y-coordinate of the third point is rational follows from the fact that the point lies on a line with rational slope and rational y-intercept, and the x-coordinate was already rational. •

Homework 2: Greatest Common Divisors

Exercise 1. Find a primitive Pythagorean triple corresponding to a right triangle with perimeter $11786 = 2 \cdot 71 \cdot 83$.

Solution. By the theorem in the text, a primitive Pythagorean triple may be found by finding selecting odd integers $s > t \geq 1$ and substituting into the formula

$$(a,b,c) := \left(\frac{s^2-t^2}{2}, st, \frac{s^2+t^2}{2}\right).$$

The perimeter of this triangle is thus

$$11786 = a+b+c = \frac{1}{2}(s^2-t^2) + st + \frac{1}{2}(s^2+t^2) = st + s^2 = s(t+s), \text{ so that}$$

$$2 \cdot 71 \cdot 83 = s(t+s).$$

We guess $s = 83$, so that $t + 83 = 2 \cdot 71$ by balancing the factorization, which gives $t = 142 - 83 = 59$. Hence, the triple determined by this is

$$(a,b,c) = \left(\frac{83^2-59^2}{2}, 83 \cdot 59, \frac{83^2+59^2}{2}\right) = \boxed{(1704, 4897, 5185)}.$$

Indeed, $c = 5185 = 5 \cdot 17 \cdot 61$, so that $\gcd(a,b,c) = 1$ as expected. •

Exercise 2. Suppose Fermat's Last Theorem holds for $n = 3$. Prove that Fermat's Last Theorem holds for $n = 12$.

Proof. For contradiction, let a,b,c be positive integers such that $a^{12} + b^{12} = c^{12}$. Let $A := a^4$, $B := b^4$, and $C := C^4$. Then we see that $a^{12} = (a^4)^3 = A^3$, and similarly for B and C, so we have $a^{12} + b^{12} = c^{12} \iff A^3 + B^3 = C^3$. However, since $a,b,c > 0$, A, B and C are also positive integers. This contradicts the fact that Fermat's Last Theorem holds for exponent $n = 3$, so Fermat's Last Theorem must hold for exponent $n = 12$. □

Exercise 3 (Chapter 5, #3)**.** Let $b = r_0, r_1, \ldots,$ be the successive remainders in the Euclidean algorithm applied to a and b. Show that after every two steps, the remainder is reduced by $1/2$, i.e., show $r_{i+2} < r_i/2$ for all $i \geq 0$.

Proof. Fix some $i \geq 0$ such that $r_i > r_{i+2} > 0$. Certainly $r_{i+2} < r_{i+1}$. Multiplying through by q_{i+2} gives $q_{i+2}r_{i+2} < q_{i+2}r_{i+1}$, which implies

$$q_{i+2}r_{i+2} + r_{i+2} < q_{i+2}r_{i+1} + r_{i+2} = r_i$$

$$\iff r_{i+2}(q_{i+2}+1) < r_i.$$

Since $q_{i+2} > 0$ is an integer, we see that $r_{i+2} < r_i/(q_{i+2}+1) < r_i/(1+1) = r_i/2$. □

Exercise 4 (Chapter 6, #2b)**.** Solve $12345x + 67890y = \gcd(12345, 67890)$ over the integers.

Solution. We start by finding $\gcd(12345, 67890)$ by the Euclidean algorithm:

$$\begin{aligned} 67890 &= 5 \cdot 12345 + 6165 \\ 12345 &= 2 \cdot 6165 + 15 \\ 6165 &= 411 \cdot 15 + 0, \end{aligned}$$

so $\gcd(12345, 67890) = 15$. We first find one solution $(x_1, y_1) \in \mathbb{Z}^2$ by back-substituting:

$$\begin{aligned} 6165 &= 67890 - 5 \cdot 12345 \\ 15 &= 12345 - 2 \cdot 6165 = 12345 - 2 \cdot (67890 - 5 \cdot 12345) = 11 \cdot 12345 - 2 \cdot 67890, \end{aligned}$$

so one solution is $(x_1, y_1) := (11, 2)$. The rest of the solutions are described by the Linear Equation Theorem: our general solution is

$$\left(x_1 + t\frac{67890}{15}, y_1 - t\frac{12345}{15}\right) = \boxed{(11 + 4526t, -2 - 823t)},$$

where $t \in \mathbb{Z}$ is any integer. •

Exercise 5 (Chapter 6, #5)**.** Suppose that $\gcd(a, b) = 1$. Prove that for every integer c, the equation $ax + by = c$ has a solution in integers x and y. Then, find an integer solution to $37x + 47y = 103$.

Proof. Suppose $\gcd(a, b) = 1$. By Bezout's Lemma, we know that the there exist $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Multiplying through by $c \in \mathbb{Z}$, we see that $a(cu) + b(cv) = c$, so setting $x := cu$ and $y := cv$ completes the proof. □

To solve $37x + 47y = 103$, we first find a solution to $37u + 47v = 1$ over the integers. We already see that $\gcd(37, 47) = 1$, and we use the Euclidean algorithm to see that

$$\begin{aligned} 47 &= 1 \cdot 37 + 10 \\ 37 &= 3 \cdot 10 + 7 \\ 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 1 &= 1 \cdot 1 + 0, \end{aligned}$$

so that

$$\begin{aligned} 10 &= 47 - 1 \cdot 37 \\ 7 &= 37 - 3 \cdot 10 = 37 - 3 \cdot (47 - 1 \cdot 37) = 4 \cdot 37 - 3 \cdot 47 \\ 3 &= 10 - 1 \cdot 7 = (47 - 37) - (4 \cdot 37 - 3 \cdot 47) = -5 \cdot 37 + 4 \cdot 47 \\ 1 &= 7 - 2 \cdot 3 = (4 \cdot 37 - 3 \cdot 47) - 2 \cdot (-5 \cdot 37 + 4 \cdot 47) = 14 \cdot 37 - 11 \cdot 47, \end{aligned}$$

so $37(14) + 47(-11) = 1$. Multiplying through by 103 gives $37(1442) + 47(-1133) = 103$, so we have the solution $(x, y) = (1442, -1133)$. Notice that $(1442 - 47k, -1133 + 37k)$ is also a solution, and we note that setting $k = 31$ gives the solution $\boxed{(-15, 14)}$, which is small.

Exercise 6. Let a, b, r, s be given constants with $a, b \neq 0$. Prove that the arithmetic progressions

$$\{ax + r : r \in \mathbb{Z}\} \text{ and } \{by + s : s \in \mathbb{Z}\}$$

intersect if and only if $\gcd(a, b) \mid (s - r)$.

Proof. ($\Longleftarrow$): Suppose $\gcd(a, b) \mid (s - r)$. By Bezout's Lemma, this implies that there exist integers u, v such that $au + bv = s - r$, so that $au + r = s - bv$. Taking $x = u$ and $y = -v$, we see that $ax + r = by + s$, so the progressions intersect.

($\Longrightarrow$): Suppose the given progressions intersect; i.e., there exist $x, y \in \mathbb{Z}$ such that $ax + r = by + s$. Rearranging, we see that $ax - by = s - r$, so Bezout's Lemma implies $\gcd(a, -b) \mid (s - r)$. But $\gcd(a, -b) = \gcd(a, b)$, so we are done. □

Exercise 7. Show that if $\gcd(a,b)=1$, then $\gcd(a-b,a+b)=1$ or 2. When is the $\gcd$ equal to 2?

Proof. Suppose $\gcd(a,b)=1$. Then there exist integers x,y such that $ax-by=1$, as $\gcd(a,b)=\gcd(a,-b)=1$. We note that

$$(a+b)(x-y)+(a-b)(x+y)=ax-by+bx-ay+ax-bx-by+ay$$

$$\implies (a+b)(x-y)+(a-b)(x+y)=2ax-2by=2(ax-by)=2.$$

Taking $u=x-y$ and $v=x+y$, we see $(a+b)u+(a-b)v=2$, so that $\gcd(a+b,a-b)\mid 2$. This implies $\gcd(a+b,a-b)=1$ or 2. □

We have $\gcd(a-b,a+b)=2$ exactly when both a and b are odd, as that implies $a\pm b$ are both even.

Homework 3: Fundamental Theorem of Arithmetic

Exercise 1. Prove that for any a,b positive integers, we have $\operatorname{lcm}(a,b)\cdot\gcd(a,b)=ab$.

Proof. Write the prime factorizations $a=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ and $b=p_1^{\beta_1}\cdots p_r^{\beta_r}$, where the p_i are pairwise distinct and the α_i and β_i are non-negative integers, possibly zero. Then we know

$$\gcd(a,b)=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\beta_i)} \text{ and } \operatorname{lcm}(a,b)=\prod_{i=1}^{r}p_i^{\max(\alpha_i,\beta_i)}, \text{ so that}$$

$$\operatorname{lcm}(a,b)\cdot\gcd(a,b)=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)}.$$

Of course, we know that $ab=p_1^{\alpha_1+\beta_1}\cdots p_r^{\alpha_r+\beta_r}$, so it suffices to show that $\alpha+\beta=\min(\alpha,\beta)+\max(\alpha,\beta)$ for any $\alpha,\beta\in\mathbb{Z}$. Without loss of generality, suppose $\alpha\le\beta$. Then $\min(\alpha,\beta)=\alpha$ and $\max(\alpha,\beta)=\beta$, so the claim immediately follows. □

Exercise 2. The squarefree integers are the positive integers k that are not divisible by the square of any prime. Prove that every integer $n\ge 2$ can be written uniquely as the product of a square and a squarefree integer.

Proof. Fix $n\in\mathbb{Z}_{\ge 2}$. By the Fundamental Theorem of Arithmetic (FTA), write $n=p_1^{a_1}\cdots p_n^{a_k}$ for unique pairwise distinct primes p_i and integers $a_i\ge 1$. By the Division Algorithm, write $a_i=2q_i+r_i$, where r_i is either 0 or 1, so that

$$n=\prod_{i=1}^{k}p_i^{a_i}=\prod_{i=1}p_i^{2q_i+r_i}=\prod_{i=1}^{k}(p_i^{q_i})^2\cdot\prod_{i=1}^{k}p_i^{r_i},$$

and set $s=(p_1^{q_1})^2\cdots(p_k^{q_k})^2$ and $t=p_1^{r_1}\cdots p_k^{r_k}$. Clearly, s is a perfect square, and since $r_i\in\{0,1\}$ for all i, t is not divisible by the square of any of the distinct primes p_i. Hence $n=st$, and such a factorization exists. The uniqueness part of the proof follows from the fact that t is uniquely determined: we must have $r_i<2$, and the Division Algorithm gives unique q_i and r_i for each a_i, so that this split can only happen in this one way. □

Exercise 3 (Chapter 7, #1)**.** Suppose that $\gcd(a,b)=1$, and $a \mid bc$. Show $a \mid c$.

Proof. Since $\gcd(a,b)=1$, there exist integers $x,y \in \mathbb{Z}$ such that $ax+by=1$. Multiplying by c gives $acx+bcy=c$, but since $a \mid bc$, we have $bc=ad$ for some $d \in \mathbb{Z}$. Hence $acx+bcy=acx+ady=a(cx+dy)=c$, which shows $a \mid c$. □

Exercise 4 (Chapter 7, #2)**.** Suppose that $\gcd(a,b)=1$, $a \mid c$, and $b \mid c$. Show $ab \mid c$.

Proof. Since $\gcd(a,b)=1$, there exist integers $x,y \in \mathbb{Z}$ such that $ax+by=1$. Multiplying by c gives $acx+bcy=c$, and since $a \mid c$ and $b \mid c$, we can write $c=as=bt$ for some $s,t \in \mathbb{Z}$. Now, substitute $c=acx+bcy=a(bt)x+b(as)y=ab(tx+sy)$, so this shows $ab \mid c$. □

Exercise 5 (Chapter 7, #3)**.** Let $s,t \in \mathbb{Z}$ be odd with $s>t\geq 1$ and $\gcd(s,t)=1$. Prove that the numbers $a:=st, b:=\frac{1}{2}(s^2-t^2)$, and $c:=\frac{1}{2}(s^2+t^2)$ are pairwise relatively prime.

Proof. For contradiction, suppose p is an arbitrary prime factor dividing a,b,c. Then by Euclid's Lemma, we have $p \mid a$, so either $p \mid s$ or $p \mid t$. Since s,t are both odd, we have that p is odd. We cannot have both $p \mid s$ and $p \mid t$, as we assumed $\gcd(s,t)=1$. Since the argument below will be symmetric with respect to s and t, we assume without loss of generality that $p \mid s$ but $p \nmid t$. Suppose for contradiction that $p \mid b = \frac{1}{2}(s^2-t^2)$, which would imply $p \mid (s^2-t^2)$. Certainly $p \mid s^2$, which would imply $p \mid t^2$. However, this is impossible, as if $t=p_1\cdots p_k$ where the p_i are unique by FTA, then $p \neq p_i$ for any $1 \leq i \leq n$. Squaring, we see that $t^2=p_1^2\cdots p_k^2$, and again $p \neq p_i$ for any $1\leq i \leq n$. This implies that $\gcd(a,b)=1$, as the prime p was picked arbitrarily. By similar argumentation, we see $\gcd(a,c)=1$.

Finally, we show $\gcd(b,c)=1$. Suppose p is a common prime factor of b and c. Then $p \mid (b+c) \iff p \mid s^2$, and $p \mid (c-b) \iff p \mid t^2$. But this is clearly impossible: by FTA write $s=p_1\cdots p_r$ and $t=q_1\cdots q_s$, for unique primes p_i and q_j. Because $\gcd(s,t)=1$, we see $p_i \neq q_j$ for all i,j, so by comparing, p cannot divide both s and t. Squaring, we see $s^2=p_1^2\cdots p_r^2$ and $t^2=q_1^2\cdots q_s^2$, which does not change the list of primes, so we cannot have both $p \mid s^2$ and $p \mid t^2$. Hence, we must have $\gcd(b,c)=1$, as p was picked arbitrarily. □

Exercise 6. Suppose that $\gcd(a,b)=1$ and $c \neq \mathbb{Z}\backslash\{0\}$. Prove that $\gcd(ab,c)=\gcd(a,c)\gcd(b,c)$.

Proof. By the FTA, write $a=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ and $b=q_1^{\beta_1}\cdots q_r^{\beta_r}$ where the primes p_i are pairwise distinct and the primes q_i are also pairwise distinct, *chosen so that* it is possible to write

$$c=p_1^{\lambda_1}\cdots p_r^{\lambda_r}q_1^{\mu_1}\cdots q_s^{\mu_s}=\prod_{i=1}^{r}p_i^{\lambda_i}\cdot\prod_{j=1}^{s}q_j^{\mu_j},$$

where the $\alpha_i,\beta_j,\lambda_i,\mu_j$ are all non-negative integers, possibly zero. Since $\gcd(a,b)=1$, we have $p_i \neq q_j$ for all $1\leq i\leq r$, $1\leq j\leq s$. Now we know

$$ab=\prod_{i=1}^{r}p_i^{\alpha_i}\cdot\prod_{j=1}^{s}q_j^{\beta_j},\text{ so that }\gcd(ab,c)=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\lambda_i)}\cdot\prod_{j=1}^{s}q_j^{\min(\beta_j,\mu_j)}.$$

Because $p_i \neq q_j$ for all i,j, write $a=p_1^{\alpha_1}\cdots p_r^{\alpha_r}\cdots q_1^0\cdots q_s^0$ and $b=p_1^0\cdots p_r^0 q_1^{\beta_1}\cdots q_s^{\beta_s}$, so now we compute $\gcd(a,c)$ and $\gcd(b,c)$:

$$\gcd(a,c)=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\lambda_i)}\cdot\prod_{j=1}^{s}q_j^{\min(0,\mu_j)}=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\lambda_i)}\text{ and}$$

$$\gcd(b,c) = \prod_{i=1}^{r} p_i^{\min(0,\lambda_i)} \cdot \prod_{j=1}^{s} q_j^{\min(\beta_j,\mu_j)} = \prod_{j=1}^{s} q_j^{\min(\beta_j,\mu_j)},$$

from which a straight-forward inspection shows $\gcd(ab,c) = \gcd(a,c) \cdot \gcd(b,c)$. □

Homework 4: Euler's Totient Function

Exercises 1 through 3 is Section 67, but in more detail. Hence, we omit those exercises.

Exercise 4 (Wilson's Theorem)**.** Let p be a prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.

Proof. We first note an easier statement: $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$. This is because $x^2 \equiv x \pmod{p}$ is equivalent to $x^2 - 1 \pmod{p}$, and by Theorem 8.2 in the text, this monic polynomial has at most 2 roots. Clearly, the (only) roots are $x \equiv \pm 1$.

Now, this theorem holds for $p = 2$: we have $1! = 1 \equiv -1 \pmod{2}$, so assume $p \geq 3$, so that p is an odd prime. Consider the product

$$(p-1)! = (p-1)[(p-2)(p-3)\cdots(3)(2)(1)] = (p-1)(p-2)! \equiv (-1)(p-2)! \pmod{p}.$$

It suffices to show $(p-2)! \equiv 1 \pmod{p}$. But this is easy, as $\gcd(r,p) = 1$ for all $2 \leq r \leq p-2$, so that there exists s, satisfying $2 \leq s \leq p-2$ (after doing reduction modulo p) such that $rs \equiv 1 \pmod{p}$.[8] In particular, $s \neq r$ by the statement we noted above. Notice that the expansion

$$(p-2)! = (p-2)(p-3)\cdots(3)(2)$$

consists of $p-1$ terms, which is an even number, and by our discussion above, these terms may be paired off into $(p-1)/2$ pairs, where the product of each pair is 1 modulo p. Hence

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

$$\implies (p-1)! \equiv (-1)(p-2)! = (-1)(1) = -1 \pmod{p},$$

so we are done. □

Exercise 5 (Chapter 10, #1a)**.** Let $b_1 < b_2 < \cdots < b_{\varphi_m}$ be the integers between 1 and m, inclusive, that are relatively prime to m, and let $B = b_1 b_2 \cdots b_{\varphi_m}$. Show that $B \equiv \pm 1 \pmod{m}$.

Proof. Obviously, this holds for $m = 2$, so assume $m > 2$. We know that $\gcd(b_i, m) = 1$ for all $1 \leq i \leq \varphi(m)$, so that the equation $b_i x \equiv 1 \pmod{m}$ has a unique solution. Either we have $x \equiv b_i$, or $x \equiv b_j$ for some $j \neq i$. In the first case, we note that $b_i^2 \equiv 1 \pmod{m}$, and in the second case, we have $b_i b_j = b_j b_i \equiv 1 \pmod{m}$, where b_i, b_j are distinct integers.

Let $S := \{b_i : b_i^2 \equiv 1\}$ and $T := \{b_i : b_i b_j \equiv 1, i \neq j\}$. Because the solution to $b_i x \equiv 1 \pmod{m}$ is unique, the elements of T must must be partitioned pairs such that the product of each pair is $1 \pmod{m}$. From the above, we see that these sets must be disjoint, but they also partition the set $\{b_1, \ldots, b_{\varphi_m}\}$. From this, we see

$$B = \prod_{b_i \in S} b_i \cdot \prod_{b_i \in T} b_i = \prod_{b_i \in S} b_i \cdot 1 = \prod_{b_i \in S} b_i,$$

[8] That is, r has an multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$.

as the elements of T occur in pairs that are mutually inverse. Now, note that if $b_i^2 \equiv 1$, then $(m - b_i)^2 \equiv (-b_i)^2 \equiv 1 \pmod{m}$, so each element $b_i \in S$ is paired up with $-b_i \in S$. Now $b_i(-b_i) = -b_i^2 \equiv -1 \pmod{m}$, so $\prod_{b_i \in S} b_i = (-1)^k$ for some $k \in \mathbb{Z}$, implying $B = \pm 1$ $\pmod{m}$. □

Exercise 6 (Chapter 10, #2)**.** Assume that $\varphi(3750) = 1000$. Use this fact to find a number a such that $a \equiv 7^{3003} \pmod{3750}$, $1 \leq a \leq 5000$, and $7 \nmid a$.

Proof. Since $\varphi(3750) = 1000$ and $\gcd(7, 3750) = 1$, it follows from Euler's Theorem that $7^{1000} \equiv 1 \pmod{3750}$. Hence

$$7^{3003} = 7^{3000+3} = (7^{1000})^3 7^3 \equiv 7^3 = 343 \pmod{3750},$$

but 343 is clearly divisible by 7. To fix this, note that $7 \nmid 3750$, so that an integer a can be found by adding 3750: $a = 3750 + 343 = \boxed{4093}$. □

Exercise 7 (Chapter 11, #2)**.** In this exercise, we discuss when $\varphi(m)$ is even and when $\varphi(m)$ is divisible by 4.

(a) If $m \geq 3$, explain why $\varphi(m)$ is even.

Proof. By the Fundamental Theorem of Arithmetic, write the prime factorization of m: $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes. It follows that $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for all $i \neq j$, so from the multiplicativity of the Euler totient function,

$$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

If there exists an odd prime p_i in the factorization of m, then $(p_i - 1)$ is even, so that the entire product above is even.

Otherwise, if no odd prime exists, we have that $r = 1$ and $p_1 = 2$, so that $m = 2^\alpha$. Since $m \geq 3$, we must have $\alpha \geq 2$, so that

$$\varphi(m) = 2^{\alpha-1}(2 - 1) = 2^{\alpha-1} \geq 2^1 = 2,$$

so that $\varphi(m)$ is still even. □

(b) $\varphi(m)$ is "usually" divisible by 4. Describe all the m's for which $\varphi(m)$ is not divisible by 4.

Solution. Write the prime factorization of m: $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes, so that

$$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

If m has at least two distinct odd prime factors $p_i \neq p_j$, then $p_i - 1$ and $p_j - 1$ are both even, so that $4 \mid (p_i - 1)(p_j - 1)$, and hence $4 \mid \varphi(m)$. Hence, we consider the following three cases.

Case I: m has no odd prime factors. Then $m = 2^k$ for some $k \geq 0$. It follows that $\varphi(m) = 2^{k-1}(2 - 1) = 2^{k-1}$, and 2^{k-1} is divisible by 4 whenever $k - 1 \geq 2 \iff k = 3$. In this case, we see that for $m = 1, 2, 4$, $\varphi(m)$ is not a multiple of 4.

Case II: $m = 2^k p^\ell$, $k > 0$, $\ell > 0$ for some odd prime p. Since $\gcd(2, p) = 1$, it follows that

$$\varphi(m) = \varphi(2^k)\varphi(p^\ell) = 2^{k-1}p^{\ell-1}(p-1).$$

Again, if $k \geq 3$, then $4 \mid \varphi(m)$, so suppose $k = 1, 2$. If $k = 2$, then $p - 1$ is always even, so that $4 \mid \varphi(m)$, so now we consider the case $k = 1$. Clearly, $4 \nmid p^{\ell-1}$, so if $4 \mid \varphi(m)$, we must have $4 \mid (p-1)$, i.e., $p \equiv 1 \pmod 4$. Hence, in this case, we see that $4 \nmid \varphi(m)$ whenever $p \not\equiv 1 \pmod 4$, i.e., $p \equiv 3 \pmod 4$, and $m = 2p^\ell$.

Case III: $m = p^\ell$ for $\ell > 0$, where p is an odd prime. Then $\varphi(m) = p^{\ell-1}(p-1)$, which is never divisible by 4 unless $p - 1 \equiv 0 \pmod 4$, i.e., $p \equiv 1 \pmod 4$. In this case, we see that $4 \mid \varphi(m)$ whenever $p \equiv 3 \pmod 4$ and $m = p^\ell$.

Hence, all the values of m where $4 \nmid \varphi(m)$ are $\boxed{m = 1, 2, 4, p^\ell, 2p^\ell}$ where p is a prime congruent to 3 modulo 4. •

Exercise 8 (Chapter 11, #3)**.** Suppose that $p_1, p_2, \ldots, p_r$ are distinct primes that divide an integer m.

(a) Show that $\varphi(m) = m \displaystyle\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

Proof. Using the list of distinct primes above, write the prime factorization of m: $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Now by multiplicativity,

$$\begin{aligned}\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) &= \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{r} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{r} p_i^{\alpha_i} \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right),\end{aligned}$$

so we are done. □

(b) Find $\varphi(1000000)$: $\varphi(10^6) = 10^6 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10^6 \cdot \frac{1}{2} \cdot \frac{4}{5} = \boxed{400000}$.

Exercise 9. Solve the following.

(a) Find a positive integer x such that $x \equiv 5 \pmod{24}$ and $x \equiv 17 \pmod{18}$.

Solution. We need to find some x such that $x = 24a + 5 = 18b + 17$, which gives the relation $24a - 18b = 12$, which reduces to $4a - 3b = 2$. This is a linear equation which we can solve by the Linear Equation Theorem, but it is easier to note $20 - 18 = 4(5) - 3(6) = 2$, so setting $a = 5$ and $b = 6$ gives the solution $x = 24(5) + 5 = \boxed{125}$. Indeed, $125 - 5 = 120$ is divisible by 24 and $125 - 17 = 108$ is divisible by 18. •

(b) Does there exist an integer x with $x \equiv 20 \pmod{24}$ and $x \equiv 16 \pmod{18}$?

Solution. We try to find some x with $x = 24a + 20 = 18b + 16$, where $a, b \in \mathbb{Z}$, which gives the relation $24a - 18b = -4$, which reduces to $12a - 9b = -2$. This is impossible as $3 \mid (12a - 9b)$, but $3 \nmid (-2)$, so no such integer can exist. •

Homework 5: Prime Numbers

Exercise 1 (Chapter 12, #2)**.** This exercise concerns generalizations of Euclid's argument that there are infinitely many primes.

(a) Show that there are infinitely many primes congruent to $5 \bmod 6$.

Proof. Take an arbitrary finite list of primes congruent to $5 \bmod 6$: $L := \{5, p_1, p_2, \dots, p_k\}$, where $p_i \neq 5$ and the p_i are pairwise distinct. Consider the number $A = 6p_1p_2 \cdots p_k + 5$; we observe $A \equiv 5 \pmod 6$. If A is prime, we note $A \notin L$ as $A > 5$ and $A > p_i$ for all i, so $L \cup \{A\}$ is a larger set of primes congruent to $5 \bmod 6$.

If A is composite, the Fundamental Theorem of Arithmetic states that A has a prime factorization $A = q_1q_2 \cdots q_r$. But by construction, $5 \nmid A$, as otherwise $5 \nmid 6p_1p_2 \cdots p_k$, and we have $p_i \neq 5$. Similarly, $p_i \nmid A$, as otherwise $p_i \mid 5$, which is impossible. Hence, $q_j \notin L$. Now, there are four types of primes, falling into the congruence classes of $1, 2, 3, 5 \pmod 6$. The only prime congruent to $2 \pmod 6$ is 2, and clearly $2 \nmid A$. Similarly, the only prime congruent to $3 \pmod 6$ is 3, and clearly $3 \nmid A$. If $q_j \equiv 1 \pmod 6$ for all $1 \le j \le r$, then

$$A = q_1q_2 \cdots q_r \equiv 1 \cdot 1 \cdots 1 = 1 \pmod 6,$$

which is impossible as $A \equiv 5 \pmod 6$. Hence, there exists some q_j congruent to $5 \pmod 6$, with $q_j \notin L$. Hence, $L \cup \{q_j\}$ is a larger set of primes congruent to $5 \bmod 6$. This demonstrates that there are infinitely many primes congruent to $5 \pmod 6$, as any finite list could be arbitrarily extended. □

(b) Try the same idea, with $A = 5p_1p_2 \cdots p_k + 4$, to show that there are infinitely many primes congruent to $4 \pmod 5$. What goes wrong?

Solution. We observe that $19 \equiv 4 \pmod 5$, so we try computing $A = 5(19) + 4 = 99 = 3 \times 3 \times 11$. This is problematic, as none of these prime factors are congruent to $4 \pmod 5$, so we cannot presume the existence of such a prime. •

Exercise 2 (Chapter 12, #5)**.** In this exercise, we determine how many times a prime occurs in the prime factorization of $n!$.

(a) Find the highest power of 2 dividing the numbers $1!, 2!, \dots, 10!$.

Number	Highest Power	Number	Highest Power
1!	0	6!	4
2!	1	7!	4
3!	1	8!	7
4!	3	9!	7
5!	3	10!	8

(b) Formulate a rule that gives the highest power of 2 dividing $n!$. Use this rule to compute the highest power of 2 dividing $100!$ and $1000!$.

Solution. There are $\lfloor n/2 \rfloor$ multiples of 2 between the integers 1 and n, inclusive, and more generally, $\lfloor n/2^k \rfloor$ multiples of 2^k between 1 and n. Each successive higher power of 2 $(2, 4, 8, 16,$ etc.) introduces one more 2 in the factorization of $n!$, so by counting, we have the formula (letting 2^m be the highest power of 2 that divides $n!$), letting $\nu_p(n)$ denote the highest exponent of p that divides n, i.e., the *p-adic valuation* of n:

$$\nu_p(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \cdots + \left\lfloor \frac{n}{2^m} \right\rfloor. \tag{2}$$

Using this, we can quickly compute

$$\begin{aligned}\nu_2(100!) &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor \\ &= 50 + 25 + 12 + 6 + 3 + 1 = \boxed{97}\end{aligned}$$

and $\nu_2(1000!) = \sum_{k=1}^{9} \left\lfloor \frac{n}{2^k} \right\rfloor = \boxed{994}$. •

(c) Prove that the rule we found in (b) is correct.

Proof. We prove by counting. There are $\lfloor n/2^k \rfloor$ multiples of 2^k between the integers 1 and n, inclusive; in particular, there are $\lfloor n/2 \rfloor$ even integers from 1 to n, which contribute at least one factor of 2 in the prime factorization of $n!$. Each multiple of 2^2 contributes an additional factor, and 2^3 another additional factor, and so on, which gives us (2). □

(d) Repeat (a), (b), and (c), but this time for the largest power of 3 dividing $n!$.

Solution. The rule we get is basically the same, with the same argument, so for brevity, we will not repeat it here:

$$\nu_3(n!) = \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{9} \right\rfloor + \cdots + \left\lfloor \frac{n}{3^m} \right\rfloor,$$

where m is the highest power of 3 dividing n. We compute

$$\nu_3(100!) = \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{9} \right\rfloor + \left\lfloor \frac{100}{27} \right\rfloor + \left\lfloor \frac{100}{81} \right\rfloor = 33 + 11 + 3 + 1 = \boxed{48}, \text{ and}$$

$$\nu_3(1000!) = \sum_{k=1}^{6} \left\lfloor \frac{1000}{3^k} \right\rfloor = \boxed{498}.$$

•

(e) What is the general rule? Then compute the highest power of 7 dividing $1000!$ and the highest power of 11 dividing $5000!$.

Solution. We have

$$\nu_p(n!) = \sum_{k=1}^{m} \left\lfloor \frac{n}{p^k} \right\rfloor, \tag{3}$$

where m is the highest power of p dividing $n!$. By computation, we establish that

$$\nu_7(1000!) = \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{49} \right\rfloor + \left\lfloor \frac{1000}{343} \right\rfloor = \boxed{164} \text{ and}$$

$$\nu_{11}(5000!) = \left\lfloor \frac{5000}{11} \right\rfloor + \left\lfloor \frac{5000}{121} \right\rfloor + \left\lfloor \frac{5000}{1331} \right\rfloor = \boxed{498}.$$

•

(f) Prove that if p is prime and $p^m \mid n!$, then $m < n/(p-1)$.

Proof. From (3), observe that we must have, letting M denote the highest exponent of p dividing $n!$,

$$m \leq \nu_p(n!) = \sum_{k=1}^{M} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{M} \frac{n}{p^k} = \frac{n}{p} + \frac{n}{p^2} + \cdots + \frac{n}{p^M} = \frac{n(1+p+\cdots+p^{M-1})}{p^M}$$

$$\implies m < \frac{n(1+p+\cdots+p^{M-1})}{(p^M-1)} = \frac{n}{p-1},$$

where we noted the identity $(p^M - 1) = (p-1)(1+p+\cdots+p^{M-1})$. This completes the proof. □

Exercise 3 (Chapter 13, #1a)**.** Explain why the statement "1/5 of all numbers are congruent to $2 \pmod 5$" makes sense using the counting function

$$F(x) = \#\{n \in \mathbb{Z}^+ : n \leq x \text{ and } n \equiv 2 \pmod 5\}.$$

Solution. Observe the weak bounds $\frac{n}{5} - 23 \leq F(n) \leq \frac{n}{5} + 37$. Now

$$\lim_{n\to\infty} \frac{\frac{n}{5} - 23}{n} = \lim_{n\to\infty} \frac{n-115}{5n} = \frac{1}{5} \text{ and}$$

$$\lim_{n\to\infty} \frac{\frac{n}{5} + 37}{n} = \lim_{n\to\infty} \frac{n+185}{5n} = \frac{1}{5},$$

so by the Squeeze Theorem, we see $\lim\limits_{n\to\infty} F(n)/n = 1/5$. Hence, asymptotically, $1/5$ of all numbers are congruent to 2 modulo 5. •

Exercise 4 (Chapter 13, #3)**.** If $n \geq 2$, show that the numbers $n!+2, n!+3, \ldots, n!+n$ are all composite.

Proof. Consider the number $n!+k$, for some $2 \leq k \leq n$, which is in the list of consecutive integers above. Notice that $k \mid n!$, as $n! = n(n-1)\cdots k \cdots (3)(2)(1)$, and clearly $k \mid k$. Hence $k \mid (n!+k)$. Now, whenever $n \geq 2$, we have $n! \geq 2$, so that $n!+k > k$. This means that k is a non-trivial proper factor of $n!+k$; i.e., $n!+k$ is not prime. □

Exercise 5. Show that for all $n \in \mathbb{N}$, there exists a positive integer x such that $x, x+1, \ldots, x+(n-1)$ are all not squarefree.

Proof. Pick n arbitrary distinct primes $p_0, p_1, \ldots, p_{n-1}$. Let x be a solution to the simultaneous congruences $x \equiv -k \pmod{p_k^2}$, which exists by the Chinese Remainder Theorem (we have $\gcd(p_i^2, p_j^2) = 1$ whenever $i \neq j$). Then $p_k^2 \mid (x+k)$, so the numbers $x+k$, for $0 \leq k \leq n-1$, are not squarefree. □

Exercise 6. Prove the following.

(a) Suppose n is a positive integer. Prove that $n!+1$ has a prime divisor larger than n.

Proof. Take an integer k with $2 \leq k \leq n$. Then $k \mid n!$ as we have seen in Exercise 4. This implies $n!+1 \equiv 1 \pmod k$, so that $k \nmid (n!+1)$. In particular, if $k = p$, where p is a prime at most n, then $p \nmid (n!+1)$. Hence, $n!+1$ has no prime divisors at most n, but prime divisors of $n!+1$ must exist by the Fundamental Theorem of Arithmetic, so any prime divisor must be greater than n. □

(b) Using part (a), prove that there are infinitely many primes.

Proof. Assume for contradiction $P = \{p_1, p_2, \dots, p_k\}$ are all the primes that exist, and suppose $p_1 < p_2 < \cdots < p_k$. Consider the number $p_k! + 1$. By part (a), if q is a prime factor of $p_k! + 1$, then $q > p_k > \cdots > p_1$, so that $q \notin P$, a contradiction. □

Exercise 7. This exercise concerns the Euler totient function.

(a) Suppose $n \in \mathbb{Z}^+$ satisfies $\varphi(n) = 36$. What are all of the possible prime factors that can possibly divide n?

Solution. Let $p \mid n$, where p is prime. We claim that $\varphi(p) \mid \varphi(n)$: notice that $\varphi(p) = p - 1$, and that if $n = p^\alpha m$, where $\gcd(p, m) = 1$, then $\varphi(n) = \varphi(p^\alpha)\varphi(m) = p^{\alpha-1}(p-1)\varphi(m)$, which obviously has a factor of $p - 1 = \varphi(p)$. Using this, we find all primes p such that $\varphi(p) = 36$, i.e., $p - 1 = 1, 2, 3, 4, 6, 9, 12, 18, 36$. By checking, we see that the possible primes are $p = \boxed{2, 3, 5, 7, 13, 19, 37}$. •

(b) Find all integers n such that $\varphi(n) = 36$.

Solution. Any such integer n must consist of powers of the primes listed above, so write $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, so that $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_n^{\alpha_n})$. We work our way from the top down on the list of primes. If $37 \mid n$, then $\varphi(n) = \varphi(37^i k)$ for some k with $\gcd(37, k) = 1$, so we have $\varphi(n) = \varphi(37^i)\varphi(k) = 36$. But $\varphi(37^1) = 36$, so the only choices we have are $k = 1, 2$, giving $n = \boxed{37, 74}$.

Now, suppose 37 does not exist in the factorization of n, but suppose $19 \mid n$. Write $n = 19^i k$, for k with $\gcd(19, k) = 1$, so that $\varphi(n) = \varphi(19^i)\varphi(k) = 36$. Again, we check that $i = 1$ is the only possibility, so that $\varphi(k) = 2$. It is readily checked that we only have $k = 3, 4, 6$, yielding $n = \boxed{57, 76, 114}$.

Now, if $n = 13^i k$, where $\gcd(k, 13) = 1$, then $\varphi(n) = \varphi(13^i)\varphi(k)$. Now $\varphi(13^2) = 13(13 - 1) = 156 > 36$, so we must have $k = 1$. But then $\varphi(k) = 3$, which is impossible as $\varphi(m)$ is even whenever $m \geq 3$, so we find no new solutions

Thus, the rest of the solutions must be of the form $n = 2^\alpha 3^\beta 5^\gamma 7^\delta$. Using the multiplicativity of the φ-function, we see that $7^{\delta-1} \mid \varphi(n) = 36$, so that $\delta = 0, 1$. We now take cases.

Case I: If $\delta = 1$, we have

$$\varphi(n) = \varphi(2^\alpha 3^\beta 5^\gamma)\varphi(7) = 36 \iff \varphi(2^\alpha 3^\beta 5^\gamma) = 6.$$

By a similar argument, if $\gamma > 0$, then $(5 - 1) = 4 \mid 6$, which is impossible, so we are forced to have $\gamma = 0$, and the factorization of n looks like $n = 2^\alpha \cdot 3^\beta \cdot 7$. Now if $\alpha > 0$, we have $\varphi(2^\alpha 3^\beta) = 2^{\alpha-1}3^{\beta-1}(3-1) = 2^\alpha 3^{\beta-1} = 6$, which yields the possibility $2^1 3^{2-1} = 6$, so that $n = 2^1 \cdot 3^2 \cdot 7 = \boxed{126}$. In the case where $\alpha > 0$, we note $\varphi(9) = 6$, so $\varphi(9 \cdot 7) = 6 \cdot 6 = 36$, yielding $n = \boxed{63}$.

Case II: If $\delta = 0$, we have $\varphi(n) = \varphi(2^\alpha 3^\beta 5^\gamma) = 36$. If $\gamma > 0$, then $\varphi(2^\alpha 3^\beta 5^\gamma) = 5^{\gamma-1}(5-1)\varphi(2^\alpha 3^\beta) = 36$, implying $5^{\gamma-1}\varphi(2^\alpha 3^\beta) = 9$, so that $\gamma = 1$. But now the situation $\varphi(2^\alpha 3^\beta) = 9$ is impossible, as $2^\alpha 3^\beta \geq 2$ whenever $\alpha > 0$, so we must have $\gamma = 0$. It is clear by brute checking that n is not a power of 2 nor a power of 3, so we must have

$$\varphi(n) = \varphi(2^\alpha)\varphi(3^\beta) = 2^{\alpha-1}3^{\beta-1}(3-1) = 2^\alpha 3^{\beta-1} = 36.$$

Clearly $\alpha = 2$ and $\beta = 3$, giving $n = 2^2 3^3 = \boxed{108}$ as the final solution. •

Exercise 8. Let p denote an odd prime. Using Wilson's Theorem, prove that

$$1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Proof. Write the product above as

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

Now, note $-k \equiv p-k \pmod{p}$ for all $1 \leq k \leq \frac{p-1}{2}$, so that $k = (-1)(-k) \equiv -(p-k) \pmod{p}$. Now, we flip some of the signs in (4) with numbers which are congruent modulo p, and note that we have flipped $(p-1)/2$ numbers:

$$\begin{aligned}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \cdot \left((-1) \cdot (-2) \cdots \left(-\frac{p-1}{2}\right)\right) \cdot (-1)^{(p-1)/2} \\ &\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) \cdot \left((p-1)(p-2) \cdots \frac{p+1}{2}\right) \cdot (-1)^{(p-1)/2} \\ &\equiv (p-1)! \cdot (-1)^{(p-1)/2} \equiv -1 \cdot (-1)^{(p-1)/2} = (-1)^{(p+1)/2} \pmod{p}\end{aligned}$$

where the last line follows from Wilson's Theorem. □

Homework 6: Modular Roots

Exercise 1. Find a solution to the congruence $x^{463} \equiv 34 \pmod{1147}$.

Solution. Notice $1156 = 34^2$, and $1147 = 1156 - 9 = 34^2 - 9^2$, so 1156 factors as $1156 = (34-3)(34+3) = 31 \times 37$. Hence $\varphi(1147) = 30 \times 36 = 1080$. Now, we find the inverse of 463 modulo 1080; i.e., we want some $x_1 \in \mathbb{Z}^+$ and $y_1 \in \mathbb{Z}$ such that $463x_1 + 1080y_1 = 1$. By inspection, $\gcd(463, 1080) = 1$, so this has linear equation has integer solutions. Now

$$\begin{aligned} 1080 &= 2 \cdot 463 + 154 \\ 463 &= 3 \cdot 154 + 1, \end{aligned}$$

so that $1 = 463 - 3 \cdot 154 = 463 - 3 \cdot (1080 - 2 \cdot 463) = 7 \cdot 463 - 3 \cdot 1080$, so take $x_1 = 7$. Now, we claim that $x := 34^7 \pmod{1147}$ is a solution, as we have

$$x^{463} = (34^7)^{463} = 34^{3 \cdot 1080 + 1} \equiv 1^3 \cdot 34 = 34 \pmod{1147}$$

by Euler's Theorem. To find $34^7 \pmod{1147}$, we successively square 34:

$$34^2 = 1156 \equiv 9 \pmod{1147}, \; 34^4 \equiv 9^2 = 81 \pmod{1147}.$$

Hence $34^7 = 34^4 34^2 34^1 \equiv 9 \cdot 81 \cdot 34 = 24786 \equiv \boxed{699} \pmod{1147}$. •

Exercise 2 (Chapter 17, #3a)**.** Let $b, k, m \in \mathbb{Z}$ satisfy $\gcd(b, m) = 1$ and $\gcd(\varphi(m), k) = 1$. Show that b has exactly one kth root modulo m.

Proof. Since $\gcd(\varphi(m), k) = 1$, there is some $u \in \mathbb{Z}$ such that $ku \equiv 1 \pmod{\varphi(m)}$, and this integer u is unique up to equivalence modulo n. Let x be any kth root of b modulo m; it suffices to show $x \equiv b^u \pmod{m}$. We know that $x^k \equiv b \pmod{m}$, so that $x^{ku} \equiv b^u \pmod{m}$. But now we know $ku \equiv 1 \pmod{\varphi(m)}$, so write $ku = q\varphi(m) + 1$, so we observe $x^{ku} = x^{q\varphi(m)}x \equiv 1^q x = x \pmod{m}$ by Euler's Theorem, so that $x \equiv x^{ku} \equiv b^u \pmod{m}$. □

Exercise 3 (Chapter 17, #4)**.** Our method for solving $x^k \equiv b \pmod{m}$ is to first find integers u, v with $ku - \varphi(m)v = 1$, and then the solution is $x \equiv bu \pmod{m}$. However, our proof of this was contingent on the assumption that $\gcd(b, m) = 1$.

(a) Prove that if m is a product of distinct primes, show that $x \equiv b^u \pmod{m}$ is always a solution to $x^k \equiv b \pmod{m}$, even if $\gcd(b, m) > 1$.

Proof. We know that $ku = 1 + \varphi(m)v$, so that $x^k \equiv b^{uk} \pmod{m}$. Write $m = p_1 p_2 \cdots p_r$ for distinct primes p_i, and if $\gcd(b, m) > 1$, set without loss of generality $\gcd(b, m) =: g = p_1 p_2 \cdots p_s$, where $s \leq r$, so that $b = gq$ for some $q \in \mathbb{Z}$ satisfying $\gcd(q, m) = 1$. Now $x^k \equiv b^{uk} = g^{uk}q^{uk} \equiv g^{uk}q \pmod{m}$ by Euler's Theorem applied to q. Hence, write

$$x^k \equiv b^{uk} \equiv g^{uk}q = p_1^{uk}p_2^{uk} \cdots p_s^{uk}q \pmod{p_1 p_2 \cdots p_r}.$$

It suffices to show $m \mid (b^{uk} - b)$, so that $b \equiv b^{uk}$, but since $m = p_1 p_2 \ldots p_r$, it suffices to check $p_i \mid (b^{uk} - b)$ for all $i \leq r$. For all primes p_i with $1 \leq i \leq s$, this is obvious, so suppose p_j $(j > s)$ is a prime that does not occur in the factorization of b; without loss of generality, assume $j = r$. Then we note $\varphi(m) = (p_1 - 1)(p_2 - 1) \ldots (p_r - 1)$; in particular, $(p_r - 1) \mid \varphi(m)$, so that $(p_r - 1) \mid \varphi(m)v$, and thus $uk \equiv 1 \pmod{p_r - 1}$. But by Fermat's Little Theorem,

$$b^{uk} = b^{1+y(p_r-1)} \equiv b \cdot (b^{(p_r-1)})^y \equiv b \pmod{1}^y \equiv b \pmod{p_r},$$

so we are done. □

(b) Show that our method does not work for the congruence $x^5 \equiv 6 \pmod{9}$.

Proof. We have $\varphi(9) = 6$, so we try to find an inverse of 5 modulo 6, which is 5 as $5 \times 5 \equiv 1 \pmod{6}$. Our method claims that $x \equiv 6^5 \mod 9$, but $6^5 = 2^5 3^5 \equiv 2^5 \cdot 0 \equiv 0 \pmod{9}$. Clearly, $0^5 \not\equiv 6 \pmod{9}$, so our method fails. □

In the main notes, we have briefly mentioned the problems with taking square roots modulo m. Exercise 4 explains this in more detail.

Exercise 4 (Chapter 17, #5)**.** In this exercise, we discuss the limits of the method described for solving $x^k \equiv b \pmod{m}$.

(a) Try to use the methods in this chapter to compute the square root of $23 \pmod{1279}$. What goes wrong?

Solution. We want to find a solution to $x^2 \equiv 23 \pmod{1279}$. Using the fact that 1279 is prime, we compute $\varphi(1279) = 1278 = 2 \times 3^2 \times 71$. But now we have an issue, as $\gcd(2, 1278) = 2 \neq 1$, so 2 does not even have an inverse modulo 1278. Hence, we are stuck. •

(b) More generally, if p is an odd prime, explain why the methods in this chapter cannot be used to find square roots modulo p.

Solution. We know that if p is an odd prime, then $\varphi(p) = p - 1$ is even. But we want a solution to $x^2 \equiv b \pmod{p}$, which involves finding an inverse to 2 modulo $p - 1$, which is impossible as $\gcd(2, p - 1) = 2$. •

(c) Even more generally, explain why our method for computing kth roots modulo m does not work if $\gcd(k, \varphi(m)) > 1$.

Solution. In this case, the inverse of k modulo $\varphi(m)$ does not exist, so we cannot proceed. •

Exercise 5 (Chapter 18, #1)**.** Decode the following message, which was sent using the modulus $m = 7081$ and $k = 1789$: $5192 \;\; 2604 \;\; 4222$.

Solution. First, note that $7081 = 73 \times 97$, so $\varphi(7081) = 72 \times 96 = 6912$. We first find an inverse u to 1789 modulo 6912, which amounts to solving $1789u + 6912v = 1$, which we can do by the Euclidean algorithm:

$$\begin{aligned} 6912 &= 3 \cdot 1789 + 1545 \\ 1789 &= 1 \cdot 1545 + 244 \\ 1545 &= 6 \cdot 244 + 81 \\ 244 &= 3 \cdot 81 + 1, \end{aligned}$$

so backsolving yields $u = 85$. Now, we must compute $5192^{85}, 2604^{85}$, and 4222^{85} modulo 7081, which we can do by computing $b, b^2, b^4, \ldots, b^{32}, b^{64}$ for $b \in \{5192, 2604, 4222\}$, and noting $85 = 64 + 16 + 4 + 1$. These computations are best done by computer: $5192^{85} \equiv 1615$, $2604^{85} \equiv 2823$, $4222^{85} \equiv 1130$. Undoing the cipher by pairing letters from each word, we get $\boxed{\text{FERMAT}}$ as the hidden message. •

Exercise 6 (Chapter 18, #2)**.** It may appear that RSA decryption does not work if we are unlucky enough to choose a message a that is not relatively prime to m. Of course, when $m = pq$ and p, q are large, this is very unlikely to occur.

(a) Show that in fact RSA decryption does work for all messages a, regardless of whether they have a factor in common with m.

Proof. Pick an exponent $k \in \mathbb{Z}^+$ which is coprime to $\varphi(m)$, and let $u \in \mathbb{Z}^+$ be such that $ku \equiv 1 \pmod{\varphi(m)}$. We know from Exercise 3a that b^u is always a solution to the congruence $x^k \equiv b \pmod{m}$, which is what we must solve to decrypt, so we just need to show that this solution is unique. Now, if $\gcd(a, m) > 1$, we must have $\gcd(a, m) = p, q, m$. If $\gcd(a, m) = m$, then $a \equiv 0 \pmod{m}$, which is obviously unique.

Now, without loss of generality let $\gcd(a, m) = p$, so that $q \nmid a$. Now, a is a solution to the congruence $x^k \equiv b \pmod{m}$, which is equivalent to solving $x^k \equiv b \pmod{p}$ and $x^k \equiv b \pmod{q}$. Since $p \mid a$, we know $p \mid b = a^k$, so that $x^k \equiv 0 \pmod{p}$, and this solution is unique. Also, the solution to $x^k \equiv b \pmod{q}$ is unique, so this gives us a system of congruences which has a unique solution via the Chinese Remainder Theorem. We know b^u is a solution, so that $b^u \equiv a \pmod{m}$ and we are done. □

(b) More generally, show that RSA decryption works for all messages a as long as m is a product of distinct primes.

Proof. This is basically the same argument as above. Let $u \in \mathbb{Z}^+$ be such that $ku \equiv 1 \pmod{\varphi(m)}$. Again, from Exercise 3a, b^u is a solution to the congruence $x^k \equiv b \pmod{m}$, which is what we need to solve if we want to decrypt. We again just need to show uniqueness. Suppose $\gcd(a, m) = 1$, so that if we write $m = p_1 p_2 \cdots p_r$, without loss of generality set $g = \gcd(a, m) = p_1 p_2 \cdots p_s$, where $s \leq r$.

Now, we know that solving $x^k \equiv b \pmod{m}$ is equivalent to solving the simultaneous congruences $x^k \equiv b \pmod{p_i}$, for all $i \leq r$. If $i \leq s$, then $a \equiv 0 \pmod{p_i}$ so $b \equiv 0 \pmod{p_i}$, so the unique solution to that subset of congruences is $x \equiv 0 \pmod{p_i}$ $(i \leq s)$. Now, if $i > s$, we appeal to Exercise 2a to obtain solutions $x \equiv x_i \pmod{p_i}$, $i > s$. Now, the Chinese Remainder Theorem gives us a unique solution to all of these congruences. We already knew b^u was a solution, so it must be unique. □

(c) Give an example with $m = 18$ and $a = 3$ where RSA decryption fails.

Solution. We have $\varphi(18) = 6$. We must find an exponent k, with $\gcd(k, 6) = 1$, such that if u is the inverse of k modulo 6, then $3^{uk} \not\equiv 3 \pmod{18}$. Take $k = 5$, so that $u = 5$ (as $5 \times 5 \equiv 1 \bmod 6$). Now $3^{25} = 3^{16} 3^8 3$, and we compute $3^2 \equiv 9$, $3^4 \equiv 9^2 \equiv 9 \pmod{18}$, so that $3^8 = 3^{16} \pmod{9}$, so $3^{25} \equiv (9)(9)(3) \equiv 9 \cdot 3 \equiv 9 \pmod{18}$, which is not congruent to 3, so we are done. •

Homework 7: Quadratic Reciprocity

We fix the following notation: If $a, m \in \mathbb{Z}$ and $\gcd(a, m) = 1$, we denote the *inverse of* a *modulo* m when it exists by writing a^{-1}. That is, $aa^{-1} \equiv 1 \pmod{m}$. This notation is well-defined, up to equivalence modulo m. We also define, for $k \geq 1$, the notation $a^{-k} := (a^{-1})^k$. It can be readily verified that the usual exponent rules over a ring of characteristic zero hold in this setting as well.

Exercise 1 (Chapter 21, #1b-c)**.** Determine whether each of the congruences has a solution: all of the moduli are primes.

(b) $x^2 \equiv 6780 \pmod{6781}$.

Solution. This is equivalent to asking if $x^2 \equiv -1 \pmod{6781}$. Now, we note $6781 \equiv 1 \pmod{4}$, so that -1 is a quadratic residue modulo 6781. Thus, this congruence has a solution. •

(c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$.

Solution. We complete the square to obtain $x^2 + 14x + 49 \equiv 84 \pmod{337}$, so we have $(x + 7)^2 \equiv 84$. We can make the change of variables $y := x + 7$ to obtain a congruence with the same number of solutions: $y^2 \equiv 84 \pmod{337}$. It is hard to tell whether 84 is a quadratic residue modulo 337, but certainly 4 is a QR, and we note $84 \times 4 = 336 \equiv -1 \pmod{337}$. Now, since $337 \equiv 1 \pmod{4}$, -1 is a quadratic residue modulo 337. Now, 4^{-1} modulo 337 (which exists because $\gcd(4, 337) = 1$) is also a quadratic residue as $(2^{-1})^2 \equiv 2^{-2} \equiv 4^{-1}$, so that we see $-1 \times 4^{-1} \equiv 84$ is also a QR by the quadratic residue multiplication rule. •

Exercise 2 (Chapter 21, #4)**.** Finish the proof of the second supplement to quadratic reciprocity for the other two cases: primes congruent to $1 \pmod 8$ and congruent to $5 \pmod 8$. Namely, prove that $\left(\frac{2}{p}\right) = 1$ when $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 5 \pmod 8$.

Proof. Let p be an odd prime. We first consider the case where $p \equiv 1 \pmod 8$, say $p = 8k+1$ for some $k \in \mathbb{Z}$. Then $p-1 = 8k$, so that $\frac{1}{2}(p-1) = 4k$. Consider now the product

$$A = 2 \cdot 4 \cdot 6 \cdots 4k \cdot [(4k+2) \cdots (8k)] = [2 \cdot 4 \cdots 4k] \cdot [8k \cdot (8k-2) \cdots (4k+2)],$$

consisting of all of the positive even numbers less than p. Now, it is easily verified that there are $4k - 2k = 2k$ even numbers greater than $\frac{1}{2}(p-1) = 4k$ and less than p, so we can write the product above as

$$A \equiv 2 \cdot 4 \cdot 6 \cdots 4k \cdot (-1) \cdot (-3) \cdot (1-4k) \equiv (-1)^{2k} \cdot (4k)! = (4k)!.$$

However, we also know by definition $A = 2^{(p-1)/2} \cdot (4k)!$, so this implies $2^{(p-1)/2} \equiv 1 \pmod p$, so that Euler's criterion gives $\left(\frac{2}{p}\right) = 1$.

The second case we consider is $p \equiv 5 \pmod 8$, say $p = 8k+5$ for some $k \in \mathbb{Z}$. Then $p-1 = 8k+4$, so that $\frac{1}{2}(p-1) = 4k+2$. Again, we consider the product

$$A = 2 \cdot 4 \cdots (4k+2) \cdot (4k+4) \cdots (8k+4) = [2 \cdot 4 \cdots (4k+2)] \cdot [(8k+4) \cdot (8k+2) \cdots (4k+4)],$$

consisting of all of the positive even numbers less than p. Again, we can count $2k+1$ even numbers greater than $\frac{1}{2}(p-1) = 4k+2$ and less than p, so by the same rearrangement trick,

$$A \equiv 2 \cdot 4 \cdots (4k+2) \cdot (-1) \cdot (-3) \cdots (-4k-1) \equiv (-1)^{2k+1} \cdot (4k+2)! = -(4k+2)!,$$

but by construction $A = 2^{(p-1)/2} \cdot (4k+2)!$, so this implies $2^{(p-1)/2} \equiv -1 \pmod p$, so that by Euler's criterion, we have $\left(\frac{2}{p}\right) = -1$. □

Exercise 3 (Chapter 21, #5)**.** Use the same ideas we used to verify Quadratic Reciprocity (Part II) to show the following.

(a) If $p \equiv 1 \pmod 5$, then $\left(\frac{5}{p}\right) = 1$.

Proof. Clearly, such a prime must be odd, so in fact $p \equiv 1 \pmod{10}$, so write $p = 10k+1$. Thus, $P := (p-1)/2 = 5k$, so consider the product

$$A = 5 \cdot 10 \cdots 25k = 5 \cdot 10 \cdot 15 \cdots \frac{5}{2}(p-1) = 5^P \cdot P!.$$

If we reduce these numbers modulo p into the range $-5k$ and $+5k$ (inclusive of the top bound), we observe that the multiples of 5 in these intervals take negative signs: $(5k, 10k+1), (15k+1, 20k+2)$. These intervals have the same length, and thus must contain the same number of multiples of 5, so the number of multiples of 5 we must replace by its negative is even; call that number $2a$ for some $a \in \mathbb{Z}$. By a similar argument as per Quadratic Reciprocity (Part II), we observe

$$A \equiv (-1)^{2a} \cdot P! = P!,$$

so that $5^P \equiv 1 \pmod 5$. Hence, by Euler's criterion, $\left(\frac{5}{p}\right) = 1$. □

(b) If $p \equiv 2 \pmod 5$ **and** p **is odd**, then $\left(\frac{5}{p}\right) = -1$.

Proof. Since p is odd, we see that in fact $p \equiv 7 \pmod{10}$, so that we may write $p = 10k + 7$ and $P := (p-1)/2 = 5k+3$. Consider the product

$$A = 5 \cdot 10 \cdots (25k+15) = 5 \cdot 10 \cdot 15 \cdots \frac{5}{2}(p-1) = 5^P \cdot P!.$$

If we reduce the numbers modulo p into the range $-(5k+3)$ and $5k+3$ (inclusive of the top bound), we observe that the multiples of 5 in these intervals take negative signs: $(5k+3, 10k+7), (15k+10, 20k+14)$. This is equivalent to finding the multiples of 5 in the following closed intervals: $[5k+5, 10k+5], [15k+15, 20k+10]$. Now, the second of these intervals contains one less multiple of 5 than the first, so the total number of multiples of 5 is odd; denote this number by $2b+1$ for some $b \in \mathbb{Z}$. By a similar argument as per Quadratic Reciprocity (Part II), we observe

$$A \equiv (-1)^{2b+1} \cdot P! = -P!,$$

so that $5^P \equiv -1 \pmod 5$. Hence, by Euler's criterion, $\left(\frac{5}{p}\right) = -1$. □

Exercise 4 (Chapter 22, #1b-c)**.** Use the Law of Quadratic Reciprocity to compute the following Legendre symbols.

(b) $\left(\dfrac{29}{541}\right) = \left(\dfrac{541}{29}\right) = \left(\dfrac{19}{29}\right) = \left(\dfrac{29}{19}\right) = \left(\dfrac{10}{19}\right) = \left(\dfrac{2}{19}\right)\left(\dfrac{5}{19}\right) = -1\left(\dfrac{19}{5}\right) = -\left(\dfrac{4}{5}\right) = \boxed{-1}$.

(c) $\left(\dfrac{101}{1987}\right) = \left(\dfrac{1987}{101}\right) = \left(\dfrac{68}{101}\right) = \left(\dfrac{4}{101}\right)\left(\dfrac{17}{101}\right) = 1 \cdot \left(\dfrac{101}{17}\right) = \left(\dfrac{-1}{17}\right) = \boxed{1}$.

Exercise 5 (Chapter 22, #3)**.** Show that there are infinitely many primes congruent to 1 $\pmod 3$.

Proof. Let $L := \{p_1, p_2, \ldots, p_r\}$ be a list of distinct primes congruent to $2 \pmod 3$. Consider the number $A = (2p_1p_2\cdots p_r)^2 + 3$. Notice that

$$A = 2^2 p_1^2 p_2^2 \cdots p_r^2 + 3 \equiv 1 \cdot 1 \cdots 1 = 1 \pmod 3,$$

so that A is congruent to 1 modulo 3. Now, if A is prime, then we are done, as $A > p_i$ for all $1 \le i \le r$. If A is composite, factor $A = q_1q_2\cdots q_s$ into a list of primes. Notice that $p_i \nmid A$ for all $1 \le i \le r$, as otherwise $p_i \mid 3 \implies p_i = 3$, which is impossible. Hence, the primes q_j are not on the list L of primes. Furthermore, A is odd, so the q_j's are all odd primes. Additionally, $A \equiv 0 \pmod{q_j}$, so that

$$(2p_1p_2\cdots p_r)^2 + 3 \equiv 0 \pmod{q_j},$$

so that $(2p_1p_2\cdots p_r)^2 \equiv -3 \pmod{q_j}$, so -3 is a quadratic residue modulo q_j. Denoting $q := q_j$, by quadratic reciprocity, write

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

so here we consider case-work. If $\left(\frac{-1}{q}\right) = \left(\frac{3}{q}\right) = 1$, then $q \equiv 1 \pmod 4$ and thus $\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = 1$. This implies q is a quadratic residue modulo 3; i.e., $q \equiv 1 \pmod 3$. On the other hand, if $\left(\frac{-1}{q}\right) = \left(\frac{3}{q}\right) = -1$, then $q \equiv 3 \pmod 4$ and thus $-1 = \left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right)$, so that again $\left(\frac{q}{3}\right) = 1$. This also implies $q \equiv 1 \pmod 3$, so we are done. □

Exercise 6 (Chapter 22, #4)**.** Let p be a prime number other than 2 and 5, and let A be some given number. Suppose $p \mid (A^2 - 5)$. Show that $p \equiv 1$ or $p \equiv 4 \pmod 5$.

Proof. Let $p \neq 2, 5$ so that p is an odd prime coprime to 5. If $p \mid (A^2 - 5)$, then $A^2 \equiv 5 \pmod p$. That is, 5 is a quadratic residue modulo p, i.e., $\left(\frac{5}{p}\right) = 1$. Since $5 \equiv 1 \pmod 4$, we see $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$, i.e., p is a quadratic residue modulo 5. The quadratic residues modulo 5 are $0, 1$, and 4, and we know $5 \nmid p$, so that $p \equiv 1$ or $p \equiv 4 \pmod 5$. □