Elementary Number Theory

Minh-Tam Trinh
after
Ngô Bảo Châu

University of Chicago
Fall 2015

Contents

0 Preface

This collection of notes summarizes the first half of the Math 175 course at the University of Chicago in the Fall 2015 quarter. Written very hastily, it has yet to be proofread carefully. All mistakes are attributable to the author, *not* to the instructor. The names we give to mathematical objects and theorems may differ from those in [JJ].

The section numbers roughly correspond to weeks of the quarter. Throughout, we use the following conventions:

$$\begin{aligned}
&\mathbb{N} = \{1, 2, 3, \ldots\}, \text{ the set of natural numbers} \\
&\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}, \text{ the set of integers} \\
&\mathbb{Q} = \{a/b : a, b \in \mathbb{Z} \text{ and } b \neq 0\}, \text{ the set of rational numbers} \\
&\mathbb{R} = \text{the set of real numbers}
\end{aligned}$$

This course is about the algebraic relationships that exist between integers, or more poetically, the patterns and symmetries hidden within $\mathbb{Z}$ and $\mathbb{Q}$. To students: *Please, do not feel as though these notes can only be read front-to-back. They were written to be a "user's manual," not a narrative!*

1 27 September

1.1 Background

Although everyone enrolled is required to have taken a previous course in proof-based mathematics, I wanted to review the "standard toolbox" of notations and techniques you should know. I am doing this because of the wide range of backgrounds that seem to be present among the students.

1.1.1 Sets

The notation $x \in X$ is to be read "x is an element of the set X." If P is a property of elements of S, then the notation $\{x \in X : x \text{ satisfies } \mathsf{P}\}$ means "the set of all elements $x \in X$ such that x satisfies P."

If X, Y are sets, then the notation $X \subseteq Y$ is to be read "X is a subset of Y." The *product of X and Y* is the set $X \times Y$ whose elements are ordered pairs (x, y) such that $x \in X$ and $y \in Y$. If X, Y are both subsets of another set Z, then we define their *intersection* to be

$$X \cap Y = \{z \in Z : z \in X \text{ and } z \in Y\} \tag{1}$$

and their *union* to be

$$X \cup Y = \{z \in Z : z \in X \text{ or } z \in Y\}. \tag{2}$$

The *complement of Y in X* is the set

$$X \setminus Y = \{x \in X : x \notin Y\}. \tag{3}$$

The *empty set* or *nullset* is the set that contains no elements, which is denoted $\varnothing$. The notation $\#X$ means "the number of elements of X," i.e., the *cardinality of X*.

1.1.2 Functions

Let $f : X \to Y$ be a map. We say that X is the *domain of f* and Y is the *codomain* or *range of f*. If $A \subseteq X$, then the *image of A under f* is the set

$$f(A) = \{f(a) : a \in A\} \subseteq Y. \tag{4}$$

If $B \subseteq Y$, then the *preimage of B under f* is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}. \tag{5}$$

If $y \in Y$, then mathematicians write $f^{-1}(y)$ in place of $f^{-1}(\{y\})$ and refer to this set as the *preimage of y under f*.

We say that f is *injective*, or an *injection*, iff it sends any pair of distinct elements of X to distinct elements of Y. In other words, f is injective if and only if, for all $x_1, x_2 \in X$, we have that $f(x_1) = f(x_2)$ implies $x_1 = x_2$. We say that f is *surjective*, or a *surjection*, iff $f(X) = Y$, i.e., every element of Y takes the form $f(x)$ for some $x \in X$.

"Super-Useful Fact"

If X, Y are finite of the same cardinality and $f : X \to Y$ is any function, then:

f is injective $\iff$ f is surjective.

Here is another way of thinking about injectivity and surjectivity:

(6) f is injective $\iff$ the preimage of any element of Y contains *at most* one element.

(7) f is surjective $\iff$ the preimage of any element of Y contains *at least* one element.

We say that f is *bijective*, or a *bijection*, iff it is both injective and surjective. If f is bijective, then every element $y \in Y$ has a unique preimage in X, so we can define the *inverse of* f to be the map $f^{-1} : Y \to X$ that sends y to this unique preimage.

As we see above, the notation f^{-1} is used in several slightly-different ways. This is an example of what's called "abuse of notation." Certain abuses of notation are tolerated in mathematical writing because they have proven more convenient than harmful.

1.1.3 Equivalence Relations

If X is a set, then to give an *equivalence relation on* X is to give a family of pairwise-disjoint subsets, called *equivalence classes*, whose union is X.

Example 1.1. This one was suggested by Professor Ngô. Let Monday be the set of all Mondays in human history, and let $\mathsf{Tuesday}, \ldots, \mathsf{Sunday}$ be defined similarly. Then

$$\mathsf{Monday}, \mathsf{Tuesday}, \ldots, \mathsf{Sunday} \tag{8}$$

gives an equivalence relation on the set of dates in human history, because each calendar date has a unique day-name.

Oftentimes, when working with equivalence relations, we introduce a symbol like $\sim$ or $\approx$ or $\equiv$ to indicate that two elements of X belong to the same equvalence class. (Naturally, we say that such elements are *equivalent*.) We write $X/\!\sim$ or an analogous notation to denote the set of equivalence classes. There is a natural map

$$X \to X/\!\sim \tag{9}$$

that sends every element $x \in X$ to the unique equivalence class containing x. We often denote this class by $[x]$, so that $x \sim y$ is equivalent to $[x] = [y]$ by definition.

Example 1.2. Fix $m \in \mathbb{N}$. Then we can define an equivalence relation on $\mathbb{Z}$ by setting $a \sim b$ if and only if m divides $a - b$. The corresponding family of subsets of $\mathbb{Z}$ is

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}, \tag{10}$$

where $a + m\mathbb{Z}$ denotes the set of integers of the form $a + mq$ for some $q \in \mathbb{Z}$. For this particular equivalence relation, it is conventional to write

$$a \equiv b \pmod{m} \tag{11}$$

to mean $a \sim b$. We will revisit this example in §3.1.

1.1.4 Factoring and Series

Exercise 1. Let x, y be indeterminates, and let $k \in \mathbb{N}$.

1. How do you factor $x^k - 1$?
2. How do you factor $x^k - y^k$?

3. How do you factor $x^k + 1$ for odd k? What goes wrong with this pattern for even k?

Exercise 2.

1. Suppose x is an indeterminate. Expand $(1 + x + x^2 + \cdots + x^n)(1 - x)$.
2. Using part (1), deduce that if x is a real number and $|x| < 1$, then

$$1 + x + x^2 + \cdots + x^n \tag{12}$$

converges to a real number as $n \to \infty$. What is this number, in terms of x?

Exercise 3.

1. Prove that

$$\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^{n+1}} \geq \frac{1}{2} \tag{13}$$

for all nonnegative integers n. You don't need induction.

2. Deduce that the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \tag{14}$$

diverges as $n \to \infty$. This argument was discovered by Nicole Oresme, a French natural philosopher of the late medieval era.

1.2 Classical Proof Techniques

I use the word "classical" in the conservative (Western) sense of, "known to the intellectual scene of the ancient Greeks."

1.2.1 Contradiction

I think everyone in the class understands how this works, so this is the only thing I want to mention about it:

> *[R]eductio ad absurdum*, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.
> —G. H. Hardy in *A Mathematician's Apology*

Disclaimer: I disagree strongly with a number of other things Hardy says in that book. On the other hand, Hardy was in a very melancholic state of mind when he wrote it.

1.2.2 Induction

In the first week, we proved that the principle of induction[1] and the well-ordering principle can be deduced from each other. Anyway, both are true.

Principle of Induction

If $\mathsf{P}(n)$ means "property P holds for the natural number n," then to prove $\mathsf{P}(n)$ for all $n \in \mathbb{N}$, it suffices to prove the following two statements:

[1] In this document, "induction" always means "strong induction."

1. *Base case.* $\mathsf{P}(1)$ holds.
2. *Inductive step.* Given any $n \in \mathbb{N}$, if $\mathsf{P}(m)$ holds for all $m < n$, then $\mathsf{P}(n)$ holds.

Exercise 4. Prove by induction that $1^3 + 2^3 + \cdots + n^3 = ((n^2 + n)/2)^2$ for all $n \in \mathbb{N}$.

Well-Ordering Principle
Every nonempty subset of $\mathbb{N}$ contains a smallest element.

Exercise 5. Using the well-ordering principle, show that every nonempty subset of $\mathbb{N}$ that is bounded above has a largest element.

1.3 Abstract Algebra

Traditionally, the subject of algebra began with the writing of *The Compendious Book on Calculation by Completion and Balancing* by al-Khwārizmī during the zenith of the Abbasid Caliphate. This is the book that introduced the idea of "solving the equation for x." But I would say that *abstract* algebra really begins with the invention of zero. What do I mean by this?

> Abstract algebra is about introducing *seemingly useless* structural abstractions into mathematics that pay back their worth enormously as more and more theory accumulates around them, until their *naturality* and *simplicity* can finally be fully appreciated.

The number 0 was such a concept. If we attribute the discovery of 0 to the Indian mathematician Pingala, circa 200 BCE, then "abstract algebra" would predate "elementary algebra!"

(To be fair, the notion of an indeterminate variable x was also a revolutionary advance. But *The Compendious Book* seems to have focused on establishing the *methods* for solving linear and quadratic equations in x, rather than cultivating their *abstraction* in the way that, say, Galois did centuries later. The distinction is quite fine and difficult to communicate.)

We here summarize the most important algebraic structures for this course. We will return to them in closer detail in subsections §3.1 and §4.2.

1.3.1 Groups

A *group* consists of a set G and a function $* : G \times G \to G$, written $(a, b) \mapsto a * b$ and called its *law* or *operation*, such that the following hold:

1. *Associativity.* $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. *Identity.* There exists an element $e \in G$, called the *identity*, such that $a * e = a = e * a$ for all $a \in G$.
3. *Inversion.* For every $a \in G$, there exists an element b, called the *inverse of* a, such that $a * b = e = b * a$.

We say that a group is *abelian* iff it furthermore satisfies:

4. *Commutativity.* $a * b = b * a$ for all $a, b \in G$.

Exercise 6. Which of the following form groups? Of those that do, which form abelian groups?

1. $\mathbb{Z}$ under addition.
2. $\mathbb{R}$ under addition.
3. $\mathbb{R}$ under multiplication.
4. $\mathbb{R} \setminus \{0\}$ under multiplication.
5. $\{+1, -1\}$ under multiplication.
6. $G_1 \times G_2$ (where G_i is a group with the operation $*_i$) under the operation $*$ defined by

$$(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2). \tag{15}$$

7. The set of pairs $(a_1, a_2) \in \mathbb{R} \times \mathbb{R}$ such that $a \neq 0$, under the operation $*$ defined by

$$(a_1, a_2) * (b_1, b_2) = (a_1 b_1, a_1 b_2 + a_2). \tag{16}$$

When the operation is unambiguous from the context, mathematicians often drop the $*$ symbol and write ab in place of $a * b$. However, if the operation is conventionally referred to as "addition," like in parts (1) and (2) of the preceding exercise, then they always keep the symbol $+$ to denote the operation, to avoid confusion with multiplication.

If G is a group, then a *subgroup of* G is a subset $H \subseteq G$ that forms a group in its own right with the same operation and identity element. This means three things: H is closed under the operation, i.e., $a, b \in H$ implies $ab \in H$; and, H contains the identity of G; and, if $a \in H$, then $a^{-1} \in H$. (Actually, the second follows from the first and third.)

Exercise 7.

1. Find all the subgroups of $\mathbb{Z}$. *Hint*: To get you started, $\{0\}$ is a subgroup.
2. Show that $\mathbb{Z} \times \mathbb{Z}$ contains subgroups that do *not* take the form $H_1 \times H_2$ for some $H_1, H_2 \subseteq \mathbb{Z}$.

If G_1, G_2 are groups, then we say that a map $f : G_1 \to G_2$ is a *group homomorphism*, or *group morphism*, iff

$$f(ab) = f(a)f(b) \tag{17}$$

for all $a, b \in G_1$. Intuitively, f is a homomorphism iff it "sends" the operation of G_1 onto that of G_2. When it is, it necessarily sends the identity of G_1 to that of G_2. We say that f is a *group isomorphism* iff it is a bijective group homomorphism. In this case we write $G_1 \simeq G_2$.

Exercise 8. Consider the groups formed by $\mathbb{Z}$ and $\mathbb{R}$ under addition. Which of the following are group homomorphisms? Of those that do, which are isomorphisms?

1. The translation map $t_a : \mathbb{Z} \to \mathbb{Z}$ defined by $t_a(n) = n + a$, where $a \in \mathbb{Z}$ is fixed.
2. The scaling map $m_a : \mathbb{Z} \to \mathbb{Z}$ defined by $m_a(n) = an$, where $a \in \mathbb{Z}$ is fixed.
3. The scaling map $m_a : \mathbb{R} \to \mathbb{R}$ defined by $m_a(x) = ax$, where $a \in \mathbb{R}$ is fixed.
4. The map $\mathbb{R} \to \mathbb{R}_{>0}$ that sends $x \mapsto e^x$, where the operation on $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ is multiplication.

1.3.2 Rings and Fields

A *ring* consists of a set R and functions $+, \times : R \times R \to R$, where $+$ is called its *addition* and $\times$ is called its *multiplication*, such that:

1. R forms an abelian group under $+$. Its identity under $+$ is called the *additive identity* and denoted 0.
2. $\times$ is associative, meaning $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.
3. There exists an element $1 \in R$, called the *multiplicative identity* or *unity*, such that $a \times 1 = a = 1 \times a$ for all $a \in R$.
4. The *distributive identities*

$$a \times (b + c) = a \times b + a \times c \tag{18}$$
$$(b + c) \times a = b \times a + c \times a \tag{19}$$

   hold for all $a, b, c \in R$.

In this course, all rings will be *commutative*, meaning the multiplication is commutative:

4. $a \times b = b \times a$ for all $a, b \in R$.

Note that the elements of R "almost" form an abelian group under $\times$. The only obstacle is that not every element may have an inverse with respect to $\times$.

Exercise 9.

1. Show that if R is a ring, then $0 \times a = 0$ for every $a \in R$. *Hint*: $0 = 0 + 0$.
2. Deduce that if R is *nontrivial*, meaning $0 \neq 1$, then 0 cannot have an inverse.

We say that an element $a \in R$ is a *unit* iff it has an inverse $b \in R$ with respect to $\times$, i.e., $a \times b = 1$. We write $R^\times$ for the set of units of R. Then, by construction, $R^\times$ forms an abelian group under $\times$, called the *unit group of* R. We say that R is a *field* iff $R^\times = R \setminus \{0\}$.

Exercise 10. Check that the following objects form rings. Which of them form fields?

1. $\mathbb{Z}$.
2. $\mathbb{Q}$.
3. $\mathbb{R}$.
4. The set $\mathbb{R}[t]$ of polynomials in t with real coefficients.
5. $R_1 \times R_2$ (where R_1, R_2 are rings), under the addition

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \tag{20}$$

   and the multiplication

$$(a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2). \tag{21}$$

Henceforth, we drop the $\times$ notation and write ab in place of $a \times b$. If R_1, R_2 are rings, then we say that a map $f : R_1 \to R_2$ is a *ring homomorphism*, or *ring morphism*, iff

$$f(a+b) = f(a) + f(b), \tag{22}$$

$$f(ab) = f(a)f(b), \tag{23}$$

$$f(1) = 1, \tag{24}$$

i.e., f preserves both the addition and the multiplication operations and preserves unity. We say that f is a *ring isomorphism* iff it is a bijective ring homomorphism. In this case we write $R_1 \simeq R_2$.

Exercise 11. Let R_1, R_2 be rings, and consider $R_1 \times R_2$ under the ring structure described in part (5) of Exercise 10. Show that the projection map $R_1 \times R_2 \to R_1$ that sends $(x_1, x_2) \mapsto x_1$ is a ring homomorphism.

2 6 October

2.1 Divisors

Let $a, b \in \mathbb{Z}$. As you know well, we say that b *divides* a, and write $b \mid a$, iff there exists $q \in \mathbb{Z}$ such that $a = bq$. In this case, we also say that b is a *divisor of* a and that a is a *multiple of* b. For example, according to this definition, 1 divides everything and everything divides 0.

Theorem 2.1 (Division Algorithm)**.** *For all $a, b \in \mathbb{N}$, there exist $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \tag{25}$$

and $0 \leq r < b$. We say that q is the quotient *and r is the* remainder *upon long-dividing a by b.*

Proof. By Cor. 5 to the well-ordering principle, there is a largest multiple of b that is less than or equal to a. We can write it as bq for some $q \in \mathbb{Z}$. It remains to show that $r = a - bq$ satisfies $r < a$. Indeed, if this were not true, then we would have $b(q+1) \leq bq + r = a$, contradicting the definition of bq. □

If $a, b \in \mathbb{N}$, then the *greatest common divisor* (*gcd*) *of* a, b is the largest $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$. It is denoted $\gcd(a, b)$. We say that a and b are *coprime* or *relatively prime* iff $\gcd(a, b) = 1$, i.e., the only (positive) common divisor of a and b is 1.

Exercise 12. In this exercise, we demonstrate that there's a fast algorithm to compute the gcd of any two natural numbers a, b.

1. Prove that if $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$, then the common divisors of a and b are precisely the common divisors of b and r.
2. Deduce that if $a, b, r \geq 1$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Part (2) implies:

Euclidean Algorithm

If we want to compute the gcd of two numbers $a, b \in \mathbb{N}$, where $a > b$, then we can replace a with b and replace b with the remainder upon long-dividing a by b, as long as this remainder is nonzero.

In practice, it looks like this:

3. Let $a_0, a_1 \in \mathbb{N}$, where $a_0 > a_1$. For $k \in \mathbb{N}$, let q_k and a_{k+1} be defined inductively as the quotient and remainder, respectively, upon long-dividing a_{k-1} by a_k:

   $$a_{k-1} = a_k q_k + a_{k+1}. \tag{26}$$

   Then $\gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{n-1}, a_n) = a_n$, where a_n is the last nonzero term in the sequence $a_0 > a_1 > \ldots$, which does in fact eventually reach zero by the well-ordering principle.
4. Using part (3), compute $\gcd(a_0, a_1)$ for $(a_0, a_1) = (2771, 1360), (3003, 770)$.

Theorem 2.2 (Bézout)**.** *For all $a, b \in \mathbb{N}$, there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = \gcd(a, b). \tag{27}$$

In particular, if a and b are coprime, then 1, and hence every integer, is a $\mathbb{Z}$-linear combination of a and b.

Proof. Set $(a_0, a_1) = (a, b)$ in the notation of Exercise 12. Assume without loss of generality that $a_0 > a_1$. The algorithm produces sequences of numbers a_k and q_k that satisfy (26) for all k and such that

$$a_0 > a_1 > \cdots > a_n = \gcd(a, b) \tag{28}$$

for some n.

The $k = n - 1$ case of (26) says $a_{n-2} = a_{n-1}q_{n-1} + a_n$. So we can express a_n as a $\mathbb{Z}$-linear combination of a_{n-1}, a_{n-2}. In general, we can express a_{k+1} as a $\mathbb{Z}$-linear combination of a_k, a_{k-1}, so by inductively substituting these expressions "back up the ladder," we can express $a_n = \gcd(a, b)$ as a $\mathbb{Z}$-linear combination of $a_0 = a$ and $a_1 = b$. □

If $a, b \in \mathbb{N}$, then the *least common multiple* (*lcm*) *of* a, b is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$. It is denoted $\operatorname{lcm}(a, b)$.

2.2 Prime Factorization

Recall, cf. §1.3.2, that the *units* of $\mathbb{Z}$ are the integers that have multiplicative inverses that are also integers. Hence, they are $+1$ and -1.

Let $n \geq 2$. We say that n is *prime* iff its only (positive) divisors are 1 and itself. We say that n is *composite* otherwise. By construction, then, $\mathbb{Z}$ consists of four kinds of numbers:

1. The additive identity 0.
2. The units ± 1.
3. The numbers $\pm p$, where $p \in \mathbb{N}$ is prime.
4. The numbers $\pm n$, where $n \in \mathbb{N}$ is composite.

We will find that the primes are the "building blocks" of the nonzero non-unit integers: Any such number *factors uniquely as a product of prime numbers*, and this factorization "knows" everything about the *divisibility properties* of the number. The theorem that says this is, for good reason, often called the Fundamental Theorem of Arithmetic:

Theorem 2.3 (Unique Prime Factorization)**.** *Let $p_1 < p_2 < \ldots$ be the ascending sequence of prime numbers. Then every natural number n can be expressed in the form*

$$\prod_{i \geq 1} p_i^{e_i} \tag{29}$$

for some sequence $e_1, e_2, \ldots$ of nonnegative integers, only finitely many of which are nonzero. Moreover, this sequence is uniquely determined by n.

Proof of the existence of the factorization. Consider the set $\mathcal{C}$ of counterexamples, i.e., the set of all natural numbers that cannot be expressed as a product of primes. If $\mathcal{C}$ is nonempty, then it contains a minimal element m. We know m can't be prime, because a prime is certainly a product of primes! So m must be composite.

The set $\mathcal{D}$ of divisors of m that are strictly between 1 and m is nonempty. So $\mathcal{D}$ has a minimal element p. If p is not prime, then there is a divisor of p strictly between 1 and p, which will also be a divisor of m, contradicting the minimality of p. Thus, p is prime. Since $m' = m/p$ is less than m, it is a product of primes. But now, $m = m'p$ is also a product of primes, a contradiction. Therefore, $\mathcal{C}$ is empty. □

Remark 2.4. I cherish the above proof, because when I was learning elementary number theory, I discovered it on my own after learning about the well-ordering principle. On the other hand, I find the justification of the uniqueness of the factorization to be tedious and not especially enlightening, so I've omitted it.

If $n \in \mathbb{N}$ and p is a prime, then we write $v_p(n)$ to denote the exponent for p in the prime factorization of n.

Exercise 13.

1. Convince yourself that $b \mid a$ if and only if $v_p(b) \leq v_p(a)$ for all prime p.
2. Convince yourself that $v_p(\gcd(a,b)) = \min(v_p(a), v_p(b))$. What is the analogous statement for $\operatorname{lcm}(a,b)$?
3. From part (2), deduce that $\gcd(a,b)\operatorname{lcm}(a,b) = ab$ for all $a, b \in \mathbb{N}$.
4. From part (2), deduce a criterion for the coprimality of a and b in terms of the values $v_p(a)$ and $v_p(b)$.

Corollary 2.5 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose there are only finitely many primes, say $p_1 < \cdots < p_r$. Let

$$N = p_1 p_2 \cdots p_r + 1. \tag{30}$$

Then no prime divides N, so the exponents in the prime factorization of N must all be zero. But now $N = 1$, whereas each p_i is larger than 1, a contradiction. □

Proof of Euler. Suppose there are only finitely many primes. Then by unique prime factorization, we can check that

$$\prod_p \frac{1}{1 - 1/p} = \sum_{n=1}^{\infty} \frac{1}{n}, \tag{31}$$

where the left-hand side converges because it is a finite product. But the right-hand side diverges by Exercise 3, a contradiction. □

Exercise 14. Show that there are infinitely many primes of the form $6k+5$, where $k \in \mathbb{Z}$. *Hint:* Look at $2\prod_{p \in \mathcal{P}_5} p + 1$, where p is the set of primes of the form $6k+5$.

3 13 October

3.1 Rings of Residues Modulo m

If you need a refresher on groups and rings, please take a look at §1.3.1 and §1.3.2.

Let $m \in \mathbb{N}$. In Example 1.2, we defined an equivalence relation on $\mathbb{Z}$ by setting

$$a \equiv b \pmod{m} \iff m \mid (a-b). \tag{32}$$

We say that integers that are equivalent under this relation are *congruent modulo* m. For any given integer a, the *residue class of* a *modulo* m is its equivalence class under $\equiv$, i.e., the set

$$[a]_m := a + m\mathbb{Z} = \{a + mq : q \in \mathbb{Z}\}. \tag{33}$$

We write $\mathbb{Z}/m\mathbb{Z}$ to denote the set of residue classes modulo m. Explicitly,

$$\mathbb{Z}/m\mathbb{Z} = \{[a]_m : 0 \leq a < m\}. \tag{34}$$

In this setting, (9) becomes a map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ called *reduction modulo* m.

Proposition 3.1. *For all $m \in \mathbb{N}$, the set $\mathbb{Z}/m\mathbb{Z}$ forms a (commutative) ring under the addition $[a]_m + [b]_m = [a+b]_m$ and the multiplication $[a]_m[b]_m = [ab]_m$. In particular, reduction modulo m is a surjective ring homomorphism.*

Exercise 15 (**Most Important**)**.**

1. Justify the preceding proposition to yourself.

Now that we know $\mathbb{Z}/m\mathbb{Z}$ is a ring, we can make the following definition: If $a \in \mathbb{Z}$, then a is *invertible modulo* m iff $[a]_m$ is a unit of $\mathbb{Z}/m\mathbb{Z}$, i.e., there exists an integer $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.

2. Using Bézout, prove that if $\gcd(a, m) = 1$, then a is invertible modulo m.
3. Prove that if $\gcd(a, m) > 1$, then there exists $c \in \mathbb{Z}$ such that $c \not\equiv 0 \pmod{m}$ but $ac \equiv 0 \pmod{m}$. *Hint:* Consider $m/\gcd(a, m)$.
4. Deduce from part (3) that if $\gcd(a, m) > 1$, then a is not invertible modulo m. *Hint:* Suppose $ab \equiv 1$ and consider abc, where c is the element from part (3).
5. Deduce that the *unit group modulo* m is

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{[a]_m : 0 \leq a < m \text{ such that } \gcd(a, m) = 1\}. \tag{35}$$

6. Deduce that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.

In light of part (6), professional number theorists will often write $\mathbb{F}_p$ in place of $\mathbb{Z}/p\mathbb{Z}$, with $\mathbb{F}$ standing for "field."

3.2 Linear Congruences

Professor Ngô had an amusing story about the apocrypha behind the Chinese Remainder Theorem.

Exercise 16. Show that a group homomorphism $f : G_1 \to G_2$ is injective if and only if $f(x)$ being the identity of G_2 implies x being the identity of G_1. *Hint:* If $a, b \in G_1$ and e_1 is the identity of G_1, then $a = b$ if and only if $ab^{-1} = e_1$, where b^{-1} is the inverse of G_1.

Exercise 17. Show that in general, if $n \mid N$, then the map $[a]_N \mapsto [a]_n$ is a surjective ring homomorphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Theorem 3.2 (Chinese Remainder)**.** *If $m, n \in \mathbb{N}$ are coprime, then the map*

$$\mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \tag{36}$$

that sends $[a]_{mn} \mapsto ([a]_m, [a]_n)$ is a ring isomorphism.

Proof. The map is at least a ring homomorphism by Exercise 17, so it remains to check its bijectivity.

Since both the domain and the codomain have mn elements, it suffices by the Super-Useful Fact (§1.1.2) to prove that the map is injective. By Exercise 16, it suffices to show that if $a \in \mathbb{Z}$ satisfies both $a \equiv 0 \pmod m$ and $a \equiv 0 \pmod n$, then it satisfies $a \equiv 0 \pmod{mn}$. For all prime p, Exercise 13(1) indicates that

$$v_p(m), v_p(n) \leq v_p(a). \tag{37}$$

But $\gcd(m, n) = 1$, so for all p, at least one of $v_p(m), v_p(n)$ equals 0. We deduce that

$$v_p(mn) = v_p(m) + v_p(n) \leq v_p(a) \tag{38}$$

for all p, meaning $mn \mid a$, as needed. □

Corollary 3.3. *If $n_1, \ldots, n_r \in \mathbb{N}$ are pairwise coprime, then the map*

$$\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \tag{39}$$

that sends $[a]_{n_1 \cdots n_r} \mapsto ([a]_{n_1}, \ldots, [a]_{n_r})$ is a ring isomorphism.

Proof. Induct on r, using the fact that $\gcd(n_1 \cdots n_{r-1}, n_r) = \gcd(\gcd(n_1 \cdots n_{r-2}, n_{r-1}), n_r)$. □

Exercise 18. If $\mathcal{N}$ is any set of natural numbers, then we define $\gcd(\mathcal{N})$ to be the largest $d \in \mathbb{N}$ such that $d \mid n$ for all $n \in \mathcal{N}$. We say that the elements of $\mathcal{N}$ are *jointly coprime* iff $\gcd(\mathcal{N}) = 1$. Show that if the elements of $\mathcal{N}$ are pairwise coprime, then they are jointly coprime, but that the converse is not true.

Corollary 3.4. *Let f be a polynomial with integer coefficients, and for all $n \in \mathbb{N}$, let c_n be the number of residue classes $[x]_n$ modulo n such that $f(x) \equiv 0 \pmod n$. If $n_1, \ldots, n_r \in \mathbb{N}$ are pairwise coprime, then $c_{n_1 \cdots n_r} = c_{n_1} \cdots c_{n_r}$.*

Exercise 19 (Systems of Linear Congruences)**.** Let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise coprime, and let $a_i, b_i \in \mathbb{Z}$ for $1 \leq i \leq r$. In this exercise, we show how to find all integers x such that

$$a_i x \equiv b_i \pmod{m_i} \tag{40}$$

for all i, i.e., how to solve a system of r simultaneous linear congruences modulo pairwise-coprime moduli. We do this in two parts.

1. **Local Solution.** To solve (40) for a single index i: In what follows, let $d_i = \gcd(a_i, m_i)$.

(a) Using Bézout, prove that $a_i x \equiv b_i \pmod{m_i}$ has a solution in x if and only if d_i divides b_i.

(b) Check that if $d_i \mid b_i$, then

$$a_i x \equiv b_i \pmod{m_i} \iff (a_i/d_i)x \equiv b_i/d_i \pmod{m_i/d_i}, \tag{41}$$

In other words, after replacing (m_i, a_i, b_i) with $(m_i/d_i, a_i/d_i, b_i/d_i)$, we reduce to solving (40) in the case where $\gcd(a_i, m_i) = 1$.

(c) Check that if $\gcd(a_i, m_i) = 1$, then (40) has a unique solution. *Hint:* Exercise 15(2).

2. **Global Solution.** Having solved (40) for individual indices, it remains to show that if we can construct $x_1, \ldots, x_r \in \mathbb{Z}$ such that

$$a_i x_i \equiv b_i \pmod{m_i}, \tag{42}$$

then we can construct $x \in \mathbb{Z}$ such that $x \equiv x_i \pmod{m_i}$, as this x will solve (40).

(a) Let $M_i = (m_1 \cdots m_r)/m_i$. Convince yourself that we can find $N_i \in \mathbb{N}$ such that $M_i N_i \equiv 1 \pmod{m_i}$ for all i.

(b) Convince yourself that $x = x_1 M_1 N_1 + \cdots + x_r M_r N_r$ is the fellow you want.

3. **Practice.**

(a) Find all $x \in \mathbb{Z}$ such that $15x \equiv 21 \pmod{24}$.

(b) Find all $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases} \tag{43}$$

simultaneously.

The Chinese Remainder Theorem has a "multiplicative" analogue for unit groups. To explain it, observe that if $f : R_1 \to R_2$ is a ring homomorphism, then f restricts to a group homomorphism $f^\times : R_1^\times \to R_2^\times$. In particular, if f is bijective, then the same is true of its inverse, so if f is a ring isomorphism, then $f^\times$ is a group isomorphism. By this argument, Cor. 3.3 implies:

Corollary 3.5. *If $n_1, \ldots, n_r \in \mathbb{N}$ are pairwise coprime, then the map*

$$(\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z})^\times \to \prod_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z})^\times \tag{44}$$

that sends $[a]_{n_1 \cdots n_r} \mapsto ([a]_{n_1}, \ldots, [a]_{n_r})$ is a group isomorphism.

3.3 The Newton-Hensel Method

In calculus, Newton's method is an algorithm to approximate the zero of a smooth function $f : \mathbb{R} \to \mathbb{R}$. Namely, one first guesses a nearby approximation x_0; then, if f is sufficiently well-behaved, the actual zero will be $\lim_k x_k$, where

$$x_{k+1} = x_k - f(x_k)/f'(x_k) \tag{45}$$

for all k.

The number theorist Kurt Hensel discovered an analogous method to solve polynomial congruences more efficiently when the modulus is a large prime power p^e. Namely, one starts with a solution to $f \equiv 0$ modulo p, then lifts it to a solution or solutions modulo p^2, then lifts those to solutions modulo p^3, and so on, using a formula similar to Newton's. Like Newton's method, the lifting step can fail if f is not well-behaved. The difference is that, while Newton's method only gives a unique x_k at the kth step, Hensel's method allows the possibility that in going from, say, p^k to p^{k+1}, there might be multiple lifts of a given solution.

In what follows, let us recall for the reader that if f is a polynomial with real coefficients, say $f(t) = a_0 + a_1 t + \cdots + a_n t^n$, then its *(formal) derivative with respect to* t is

$$f'(t) = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}. \tag{46}$$

For all $x, \varepsilon \in \mathbb{R}$, we find that

$$\begin{aligned} f(x+\varepsilon) - f(x) &= (a_0 + a_1(x+\varepsilon) + \cdots + a_n(x+\varepsilon)^n) - (a_0 + a_1 x + \cdots + a_n x^n) \\ &= \varepsilon \cdot a_1 + (\varepsilon \cdot 2a_2 x + \varepsilon^2 \cdot a_2) + \cdots + (\varepsilon \cdot n a_n x^{n-1} + \cdots + \varepsilon^n \cdot a_n) \\ &= \varepsilon f'(x) + \varepsilon^2 g(x), \end{aligned} \tag{47}$$

where g is some "error-term" polynomial. This should be familiar to you: If $\varepsilon \neq 0$, then dividing both sides by ε and letting $\varepsilon \to 0$ gives us the limit definition of the derivative f'.

Theorem 3.6 (Hensel)**.** *Let f be a polynomial with integer coefficients. Suppose there exist $k \in \mathbb{N}$ and $x_k \in \mathbb{Z}$ such that $f(x_k) \equiv 0 \pmod{p^k}$ and $f'(x_k) \not\equiv 0 \pmod{p}$. Then there exists $x_{k+1} \in \mathbb{Z}$ such that $x_{k+1} \equiv x_k \pmod{p^k}$ and $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$, i.e., x_{k+1} is a "lift" of x_k to a solution of f modulo p^{k+1}.*

Explicitly, if $y_k \in \mathbb{Z}$ reduces to the multiplicative inverse of $f'(x_k)$ modulo p, then

$$x_{k+1} \equiv x_k - f(x_k) y_k \pmod{p^{k+1}}, \tag{48}$$

i.e., the analogue of the Newton formula holds.

Proof that x_k exists. First, there exists y_k such that $f'(x_k) y_k \equiv 1 \pmod{p}$ by Exercise 15. Let $\varepsilon_k = f(x_k) y_k$.

If $x_{k+1} \in \mathbb{Z}$ satisfies (48), then $x_{k+1} \equiv x_k \pmod{p^k}$ because $\varepsilon_k \equiv 0 \pmod{p^k}$. To show that $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$, use (47) to expand

$$f(x_{k+1}) = f(x_k - \varepsilon_k) = f(x_k) - \varepsilon_k f'(x_k) + \varepsilon_k^2 \cdot g(x_k) \tag{49}$$

for some polynomial g. Since $\varepsilon_k^2 \equiv 0 \pmod{p^{k+1}}$, reducing modulo p^{k+1} gives

$$f(x_{k+1}) \equiv f(x_k)(1 - \varepsilon_k) \pmod{p^{k+1}}. \tag{50}$$

But $p^k \mid f(x_k)$ and $p \mid (1 - \varepsilon_k)$, so $p^{k+1} \mid f(x_k)(1-\varepsilon_k)$. Therefore, $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$. □

Proof that any lift of x_k must satisfy (48). Suppose $\tilde{x}_{k+1} \in \mathbb{Z}$ satisfies $\tilde{x}_{k+1} \equiv x_k \pmod{p^k}$ and $f(\tilde{x}_{k+1}) \equiv 0 \pmod{p^{k+1}}$. We can write $f(x_k) = p^k a_k$ and $\tilde{x}_{k+1} = x_k + p^k \delta_k$ for some $a_k, \delta_k \in \mathbb{Z}$. Now, using (47),

$$0 \equiv f(\tilde{x}_{k+1}) \equiv f(x_k) + p^k \delta_k f'(x_k) \equiv p^k a_k + p^k \delta_k f'(x_k) \pmod{p^{k+1}}, \tag{51}$$

from which $0 \equiv a_k + \delta_k f'(x_k) \pmod{p}$. Rearranging, we obtain $\delta_k \equiv -a_k y_k \pmod{p}$, from which $p^k \delta_k \equiv -f(x_k) y_k \pmod{p^{k+1}}$. The result follows. □

Exercise 20. Suppose instead that, in the notation of Theorem 3.6, we have $f(x_k) \equiv 0 \pmod{p^k}$ but $f'(x_k) \equiv 0 \pmod{p}$ as well. Show that:

1. If $f(x_k) \equiv 0 \pmod{p^{k+1}}$, then $f(x_k + p^k\delta) \equiv 0 \pmod{p^{k+1}}$ for all $\delta \in \mathbb{Z}$, i.e., x_k has p distinct lifts to solutions of f modulo p^{k+1}. This is what we meant by Hensel's method allowing the possibility of multiple lifts from p^k to p^{k+1}.
2. If $f(x_k) \not\equiv 0 \pmod{p^{k+1}}$, then $f(x_k + p^k\delta) \not\equiv 0 \pmod{p^{k+1}}$ for all $\delta \in \mathbb{Z}$, i.e., x_k does not lift to any solution of f modulo p^{k+1}. This is what we meant by Hensel's method "failing" when f is not sufficiently well-behaved.

Exercise 21.

1. Find all $x \in \mathbb{Z}$ such that $x^3 + 1 \equiv 0 \pmod{11}$.
2. Using part (1), find all x such that $x^3 + 1 \equiv 0 \pmod{11^2}$.

4 20 October

4.1 Arithmetic Functions

An *arithmetic function* is just a function from $\mathbb{N}$ into $\mathbb{R}$ (or even more generally, into the complex numbers $\mathbb{C}$). Equivalently, it can be pictured as an infinite sequence in $\mathbb{R}$ or $\mathbb{C}$, indexed by the natural numbers.

We say that an arithmetic function $f : \mathbb{N} \to \mathbb{R}$ is *multiplicative* iff, for all coprime $m, n \in \mathbb{N}$, we have

$$f(mn) = f(m)f(n). \tag{52}$$

We say that f is *totally multiplicative* iff (52) holds even without the assumption that m and n are coprime. In general, we really only ever care about arithmetic functions when they're multiplicative or totally multiplicative.

Example 4.1. Here is a bestiary of multplicative arithmetic functions in number theory:

1. The constant function that sends every natural number to 1.
2. The *Euler totient function* φ defined by

   $$\varphi(n) = \#\{a \in \mathbb{N} : a \leq n \text{ and } \gcd(a, n) = 1\}. \tag{53}$$

   By Exercise 15,

   $$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times, \tag{54}$$

   so φ is multiplicative by Cor. 3.3 of the Chinese Remainder Theorem. It is not totally multiplicative because $\varphi(4) = 2$ but $\varphi(2) = 1$.
3. Fix $k \geq 0$. The *kth-power divisor function* σ_k is defined by

   $$\sigma_k(n) = \sum_{d|n} d^k, \tag{55}$$

   where the sum runs over positive divisors of n. For example, σ_0 computes the number of positive divisors of n, whereas σ_1 computes their sum. For this reason, σ_0 is called the *divisor-counting function*, whereas σ_1 is called simply the *divisor function* and alternatively denoted σ.
4. Fix a prime p. If $a \in \mathbb{Z}$, then we say that a is a *quadratic residue* (*QR*) *modulo* p if $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}$, and we say that a is a *quadratic non-residue* (*QNR*) *modulo* p otherwise. We define the *Legendre symbol of conductor* p to be the function $\left(\frac{\cdot}{p}\right)$ such that:

   $$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \not\equiv 0 \text{ and } a \text{ is a QR modulo } p \\ -1 & a \not\equiv 0 \text{ and } a \text{ is a QNR modulo } p \\ 0 & a \equiv 0 \pmod{p} \end{cases} \tag{56}$$

   Despite the awful notation, $\left(\frac{a}{p}\right)$ does not mean the rational number a/p. When we discuss the Legendre symbol in person, we usually pronounce $\left(\frac{a}{p}\right)$ as "the Legendre symbol of a over p" or "a on p." In Exercise 24, we'll show that it is *totally* multiplicative as a function of a.

Exercise 22. Use unique prime factorization to do the following:

1. Prove that σ_k is multiplicative for all $k \geq 0$. You might need parts (4) and (5) of the next exercise.
2. Convince yourself that a multiplicative arithmetic function is determined by its behavior on prime powers. As a special case, a totally multiplicative function is determined by its behavior on primes.

Exercise 23 (Important).

1. What is $\varphi(p)$ for prime p?
2. What is $\varphi(p^k)$ for prime p and arbitrary $k \in \mathbb{N}$?
3. Using the multiplicativity of φ, deduce a formula for $\varphi(n)$ in terms of the unique prime factorization of n.
4. What is $\sigma_k(p)$ for prime p?
5. What is $\sigma_k(p^\ell)$ prime p and arbitrary $\ell \in \mathbb{N}$?
6. Using the multiplicativity of σ_k, deduce formulae for $\sigma_0(n)$ and $\sigma_1(n)$ in terms of the unique prime factorization of n.

Exercise 24 (Important). Let p be a prime. We write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Show that a product of QR's modulo p is a QR modulo p. Deduce that the set of QR's modulo p forms a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Show that the product of a QR and a QNR modulo p is a QNR modulo p.
3. Show that if $p \geq 3$, then the homomorphism $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ that sends $x \mapsto x^2$ is 2-to-1, i.e., every element in the image has exactly 2 elements in its preimage.
4. Using part (3), deduce that there are as many nonzero QR's as QNR's modulo p.
5. Using part (4), show that a product of QNR's modulo p is a QR modulo p. (Tricky!)
6. Deduce that the Legendre symbol of conductor p is totally multiplicative.

4.2 Unit Groups Modulo m

Let G be a finite abelian group with identity e. If $x \in G$, then we write x^k to denote the composition of k copies of x under the operation of G. The *order of* x is the smallest natural number k such that $x^k = e$.

Exercise 25 (Euler-Fermat)**.** Let $m \in \mathbb{N}$. Recall from §1.3.2 that the unit group $(\mathbb{Z}/m\mathbb{Z})^\times$ is a finite abelian group under the operation of multiplication. Recall from Exercise 15 that it consists of the residue classes $[a]_m$ for precisely those a that are relatively prime to m.

1. Show that if G is a finite group and $g \in G$ is fixed, then the multiplication-by-g map $x \mapsto gx$ is a bijection from G to itself. *Hint:* What is the inverse?

2. Setting $G = (\mathbb{Z}/m\mathbb{Z})^\times$, deduce that if $g \in (\mathbb{Z}/m\mathbb{Z})^\times$ is fixed and $x_1, \ldots, x_{\varphi(m)}$ are all the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$, then

$$(gx_1, \ldots, gx_{\varphi(m)}) \tag{57}$$

is the same sequence of elements as

$$(x_1, \ldots, x_{\varphi(m)}) \tag{58}$$

but in a different order.

3. Deduce that $g^{\varphi(m)}$ is the identity of $\mathbb{Z}/m\mathbb{Z})^\times$. *Hint:* Using the two sequences in part (2), write the product of all the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ in two different ways. Since every element of the group has an inverse, you'll be able to cancel a certain term.

4. *Euler's Theorem.* Deduce that if a is relatively prime to m, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

5. *Fermat's Little Theorem.* Deduce that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

The theorems of Euler and Fermat concluding the previous exercise are special cases of Lagrange's Theorem on the orders of subgroups in finite groups:

Theorem 4.1 (Lagrange)**.** *If G is a finite group and H is a subgroup of G, then $\#H$ divides $\#G$.*

To see why Lagrange's Theorem implies Euler's: Let a be relatively prime to m. The residues modulo m of the integer powers of a are precisely $1, a, a^2, \ldots, a^{\ell-1}$, where ℓ is the order of a. We see that they form a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. By Lagrange, we deduce that ℓ divides $\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$. Therefore, $a^{\varphi(m)} \equiv (a^\ell)^{\varphi(m)/\ell} \equiv 1 \pmod{m}$.

Let G be a group. We say that G is *cyclic* iff all of its elements can be written as powers of a fixed element. Such an element is called a *generator*, or *primitive root, of G*. For example, $\mathbb{Z}$ under addition is a cyclic group because each integer is an "additive power" (i.e., a multiple) of 1. This example also shows that there can be multiple generators for a cyclic group: Every integer is also a multiple of -1, so ± 1 are both generators for $\mathbb{Z}$ (in fact, the only generators). Another example is $\mathbb{Z}/m\mathbb{Z}$ under addition, for any $m \in \mathbb{N}$.

Exercise 26. Show that the additive group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$. *Hint:* The Chinese Remainder Theorem.

Exercise 27 (**Important**)**.** Do this exercise without looking at the theorems below. For which natural numbers $m \leq 12$ is the unit group $(\mathbb{Z}/m\mathbb{Z})^\times$ cyclic? Can you give a generator of each such group?

Exercise 28 (**Important**)**.** While $(\mathbb{Z}/m\mathbb{Z})^\times$ forms an abelian group under multiplication, $\mathbb{Z}/m\mathbb{Z}$ forms an abelian group under addition, being a ring. Show that the following maps are uniquely-defined group homomorphisms. Which are isomorphisms?

1. The map $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that sends $[1]_4 \mapsto ([1]_2, [1]_2)$.

2. The map $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ that sends $[1]_6 \mapsto ([1]_2, [1]_3)$.

3. The map $(\mathbb{Z}/6\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z}$ that sends $[5]_6 \mapsto [1]_2$.

4. The map $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{Z}/6\mathbb{Z}$ that sends $[3]_7 \mapsto [2]_6$.

5. The map $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{Z}/6\mathbb{Z}$ that sends $[3]_7 \mapsto [1]_6$.

6. The map $(\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that sends $[3]_{12} \mapsto ([1]_2, [0]_2)$ and $[5]_{12} \mapsto ([0]_2, [1]_2)$.

Theorem 4.2 (Structure of Finite Abelian Groups)**.** *Every finite abelian group is isomorphic to a group of the form*

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \tag{59}$$

for some $r \in \mathbb{N}$ and $n_1, \ldots, n_r \in \mathbb{N}$.

Proof. See any decent textbook on abstract algebra. □

The power of the following theorem only becomes evident once you remember that the structure of $(\mathbb{Z}/m\mathbb{Z})^\times$ is "multiplicative," cf. Cor. 3.5 to the Chinese Remainder Theorem.

Theorem 4.3 (Structure of Unit Groups)**.** *Let p be prime and let $e \in \mathbb{N}$. Then*

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \simeq \begin{cases} 0 & p = 2,\ e = 1 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z} & p = 2,\ e \geq 2 \\ \mathbb{Z}/p^{e-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ odd} \end{cases} \tag{60}$$

Proof. Interesting but not essential. See [JJ, §6.3-6.4]. □

Corollary 4.4. *If p is odd, then $(\mathbb{Z}/p^e\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^e)\mathbb{Z}$, a cyclic group.*

5 27 October

5.1 Criteria for Quadratic Residues

Lemma 5.1 (Wilson)**.** *If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. Every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ has a distinct inverse, except for the elements $[1]_p$ and $[-1]_p$. By pairing together the elements that do have distinct inverses, we find that they "cancel out" in the product over all elements of $(\mathbb{Z}/p\mathbb{Z})^\times$, so that we're left with $[1]_p[-1]_p = [-1]_p$. □

Proposition 5.2 (Euler's Criterion)**.** *If p is prime and $p \nmid a$, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Proof. There are $p-1$ residues modulo p and Wilson's Lemma says that their combined product is $[-1]_p$. If a is a QNR, then the residue class $[x]_p$ will always be distinct from the residue class $[a]_p[x]_p^{-1}$, so pairing up these classes, we find that the product over all elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ is also equal to $[a]_p^{(p-1)/2}$:

$$a \text{ is a QNR} \implies a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{61}$$

If a is a QR, then $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}$, so by Fermat's Little Theorem, $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$:

$$a \text{ is a QR} \implies a^{\frac{p-1}{2}} \equiv +1 \pmod{p}. \tag{62}$$

The proof is complete. □

Proposition 5.3 (Gauss's Lemma)**.** *Let p be an odd prime. If $p \nmid a$, then*

$$\left(\frac{a}{p}\right) = (-1)^{\#(\mathcal{M}(a) \cap \mathcal{M}(-1))}, \tag{63}$$

where $\mathcal{M}(n) = \{[n]_p, [2n]_p, \ldots, [(p-1)n/2]_p\}$.

Proof. This is Theorem 7.9 in [JJ]. □

5.2 Quadratic Congruences

The law of quadratic reciprocity was known to Euler, but astonishingly, he was not able to prove it. Gauss apparently discovered the first proof around the age of 19; it was published in his monumental *Disquisitiones Arithmeticae*. He attached great personal significance to the result, referring to it as the *Aureum Theorema* or *Golden Theorem*. In the course of his lifetime he published six proofs and wrote down two more.

Theorem 5.4 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{64}$$

In addition,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{65}$$

Proof. Stop by my office hours to see a panoply of cool proofs! □

The quadratic reciprocity law gives us an extremely efficient way to compute whether an odd prime p is a quadratic residue modulo a larger prime q. Indeed, it implies

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right), \tag{66}$$

and the value of $\left(\frac{q}{p}\right)$ depends only on the residue class of q modulo p, hence on the remainder upon long-dividing q by p. This remainder might no longer be prime, but the Legendre symbol is totally multiplicative, so we can break the remainder up into individual primes and compute the Legendre symbols of those, etc. In short, we have:

Legendre's Algorithm

Let $p < q$ be odd primes. To compute $\left(\frac{p}{q}\right)$, compute the prime factorization $q_1^{e_1}\cdots q_r^{e_r}$ of the remainder upon long-dividing q by p, then compute the right-hand side of

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\prod_{i=1}^{r}\left(\frac{q_i}{p}\right)^{e_i}. \tag{67}$$

Exercise 29. Compute the Legendre symbol $\left(\frac{101}{8191}\right)$.

Exercise 30. Here we count, and find, the solutions of a quadratic congruence in an arbitrary modulus $m \in \mathbb{N}$, not necessarily prime.

1. Show that if p is an odd prime and $e \in \mathbb{N}$, then the number of residual solutions to $x^2 \equiv 1 \pmod{p^e}$ is 2, cf. Exercise 24(3).
2. Show that if $e \in \mathbb{N}$, then the number of residual solutions to $x^2 \equiv 1 \pmod{2^e}$ is $\psi_2(e)$, where
$$\psi_2(e) = \begin{cases} 1 & e = 1 \\ 2 & e = 2 \\ 4 & e \geq 3 \end{cases} \tag{68}$$
3. Using Theorem 3.4, give a formula for the number of residual solutions to $x^2 \equiv 1 \pmod{m}$ in terms of the unique prime factorization of m.
4. Show that if $[a]_m, [x_0]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$ satisfy $x_0^2 \equiv a \pmod{m}$, then the general solution to $x^2 \equiv a \pmod{m}$ is $x = x_0 y$, where $[y]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$ satisfies $y^2 \equiv 1 \pmod{m}$.
5. Using part (4), show that the formula obtained in part (3) stays the same if we replace $x^2 \equiv 1$ with $x^2 \equiv a$ for any $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$ that yields at least one solution for x.

References

[H] G. H. Hardy. *A Mathematician's Apology* (1940).

[JJ] G. A. Jones & J. M. Jones. *Elementary Number Theory*. Springer-Verlag (1998).