A (Somewhat Less Insane) Introduction to Number Theory

1 Preliminaries: Definitions and Notation

We begin with some notation and definitions:

Definition 1.1. The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\mathbb{N} \overset{\text{def}}{=} \{1,2,3,4,\cdots\}$.

Definition 1.2. The set of *integers*, denoted $\mathbb{Z}$, is the set $\mathbb{Z} \overset{\text{def}}{=} \{\cdots,-4,-3,-2,-1,0,1,2,3,4,\cdots\}$.

Definition 1.3. Let $a,b \in \mathbb{Z}$. Then we say *a divides b* (or, more precisely, *a* divides *b in* $\mathbb{Z}$), denoted $a \mid b$, if and only if there exists some $x \in \mathbb{Z}$ such that $ax = b$. Further, if a does *not* divide b, we shall write $a \nmid b$.

Definition 1.4. If $a,b \in \mathbb{Z}$, then we say that $d \in \mathbb{Z}$ is a *common divisor of a and b* if and only if $d \mid a$ and $d \mid b$.

Definition 1.5. For integers $a,b \in \mathbb{Z}$, a *greatest common divisor* of a and b, denoted $\gcd(a,b)$ is a nonnegative integer d such that

- $d \mid a$ and $d \mid b$, and
- If $\ell \in \mathbb{Z}$ satisfies $\ell \mid a$ and $\ell \mid b$, then $\ell \mid d$.

That is, a greatest common divisor of integers a and b is a nonnegative integer d that *is* a common divisor of a and b and it is *divisible by* every common divisor of a and b.

Definition 1.6. If $a,b \in \mathbb{Z}$, then we shall say that a and b are *relatively prime* or *coprime* if and only if $\gcd(a,b) = 1$.

Definition 1.7. Assume that $a,b,m \in \mathbb{Z}$. Then *a is congruent to b modulo m*, denoted $a \equiv b \pmod{m}$ and read "a is congruent to b mod m", if and only if $m \mid a-b$. The following notation is equivalent: $a \equiv b \mod m$, $a \equiv b \ (m)$, etc. (Where the modulus m is implicit, we may simply write $a \equiv b$.) If a is *not* congruent to b modulo m, then we shall write $a \not\equiv b \pmod{m}$, $a \not\equiv b \mod m$, or $a \not\equiv b \ (m)$.

Remark. Certain examples of modular arithmetic should be familiar from everyday experience. For example, if today is Saturday, what day will it be 23 days from now? (This is addition modulo 7.) If it is currently 11:00AM, then what time will it be 73 hours from now? (This is addition modulo 12, ignoring the AM/PM distinction, or modulo 24, using 24-hour/military time.)

Definition 1.8. An integer $p \in \mathbb{Z}$ is a *prime number* or *irreducible* if and only if

- $p \neq 0$ *and* $p \neq \pm 1$, and
- If $p = ab$, where $a,b \in \mathbb{Z}$, then $a = \pm 1$ or $b = \pm 1$.

Remark. Note that under this definition, negative integers—such as -3, -17, or -101—*are* considered prime.

2 Assertions You May Use Without Proof

Note: All of the following propositions *can be proven*—and it's worth trying to prove them, too! For the subsequent sections in this handout, however, feel free to use any or all of the following without having to prove them.

Proposition 2.1 (The Division Algorithm in $\mathbb{Z}$)**.** *For all $a,b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q,r \in \mathbb{Z}$ such that*

$$a = bq + r, \text{ where } 0 \leq r < |b|.$$

We call q the integer quotient *and r* the remainder*, respectively, when dividing a by b.*

Proposition 2.2 (Alternate, equivalent formulation of $\gcd(a,b)$ in $\mathbb{Z}$)**.** *Let $a,b \in \mathbb{Z}$. Then* as a consequence of the division algorithm (Proposition 2.1),[1] $\gcd(a,b)$*, as defined in Definition 1.5 above, is uniquely determined.*

Finally, if a and b are not both zero, then $\gcd(a,b) = \max\{d \in \mathbb{N} : d \mid a \text{ and } d \mid b\}$*. That is, if at least one of a and b is nonzero, then* $\gcd(a,b)$ *is the greatest* of *the common divisors of a and b.*[2]

Proposition 2.3 (Euclid's Algorithm in $\mathbb{Z}$)**.** *Let $a,b \in \mathbb{Z}$ with $b \neq 0$.* As a consequence of the division algorithm (Proposition 2.1)*, we may form the following:*

$$\begin{aligned}
a &= bq_1 + r_1, && \textit{where } 0 \le r_1 < |b| \\
b &= r_1 q_2 + r_2, && \textit{where } 0 \le r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && \textit{where } 0 \le r_3 < r_2 \\
\vdots &= \quad \vdots && \qquad \vdots \\
r_j &= r_{j+1} q_{j+2} + r_{j+2}, && \textit{where } 0 \le r_{j+2} < r_{j+1} \\
\vdots &= \quad \vdots && \qquad \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, && \textit{where } 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Then for all such $a,b \in \mathbb{Z}$, this process always terminates, and $\gcd(a,b) = r_n$*. That is,* $\gcd(a,b)$ *is the last* nonzero *remainder above.*

Proposition 2.4 (Properties of Modular Arithmetic)**.** *Let $m \in \mathbb{N}$ be a fixed natural number with $m > 1$. Then for all $a,b,c,d \in \mathbb{Z}$ and $n \in \mathbb{N}$, we have the following:*

- *If $a \in \mathbb{Z}$, then there exists a* unique *$r \in \{0,1,\ldots,m-1\}$ such that $a \equiv r \pmod{m}$. (In particular, $a \equiv 0 \pmod{m}$ if and only if the remainder when dividing a by m is 0.)*
- *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$ and $a-c \equiv b-d \pmod{m}$.*
- *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.*
- *If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.*

Based on the above, we can "identify"[3] *the collection of integers modulo m with the set* $\mathbb{Z}/m\mathbb{Z} \overset{def}{=} \{0,1,\ldots,m-1\}$*. Further, we can perform all addition, subtraction, multiplication, and (positive integer) exponentiation modulo m via manipulating remainders modulo m.*

Remark. In Proposition 2.4 above, we must use the *same* modulus m throughout. If we have *different* moduli $m,n \in \mathbb{N}$, respectively, then in general, knowing $a \equiv c \pmod{m}$ and $b \equiv d \pmod{n}$ gives us no useful information to compare $a+c$ to $b+d$, nor ac to bd.

Proposition 2.5 (The Fundamental Theorem of Arithmetic in $\mathbb{Z}$)**.** *Let $n \in \mathbb{N}$ with $n \ge 2$. Then there exist positive primes $p_1 < p_2 < \cdots < p_k$ and positive integers $a_1, a_2, \ldots, a_k$ such that*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Further, the primes $\{p_j\}$ and the exponents $\{a_j\}$ are uniquely determined by n. In other words, every positive integer greater than 1 has some *factorization into positive primes, and up to reordering it has* exactly one *factorization into* positive *primes.*

[1] Here, the point is not simply that the gcd exists as it is officially defined above, but its existence *is a corollary to* the division algorithm in $\mathbb{Z}$.

[2] This notion that "the gcd is the maximum *of* the common divisors" is the most common way the notion of greatest common divisor is first presented to students, and it's therefore typically easier to understand. The original definition above, however, is nearly always more *useful* in number theory.

[3] *Note:* I am leaving the term "identify" intentionally vague here, as well as (deliberately) using nonstandard notation for $\mathbb{Z}/m\mathbb{Z}$ here. Nonetheless, there's a way in which this can be made mathematically precise and rigorous. To give an example of what I have in mind, note that $27 \equiv 2 \pmod{5}$ and $109 \equiv 4 \pmod{5}$. Then $27 \cdot 109 \equiv 2 \cdot 4 \pmod{5}$. Further, $2 \cdot 4 = 8$, and $8 \equiv 3 \pmod{5}$. Therefore, $27 \cdot 109 \equiv 3 \pmod{5}$. This is considerably simpler than first calculating $27 \cdot 109 = 2943$, then simplifying *that* modulo 5.

3 Numerical Examples

3.1. Simplify the following. That is, for each modulus m, compute the integer $r \in \mathbb{Z}/m\mathbb{Z} \overset{\text{def}}{=} \{0, 1, \ldots, m-1\}$ such that your result is congruent to r modulo m.

- $5 + 7 \pmod 4$.
- $5 \cdot 7 \pmod 4$.
- $37 \cdot 37 \pmod{38}$.
  Hint: don't bother multiplying $37 \cdot 37$, since there's a much easier way.
- $25 \cdot (34 + 78) \pmod 7$.
- 5, 5^2, 5^3, 5^4, 5^5, 5^6, and $5^7 \pmod 8$.

3.2. Compute $\gcd(a, b)$ for each of the following using Euclid's algorithm. Can you see how to compute these using the respective prime factorizations of a and b?

- $\gcd(4, 10)$.
- $\gcd(7, 30)$.
- $\gcd(120, 180)$.
- $\gcd(999, 1000)$.
- $\gcd(3297, 6363)$.

3.3. As in Proposition 2.4, fix a natural number $m > 1$, and set $\mathbb{Z}/m\mathbb{Z} \overset{\text{def}}{=} \{0, 1, \ldots, m-1\}$. We shall say that $a \in \mathbb{Z}/m\mathbb{Z}$ is a *unit modulo m* if and only if there exists some $b \in \mathbb{Z}/m\mathbb{Z}$ such that $ab \equiv 1 \pmod m$. We call b the *inverse of a mod m*. For example, 3 is a unit modulo 10, since $3 \cdot 7 = 21 \equiv 1 \pmod{10}$, and therefore 7 is the inverse of 3 modulo 10.

For the following m, find all the units modulo m in $\mathbb{Z}/m\mathbb{Z}$. How many such units are there modulo m in each case?

- $m = 5$.
- $m = 7$.
- $m = 11$.
- $m = 12$.
- $m = 16$.
- $m = 17$.

3.4. For the given integers a and b, find the smallest *positive* integer of the form $ax + by$, where $x, y \in \mathbb{Z}$. (Note: in general, at least one of x and y may be negative, but we must have $ax + by > 0$.) Is our choice of (x, y) unique for producing this smallest positive element of the form $ax + by$?

- $a = 2$, $b = 4$.
- $a = 4$, $b = 11$.
- $a = 10$, $b = 25$.
- $a = 7$, $b = 30$.
- $a = 3297$, $b = 6363$.

3.5. Fix $m \in \mathbb{N}$ with $m > 1$, and let $\mathbb{Z}/m\mathbb{Z}$ be as above. If $a \in \mathbb{Z}/m\mathbb{Z}$ and there is some *positive* integer $n \in \mathbb{N}$ such that $a^n \equiv 1 \pmod{m}$, then we define the *order of a modulo m*, denoted $\operatorname{ord}_m a$, to be the smallest positive integer n such that $a^n \equiv 1 \pmod{m}$; that is

$$\operatorname{ord}_m a \overset{\text{def}}{=} \min\{n \in \mathbb{N} : a^n \equiv 1 \pmod{m}\}.$$

Example:

$$3^1 \equiv 3 (\operatorname{mod} 10),\ 3^2 \equiv 9 (\operatorname{mod} 10),\ 3^3 = 27 \equiv 7 (\operatorname{mod} 10),\ \text{and}\ 3^4 = 81 \equiv 1 (\operatorname{mod} 10).$$

Therefore, $\operatorname{ord}_{10} 3 = 4$ because $3^4 \equiv 1 \pmod{10}$ and no smaller positive integer power of 3 yields $1 \pmod{10}$.

Compute the following, or explain why it does not exist.

- $\operatorname{ord}_5 3$.
- $\operatorname{ord}_{10} 2$.
- $\operatorname{ord}_{11} 6$.
- $\operatorname{ord}_{11} 6^2$, $\operatorname{ord}_{11} 6^3$, ..., $\operatorname{ord}_{11} 6^k$, for each $k \in \mathbb{N}$.
- $\operatorname{ord}_{17} 3$.

3.6. Simplify the following, in the sense of Exercise #3.1 above.

- $2^4 \pmod{5}$.
- $3^6 \pmod{7}$.
- $6^{16} \pmod{17}$.
- $2^8 \pmod{9}$.
- $2^6 \pmod{9}$.

3.7. Let $U_m \overset{\text{def}}{=} \{a \in \mathbb{Z}/m\mathbb{Z} : a \text{ is a unit modulo } m\}$; that is, U_m is the subset of $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$ consisting of all units mod m. We say that U_m is *cyclic* if and only if there exists some $g \in U_m$ such that every $a \in U_m$ is congruent to some nonnegative integer power of g modulo m. Such a $g \in U_m$ is called a *generator* or *primitive root* modulo m.

Example #1: for $m = 5$, consider $g = 2$. Then $U_5 = \{1, 2, 3, 4\}$, and we have $2^0 \equiv 2^4 \equiv 1 \pmod{5}$, $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, and $2^3 \equiv 3 \pmod{5}$, so $g = 2$ is a generator, and U_5 is cyclic.

Example #2: For $m = 15$, $U_m = \{1, 2, 4, 7, 8, 11, 13, 14\}$. However, we have $1^4 \equiv 2^4 \equiv 4^4 \equiv 7^4 \equiv 8^4 \equiv 11^4 \equiv 13^4 \equiv 14^4 \equiv 1 \pmod{5}$. (I.e., for all $a \in U_{15}$, $a^4 \equiv 1 \pmod{15}$.) Why does this mean that U_{15} *cannot* be cyclic?

For each m, determine whether U_m is cyclic. If so, produce at least one generator $g \in U_m$, and compute $\operatorname{ord}_m g$.

If U_m is cyclic and g is a generator, then by the definition of a generator, all elements of U_m are powers of g, *including any other generators of* U_m. For cyclic U_m, can you find *all* generators of U_m?

- U_4.
- U_8.
- U_9.
- U_{12}.
- U_{17}.
- U_{18}.

4 Conjectures

Now that you're more familiar with some of these ideas, try to deduce some more general results. (If you can *prove* your conjecture is true, even better!) But for now, simply try to produce an educated guess for the following.

4.1. Assume a, b are both integers greater than 2. By the Fundamental Theorem of Arithmetic (Theorem 2.5), each of a and b has a (unique) factorization into primes. Conjecture a formula for $\gcd(a,b)$ in terms of the prime factorizations of a and b. (Cf. Exercise #3.2.)

4.2. Let $m \in \mathbb{N}$ be fixed, with $m \geq 2$.

- For which $a \in \mathbb{Z}/m\mathbb{Z} \overset{\text{def}}{=} \{0, 1, \ldots, m-1\}$ is a a unit modulo m?
- Let $\varphi(m)$ denote $|U_m|$, the number number of distinct units modulo m. Provide a formula for $\varphi(m)$ in terms of m.

  Suggestion: begin by considering simple cases. What if $m = p$, a prime? What if m is a power of a prime? What if m is a product of two or more distinct positive primes? What if $m = p^j q^k$, where $j, k \in \mathbb{N}$, and p and q are distinct positive primes?

(Cf. Exercise #3.3.)

4.3. Let $a, b \in \mathbb{Z}$, not both zero. If ℓ is the smallest positive integer of the form $ax + by$, where $x, y \in \mathbb{Z}$, then what is ℓ in terms of a and b? (Cf. Exercise #3.4.) For your conjectured value of ℓ, can you describe a method for producing suitable $x, y \in \mathbb{Z}$ such that $ax + by = \ell$?

4.4. Let $m \in \mathbb{N}$ with $m \geq 2$, and let $a \in U_m$ be arbitrary.

- If $m = p$, a prime, then what is $a^{p-1} \pmod{p}$? If m is *not* prime, do we in general have the same result for $a^{m-1} \pmod{m}$?
- If m is not a prime, then can you find an exponent k in terms of m such that for all $a \in U_m$, $a^k \equiv 1 \pmod{m}$?
- If $\operatorname{ord}_m a = n$, what is
$$\operatorname{ord}_m a^k$$
for each $k \in \mathbb{N}$?
- For which m is U_m cyclic? If $g \in U_m$ is a generator, what is $\operatorname{ord}_m g$? For a *cyclic* U_m, how many generators are in U_m?

(Cf. Exercises #3.5, #3.6, and #3.7.)

5 A Generalization and More Conjectures: The Gaussian Integers

Consider the following generalization beyond $\mathbb{Z}$.

Definition 5.1. The set of *Gaussian integers*, denoted $\mathbb{Z}[i]$ (and read "$\mathbb{Z}$ square-bracket i"), is the set

$$\mathbb{Z}[i] \overset{\text{def}}{=} \{a + bi : a, b \in \mathbb{Z}\},$$

where $i^2 = -1$. (That is, i is a complex square root of -1.) For $a, b, c, d \in \mathbb{Z}$, we have $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Definition 5.2. Let $a, b \in \mathbb{Z}$, and set $\alpha = a + bi \in \mathbb{Z}[i]$.

- The *conjugate* (or *complex conjugate*) of α, denotes $\overline{\alpha}$, is defined by $\overline{\alpha} \overset{\text{def}}{=} a - bi$.

- The *norm of* α, denoted $N(\alpha)$, is defined by $N(\alpha) \overset{\text{def}}{=} a^2 + b^2$.

In particular, for all $\alpha \in \mathbb{Z}[i]$, $N(\alpha) = \alpha\overline{\alpha}$.

5.1. Let $\alpha, \beta \in \mathbb{Z}[i]$. How would you define divisibility in $\mathbb{Z}[i]$? Common divisors? Greatest common divisor? An irreducible element of $\mathbb{Z}[i]$? Which elements $\alpha \in \mathbb{Z}[i]$ are irreducible?

Note: integers $p \in \mathbb{Z}$ which are irreducible in $\mathbb{Z}$ need not be irreducible in $\mathbb{Z}[i]$. For example, 5 is irreducible in $\mathbb{Z}$, but in $\mathbb{Z}[i]$ we have $5 = (1+2i)(1-2i)$. Are the numbers 11, 13, 17, and 19, all irreducible in $\mathbb{Z}$, still irreducible in $\mathbb{Z}[i]$?

5.2. If $\alpha, \beta, \mu \in \mathbb{Z}[i]$, how would you define the statement

$$\alpha \equiv \beta \pmod{\mu}$$

in $\mathbb{Z}[i]$? How many of the properties from Proposition 2.4 carry over into modular arithmetic in $\mathbb{Z}[i]$? How many distinct elements are there modulo μ?

5.3. Do we have a version of the division algorithm (Proposition 2.1) in $\mathbb{Z}[i]$? If so, state your variant of the division algorithm in $\mathbb{Z}[i]$. If not, explain why not.

5.4. Do we have a version of Euclid's algorithm (Proposition 2.3) in $\mathbb{Z}[i]$?

5.5. If $\alpha, \beta \in \mathbb{Z}[i]$ and $\delta \in \mathbb{Z}[i]$ is a greatest common divisor of α and β, then do there exist $\chi, \gamma \in \mathbb{Z}[i]$ such that $\alpha\chi + \beta\gamma = \delta$? If so, how can you produce such χ and γ? Further, how do you take into account that "greatest common divisor" in $\mathbb{Z}[i]$ is no longer *uniquely* determined?

5.6. Is there an analogous form of the Fundamental Theorem of Arithmetic (Proposition #2.5) for $\mathbb{Z}[i]$, including a property of uniqueness? Consider that we have $2 = (1+i)(1-i) = -i(1+i)^2$.

5.7. How would you define a *unit modulo* μ in $\mathbb{Z}[i]$? If $\mu \in \mathbb{Z}[i]$ (with possible suitable restrictions on μ), then which $\alpha \in \mathbb{Z}[i]$ are units modulo μ? If U_μ is a set containing all the units mod μ (with no repetition mod μ), then how big is U_μ in terms of μ?

5.8. Can you generalize your conjectures from Exercise #4.4 to $\mathbb{Z}[i]$?