Prime Numbers and Factorizations

Yan Tao

Advanced 1

1 The Fundamental Theorem of Arithmetic

Prime integers (often just called prime numbers, though we'll use the term integer as we'll look at different number systems as well) are among the first kind of mathematical things humans ever studied - ancient Egyptian documents have been discovered showing that they knew how to factor numbers into primes. The first known mathematical textbook to cover this, however, came centuries later - Euclid's *Elements*, which contains theorems that are still relevant to modern mathematics. The two most notable theorems about prime numbers are as follows:

Theorem 1 *(Euclid's Theorem) There are infinitely many prime numbers.*

Theorem 2 *(Fundamental Theorem of Arithmetic) Every positive integer can be uniquely written as a product of prime factors.*

For now, we'll take prime numbers to mean Euclid's definition - that is, a positive integer p which cannot be written $p = ab$ where a, b are both smaller positive integers.

The following proofs look different than how Euclid originally wrote them, but they will be more illustrative in more general examples.

Problem 1 *Prove Euclid's Theorem by contradiction. (Hint: Use the fact that no number is divisible by a larger number.)*

Problem 2 *Prove the Fundamental Theorem of Arithmetic:*

a. *Show the existence part - that is, that every number has a prime factorization. (Hint: Again, use the fact that no number is divisible by a larger number.)*

b. *Show the uniqueness of this factorization. (Hint: Use the fact that if there exists a positive integer with some property, there is a smallest positive integer with that property. In this case, if there were some integer without a unique factorization, consider the smallest integer without a unique factorization.)*

In *Elements*, the following lemma was used in the proof of the Fundamental Theorem of Arithmetic. These statements can be proven in either order, and we're doing so backwards because it will be more illustrative.

Problem 3 *Prove* ***Euclid's Lemma****, which states that a positive integer p is prime if and only if whenever p divides ab, p must divide either a or b.*

2 More Number Systems

Euclid originally proved these theorems for the integers, so it is natural to ask how they generalize to different kinds of numbers. The first theorem will not generalize - consider sets like the integers mod n, where there are only n numbers, and of course there will not be infinitely many primes. So we'll study some generalizations of the Fundamental Theorem of Arithmetic as well as Euclid's Lemma.

For all examples in this worksheet, number systems will be sets of "numbers" where addition, subtraction, and multiplication work exactly like they do with usual numbers - but not necessarily division (for instance, we cannot divide any two integers and get an integer, so we say the integers don't have division). Instead, we'll generalize the limited notion of division that we do have.

Definition 1 *We say a number b is **divisible** by a number a, or that a divides b, if there is a number c such that $b = ac$.*

In the integers, 2 divides 4 because $4 = 2 \times 2$, but 2 doesn't divide 5 despite $5 = 2 \times 5/2$, because $5/2$ is not an integer. (2 does divide 5 if $5/2$ is in our set of numbers - for instance, 2 divides 5 in the set of rational numbers.)

Problem 4 *Consider the integers mod 4, denoted $\mathbb{Z}/4\mathbb{Z}$. Show that every number mod 4 is divisible by 3.*

Problem 5 *Find two different factorizations of 2 in $\mathbb{Z}/4\mathbb{Z}$, using numbers that are prime integers.*

This is the first problem we face, and the easiest to solve. In every example, we'll have a multiplicative identity, which we'll name 1 (which may or may not be the number 1), and we define

Definition 2 *A number u is called a **unit** if it divides 1; that is, there exists a number v such that $uv = 1$.*

From now on, we'll just ignore units any time we factorize a number, the same way we don't include 1 in any factorizations. This will deal with cases like $\mathbb{Z}/4\mathbb{Z}$ above (because in this case, 3 is a unit mod 4.)

Problem 6 *What are the units of $\mathbb{Z}$? That is, which integers are units?*

Problem 7 *What are the units of $\mathbb{Z}/n\mathbb{Z}$? That is, which numbers are units mod n?*

Problem 8 *Show that a number u is a unit if and only if every number is divisible by u.*

In the previous example, 3 is a prime integer, but we should not consider it a prime number in mod 4, because it's a unit and should be ignored in factorizations. This leads us to a new definition, or more precisely, new definitions:

Definition 3 *A number p is **prime** if it is not zero or a unit, and whenever p divides ab, p must divide a or b.*

Definition 4 *A number p is **irreducible** if it is not zero or a unit, and p cannot be written as the product of "smaller things" - that is, whenever $p = ab$, either a or b is a unit.*

Problem 9 *Which elements of $\mathbb{Z}$ (that is, which integers) are prime? Which are irreducible?*

Problem 10 *Which numbers are prime mod 4? Irreducible?*

In these examples, primes and irreducibles are the same, but unfortunately, this is not the case in general. Consider the set $\mathbb{Z}^2$ consisting of ordered pairs of integers. We can add, subtract, and multiply as follows:

$$(a, b) + (c, d) = (a + c, b + d) \text{ and } (a, b) - (c, d) = (a - c, b - d) \text{ and } (a, b) \times (c, d) = (ac, bd)$$

Problem 11 *Which element is the "1" in $\mathbb{Z}^2$? (That is, what is the multiplicative identity?)*

Problem 12 *Show that:*

a. $(1,0)$ *is not a unit in* $\mathbb{Z}^2$.

b. $(1,0)$ *is prime in* $\mathbb{Z}^2$.

c. $(1,0)$ *is not irreducible in* $\mathbb{Z}^2$.

As we have been doing, we restrict our attention to certain kinds of number systems, so that we (hopefully) have only one notion of what it means for a number to be prime.

Definition 5 *A number system is an* ***integral domain*** *(domain for short) if no two nonzero numbers can multiply to zero. In other words, if* $ab = 0$*, then* $a = 0$ *or* $b = 0$

As the name suggests, this definition is based on the property of the integers $\mathbb{Z}$ (which is a domain). The two previous examples are not domains - in the integers mod 4, $2 \times 2 = 0$, and in $\mathbb{Z}^2$, $(1,0) \times (0,1) = 0$. Even so, we saw that all primes in $\mathbb{Z}/4\mathbb{Z}$ were irreducible, but being a domain *guarantees* this property.

Problem 13 *Show that all prime elements of a domain are irreducible. Where in the proof did you use the fact that the numbers are in a domain?*

Problem 14 *Consider the integers mod* n*,* $\mathbb{Z}/n\mathbb{Z}$*. For which* n *is this a domain?*

3 Examples of Domains (The Gaussian Integers)

So far, we've only encountered two examples of domains - the integers, which we've become familiar with in school and at the Math Circle, and the integers mod p for a prime integer p, which is more trivial in the sense that every nonzero element is a unit. From these examples, it seems like primes and irreducibles are the same in all domains. To see whether this is true, we introduce more examples of domains.

Definition 6 *The **Gaussian integers** are defined as numbers of the form $a + b\sqrt{-1}$, where a and b are integers.*

Note that $\sqrt{-1}$ is just the imaginary number i. But for our purposes it's just as good to just think of it as a symbol that becomes -1 when we square it, so that we can add, subtract, and multiply Gaussian integers by treating the $\sqrt{-1}$ like a variable. The set of Gaussian integers is denoted $\mathbb{Z}[\sqrt{-1}]$.

Problem 15 *Compute:*

- $(1 + \sqrt{-1}) - (4 - 5\sqrt{-1})$
- $(3 + \sqrt{-1}) \times (3 - 2\sqrt{-1})$
- $(1 + \sqrt{-1}) \times (1 - \sqrt{-1})$

Problem 16 *Show that $\mathbb{Z}[\sqrt{-1}]$ is a domain.*

We didn't have to put a -1 under the square root - for instance, we could define the set $\mathbb{Z}[\sqrt{-5}]$, the set of numbers of the form $a + b\sqrt{-5}$ for integers a, b.

Problem 17 *Compute:*

- $(1 + \sqrt{-5}) - (4 - 5\sqrt{-5})$
- $(3 + \sqrt{-5}) \times (3 - 2\sqrt{-5})$
- $(1 + \sqrt{-5})(1 - \sqrt{-5})$

Problem 18 *Show that $\mathbb{Z}[\sqrt{-5}]$ is also a domain.*

Problem 19 *Show that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$. (Hint: If $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, then a, b, c, d have to satisfy some conditions in order for the product to be a real number.)*

Problem 19 shows an example of a domain where Euler's Lemma (problem 3) fails. In fact, there is a family of related examples where this is the case - we can just put any integer under the square root to make $\mathbb{Z}[\sqrt{n}]$. We can assume n is squarefree (that is, it is not divisible by any perfect squares) as otherwise we can just pull the perfect square factor out of the square root, and we'll only consider negative n for now, as positive n are more difficult. Finally, we'll deal with $n = -1$ and $n = -2$ next week.

Problem 20 *(Challenge) Let d be a positive squarefree integer greater than or equal to 3. Show that 2 is also irreducible but not prime in $\mathbb{Z}[\sqrt{-d}]$*

4 Bonus Section: Polynomial Rings

When we (loosely) defined a number system, the only conditions were that we could add, subtract, and multiply numbers. The astute reader will notice that we can also add, subtract, and multiply polynomials, so the set of polynomials with (say) integer coefficients should also be a number system. This is intended - a lot of algebraic results come from studying polynomials like we study numbers. We'll denote a general number system with R (which stands for "ring", a term borrowed from German mathematics).

Definition 7 *The **polynomial ring over R**, denoted $R[x]$, is the set of all polynomials in the variable x (we could use any letter, for instace $R[t]$ would be polynomials in t) with coefficients that are numbers (elements) of R.*

Problem 21 *Show that if R is a domain, so is $R[x]$.*

The *Fundamental Theorem of Algebra*, which we studied a few weeks ago, helps us figure out which polynomials are irreducible and prime elements.

Problem 22 *Find all irreducible polynomials in $\mathbb{C}[x]$.*

Problem 23 *Find all prime polynomials in $\mathbb{C}[x]$.*

Problem 24 *(Challenge) Find all irreducible and all prime polynomials in $\mathbb{R}[x]$.*