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.)*

Solution: If there were finitely many primes, say $p_1, ..., p_n$, then the number $N = p_1 p_2 ... p_n + 1$ would not divide any of them, because if it did divide p_1 then so would $N - p_1(p_2...p_n) = 1$, which is a contradiction, because no prime divides 1.

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.)*

   Solution: Let n be some positive integer. If n is not divisible by any of $1, ..., n-1$, then it must be prime, since it cannot be divisible by any other number. If it is divisible by some a, write $n = ab$. Then each of a and b are smaller numbers, and we repeat the same argument for both of them. Since the numbers get smaller, this algorithm terminates.

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.)*

   Solution: Suppose there is some positive integer without a unique factorization, and let n be the smallest such integer. Then we can factorize n into primes two different ways as

$$n = p_1 ... p_k = q_1 ... q_l$$

   If some p_i equals some q_j, then dividing n by p_i produces a smaller number with two different prime factorizations, which cannot be the case, so the two lists are disjoint. Therefore $p_1 < q_1$ or $p_1 > q_1$ (without loss of generality assume the former). Now write $n = p_1 P = q_1 Q$ - so that $Q < P$, and therefore $0 < n - p_1 Q < n$. $n - p_1 Q$ must have a unique prime factorization since it's less than n, and p_1 must be in it since both are divisible by p_1. But $n - p_1 Q = (q_1 - p_1)Q$, and p_1 does not occur in Q (since the factorization of Q must also be unique) or $q_1 - p_1$ (since q_1 is a different prime), which gives a contradiction.

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.*

Solution: If p is not prime, write $p = ab$ where a, b are smaller, then p divides neither. Conversely, if p is prime, then suppose p divides ab. By FTA, we uniquely factor each of a and b, and multiplying those factorizations gives the unique factorization of ab, where p must appear, so it must appear in either factorization.

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.*

Solution: We have $3 \times 3 = 1$, so $n = 3 \times (3n)$ mod 4.

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

Solution: $2 = 2 \times 3 = 2 \times 3 \times 3$ (and so on).

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 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?*

Solution: ± 1

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

Solution: The numbers relatively prime to n. Any number with a common factor with n keeps that common factor through all multiples, and every number that is relatively prime has a multiplicative inverse (check some cases and/or give some reason for that).

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

Solution: If u is a unit, then $1 = uv$ is divisible by u, and every number is divisible by 1, so every number is divisible by u. Conversely, if every number is divisible by u, 1 is divisible by u, so we write $1 = uv$ which shows that u is a unit.

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?*

Solution: The irreducibles are $\pm p$, where p is a "prime number" in the traditional meaning. By Euclid's Lemma (problem 3), the primes are the same.

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

Solution: 2 is the only nonzero number that isn't a unit mod 4, so we check that it is both prime and irreducible by just checking all the cases.

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?)*

Solution: $(1,1)$

Problem 12 *Show that:*

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

Solution: $(1, 0)$ *is not a unit because nothing multiplied by* 0 *will equal* 1 *in the second coordinate.*

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

Solution: Suppose $(a, b) \times (c, d)$ *is divisible by* $(1, 0)$. *Then* $bd = 0$, *since* 0 *is the only integer divisible by* 0, *so either* $b = 0$ *or* $d = 0$. *Whichever one it is,* $(1, 0)$ *divides* $(a, 0)$ *or* $(c, 0)$ *because* 1 *divides every integer.*

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

Solution: $(1, 0) = (1, 0)^2$.

As we have been doing, we introduce a new definition to fix this issue.

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), but the two previous examples are not. 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?*

Solution: Let p be prime in a domain, and suppose $p = ab$. Then by primeness, p divides either a or b, so without loss of generality, write $a = cp$. Then $p = bcp$, so $p(1 - bc) = 0$. Since these numbers are in a domain, either $p = 0$ (which is not the case because p is prime) or $1 - bc = 0$. But then $1 = bc$, so b is a unit. Therefore p is irreducible.

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

Solution: For two nonzero numbers smaller than n to multiply to zero, they would have to multiply to a multiple of n. n has factors smaller than itself if and only if it's not prime, so the n for which it's a domain are the prime integers.

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:*

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

  Solution: $-3 + 6\sqrt{-1}$
- $(3 + \sqrt{-1}) \times (3 - 2\sqrt{-1})$

  Solution: $11 - 3\sqrt{-1}$
- $(1 + \sqrt{-1}) \times (1 - \sqrt{-1})$

  Solution: 2

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

Solution: Suppose two Gaussian integers $a + b\sqrt{-1}$ and $c + d\sqrt{-1}$ multiply to zero. Then

$$(ac - bd) + (ad + bc)\sqrt{-1} = 0$$

so both $ac - bd$ and $ad + bc$ are zero. Then $acd = bd^2 = -bc^2$, so either $c = d = 0$ and $c + d\sqrt{-1} = 0$, or $b = 0$, in which case $ac = ad = 0$, which means either $a = 0$ and $a + b\sqrt{-1} = 0$, or $c = d = 0$ and we go back to the previous case.

(Alternatively: Use the fact that the complex numbers form 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:*

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

  Solution: $-3 + 6\sqrt{-5}$
- $(3 + \sqrt{-5}) \times (3 - 2\sqrt{-5})$

  Solution: $19 - 3\sqrt{-5}$
- $(1 + \sqrt{-5})(1 - \sqrt{-5})$

  Solution: 6

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

Solution: Follow the proof of Problem 16.

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.)*

Solution: Suppose $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. In order to be a real number, the latter expression must satisfy $ad = -bc$ - writing this in terms of ratios shows that $c + d\sqrt{-5}$ must be a multiple of a complex conjugate of $a + \sqrt{-5}$. (We could have also gotten this fact by using the polar form of a complex number, but that's less algebraic.) Since $(a + b\sqrt{-5})\overline{(a - b\sqrt{-5})} = a^2 + 5b^2$, 2 must be a multiple of $a^2 + 5b^2$, for integers a, b. Then $b = 0$ and $a = 1$. But then $a + b\sqrt{-5} = 1$ is a unit, so 2 is irreducible. 2 is not prime because by the previous problem, 2 divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but doesn't divide either factor.

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* $\mathbb{Z}[\sqrt{-d}]$

Solution: The proof of irreducibility goes the same way as Problem 19 for $d \geq 3$. For nonprime, if d is even then 2 divides $-d = (\sqrt{-d})^2$ but doesn't divide either factor, and if d is odd then 2 divides $d + 1 = (1 + \sqrt{-d})(1 - \sqrt{-d})$.

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 $R[x]$.*

Solution: Let $f = a_n x^n + ... + a_0$ and $g = b_m x^m + ... + b_0$ be nonzero polynomials. Similarly to what we did a couple weeks ago, we can assume the leading terms are nonzero. Then fg has the term $a_n b_m x^{n+m}$, which is the only term of such a high degree, and since $a_n, b_m \neq 0$ and R is a domain, this term is nonzero, so fg is nonzero, and $R[x]$ is a domain.

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 $\mathbb{C}[x]$.*

Solution: By FTA, no degree 2 or higher polynomial is irreducible. Constant polynomials are all units because $\mathbb{C}$ has division, so the only candidates are degree 1 polynomials. These are all irreducible, because consider $f = ax + b$, and suppose $f = gh$. Then $1 = \deg(f) = \deg(g) + \deg(h)$, so either g or h is constant (degree 0), and therefore a unit.

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

Solution: Since $\mathbb{C}[x]$ is a domain, all primes are irreducible, so again the only candidates are the degree 1 polynomials, which are all prime because if $f = ax + b$ divides gh, then $g(-b/a)h(-b/a) = 0$ (since $-b/a$ is the root of f). Then either $g(-b/a) = 0$ or $h(-b/a) = 0$ because $\mathbb{C}$ is a domain, so $-b/a$ is a root of either g or h, and therefore f divides either g or h.

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