Math 5330 **The Fundamental Theorem of Arithmetic**
Spring 2018

Our discussion of integer solutions to various equations was incomplete because of two unsubstantiated claims. The most obvious is the unproven theorem in the last section:

1. If xy is a square, where x and y are relatively prime, then both x and y must be squares.

It turns out that there was a hidden assumption in our geometric approach to Pythagorean triples as well. That assumption was the following:

2. If $\frac{x}{y} = \frac{a}{b}$, where x and y are relatively prime and a and b are relatively prime, then $x = a$ and $y = b$.

We saw that (1) was actually false for the exotic extensions of integers. It turns out that (2) is also false in these systems of strange integers, so there must be something special about the ordinary integers that makes (1) and (2) true. There is such a property of integers and it is called the Fundamental Theorem of Arithmetic, or the Unique Factorization theorem. First, we need some terms.

Given a positive integer, n, we say k is a proper factor of n if $n = qk$ for some integer k, and $k < n$. Thus, 8 is a proper factor of 24, but 24 is not a proper factor of 24. A number, p is said to be **prime** if 1 is its only proper factor. With this definition, 1 is not prime because 1 has no proper factors. We call 1 a **unit**. Any integer greater than 1 which is not prime is called a **composite**. Thus, the positive integers consists of the union of three disjoint sets:

The unit,	1
the primes,	2, 3, 5, 7, 11, 13, ...,
and the composites,	4, 6, 8, 9, 10, 12, ...

Theorem 1 (The Fundamental Theorem of Arithmetic) *Every positive integer can be expresses as a product of primes, and this producet is unique up to the order of the factors.*

This is definitely the most important theorem in number theory. We begin with some comments about it. First, we allow "products" with only one element, so every prime is the product of primes, just itself. Second, we even allow for the empty product, the product of no primes, and this is defined to be 1. Every composite can be written as the product of primes, and this product will contain more than one term. So $6 = 2 \cdot 3$, $525 = 5 \cdot 3 \cdot 7 \cdot 5$, and so on. If we list the primes in increasing order, then we can ignore the statement about the order of the terms. Also, it is customary to collect product of the same prime to gather as an expression with an exponent as in $24 = 2^3 \cdot 3$, $525 = 3 \cdot 5^2 \cdot 7$, etc. If we require these conventions, we can restate the theorem as saying that each positive integer can be expressed as a product of primes in exactly one way. One way of phrasing this:

Theorem 2 (Still the Fundamental Theorem) *If $n > 0$, then there is an integer, k and primes $p_1, p_2, \cdots, p_k$ with $p_1 < p_2 < \cdots < p_k$ and $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Moreover, k, the p's and a's are uniquely determined by n. That is, if $n = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$ for some primes $q_1, q_2, \cdots, q_l$ with $q_1 < q_2 < \cdots < q_l$, then $k = l$, $p_1 = q_1, \ldots, p_k = q_k$ and $a_1 = b_1, \ldots, a_k = b_k$.*

Intuitively, this theorem says that if two different people in different parts of the world factor the same number by different legal methods, they must get the same answer. Gauss appears to be the first person to realize that this theorem actually needs proving. Before Gauss, people took this theorem for granted. They also took for granted that the same property would be true for different number systems. Examples like $25 = 5^2 = (1+2\sqrt{-6})(1-2\sqrt{-6})$, where $5, 1+2\sqrt{-6}, 1-2\sqrt{-6}$ are all primes in $Z[\sqrt{-6}]$ came as a bit of a shock to people. We say that $Z[\sqrt{-6}]$ does NOT have unique factorization. Since some sets have unique factorization and some don't, we really have to prove Theorem 1. Before doing that, we give some examples to show its usefulness.

Recall from the last set of notes:

Theorem 3 (Theorem 3 from the previous notes) *If two positive integers are relatively prime and their product is a square, then both integers are squares.*

Proof: Let $uv = y^2$, where u and v are relatively prime positive integers. By the Fundamental Theorem, $y = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ for some primes p_i and exponents a_i. This means that $y^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$. Now let q be a prime dividing u. Since $uv = y^2$, q is a prime dividing y^2 so $q = p_j$ for some index j. This means that $uv = y^2$ is divisible by q^{2a_j}. Since u and v are relatively prime, q is not a divisor of v, so u must be (exactly) divisible by q^{2a_j}. We can do this for any prime divisor of u, which means that every prime divisor of u is raised to an even power so u is a square. Similarly, v is a square. ■

This is a common technique: to argue prime by prime in some factorization. Next, consider the other loose end from the set of notes on Pythagorean triples:

Theorem 4 (Point 2 at the beginning of these notes) *If $\frac{x}{y} = \frac{a}{b}$, where x and y are relatively prime and a and b are relatively prime, then $x = a$ and $y = b$.*

Proof: If $\frac{x}{y} = \frac{a}{b}$ then $bx = ay$. Suppose that p^m is part of the prime factorization of a and p^n is part of the prime factorization of y. Then p^{m+n} will be part of the prime factorization of ay. Since $ay = bx$, it must be that p^{m+n} is also part of the prime factorization of bx. But a and b are relatively prime so p is not a divisor of b. This means that p^{m+n} is part of the prime factorization of x. Since x and y are relatively prime and x is divisible by p, y will not be divisible by p. From this, we conclude that $n = 0$. Consequently, if p^m is a factor of a, then p^m is also a factor of x. By symmetry, if p^m is a factor of x then p^m is also a factor of a, which means that x and a have the same factorizations. Since they have the same factorization, $x = a$. Since $bx = ay$ and $x = a$, we have $bx = xy$, so $b = y$. ■

Theorem 5 *$\sqrt{2}$ is irrational. That is, there are no integers m and n with $n \neq 0$ for which $\sqrt{2} = \frac{m}{n}$.*

Proof: We should all have seen a proof that $\sqrt{2}$ is irrational in a previous course but it probably was not this one. This proof, using the Fundamental Theorem is nice in part because it easily generalizes to many numbers other than 2. Suppose, by way of contradiction, that there are such integers m and n. We can make them both positive integers. Multiplying by n and squaring gives $m^2 = 2n^2$. Now we look at the prime 2, and its contribution to the prime factorizations of the right and left hand sides of this equation. If $m = 2^{a_1}p_2^{a_2}\cdots$ then $m^2 = 2^{2a_1}p_2^{2a_2}\cdots$. If $n = 2^{b_1}q_2^{b_2}\cdots$ then $2n^2 = 2^{2b_1+1}q_2^{2b_2}\cdots$. Since $m^2 = 2n^2$ by unique factorization, the factorizations of m^2 and $2n^2$ must be the same. In particular, the role that 2 plays must be the same. Thus, $2^{2a_1} = 2^{2b_1+1}$ meaning that $2a_1 = 2b_1 + 1$. But this can't be, since $2a_1$ is even and $2b_1 + 1$ is odd. ∎

We can, of course, give countless additional applications of unique factorization. Let us concede that unique factorization is important, and try to prove it. A proof can be given using Mathematical Induction. We do something equivalent, but with more historical import. We introduce a proof technique used by the Greeks, but popularized by Fermat. It is called a **proof by infinite descent**. A proof by infinite descent is a proof that something does not exist. It goes like this: you are given the problem of showing no positive integer (or collection of integers) has some property. You start by assuming that some integer DOES have that property. From this you show that a smaller positive integer also has the property. This cannot happen: there are only finitely many positive integers less than any given number, but the above would imply the existence of infinitely many positive integers smaller than some bound.

Some examples of proofs by infinite descent:

Example 1. $\sqrt{2}$ is irrational.

Proof: We already proved this once, assuming the Fundamental Theorem. This will be an alternate proof using infinite descent. We want a property related to numbers being rational, and we wish to show that there are no numbers with this property with respect to $\sqrt{2}$. Here is the property: **If a is rational, then there is a positive integer, n, with the property that na is an integer.** (Can you prove this?)

If $\sqrt{2}$ is rational, then for some positive integer, n, $n\sqrt{2}$ is an integer. Given such an integer, n, let $n_1 = n\sqrt{2} - n = n(\sqrt{2} - 1)$. Since $1 < \sqrt{2} < 2$, we have $0 < \sqrt{2} - 1 < 1$. Multiplying by n, $0 < n(\sqrt{2} - 1) < n$, or $0 < n_1 < n$. Since n has the stated property, n_1 is also an integer. Finally, if we multiply n_1 by $\sqrt{2}$, then $n_1\sqrt{2} = (n\sqrt{2} - n)\sqrt{2} = 2n - n\sqrt{2}$, which is the difference of two integers, so $n_1\sqrt{2}$ is an integer. Thus, given a positive integer, n with the property that $n\sqrt{2}$ is an integer, we have constructed a smaller positive integer, n_1, with the same property (that $n_1\sqrt{2}$ is an integer). By infinite descent, there can be no such n so $\sqrt{2}$ is irrational. ∎

Here is an easy variation: $\sqrt{45}$ is irrational.

Proof: Suppose that $\sqrt{45}$ is rational. Then there is a positive integer, n, for which $n\sqrt{45}$ is an integer. Now $6 < \sqrt{45} < 7$ so $0 < \sqrt{45} - 6 < 1$. Multiplying by n gives $0 < (\sqrt{45} - 6)n < n$. Define $n_1 = n\sqrt{45} - 6n$. Then by n's property, n_1 is an integer. By the inequality above, $0 < n_1 < n$ so n_1 is a positive integer strictly smaller than n. Finally, $n_1\sqrt{45} = (n\sqrt{45} - 6n)\sqrt{45} = 45n - 6n\sqrt{45}$ is an integer so n_1 has n's property. By infinite descent, there can be no such n so $\sqrt{45}$ is irrational. ■

A more modern way to think about a proof by infinite descent is with a slight modification called **proof by minimal counterexample.** In this formulation, one says that if a property is indexed by the positive integers, then nothing can have that property unless some smallest one does. That is, if you want to prove something does not happen, you assume it does, and say that some smallest instance of it (the minimal counterexample) must happen. You then show something smaller also works, contradicting the minimal nature of the counterexample. For example, in our proof that $\sqrt{45}$ is irrational, if we were to use the minimal counterexample approach, we would proceed as follows: **Proof:** If $\sqrt{45}$ is rational, then there is a smallest positive integer, n, with the property that $n\sqrt{45}$ is an integer. However, if we let $m = n\sqrt{45} - 6n$, then m is a smaller positive integer than n and $m\sqrt{45}$ is an integer, contradicting the fact than n is minimal. ■

I have not repeated the work needed to prove that $0 < m < n$, or that $m\sqrt{45}$ is an integer because these details were filled in above. But they would be needed in a real proof by minimal counterexample.

Example 2. There are no positive integers x, y, z for which $x^2 + y^2 = 3z^2$.

Proof: In this case, we will perform an infinite descent on z. We suppose that there is such a triple, and z is a positive integer for which $x^2 + y^2 = 3z^2$. We need the following fact: When a square is divided by 3, the remainder is either 0 or 1. To see this, given a number, m, we can write $m = 3q + r$, where $r = 0, 1$, or 2. Now $m^2 = 9q^2 + 6qr + r^2$ so when we divide by 3, the remainder m^2 has is the same as the remainder for r^2. Since $r^2 = 0, 1$, or 4, the remainder will be 0, or 1, as stated.

Now let r_1 be the remainder when x^2 is divisible by 3 and let r_2 be the remainder when y^2 is divisible by 3. Then the remainder when $x^2 + y^2$ is divided by 3 is $r_1 + r_2$. Since $x^2 + y^2 = 3z^2$, this remainder must be 0. We look for cases where $r_1 + r_2 = 0$, and find only $r_1 = 0$ and $r_2 = 0$. That is, if the sum of two squares is divisible by 3, then both numbers must be divisible by 3. This means $x = 3x_1$ and $y = 3y_1$ for some integers x_1, y_1. Hence, $3z^2 = (3x_1)^2 + (3y_1)^2 = 9x_1^2 + 9y_1^2$, so $z^2 = 3(x_1^2 + y_1^2)$. Consequently z^2, and therefore, z is divisible by 3, so let $z = 3z_1$. Plugging this in for z, $9z_1^2 = 3(x_1^2 + y_1^2)$, or $x_1^2 + y_1^2 = 3z_1^2$. That is, given a triple (x, y, z), we constructed a smaller triple (x_1, y_1, z_1) with the same property. By infinite descent, there can't be any such triple. ■

As an aside, I mention in the homework that $ax^2+by^2 = cz^2$ has either no solutions other than (0, 0, 0) or infinitely many primitive solutions. Here is how one might get infinitely many primitive solutions for, say, $x^2 + y^2 = 17z^2$. One could do this geometrically. First divide by z^2 and relabel variables to get the circle $x^2 + y^2 = 17$. Next, find a point on the circle. Note that (-1, 0) will NOT work. A point that works is (-4, 1). Now proceed as before: find all lines through this point with rational slope m, to get a formula for all rational points in the first quadrant as functions of m. Replace m by, say, $\frac{q}{p}$ and get back to the original (x, y, z). One would have to take care to use only those p's and q's for which (x, y, z) is primitive. Also, since we are not interested in all primitive triples, but only infinitely many, we could just use m of the form $\frac{1}{p}$ or $\frac{7}{p}$, or any other specific value of q, so there is only one variable, p to worry about.

Instead of the geometric approach, I will use the Gaussian integers to find infinitely many primitive triples. The first step in this approach is to factor both sides: $x^2 + y^2 = 17z^2 \rightarrow (x + iy)(x - iy) = (4 + i)(4 - i)z^2$. This suggests letting 4 + i divide $x + iy$ and 4 - i divide $x-iy$. Let $x+iy = (4+i)$(square) $= (4+i)(p+qi)^2$. We have $x+iy = (4+i)(p^2-q^2+2pqi) = 4p^2-2pq-4q^2+i(p^2+8pq-q^2)$, so $x = 4p^2-2pq-4q^2$, $y = p^2+8pq-q^2$. If $x+iy = (4+i)(p+iq)^2$ then $x - iy = (4 - i)(p - iq)^2$, and multiplying these together gives $x^2 + y^2 = 17(p^2 + q^2)^2$, from which we derive $z = p^2+q^2$. This gives the triple $(4p^2-2pq-4q^2, p^2+8pq-q^2, p^2+q^2)$. I will mention that we could replace x and y by $|x|$ and $|y|$. For example, when $p = 0, q = 1$ we could get the solution (4, 1, 1). One thing remains: to determine what has to be true about p, q in order for the triple to be primitive. Since we don't need all primitive triples, but only infinitely many, one approach is to specialize to $q = 1$, and only worry about p. Our new triple is $(4p^2 - 2p - 4, p^2 + 8p - 1, p^2 + 1)$. If we let d divide both x and y then d also divides $4y - x = 34p$. Since p and $p^2 + 1$ have no common factors, the only possible problems would come from $d = 2$ and $d = 17$. If we take p to be even, then z is odd, so d can't be 2. Finally, if we avoid p of the form $17n + 4$ or $17n + 13$ then $p^2 + 1$will not be divisible by 17 either. So pick p according to these two rules and we get infinitely many primitive triples. In particular, if we let $p = 34n$ then both conditions are satisfied. This leads to the rather annoying family $(4624n - 68n - 4, 1156n^2 + 272n - 1, 1156n^2 + 1.)$ Picking $n = 1$, for example, gives (4552, 1427, 1157). Checking, $4552^2 + 1427^2 = 20720704 + 2036329 = 22757033 = 17 \times 1338649 = 17 \times 1157^2$, as expected.

In order to prove the fundamental theorem, we need one more tool:

Lemma 1 *If p is a prime and ab is divisible by p, then a is divisible by p or b is divisible by p.*

It is important to note that p must be prime: 300 is divisible by 6 even though $300 = 15 \cdot 20$ and neither 15 more 20 is divisible by 6.

A proof of the Fundamental Theorem

We proceed in two steps. First, we show that every positive integer has a factorization into primes, and then that that factorization is unique. Each step is done by infinite descent. For the existence of a factorization, suppose that n is a positive integer that does not factor into primes. Then n cannot itself be prime because we allow that to count as a factorization. So n must be a product, $n = ab$ where a and b are integers with $1 < a < n$ and $1 < b < n$. If a and b each have a factorization into primes, then we can lump those together to get a factorization for n. (That is, knowing, say, that $300 = 30 \cdot 10$ and that $30 = 2 \cdot 3 \cdot 5$ and $10 = 2 \cdot 5$ tells us that $300 = 30 \cdot 10 = (2 \cdot 3 \cdot 5)(2 \cdot 5) = 2 \cdot 3 \cdot 5 \cdot 2 \cdot 5$, which is a product of primes.) Consequently, if n does not have a prime factorization, then either a or b does not have a factorization into primes. This produces a smaller positive integer with the same property. By infinite descent, no such number n can exist.

This proof could be easily modified to show that the Gaussian integers, $Z[\sqrt{-2}]$, and all similar sets of exotic integers also have a factorization into primes. The trick, say for the Gaussian integers, is to use an infinite descent on the square of the absolute value of the number. That is, given a Gaussian integer, $a + bi$, consider the quality $a^2 + b^2$. All the exotic integers we have talked about have factorizations into primes, it is just that those factorizations are not always unique. On to the second part of the proof.

Next, we show that (for the ordinary integers) factorization into primes is unique (up to the order of the primes). So suppose that n does not have a unique factorization. This means that n must possess two different factorizations:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n = q_1^{b_1} q_2^{b_2} \cdots q_i^{b_i}.$$

From the first factorization, we have that p_1 is a divisor of n. By the second factorization, p_1 is a divisor of $q_1^{b_1} q_2^{b_2} \cdots q_i^{b_i}$. But the lemma, p_1 must be a divisor of one of the terms q^j. But since the q's are primes, this can only happen if p_1 is one of the q's. Say, for example, that $p_1 = q_2$. Then we can divide both factorizations by p_1 to get

$$n/p_1 = p_1^{a_1 - 1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n = q_1^{b_1} q_2^{b_2 - 1} \cdots q_i^{b_i}.$$

Since the original factorizations for n were different, these have to be two different factorizations for n/p_1. Thus, we have produced a smaller positive integer without unique factorization. By infinite descent, such a thing is impossible, so there is no such n, meaning that every positive integer n has unique factorization.