

# MATH 25 CLASS 5 NOTES, SEP 30 2011

## CONTENTS

1. Prime numbers and prime factorization 1

### Quick links to definitions/theorems

- The Fundamental Theorem of Arithmetic

#### 1. PRIME NUMBERS AND PRIME FACTORIZATION

We've spent a good amount of time discussing divisibility, solving  $ax + by = c$  in integers, and greatest common divisors. We'll now put what we've learned to good use by studying properties of prime numbers more closely.

It all starts with Euclid's Lemma, which I'll repeat again:

**Lemma 1** (Euclid's Lemma, 2.1b, 2.2). *Let  $p$  be a prime. If  $p|ab$ , then  $p|a$  or  $p|b$ . More generally, if  $p|(a_1 \dots a_n)$ , then  $p|a_i$  for some  $i$ .*

*Proof.* We saw the proof for  $n = 2$  last class. The proof for general  $n$  uses induction. Suppose we know this statement for a given  $n$ . We want to prove the corresponding statement for  $n + 1$  terms; that is, we want to prove the statement that if  $p|(a_1 \dots a_{n+1})$ , then  $p|a_i$  for some  $i$ . Let  $a = a_1 \dots a_n, b = a_{n+1}$ . Then  $p|ab \implies p|a$  or  $p|b$ . If  $p|a_{n+1}$ , we are done. If  $p|a = (a_1 \dots a_n)$ , use the inductive hypothesis to conclude that  $p|a_i$  for some  $1 \leq i \leq n$ .  $\square$

A quick corollary of Euclid's Lemma is the following:

**Corollary 1** (Exercise 2.1). *If  $p$  is a prime, and  $p|a^k$ , then  $p|a$ .*

This is easily proven by just applying Euclid's Lemma to  $a_1 = a, \dots, a_k = a$ .

Why is Euclid's Lemma so important? It allows us to prove the following theorem, one of the most important in the class:

**Theorem 1** (The Fundamental Theorem of Arithmetic, Theorem 2.3). *Let  $n > 1$  be an integer. Then there exists a unique prime power factorization*

$$n = p_1^{e_1} \dots p_k^{e_k},$$

where  $p_1, \dots, p_k$  are distinct prime numbers, and  $e_i > 0$  are positive integers. (When we say this factorization is unique, we really mean unique up to permutation of the prime-power factors. For instance, we consider  $12 = 2^2 \cdot 3^1$  to be the same factorization as  $12 = 3^1 \cdot 2^2$ , since we just moved around the powers of 2, 3.)

*Proof.* We'll begin by proving the existence of such a factorization. Again, we do so by induction. Suppose we know that every integer between 2 and  $n - 1$  has a prime power factorization. Consider the number  $n$ . If  $n$  is prime, then  $n = n^1$  is a prime power factorization of  $n$ , and we are done. So suppose  $n$  is not prime. Then we can write  $n = ab$ , where  $1 < a, b < n$ . But then  $a, b$  have prime power factorizations, and when we multiply them together, we get a factorization of  $n$ . So this proves the existence of a prime power factorization.

Now let's prove uniqueness. Suppose  $n$  has two prime power factorizations

$$(1) \quad n = p_1^{e_1} \dots p_k^{e_k} = q_1^{f_1} \dots q_\ell^{f_\ell}.$$

(The  $q_j$ s are prime numbers, and  $f_j > 0$  are positive integers.) Notice that  $p_1$  divides  $n$ . In particular,  $p_1$  divides the right hand side, so  $p_1 | q_1^{f_1} \dots q_\ell^{f_\ell}$ . Euclid's Lemma tells us that  $p_1 | q_j^{f_j}$ , for some  $1 \leq j \leq \ell$ . Then the corollary to Euclid's Lemma tells us that  $p_1 | q_j$ . Because  $q_j$  is a prime number, we must have  $p_1 = q_j$ . Switching  $q_1$  with  $q_j$  (and  $f_1$  with  $f_j$ ), we can assume that  $p_1 = q_1$ . (This relabeling is legal because we said factorization was unique up to a permutation of the factors.)

Now we claim that  $e_1 = f_1$ . Suppose that  $e_1 \neq f_1$ , say  $e_1 > f_1$ . (If the reverse inequality is true, just flip the roles of the  $e, f$ s in this argument.) Then after dividing both sides of Equation 1 by  $p_1^{f_1}$ , we get

$$p_1^{e_1 - f_1} \dots p_k^{e_k} = q_2^{f_2} \dots q_\ell^{f_\ell}.$$

The exponent of  $p_1$  on the left hand side is positive, so  $p_1$  divides the left hand side. However, notice that  $p_1$  cannot divide the right hand side: if  $p_1$  did divide the right hand side, then we could conclude (exactly as we did before) that  $p_1 = q_j$  for some  $2 \leq j \leq \ell$ . This is impossible because we initially assumed all the  $q$ s to be distinct primes. So the original assumption that  $e_1 \neq f_1$  must be false; that is, we must have  $e_1 = f_1$ .

At this point, we can divide  $p_1^{e_1}$  from both sides of Equation 1 to get an equation

$$p_2^{e_2} \dots p_k^{e_k} = q_2^{f_2} \dots q_\ell^{f_\ell}.$$

We can repeat the above argument multiple times to show that each  $p_i = q_i$ , and  $e_i = f_i$ , and  $k = \ell$ . In particular, we know that  $k = \ell$ , because if not, we end up with the equation

$$1 = q_{k+1}^{f_{k+1}} \dots q_\ell^{f_\ell},$$

(or perhaps  $1 =$  a product of  $ps$ ), which is impossible since the right hand side is greater than 1. □

This is a great result. One advantage of knowing that a unique prime factorization exists is that it provides a way for us to think about products, quotients, gcds, and lcms of pairs of integers in an efficient way. For instance, suppose we know that

$$a = p_1^{e_1} \dots p_k^{e_k}, b = p_1^{f_1} \dots p_k^{f_k},$$

where this time we let  $e_i, f_i \geq 0$ , although we do insist that at least one of  $e_i, f_i > 0$ . (We do this to simplify notation, since we're allowing for the possibility that a certain prime only divides one of  $a, b$ .) Then we have the following convenient formulas:

$$\begin{aligned} ab &= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}, \\ \text{if } b|a, \text{ then } f_i &\leq e_i \text{ for all } i, \text{ and } \frac{a}{b} = p_1^{e_1-f_1} \cdots p_k^{e_k-f_k}, \\ \gcd(a, b) &= p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}, \text{ and} \\ \text{lcm}(a, b) &= p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}. \end{aligned}$$

In contrast to these above formulas, there is no nice way of expressing the prime factorization of  $a + b$  in terms of the factorizations of  $a, b$ . Here is a frequently useful notation. Suppose that  $p|n$ , where  $p$  is a prime. Then the factorization of  $n$  has some positive power of  $p$  in it, say  $p^e$ . We write  $p^e || n$  in this situation. For instance,  $2^2 || 12$ , since the highest power of 2 dividing 12 is  $2^2$ . We also sometimes write  $v_p(n)$  for the exponent of the highest power of  $p$  dividing  $n$ ; that is, if  $p^e || n$ , then  $v_p(n) = e$ . For example,  $v_2(40) = 3$ , since  $2^3 | 40$  but  $2^4 \nmid 40$ . The number  $v_p(n)$  is sometimes called the *p-adic valuation of n*. As a matter of fact, these definitions work even if  $p \nmid n$ , since the highest power of  $p$  dividing  $n$  is then  $p^0$ .

### Examples.

- Find the prime factorization of 30. One method of finding the prime factorization of an integer is trial division. That is, we simply test the divisibility of 30 by small integers which get larger and larger until we find one which works, and then start over with whatever's left, until we reach a prime.

In this example, we see that  $2|30$ . So  $30 = 2^1 \cdot 15$ . Since  $2 \nmid 15$ , but  $3|5$ , we have  $30 = 2 \cdot 3 \cdot 5$ . Since 2, 3, 5 are all primes, this is the prime factorization of 30.

- Find the prime factorizations of 994, 399, and verify that the above formulas for gcd, lcm are true. We already know that  $7|994$ , and  $994 = 7 \cdot 142$ . Since  $2|142$ , we know  $944 = 7 \cdot 2 \cdot 71$ . If you spend a while testing 71, you will eventually find that 71 is prime (we will go back to the question of how to more efficiently test for primality later). So the prime factorization of 944 is  $944 = 2 \cdot 7 \cdot 71$ .

As for 399, notice that  $399 = 7 \cdot 57$ , and  $3|57$ , so  $399 = 7 \cdot 3 \cdot 19$ . Since 19 is prime, the factorization of 399 is  $399 = 3 \cdot 7 \cdot 19$ .

So we indeed see that  $\gcd(994, 399) = 7^1$ , as expected, and one can check that  $\text{lcm}(944, 399) = 2 \cdot 3 \cdot 7 \cdot 19 \cdot 71$ .

- Notice that the above formulas give an easy verification of the fact that  $ab = \gcd(a, b)\text{lcm}(a, b)$ , because  $e_i + f_i = \min(e_i, f_i) + \max(e_i, f_i)$  is always true.
- One consequence of the above formulas is that if  $n = p_1^{e_1} \cdots p_k^{e_k}$ , then  $n^m = p_1^{me_1} \cdots p_k^{me_k}$  is the prime factorization of  $n^m$ .
- Why don't we use prime factorizations to calculate gcds? Because it is very computationally intensive to calculate a prime factorization! After all, finding a prime factorization is equivalent to listing all the factors of a number.

- One consequence of the above formulas is that it becomes very easy to calculate the number of factors a number has if you know its prime factorization. For example, the number  $p^n$  has factors  $p^0, p^1, \dots, p^n$ , which are  $n + 1$  factors altogether. More generally,  $n = p_1^{e_1} \dots p_k^{e_k}$  has  $(e_1 + 1) \dots (e_k + 1)$  factors, since the set of factors of  $n$  is described by  $p_1^{f_1} \dots p_k^{f_k}$ , where  $0 \leq f_i \leq e_i$  for all  $i$ .
- Exercise: Let  $p$  be a prime. Show that  $v_p(n!)$  (that is, the exponent of the highest power of  $p$  dividing  $n!$ ) is given by the formula

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

We'll conclude by showing that  $\sqrt{2}$  is irrational.

**Theorem 2** (Corollary 2.5).  $\sqrt{2}$  is irrational.

*Proof.* Recall that a number is rational if we can write it in the form  $a/b$ , where  $a, b$  are integers. We will proceed by contradiction. Suppose  $\sqrt{2} = a/b$  for integers  $a, b$ . Then  $2 = a^2/b^2$ , or

$$2a^2 = b^2.$$

Now consider the prime factorizations of  $a, b$ . In particular, think about the exponent of the prime 2 in these prime factorizations. On the one hand, both  $a^2$  and  $b^2$  will have factorization where the exponent of 2 is even (possibly 0). On the other hand, the power of 2 appearing in  $2a^2$  must be odd. This is a contradiction, so  $\sqrt{2}$  must be irrational.  $\square$

Of course, you can see how this generalizes to  $\sqrt{m}$ , where  $m$  is any positive integer which is not a perfect square.