

M316K – Foundations of Arithmetic
Spring 2009
Some Notes on Number Theory

I. Divisibility

One of the main areas of study in number theory deals with *divisibility*; that is, the question of whether one integer is divisible by another. For integers a and d , d nonzero, we say that a is *divisible* by d if dividing a by d yields an integer result. (For whole numbers a and d , to say that a is divisible by d means that you can divide a things equally into d groups; this is probably where the word “divisible” comes from.)

We have several different ways of saying that a is divisible by d :

- We say that d is a *divisor* of a . (In the relationship between a and d , the number a is being divided, and the number d is doing the dividing.)
- We say that d is a *factor* of a . (You’re familiar with the idea of factoring a number into primes; in the equation $35 = 5 \cdot 7$, 5 and 7 are factors of 35.)
- We say that a is a *multiple* of d . (This is because we can obtain a by multiplying d by an integer m ; this relationship can be expressed with the equation $a = d \cdot m$. Note that this is equivalent to $a/d = m$.)
- We use the notation $d|a$, pronounced “ d divides a .” The order is very important here! Remember, in the relationship between a and d , it is d that is doing the dividing, and a that is being divided. So it is correct to say that 3 divides 15 (in other words, you can divide 15 evenly by 3), but not that 15 divides 3.

Usually, the most straightforward way to determine whether a number a is divisible by a number d is to simply try dividing a by d , and see whether you get a remainder. If you get a remainder of zero, then d is a divisor of a ; if your remainder is nonzero, then d doesn’t divide a . Some (potential) divisors have special divisibility tests:

- 1: Every whole number is divisible by 1.
- 2: A whole number is divisible by 2 if and only if its ones digit is divisible by 2. *Example:* 4896 is divisible by 2 because its ones digit, 6, is even.
- 3: A whole number is divisible by 3 if and only if the sum of its digits is divisible by 3. *Example:* 576 is divisible by 3 because the sum of its digits, $5 + 7 + 6 = 18$, is divisible by 3. (If you’re not convinced that 18 is divisible by 3, run the test on 18: 18 is divisible by 3 because the sum of its digits, $1 + 8 = 9$, is divisible by 3.)
- 4: A whole number is divisible by 4 if and only if the two-digit number consisting of its tens and ones digits is divisible by 4. *Example:* 824 is divisible by 4 because 24 is divisible by 4.
- 5: A whole number is divisible by 5 if and only if its ones digit is divisible by 5.
- 6: A whole number is divisible by 6 if and only if it is divisible by both 2 and 3.
- 8: A whole number is divisible by 8 if and only if the three-digit number consisting of its last three digits is divisible by 8.
- 9: A whole number is divisible by 9 if and only if the sum of its digits is divisible by 9.
- 10: A whole number is divisible by 10 if and only if its ones digit is 0.
- 11: A whole number is divisible by 11 if and only if its *alternating digit sum* is divisible by 11. *Example:* 4917 is divisible by 11 because its alternating digit sum, $4 - 9 + 1 - 7 = -11$, is divisible by 11.

Each of these divisibility tests comes as a result of our working in a base-ten system. Note that divisibility tests where you knock off all but the last few digits (2, 4, 5, 8) all bear a special relationship to the number 10 (I'll leave you to think about how that relationship can be summed up). Divisibility tests where you add up the digits (3, 9) all bear a special relationship to the number $10 - 1$, or 9. Divisibility tests where you take the alternating digit sum (11) all bear a special relationship to the number $10 + 1$, or 11. Based on this information, can you guess what the divisibility tests would be in base 16? How about base 20? Can you think of a base in which there is a divisibility test for 7?

II. Prime numbers

A *prime number* is a number that has exactly two divisors: 1 and itself. Note that the “exactly two divisors” part is important; it means that 1 is not a prime number, even though it is divisible only by 1 and itself. The reason we don't consider the number 1 a prime (that is, the reason we insist that the definition of prime should include the “exactly two divisors” clause) is structural, not historic; in other words, it's not a matter of convention. To give you an idea of the reason, we tend to classify numbers as prime, composite, or “other” (1 is “other”) based on their multiplicative properties. The prime numbers and composite numbers (all integers greater than 1) don't have multiplicative inverses in the set of integers, but the number 1 does (its inverse is 1). So rather than calling 1 a prime or a composite number, we call it a *unit*.

A *composite number* is a number that has more than two divisors; that is, that has divisors other than 1 and itself. Put differently, a counting number n is composite if and only if it can be expressed in the form $n = a \cdot b$, where both a and b are less than n .

How do we tell whether a number is prime or composite? Depending on how you look at this question, it can be either ridiculously easy or ridiculously hard. The “easy” answer is that you can determine whether a number is prime (this process is called “primality testing”) by checking all the counting numbers between 1 and the number, and seeing if any of them are divisors. However, this process takes an excruciatingly long time, and that's the “hard” part of the question – how do we perform this task more efficiently? Believe it or not, this question is still of great interest to mathematicians and computer scientists (who rely on primality testing – and on the difficulty of primality testing! – to send information securely over computer networks).

Much progress has been made on this question, including some very significant progress that has been made in the last ten years, but for purposes of this class, we'll just focus on one algorithm that is still fairly inefficient. To determine whether a number n is prime, check n for divisibility by prime numbers less than or equal to \sqrt{n} . If n is divisible by any of these prime numbers, then n is composite (as you should know from the definition). If n isn't divisible by any of these primes, then n itself is prime!

Example: Suppose we want to determine whether 233 is prime (you found out that it is on a recent problem set). We know that $\sqrt{233} \approx 16$, so it's enough for us to check whether 233 is divisible by any prime number less than or equal to 16. We can use divisibility tests to see easily that 233 isn't divisible by 2, 3, or 5. If we try dividing 233 by 7, we get a remainder of 2, so 7 isn't a divisor. Neither is 11 (the remainder is also 2) or 13 (the remainder is 12). These are all of the primes less than 16, so we can now say with complete confidence that 233 is prime.

Example: Many of you incorrectly said on the problem set that 817 is prime, because you checked for divisibility by 2, 3, 5, and 7 (or you checked for divisibility by any number less than 10). That's a good start, but since $\sqrt{817} \approx 29$, we need to check for prime factors up to and including 29. If we keep testing, we'll see that 11, 13, and 17 are not divisors, but 19 is. By dividing 817 by 19, we see that $817 = 19 \cdot 43$.

How is it that we can know so much about n just by checking potential divisors up to \sqrt{n} ? We can demonstrate (or “prove”) this using the following argument: Suppose that n is composite. Then n

must factor as a product of two smaller numbers a and b . We can assume that a is less than or equal to b (by switching the roles of a and b if necessary). Then we must have $a \leq \sqrt{n}$, because otherwise, we would have $\sqrt{n} < a \leq b$, and this would mean that $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. Compressing that last inequality, we get $n > n$, which is plainly ridiculous. So we must have $a \leq \sqrt{n}$, and a has a prime factor p (because a isn't 1, and every natural number greater than 1 has a prime factor). That prime factor p must be less than or equal to a . So p is a factor of a , and a is a factor of n ; this means that p is a factor of n ; and because $p \leq a \leq \sqrt{n}$, we have $p \leq \sqrt{n}$. So if n is composite, then n must have a prime factor less than or equal to \sqrt{n} . This means that if there is no such prime factor, n must be prime.

Don't feel bad if you didn't follow the above argument; students typically learn to follow arguments like these when they train to be mathematicians. The key to following an argument like this is to try to link it to something that you know; in your case, the best thing to use is concrete numerical examples. So consider the number 73. We know that $\sqrt{73}$ is between 8 (whose square is 64) and 9 (whose square is 81). So if 73 factors as a product of two smaller numbers, then one of those numbers must be less than 9. After all, the alternative is for both numbers to be 9 or greater, in which case their product will be at least $9 \cdot 9$, or 81 (which is bigger than 73). So if 73 is composite, it has to have a factor that is greater than 1 but less than 9. But if there is such a factor, then we can also find a prime factor. If 73 were divisible by a composite number, like 6 (obviously 73 isn't divisible by 6, but play along for the moment), then we could observe that 6 has a prime, 2, as a factor, and so 2 is also a factor of 73. So if we just look for prime factors, we're doing enough work to detect any proper divisors 73 might have.

At this point I would ask, "How many of you now understand this argument better than when I used variables?" And about five of you would raise your hands, and I would ask if there are any questions, and there wouldn't be any. So the rest of you, if you want to understand this argument better, can talk to me after class or during office hours. It's not essential for you to be able to write a mathematical proof like the one above (the one with variables), but I'd like for you to understand the ideas. If you don't understand them, then when you do the square-root trick to check for primality, you're just doing what everybody else does, which is the sort of behavior that keeps math from making sense.

If you want to find a lot of prime numbers – say, all of them – one trick you can use is the *sieve of Eratosthenes*. Bassarear explains the process pretty well, so I won't say much about it here, but the idea is that you write down all the numbers from 1 to N (you pick the value of N , depending on how many prime numbers you want to find), and identify the number 2 as prime. You then eliminate all the multiples of that prime greater than 2 (because those multiples are composite). You then identify the first number that hasn't been eliminated – namely, 3 – and observe that it is prime, because if it were composite, it would have had a prime factor (by our argument above), and thus would have been eliminated at a previous stage of the process. We then identify 3 as prime and eliminate all other multiples of 3. We continue this process, at each step identifying the first non-eliminated number as prime, because if it were composite it would have been eliminated already, and eliminating all other multiples of that prime. See the visual in the book, which is much better (for most of you, at least) than a wordy explanation.

The ancient Greek mathematician Euclid proved that there are infinitely many prime numbers; in other words, if you were to write all the prime numbers in a list, the list would go on forever. The proof is wonderfully clever; the idea is to assume the opposite – that the list would end somewhere, giving you a finite list of prime numbers – and multiply all of those prime numbers and add one to the product. This gives you a number that isn't divisible by any of the prime numbers in your list (because the remainder when you divide your new number by any of those primes would be 1). But your number has to have a prime factor (which wouldn't be on the list), or be prime itself (and certainly not on the list, because we got it by multiplying everything on the list and adding one). That's a contradiction, and when we get a contradiction in mathematics, it means we've assumed something that is wrong. Here, the wrong assumption we made is that the list of primes doesn't go on forever.

As simple as prime numbers seem to be, we don't know nearly as much as we'd like to know about

them (and by “we,” I don’t mean “our class”; I mean “mankind.”) Here are some things we don’t know about prime numbers:

- Is there a largest pair of twin primes, or do pairs of twin primes go on forever? (*Twin primes* are pairs of primes that are 2 apart, such as 3 and 5, 5 and 7, 11 and 13, and 17 and 19.)
- Is there an even number greater than 4 that cannot be written as a sum of two prime numbers? (Try this for any even number less than 200 or so; for example, $152 = 73 + 79$. Mathematicians have computer-tested approximately 10^{18} even numbers, and every single one so far has been expressible as a sum of two primes. And yet we don’t know of a really good reason why it should always be possible to do this. When you look at the integers as a whole, prime numbers are relatively scarce, so there isn’t any immediate way to see that every even number can be expressed as a sum of two primes.)

III. Prime factorization

Prime factorization is the most important topic in this chapter because of the immense power that comes from knowing a number’s prime factorization. But before we explore that power, let’s recall what a prime factorization is. A *prime factorization* of an integer n is a way of writing n as a product of prime numbers (some of which may be repeated). For example, a prime factorization of 78 is $78 = 2 \cdot 3 \cdot 13$. A prime factorization of 300 is $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$, which we often write as $300 = 2^2 \cdot 3 \cdot 5^2$.

You may find it strange that I used the phrase “a prime factorization” when I (and most other people) usually say “the prime factorization.” The reason I used the phrase “a prime factorization” is that, for all we know (before we learn number theory), a number could have several different prime factorizations. Perhaps there is a number out there that has $3 \cdot 7^2 \cdot 13$ as a prime factorization, but also has $5 \cdot 11^2$ as a prime factorization. (You should be able to tell without much work that those aren’t the same number, and I’m just making things up.)

It turns out that you don’t have to worry about this sort of thing. One of the greatest things about prime factorizations is that the prime factorization of a number is *unique*; that is, if Sakeenah and Tina both find prime factorizations of the same number, they should get the same prime factorization (assuming that both factorizations are correct). Sakeenah’s primes might be in a different order than Tina’s, but there shouldn’t be any essential difference between the two factorizations. This fact is called the *Fundamental Theorem of Arithmetic*.

In practice, we find the prime factorization of a number using a “factor tree”; I won’t do any examples of that here because you can find them in the book (and the vast majority of you can already do them quite well anyway).

IV. Divisor counting

Now that we have prime factorizations in our toolbox, let’s take a look at some of the wondrous things we can do with them. We’ll start with the task of counting the divisors of a positive integer. In this chapter (and in these notes), when we say “divisor,” we mean “positive divisor.” In number theory, negative numbers are allowed to be divisors as well (because after all, one can certainly get an integer by dividing an integer by a negative integer).

Example: Suppose we want to find out how many divisors the number $72 = 2^3 \cdot 3^2$ has. There are several ways to do this, from “completely unsophisticated” to “slicker than a used car salesman.” The completely unsophisticated approach is to haphazardly guess numbers and hope that in the process, you find all the divisors. Once you get tired of doing that (which hopefully doesn’t take too long), you start to notice that the divisors of 72 come in pairs:

$$72 = 1 \cdot 72 \quad 72 = 2 \cdot 36 \quad 72 = 3 \cdot 24 \quad 72 = 4 \cdot 18 \quad 72 = 6 \cdot 12 \quad 72 = 8 \cdot 9$$

This pairing allows us to count the divisors of 72 more quickly. If we start at 1 and identify the divisors in increasing order, once we reach a divisor that is the “partner” of a divisor we’ve already found, we can count all the divisors we’ve already found (prior to discovering the partner), and multiply that count by 2. In this case, we’d keep going until we found 9, which is the partner of 8. By this time we’ve found six divisors between 1 and 8, inclusive, so 72 has twice this many (twelve) divisors. A word of caution, though: some numbers have divisors which are their own partners (which numbers are these?), and in these cases, you won’t be able to get the number of divisors by multiplying your count by two.

Once you get tired of doing *that*, it’s time to find a much better way to handle problems like these. One useful thing to do is to think about the divisors of 72 and their prime factorizations. Each divisor of 72 is a “combination” (via multiplication) of 2’s and 3’s – the same numbers that appear in the prime factorization of 72 itself. We can arrange the divisors of 72 in a table according to how many 2’s and how many 3’s each divisor has:

	2^0	2^1	2^2	2^3
3^0	1	2	4	8
3^1	3	6	12	24
3^2	9	18	36	72

This table gives us much more insight about relationships between the divisors of 72 than a simple list would. For example, we notice that in many cases, we can obtain a divisor of 72 by multiplying another divisor by 2 or 3. You may also find it useful to try answering the following questions:

- Which divisors of 72 are odd? (Where are they in the table?)
- Which divisors of 72 are not divisible by 3?
- For a given divisor of 72 in the table, where can you find its “partner”?
- Which divisors of 72 are perfect squares? (Where are they in the table?)

But the question we’re most interested in right now is “How many divisors does 72 have?” From the table, it is readily apparent that there are 12, but notice that this 12 arises in a nice, natural way. The table has four columns (because there are four different powers of 2 we can use: 2^0 , 2^1 , 2^2 , and 2^3) and three rows (because there are three different powers of 3 we can use: 3^0 , 3^1 , and 3^2). Because we need to choose a power of two and a power of three, we have a total of $4 \times 3 = 12$ choices. (Which model of multiplication are we using here?)

Example: Let’s suppose we want to count the divisors of a much larger number, such as $5^{13} \cdot 11^4 \cdot 17$. (Good luck calculating this by hand, let alone counting the divisors using the hunt-and-peck method!) Then we know that there are

- 14 powers of 5 we can use: $5^0, 5^1, 5^2, \dots, 5^{12}, 5^{13}$ (notice that the 5^0 is important, because we can choose divisors that are not divisible by 5)
- 5 powers of 11 we can use: $11^0, 11^1, 11^2, 11^3$, and 11^4
- 2 powers of 17 we can use: $17^0, 17^1$

Since we must choose one of each, the number of divisors of $5^{13} \cdot 11^4 \cdot 17$ is $14 \times 5 \times 2 = 140$. Again, not something you would have been likely to find by simply making a list!

Here are some questions you’d do well to try to answer:

- How many divisors of $5^{13} \cdot 11^4 \cdot 17$ are less than 100?
- How many divisors of $5^{13} \cdot 11^4 \cdot 17$ are perfect squares?
- How many divisors of $5^{13} \cdot 11^4 \cdot 17$ have ones digit 5?

V. Greatest common factors, Least common multiples

One reason we cover the basic principles of number theory in this course is that we use the ideas of GCF (greatest common factor) and LCM (least common multiple) when performing operations with fractions. Of course, even if these ideas weren't useful when we deal with fractions, they'd still be worth learning in their own right (obviously), but the fact that fraction operations rely on these ideas makes this discussion even more worthwhile.

First, let's define the GCF and LCM of two numbers. For two whole numbers a and b (not both zero), the *greatest common factor* (or GCF) of a and b is the greatest whole number d such that $d|a$ and $d|b$. For those of you who don't like symbols so much, another way to say this is that the GCF is the largest number that is a factor of both a and b . (*Note:* Every mathematician I know of calls this the GCD; I don't know why Bassarear sticks with the name GCF, unless maybe the word "factor" is more popular than the word "divisor" in mathematics education.)

For two positive integers a and b , the *least common multiple* (or LCM) of a and b is the smallest positive integer m such that $a|m$ and $b|m$. Again, to recast it for those who are allergic to symbols, m is the smallest positive integer that is divisible by both a and b . (Note the contrast with the definition of GCF.) Notice that I'm requiring m to be a *positive* integer; this is important. If you were just looking for any old common multiple of a and b , the number 0 would always work, because 0 is a multiple of everything. But we don't consider that the "least common multiple" because for the tasks we use the LCM for, an answer of 0 (while not necessarily wrong) typically isn't that useful. (Think back to the Exploration in which you used the LCM to determine the next time two people on different ferris wheels would both meet at the bottom; it would be silly, though not really incorrect, to say that the two people would meet again 0 seconds from now. And besides that, it wouldn't give you the *next* time.)

Again, there are several methods for finding the GCF and LCM of two numbers, at varying levels of sophistication. We'll illustrate these with an example.

Example: Suppose we want to find the GCF and LCM of 24 and 40. We'll start with the GCF. Since we're looking for the greatest common factor of 24 and 40, one way to get at this is to list all the divisors of 24 and 40, and identify those that are common to both:

Divisors of 24: **1**, **2**, 3, 4, 6, **8**, 12, 24
Divisors of 40: **1**, **2**, 4, 5, **8**, 10, 20, 40

I identified the common factors by bolding them; you'll probably want to use a convention that is easier to do with paper and pencil, such as circling. Anyway, you can easily see here that the greatest common factor, or GCF, is 8.

What about the LCM? We can try using the same sort of technique to find the LCM, but it's a bit tricky, since we can't list all the multiples of 24 or 40; these go on forever. Still, since we're just looking for the first (positive) common multiple on our list, we can try listing a few multiples of each and hope we find a common one:

Multiples of 24: 24, 48, 72, 96, **120**, 144, 168, 192, 216, **240**, ...
Multiples of 40: 40, 80, **120**, 160, 200, **240**, 280, 320, **360**, 400, ...

Aha! We find that the number 120 is the first number to appear on both lists, so 120 is the LCM. (Notice that I bolded 360, a multiple of 40, even though it doesn't appear to be on the first list. If we continued the first list far enough, we'd see that 360 actually is on the list. Of course, even if we hadn't caught this, we still would have correctly identified 120 as the LCM.)

The problem with these methods is that listing things out in this way is a tedious, time-consuming process. Furthermore, if you make an error (say, in calculating multiples of a number, which I did by counting up by the appropriate amount), you may end up never finding a common multiple. So let's

see if we can use prime factorizations to make our job easier. We have $24 = 2^3 \cdot 3$ and $40 = 2^3 \cdot 5$, so keep that in mind as we proceed:

Let's start by finding the GCF of 24 and 40. We know that if d is a common factor of 24 and 40, then d can't have a 3 in its prime factorization, because 40 is not divisible by 3. Also, d can't have a 5 in its prime factorization, because 24 is not divisible by 5. Of course, d can't have any larger primes, like 7, 11, or 13, in its prime factorization, because neither 24 nor 40 is divisible by any of these. So the only prime number d can have in its prime factorization is 2. But we do know that d can have up to three "copies" of the number 2 in its prime factorization, because both 24 and 40 have three copies of 2 in their prime factorizations. So the largest common divisor we can come up with is the product of three copies of 2, and no other primes. That's 2^3 , or 8.

What about the LCM? If m is to be a multiple of both 24 and 40, then m must have the prime factors 2, 3, and 5 in its prime factorization. This is because in order for m to be divisible by 24, it must be divisible by 2 and 3 and for it to be divisible by 40, it must be divisible by 2 and 5. But we have to do a bit better: notice that if we want m to be divisible by 24, we actually need the prime factorization of m to contain three copies of 2, not just one. The same goes for 40, which also contains three copies of 2 in its prime factorization. So m needs to have three copies of 2, a 3, and a 5. So m must be at least $2^3 \cdot 3 \cdot 5 = 120$. We can check that 120 is indeed divisible by both 24 and 40 (we've already done this using our lists above); this means that 120 is the least common multiple.

This method of using prime factorizations is so powerful that it's worth trying out on a couple more examples.

Example: Let's find the GCF and LCM of 900 and 750. If we find the prime factorizations of 900 and 750 (you should do this on your own!), we get $900 = 2^2 \cdot 3^2 \cdot 5^2$ and $750 = 2 \cdot 3 \cdot 5^3$.

If d is a number that divides both 900 and 750, then d must contain only the primes 2, 3, and 5, which are common to 900 and 750. How many copies of each prime factor can d contain? If d has more than one 2, then it won't be a factor of 750, which has only one copy of 2 in its prime factorization. So d can only have one 2. For the same reason, d can only have one 3. However, d can have two 5's, since both 900 and 750 have at least this many. (It can't have three, though, because 900 only has two.) So the GCF of 900 and 750 is $2 \cdot 3 \cdot 5^2 = 150$.

What about the LCM? If m is to be divisible by both 900 and 750, then m needs to have at least two 2's (since 900 has this many), at least two 3's (since 900 has this many), and at least three 5's (since 750 has this many). So the LCM of 900 and 750 is $2^2 \cdot 3^2 \cdot 5^3 = 4500$.

Example: Let's do one more example, and find the GCF and LCM of 33 and 35. The prime factorizations of these numbers are $33 = 3 \cdot 11$ and $35 = 5 \cdot 7$.

First we'll find the GCF. If d divides both 33 and 35, then d can only have ... Hey, wait a minute! There isn't a single prime that d can have in its prime factorization, because there are no prime factors common to 33 and 35. This means that d must have *no* factors in its prime factorization! If a positive integer doesn't have any prime factors, that means it's the number 1 (you can see for yourself that 1 has no prime factors). So the GCF of 33 and 35 is 1. You can see this in this particular example by just listing divisors (a.k.a. the "brute force method"), but make sure you understand what it means when the prime factorizations have nothing in common; this is important.

Now let's find the LCM. If m is divisible by both 33 and 35, then m must have a 3, an 11, a 5, and a 7 in its prime factorization; it only needs one of each. So the least common multiple of 33 and 35 is $3 \cdot 5 \cdot 7 \cdot 11 = 1155$.

There is one more method for finding the GCF of two numbers, and it's called the *Euclidean algo-*

rithm. It was discovered (along with most basic results in number theory) by Euclid, and what is really remarkable about this method is that it remains the most efficient way (within classical number theory, at least) to find the GCF of two numbers. The great strength of this method is that you don't have to know the prime factorizations of your two numbers in order to use it! (This is especially important with larger numbers, because we – and again, I mean “mankind,” not “this class” – don't have an efficient way to find prime factorizations of very large numbers.) I'm not going to give a step-by-step explanation of the method, because I think the better way to show you how to use it is to do an example. I'll use the algorithm to find the GCF of 374 and 527. I'll start by dividing the larger number by the smaller; watch what I do after that:

$527 \div 374$ is 1 with a remainder of 153

$374 \div 153$ is 2 with a remainder of 68

$153 \div 68$ is 2 with a remainder of 17

$68 \div 17$ is 4 with a remainder of 0

At this point, since I have a remainder of zero, I stop the process. The last nonzero remainder I get – 17 in this case – is the GCF of the two numbers. Pretty cool, huh? (In case you're wondering what I did with the quotients I got – 1, 2, 2, 4 – the answer is “Nothing.” They don't matter here.)

We can also use the GCF of two numbers to find the LCM, using the following theorem:

Theorem: For two positive integers a and b , we have $a \cdot b = GCF(a, b) \cdot LCM(a, b)$.

Example: The LCM of 527 and 374 satisfies the equation $527 \cdot 374 = GCF(527, 374) \cdot LCM(527, 374)$. We know that the GCF is 17, so we have $527 \cdot 374 = 17 \cdot LCM(527, 374)$. (Notice I'm hesitant to multiply the numbers on the left; that's because I don't have to.) So the LCM is $527 \cdot 374 / 17 = 11594$. (Don't worry, the numbers on the test won't be that big.)

If you want to know why this theorem works, think about the prime factorizations of a and b (looking at the examples we did might be helpful), and the prime factorizations of the GCF and LCM. Compare the first pair of prime factorizations (a and b) with the second pair (the GCF and LCM). And if you want to know more, as always, come visit me in my office. I'd love to talk to you about it; if you don't show up, I'll probably just be sitting around looking at lolcats or something. I can haz office hrz?