MATH 115, SUMMER 2012
LECTURE 3
WEDNESDAY, JUNE 20TH

JAMES MCIVOR

Last time:
- The ideal consisting of linear combinations of a and b is generated by their gcd.
- how to calculate gcd and write it as a linear combination of a and b.
- properties of gcd, especially $(a, b) = (a, b + ax)$

Today - LCM and primes

Random definition - for sets of more than two integers, relatively prime vs. relatively prime in pairs. If we have more than two integers, say $a_1, \dots, a_n$, then there are two types of "relative primes-ness" we can require. Firstly, if the gcd $(a_1, \dots, a_n)$ of all n of them is 1, we say they are **relatively prime**. If, taken two at a time, the gcds (a_i, a_j) are each 1, we say they are **relatively primes in pairs** or **pairwise relatively prime**. This is stonger than just being relatively prime

Example 0.1. 4,6, and 3 are relatively prime (the only positive divisor common to all three is 1), but not pairwise relatively prime, since $(4, 6) = 2$ and $(6, 3) = 3$.

This next property will be crucial when we study primes:

Proposition 1. *If $c|ab$ and b and c are coprime, then c must divide a.*

Proof. The conlcusion is the same as saying that $a \in (c)$. We're given that $ab \in (c)$, and that 1 can be written as a linear combination of b and c, say $1 = bx + cy$. Multiply by a, so $a = abx + acy$. Since abx and acy are both in (c), so is a (using closure uner $+$) □

1. LCM

There is a sort of counterpart to gcd, the least common multiple:

Definition 1. If $a_1, \dots, a_n$ are n nonzero integers, we say that b is a **common multiple** of the a_i if each a_i divides b. The **least common multiple (lcm)** of the a_i is the smallest positive integer which is a common multiple of all the a_is. It is denoted $[a_1, \dots, a_n]$.

The lcm can also be characterized in terms of ideals:

Theorem 1. *Let $a_1, \dots, a_n$ be nonzero integers. The set of common multiples of the a_i forms an ideal, which is generated by the lcm of the a_i.*

Proof. - Set of common multiples of the a_i closed under $+$ and scalar mult.
- So it's an ideal, call it I, therefore principal, generated by some $l \in \mathbb{Z}$.

- This l is therefore *a* common multiple. Why the least? If there were a smaller one, it would generate I instead of l.

□

gcd and lcm have a nice relationship:

Proposition 2. *For a, b not both zero (so their gcd and lcm actually exist), we have the formula*

$$(a, b) \cdot [a, b] = |ab|$$

- The vertical lines on the right hand side are absolute value.
- We'll prove this soon using prime factorization.

2. Primes and Unique Factorization

The basic building blocks for integers using multiplication are the primes:

Definition 2. An integer $p > 1$ is **prime** if it has no positive divisors except 1 and p.

- sieve of eratosthenes?
- infinitely many primes. The classic proof: Suppose for contradiction there are finitely many, say $p_1, \dots, p_k$. Then look at the number $1 + p_1 \cdots p_k$. You may think at first that this number is itself prime, but that's not necessarily true. If it is prime, then we're done, since it's a new prime and that contradicts the fact that $p_1, \dots, p_r$ were the only ones. If it's not prime, then it at least has a prime factor q, say $n = qr$ (where r may or may not be prime). But then this q is a new prime, not in the list. If it were one of the p_i, then we would have $q|n$ and $q|p_1 \cdots p_k$, so $q|(n - p_1 \cdots p_k) = 1$, contradiction - primes can't divide 1!

The gcd is easy to calculate when one of the terms is prime:

Lemma 1. *1) if $p \not| a$, the gcd of a and p is 1.*
2) if $p|a$, the gcd of a and p is a.

This comes straight from the definition: first we consider the positive common divisors of p and a. They can only be 1 or p, since these are the only positive divisors of p. If we assume that p is not a divisor of a, then 1 is the only positive common divisor, and it is therefore their gcd. If p *is* a divisor of a, then 1 and p are the only positive common divisors, so p is the greatest one.

Here's a key property of primes, that we will use all the time:

Lemma 2. *If p is prime, and a, b are any integers, then $p|ab$, then either $p|a$ or $p|b$.*

Proof. Let p be a prime, and suppose $p|ab$ but $p \not| a$. We will show that $p|b$. As noted above, the gcd $(a, p) = 1$. Now remember from last lecture that the ideal generated by the gcd is the same as the set of $\mathbb{Z}$-linear combinations of a and p. This means that the gcd itself can be written as a linear combination:

$$1 = ax + py$$

for some integers x and y; now multiply by b:

$$b = abx + pyb.$$

Since $p|ab$, it divides abx, and it clearly divides pyb, so $p|b$. Done.

□

The same argument shows that if p divides $a_1 \cdots a_n$, then it must divide at least one of the a_is. The most familiar fact about primes is that we can decompose any (nonzero) integer into a product of primes.

Theorem 2 (Fundamental Theorem of Arithmetic)**.** *If n is any nonzero integer, then n can be* uniquely *expressed as $n = \pm p_1^{a_1} \cdots p_r^{a_r}$, where the p_i are prime numbers, with $p_1 < p_2 < \ldots < p_r$, and each $a_i > 0$.*

Note that we can even obtain 1 in this way, by taking $r = 0$. In other words, "1 is the product of no primes", sometimes called the "empty product". Note also that we usually only care about factoring positive integers, in which case we can drop the ±.

Proof. The proof has two main steps: first we show that every integer can be factored in this way, and then we show that it's unique. First note that if n can be factored uniquely, then so can $-n$, so we might as well assume n is positive from now on. To see that there is a factorization, we may use ("strong") induction. The base case, $n = 1$, gives the "empty product" mentioned above. So now assume that all integers $\leq n$ can be factored into primes (we don't care about uniqueness yet). We show n can be factored into primes. Well, n is either prime, or not. If n itself is prime, we're done: take $r = 1$, $p_1 = n$, and $a_1 = 1$. If n is composite (not prime), then by definition n has a proper divisor $a|n$, where $1 < a < n$. Thus there is some b such that $ab = n$. But a and b are both less than n, so they each factor into primes, hence so does n.

Next we show the uniqueness. In general, to show something's unique, you take two of them, and then prove that they must be the same. So for a given integer n, we will pick two factorizations by primes:

$$n = p_1^{a_1} \cdots p_r^{a_r} \quad \text{and} \quad n = q_1^{b_1} \cdots q_s^{b_s}$$

where the q_i and p_i are primes, with $p_1 < \ldots p_r$ and $q_1 < \ldots < q_s$. We wish to show that these are the same factorization, i.e., that $r = s$, $p_i = q_i$ for all i, and $a_i = b_i$ for all i. We can use induction on n. For the base case, if $n = 1$, then there are no primes in either factorization (the "empty product" again). So $r = s = 0$ and there is nothing else to say. Now assume we've proved that every integer $< n$ can be factored uniquely into primes. Looking at the first factorization, we see that p_r divides n. So p_r must divide $q_1^{b_1} \cdots q_s^{b_s}$, since it's equal to r. But by the lemma above, since p_r is prime, it must divide one of the factors. Since they're all prime, this means $p_r = q_i$ for some i. Now we cancel out this term from both factorizations. Then the resulting number, which is $n/p_r = n/q_i$, is smaller than n, so can be factored uniquely, so all the other primes in the two factorization are equal, i.e., $p_1 = q_1$, $a_1 = b_1$, etc. Thus our factorizations of n are both the same. □

Other Notation

We will also write

$$n = \prod_p p^{\alpha(p)}$$

for the factorization of n into primes. The notation $\prod$ just means product, and the subscript p means we take the product over all primes p - namely, for each p, we take p to some power $\alpha(p)$, and multiply these all together. It doesn't make sense to multiply the infinitely many primes (we will see that there are infinitely many shortly), so most of the $\alpha(p)$'s must be zero.

For example, let $n = 84$. It factors as $84 = 2 \cdot 2 \cdot 3 \cdot 7$. So if we write $84 = \prod p^{\alpha(p)}$, then in this case $\alpha(2) = 2$, $\alpha(3) = 1$, and $\alpha(7) = 1$, while all other α's are zero, meaning those other primes do not occur in the factorization.

This notation can be useful for working with gcd and lcm:

Lemma 3. *Let* $a = \prod_p p^{\alpha(p)}$ *and* $b = \prod_p p^{\beta(p)}$. *Then*

(1) $(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}$, *and*

(2) $[a, b] = \prod_p p^{\max(\alpha(p), \beta(p))}$

This makes sense intuitively: how do you form the biggest common divisor? Just take as many primes as you can that occur in both factorizations.