Math 126 Number Theory

Prof. D. Joyce, Clark University

30 Jan 2006

Due Wednesday. From page 26, exercises 2, 3, 4, 5, 6, 11, 12, 13.

For next time. Read through section 2.3.

Last meeting. Some elementary properties of divisibility, prime numbers, greatest common divisors, and the Euclidean algorithm.

Today. More on divisibility, prime numbers, greatest common divisors, and the Euclidean algorithm. We'll continue to assume all the numbers under discussion are positive integers.

We've seen how the Euclidean algorithm computes the greatest common divisor (m, n) of two numbers m and n by repeatedly subtracting the smaller from the larger until they're reduced to the same number d, their GCD. That worked because at each step a number divided the two current numbers in the process, a and b, if an only if it divided the two next numbers $a - b$ and b. That implies that a number divides d if and only if it divides both m and n. In summary, we have the following theorem.

Theorem. Let d be the result of applying the Euclidean algorithm to m and n. Then d is the greatest common divisor (m, n). Furthermore, every divisor k of m and n divides $d = (m, n)$. Finally, every divisor of d is a common divisor of m and n.

Proof: The remarks above show that every divisor k of m and n also divides the result d of applying the Euclidean algorithm to m and n. They also show that the result d also divides m and n. Thus, d is a divisor of m and n, and since every other divisor divides d, it is the greatest common divisor. Finally, if $k|d$, since $d|m$ and $d|n$, therefore $k|m$ and $k|n$. Q.E.D.

There's still more that we can get out of the algorithm. Let's use the division form for it. Let's suppose that $m > n$ to begin with. We divide n into m and get a quotient of q_1 and remainder of r_1, that is

$$m = q_1 n + r_1,$$

with r_1 between 1 and n. Then we work with n and r_1 instead of m and n. Divide r_1 into n to get q quotient of q_2 and a remainder of r_2, that is,

$$n = q_2 r_1 + r_2.$$

And we keep going until eventually we get a remainder of 0.

$$\begin{aligned} r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{s-3} &= q_{s-1} r_{s-2} + r_{s-1} \\ r_{s-2} &= q_s r_{s-1} + 0 \end{aligned}$$

We have

$$m > n > r_1 > r_2 > \cdots > r_{s-1}$$

and r_{s-1} is d, the GCD we're looking for.

We can use these equations to find d as a linear combination of the original numbers m and n as we did in an example last time. The first equation implies that r_1 is a linear combination of m and n. The next implies that r_2 is a linear combination of n and r_1, therefore a linear combination of m and n. Likewise the next shows r_3 is a linear combination of m and n, and so forth until we get to the next to the last equation which shows that r_{s-1}, which is

the GCD of m and n is a linear combination of m and n. Thus, we've shown the following theorem.

Theorem. The greatest common divisor $d = (m, n)$ of m and n is a linear combination of m and n. That is, there exist numbers a and b such that

$$d = am + bn.$$

Now that we have the major theorems on GCDs, there are a few more fairly elementary proprieties of GCDs that are straightforward to prove, such as these.

Theorem.

(a). $(a, b + ka) = (a, b)$.

(b). $(ak, b,) = k(a, b)$.

(c). If $d = (a, b)$, then $(a/d, b/d) = 1$.

We may do the proof of one or two of these in class.

Greatest common divisors of more than two numbers. The GCD of more than two numbers is defined the same way as for two numbers: the GCD of a set of numbers the largest number that divides them all. For example, $(14, 49, 91) = 7$. To find a GCD of three numbers, a, b, and c, first find $d = (a, b)$, then find $e = (d, c)$. Thus,

$$(a, b, c) = ((a, b), c),$$

a statement that is easy to show.

Pairwise relatively prime numbers. A set of numbers is said to be *pairwise relatively prime* if any two of them are relatively prime. For instance, 15, 22, and 49 are three pairwise relatively prime numbers. Thus, a, b, and c are pairwise relatively prime when

$$(a, b) = (a, c) = (b, c) = 1.$$

Note that (a, b, c) can be 1 without a, b, and c being pairwise relatively prime. For instance, $(4, 3, 9) = 1$, but $(3, 9) = 3$.

The unique factorization theorem, a.k.a., the fundamental theorem of arithmetic. Last time we proved that every number could be written as a product of primes, that is, it could be factored as a product of primes. But we know more, and that is that there is only one way that it can be factored as a product of primes. That's something we'll prove soon, and it's called the unique factorization theorem, or, by some people, the fundamental theorem of arithmetic. It's not difficult to prove, but the job is simpler if we first prove a couple more proprieties of divisibility.