MATH 22

Lecture Q: 10/28/2003

DIVISIBILITY

Marriage and death and division
Make barren our lives.
—Swinburne, ‘Dolores’

Administrivia

- http://denenberg.com/LectureQ.pdf

- Any blowback from the exam?

Divisibility

Suppose x and y are integers with $x \neq 0$. We say that *x divides y*, or *y is divisible by x*, and write $x \mid y$, if there exists an integer z such that $xz = y$.

(We also say *x is a divisor of y* and *y is a multiple of x*.)

Examples:

$3 \mid 12$ $9 \mid 0$ $-1 \mid 39$ $-3 \mid -12$ $15 \mid 60$ $6 \mid 6$

It's obvious that $1 \mid x$ for any integer x, and if $x \neq 0$, then $x \mid 0$ and $x \mid x$. This last means that $\mid$ is a *reflexive* binary relation **on the nonzero integers**.

Note that sign never makes a difference: if $x \mid y$, then $x \mid -y$ and $-x \mid y$ and $-x \mid -y$. (Prove this formally as an exercise.)

The definition is phrased purely in terms of integers; there's nothing like "x divides y if y/x has no fractional part" or anything else that requires real numbers.

More Properties of $\mid$

[All variables range over the integers. Anything on the left of a $\mid$ is assumed nonzero.]

If $x \mid y$ and $y \mid x$, then either $x = y$ or $x = -y$.

If $x \mid y$ and $y \mid z$, then $x \mid z$. That is, $\mid$ is a *transitive* binary relation.

If $x \mid y$, then $x \mid yz$.

If $x = y + z$, and w divides two of x, y, and z, then it divides the third.

If $x \mid y_1$, $x \mid y_2$, . . ., $x \mid y_n$, then x divides any *linear combination* of the y_i, that is,

$$x \mid (z_1y_1 + z_2y_2 + . . . + z_ny_n)$$

As a special case, if $x \mid y$ and $x \mid z$, then $x \mid (ay + bz)$.

In the text and on the blackboard, we can put a slash through $\mid$ to denote "does NOT divide".

Primes

Suppose p is an integer greater than 1. It's always the case that $p \mid p$ and $1 \mid p$. If there are no other positive integers that divide p, then p is called *prime*.

An integer $n > 1$ that isn't prime is called *composite*.

Lemma: Every composite number has a prime divisor.

Proof: Suppose to the contrary that there exist composite numbers with no prime divisors. Let n be the smallest such number. Since n is composite, it has a divisor m which is greater than 1.
Now m must itself be composite since n has no prime divisors by assumption. But also m is smaller than n. So m has a prime divisor (since n is the smallest composite with no prime divisors). But any divisor of m must divide n as well, a contradiction.

Comment: We used this Lemma without proof back in Lecture A.

How Many Primes?

As we proved in Lecture A, there are infinitely many primes. There are nearly as many proofs of this fact! [Quick review of Euclid’s proof.]

Of interest: Let N_n be the product of the first n primes. It is unknown whether or not there are infinitely many n such that $N_n +1$ is prime. It is unknown whether or not there are infinitely many n such that $N_n +1$ is composite.

Another proof (Kummer): Suppose there are finitely many primes and let N be their product. Then $N–1$ (a product of primes) and N have a common divisor p. But then p also divides $N – (N–1) = 1$, an absurdity.

A strengthening of the Lemma: If n is any composite, then there is a prime $p \leq \quad n$ that divides n.

Proof: By the Lemma, there must be a prime q that divides n. If $q \leq \quad n$ then we’re done. Otherwise, we have $n = qx$ (since $q \mid n$) with $q > \quad n$. But if the product of two numbers is n, they can’t both be greater than $\quad n$. So $x \leq \quad n$. Now $x > 1$ since $q < n$, so x is either prime, in case we’re done, or composite, in which case it has a smaller prime divisor which also divides n. QED

The Division Theorem

If x and y are integers with $y > 0$, then there exist unique integers q and r such that $x = qy + r$ with $0 \leq r < y$.

We call q the *quotient* and r the *remainder*.

Examples:

If $x = 38$ and $y = 7$, then $q = 5$ and $r = 3$

If $x = 33$ and $y = 11$, then $q = 3$ and $r = 0$

If $x = 12$ and $y = 20$, then $q = 0$ and $r = 12$

If $x = 14$ and $y = 1$, then $q = 14$ and $r = 0$

If $x = -20$ and $y = 5$, then $q = -4$ and $r = 0$

If $x = -9$ and $y = 4$, then $q = -3$ and $r = 3$ [!!]

If $x = -9$ and $y = -4$, then the Theorem doesn't apply

The Theorem guarantees that q and r exist, but doesn't tell how to find them. We can find them by repeatedly subtracting y from x (if $x \geq 0$) or adding y to x (if $x < 0$) until the result is between 0 and y; the number of times we subtracted or added is q.

Proof of the Division Thm

Part I: Existence. (Sketch)

If $y \mid x$, then $x = zy$ and we just take $q = z$ and $r = 0$. Otherwise, let S be the set of all values of $x - zy$ for all integer z such that $x - zy$ is positive. [Prove that S is nonempty.] So S has a least element, call it r, which equals $x - qy$ for some q. We know that $r > 0$ so all we need prove is that $r < y$.

If $r = y$ then $x - qy = y$ so $x = (q+1)y$, which means $y \mid x$, a contradiction. But if $r > y$ then $r = y + c$ for some positive $c < r$, and $x - qy = y + c$ implies $x - (q+1)y = c$, contradicting the fact that r is the smallest such number.

Part II: Uniqueness.

Suppose that $x = q_1y + r_1 = q_2y + r_2$, with $0 \leq r_1, r_2 < y$. Then $y(q_1 - q_2) = r_1 - r_2$. If $q_1 \neq q_2$ then the absolute value of the LHS is at least y, which means r_1 and r_2 must differ by at least y, which is impossible. So $q_1 = q_2$ and the RHS is zero, so $r_1 = r_2$.

[This is the standard pattern for an existence-and-uniqueness proof: Prove existence, then assume the existence of more than one and prove a contradiction.]

Change of Radix

We can write numbers using radix (base) other than 10.

Example: 18 can be written 10010 (base 2), since

$$1(2^4) + 0(2^3) + 0(2^2) + 1(2^1) + 0(2^0) \quad = \quad 18$$

Example: 55 can be written 106 (base 7), since

$$1(7^2) + 0(7^1) + 6(7^0) \; = \; 70$$

Example: 7530 can be written 1D6A (base 16), since

$$1(16^3) + 13(16^2) + 6(16^1) + 10(16^0) \quad = \quad 7530$$

Note that in base 16 we must use A,B,C,D,E,F as "digits" representing 10,11,12,13,14,15.

Example: 25 can be written 31(base 8), since 3(8)+1=25. The fact that 25(dec) = 31(oct) can be used to prove the equivalence of Christmas and Halloween.

In all cases (including b = 10)

$$\mathrm{d}_n\, \mathrm{d}_{n-1} \ldots \mathrm{d}_0 \text{ (base } b) \; = \; \mathrm{d}_n b^n + \mathrm{d}_{n-1}\mathrm{b}^{n-1} + \ldots + \mathrm{d}_0 b_0$$

where the "digits" in base b are 0, 1, 2, . . ., b–1.

Base Conversion

What does this have to do with the Division Theorem? Here's how to convert a positive number x to base b:

Apply the Theorem to x and b, getting $x = q_0 b + r_0$.
Apply it to the quotient q_0 and b, getting $q_0 = q_1 b + r_1$.
Apply it yet again to q_1 and b, getting $q_1 = q_2 b + r_2$.
Continue in this way until some quotient q_n is 0.

Then x in base b is $r_n r_{n-1} r_{n-2} \ldots r_0$, that is, take the remainders $r_0, r_1, \ldots$ in reverse order.

[Blackboard demo using the previous slide's examples]

Why does this work? First, $q_0 b$ in base b is just q_0 in base b followed by 0, since that's how you multiply by b in base b. Furthermore, r_0 is a single digit in base b since it's less than b but at least 0. So $x = q_0 b + r_0$ in base b is just q_0 in base b with r_0 appended. To find q_0 in base b we just repeat the process.

Comment: This works only for *positive* x and b. To convert a negative number, convert its absolute value and tack on a minus sign. The case of negative b (e.g. 7 (base –2) = 11011) isn't handled in this way. There are also shortcuts in particular cases, e.g. 2 <-> 16.

GCD

Suppose y and z are integers, and that x is a *positive* integer such that $x \mid y$ and $x \mid z$. Then x is said to be a *common divisor* of y and z.

Examples: The common divisors of 60 and 108 are 1, 2, 3, 4, 6, and 12. The common divisors of -4 and 18 are 1 and 2. The only common divisor of 8 and 9 is 1. The common divisors of 15 and 60 are 1, 3, 5, and 15.

Now suppose that x is a common divisor of y and z, which are *not both zero*. If in addition every other common divisor of y and z divides x, then x is a *greatest common divisor* (GCD) of y and z.

Examples: 12 is a GCD of 60 and 108 since 1, 2, 3, 4, and 6 all divide 12. 15 is a GCD of 15 and 60.

Note that, for Grimaldi, the term “greatest common divisor” does NOT mean “the numerically largest of all the common divisors”. It turns out that the two are the same, that is, there is only one Grimaldi-style GCD and it is in fact the largest common divisor. But we have to prove this. (If we defined GCD the sane way, we’d have to prove that every common divisor divides the GCD.)

Existence & Uniqueness

Any two integers x and y not both 0 have a unique GCD.

Part I: Existence (same Well-Ordering trick as before)

Let S be the set of all positive values $ax+by$ for all integers a and b. Clearly S is nonempty, so it has a smallest element c, which we will prove is a GCD of x and y. There are several things to prove:

c is a positive integer. Clear from the definition of c.

Any divisor of both x and y divides c. If $d \mid x$ then $d \mid ax$, and if $d \mid y$ then $d \mid by$, so if d divides both x and y then it divides $c = ax + by$.

c divides x. Suppose otherwise. Then by the Division Theorem $x = qc + r$ with $0 < r < c$. But then

$$r = x - qc = \ldots = (1 - qa)x + (-qb)y \quad \square \quad S$$

which, since $r < c$, contradicts the fact that c is the smallest element of S.

c divides y. Same proof, with x and y swapped!

Part II: Uniqueness

Suppose c_1 and c_2 are GCDs of x and y. Then $c_1 \mid c_2$ since c_2 is a GCD, and also $c_2 \mid c_1$ since c_1 is a GCD. This means that either $c_1 = c_2$ or $c_1 = -c_2$. But both c_1 and c_2 must be positive (by defn of GCD) so $c_1 = c_2$.

Properties of GCD

For integers *x, y* not both zero, we write gcd(*x*,*y*) for the (now known unique) GCD of *x* and *y*. Simple results:

gcd(*x*,*x*) = *x* and gcd(*x*,*y*) = gcd(*y*,*x*), so gcd is an *idempotent* and *symmetric* closed binary operation on ***Z*** (except for the peculiarity that gcd(0,0) is not defined).

If gcd(*x*,*y*) = 1, then *x* and *y* are called *relatively prime*. Intuition: A single prime *p* has no factors except itself and 1. Two relatively prime numbers have no *common* factors except 1. Examples: 32 and 9, 28 and 45.

For any nonzero *x* and integer *k*, gcd(*x*, *kx*) = *x*.
Examples: gcd(15,60) = 15 gcd(–29,290) = 29.

gcd(*x*,*y*) is the smallest positive integer that can be written as a *linear combination* of *x* and *y*. (This follows directly from the proof on the preceding slide.)

For any nonzero *x*, gcd(*x*,0) = *x*. For *x* and *y* not both zero, gcd(*x*,*y*) = gcd(–*x*,*y*) = gcd(*x*,–*y*) = gcd(–*x*,–*y*). (So henceforth we assume that *x* and *y* are both positive.)

The Euclidean Algorithm

Now, given x and y, how do we calculate gcd(x,y)?
Find all divisors of both and rummage through them?
There is a better way, due to Euclid.

Given positive integers x and y, to find gcd(x,y):

```
[1]  Start with  $a := x$  and  $b := y$
[2]  By the Division Thm, write  $a = qb+r$  with $0 \le r < b$
[3]  If  $r = 0$, stop, and return  $b$  as  gcd($x$,$y$)
[4]  Set  $a := b$  and  $b := r$  and go back to step 2
```

Example: Find gcd(306, 90)

```
[1]  a := 306,   b := 90
[2]  a = 3b + 36,   so  q = 3  and  r = 36
[4]  a := 90,   b := 36
[2]  a = 2b + 18,   so  q = 2  and  r = 18
[4]  a := 36,   b := 18
[2]  a = 2b + 0,  so  q = 2 and  r = 0
[3]  stop;   gcd(306,90) = 18
```

Next lecture we'll prove the correctness and (if we have time) the time complexity of Euclid's Algorithm.

Understanding the E.A.

What is going on in the Euclidean Algorithm?

We start with a and b.

First, we arrange that $a \geq b$. (Note that the first time through the loop simply exchanges a and b if $a < b$!)

If now $b \mid a$, then the answer is b. Otherwise we replace a and b (respectively) with b and the remainder when a is divided by b, and we start again. "The remainder when a is divided by b" is written $a \bmod b$. (Much more on the "mod" operator later.)

The algorithm's correctness rests on the following fact:

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

We could show this explicitly by changing step [4] to

[4] Calculate $\gcd(b,r)$ and return it as the answer

which yields an absolutely equivalent algorithm.

We can show that, in each iteration of the loop, the value of at least one of a or b must decrease by a factor of at least 1/3. This guarantees that the algorithm is $O(\lg x)$, just as binary search achieves logarithmic time by cutting the search space by a factor of 1/2 on each iteration.

Least Common Multiple

Suppose x and y are positive integers. A positive integer z is called a *common multiple* of x and y if z is a multiple of both x and y, that is, if $x \mid z$ and $y \mid z$.

Clearly any x and y have a common multiple, since xy is always a common multiple. The smallest common multiple of x and y is called their *least common multiple* (LCM) and is written lcm(x,y). Uniqueness is trivial.

Examples: $\mathrm{lcm}(12,20) = 60$ $\mathrm{lcm}(8,60) = 120$
$\mathrm{lcm}(8,9) = 72$ $\mathrm{lcm}(1,x) = x$ $\mathrm{lcm}(x,kx) = kx$

Theorem: lcm(x,y) divides any common multiple of x and y. (Nontrivial proof, in Grimaldi.)

Theorem: For any positive x and y,

$$xy = (\mathrm{gcd}(x,y))(\mathrm{lcm}(x,y))$$

Corollary: If x and y are relatively prime, $\mathrm{lcm}(x,y) = xy$.

Corollary: It's easy to calculate lcm(x,y). Calculate gcd(x,y) using Euclid's Algorithm, and divide it into xy.

More on lcm next time.