MATH 25 CLASS 3 NOTES, SEP 26 2011

Contents

Quick links to definitions/theorems

- Uniqueness, existence of Euclidean division
- Definition of common divisor, greatest common divisor
- The key lemma behind the Euclidean algorithm
- The Euclidean algorithm for computing gcd

1. Euclidean division

A concept related to the notion of divisibility is *Euclidean division*. How does this differ from ordinary division? Euclidean division is simply the name we give to the elementary school calculation of division with remainder. For example, suppose we want to divide 13 by 5. On the one hand, the answer is 13/5, but it is also 2 with a remainder of 3, because $13 = 2(5) + 3$. The following theorem tells us that this remainder is unique. Notice that although it might be intuitively obvious that the remainder is unique, the following proof establishes this fact rigorously.

Theorem 1 (Theorem 1.1 of text)**.** *Let a, b be integers, with $b > 0$. Then there exists a unique integer r such that $0 \leq r < b$, with*

$$a = qb + r$$

for some unique integer q. We call r the remainder *of a divided by b.*

Proof. Let's prove this theorem. First, let's show that we can find some q, r satisfying the above, and take care of the uniqueness later. Consider the set of integers $S = \{a - qb | q \in \mathbb{Z}, a - qb \geq 0\}$. This is the set of integers which differ from a by a multiple of b, and such that the difference $a - qb$ is non-negative. This set consists solely of non-negative integers, and is non-empty. To see why this is non-empty, all we need to do is choose q sufficiently negative to ensure that $a - qb > 0$. It is a fact (actually, an axiom, in the sense that we can't prove it from simpler statements) that any non-empty set of positive integers (or non-negative integers) has a least element. This is called the *well-ordering principle*. It seems obvious; however, note that this is false if we replace $\mathbb{N}$ with $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. In any case, we know that S has a least element by this principle. Call this least element r. Then obviously $r = a - qb$ for some integer q. How do we know that $0 \leq r < b$? First, we know that $0 \leq r$, by the fact that $r \in S$ and S consists only of positive integers. To show that $r < b$, we will use a proof by contradiction. If $r \geq b$, then $a - (q + 1)b = r - b \geq 0$. However, this

means that $(r-b) \in S$, and $r-b < r$, which contradicts the fact that r is the least element in S. Therefore, we must have $r < b$.

So we've shown the existence of integers q, r such that $a = qb + r$ and $0 \leq r < b$. Now let's show that they're unique. Suppose that there are two pairs q_1, r_1, q_2, r_2 satisfying the above. Then equating the two equations, we get

$$q_1 b + r_1 = a = q_2 b + r_2.$$

This is equivalent to

$$(r_1 - r_2) = b(q_2 - q_1).$$

However, notice that because $0 \leq r_1, r_2 < b$, we must have $-b < r_1 - r_2 < b$. On the other hand, the right hand side is a multiple of b; that is, $b|(r_1 - r_2)$. But the only way this is possible is if $r_1 - r_2 = 0$, or $r_1 = r_2$. This immediately tells us that $q_1 = q_2$ as well. So the pair (q, r) must be unique. □

There are a few key ideas to take away from this proof. First, the remainder r is characterized by being the smallest non-negative integer of the form $a - qb$, where q is some integer. Second, a common way to prove that a there is a unique object satisfying a certain set of properties is to show that if two objects satisfy that set of properties, those objects must be equal. On the other hand, you should remember that proving uniqueness is separate from proving existence: in the proof above, we prove existence of a remainder using totally separate methods from proving uniqueness.

Examples.

- We saw earlier that 13 divided by 5 with remainder gives $q = 2, r = 3$.
- Let $a = -7, b = 4$. Then -7 divided by 4 with remainder gives $q = -2, r = 1$, since $-7 = (-2) \cdot 4 + 1$. Notice that q is allowed to be negative, but the remainder never is.
- (Example 1.2 of the text) We can use division with remainder to determine all possible remainders of x^2 when divided by 4. Before working out this example, list the first few squares $(0, 1, 4, 9, \ldots)$, and find their remainders when you divide by 4. What do you notice? Let's prove this observation. For any x, we can find q, r such that $x = 4q + r$, with $0 \leq r < 4$. Then $x^2 = (4q + r)^2 = 16q^2 + 8rq + r^2$. When we divide this by 4, notice that because $4 \mid 16q^2$ and $4 \mid 8qr$, the remainder when we divide x^2 by 4 is the same as when we divide r^2 by 4. But since $r = 0, 1, 2, 3$, we need only check that $0, 1, 4, 9$ leave remainders of $0, 1, 0, 1$, respectively. So the only possible remainders for squares when divided by 4 are 0 and 1. We'll come back to many calculations like this later in the class.

2. Greatest common divisor

Suppose a, b are two integers. If another integer d satisfies $d|a, d|b$, we call d a *common divisor* of a, b. Notice that as long as at least one of a, b is nonzero, then there will be a largest positive common divisor. We call this number the *greatest common divisor* of a, b. We will write this number as $\gcd(a, b)$, or if we are really lazy, just (a, b). (Yes, this last notation is very ambiguous, since (a, b) is more familiar as the ordered pair (a, b), but the context should usually make what we mean clear.

To make things worse, (a, b) sometimes might even mean the open interval $a < x < b$. Having three totally unrelated uses of the same notation is not the best, but it usually should be clear what we mean!)

Examples.

- Suppose $a = 8, b = 12$. The (positive) divisors of a are $1, 2, 4, 8$, while the divisors of b are $1, 2, 3, 4, 6, 12$. Looking at this list, the greatest common divisor of $8, 12$ is evidently 4.
- Suppose $a = 72, b = 74$. The most naive way of computing the gcd is to enumerate all the divisors of 72 and 74, and then compare the list. But suppose we don't want to do that – after all, it looks like it'll take a lot of work to find all the divisors of 72 and 74! How might we save the amount of calculations we have to make? Suppose $d|a, b$, so that d is any common divisor of a, b. Then $d|(b - a)$. But in this case, $b - a = 2$, so $d|2$. Therefore, the only possible common divisors are $1, 2$. We easily can see that $2|72, 74$, so this means that $\gcd(72, 74) = 2$. The moral of this example is that there are more efficient ways of calculating gcds than simply jumping right in and enumerating divisors, which in general will take a very long time.
- Suppose $b|a$, and $b > 0$. What is $\gcd(a, b)$?
- We can also extend the definition of gcd to more than two integers. The greatest common divisor of a set of integers $a_1, \ldots, a_k$ is the largest positive integer d such that $d|a_1, \ldots, a_k$. For example, if $a = 4, b = 6, c = 8$, then $\gcd(4, 6, 8) = 2$. We can show this by either enumerating all the divisors of a, b, c, or by applying the following fact (exercise 1.9 of the text): If $a_1, \ldots, a_k$ are integers, then $\gcd(a_1, \ldots, a_k) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_k)$. In practice, what this means is that we can calculate the gcd of k integers by taking the gcd of $k - 1$ pairs of integers. For example, $\gcd(4, 6, 8) = \gcd(\gcd(4, 6), 8) = \gcd(2, 8) = 2$.
- Notice that $1|a$ for all integers a. So a greatest common divisor is always at least 1. In the case that $\gcd(a, b) = 1$, we say that a, b are *relatively prime* or *coprime*. A list of integers $a_1, \ldots, a_k$ is called *coprime* if $\gcd(a_1, \ldots, a_k) = 1$, and is called mutually coprime if $\gcd(a_i, a_j) = 1$ for all distinct pairs a_i, a_j.
- For instance, since $\gcd(8, 9) = 1$, $8, 9$ are coprime. To see that a list of integers being coprime is distinct from being mutually coprime, consider the list $8, 12, 7$. This list is coprime, since $\gcd(8, 12, 7) = 1$, but is not mutually coprime, because $\gcd(8, 12) = 4$. A list like $6, 11, 17$ is both coprime and mutually coprime.

3. The Euclidean algorithm for calculating gcds

What's the relationship between Euclidean division and gcds? It turns out that Euclidean division is the key tool for a very efficient method of calculating the gcd of two integers. We call this method the Euclidean algorithm, and it is based on the following simple lemma:

Lemma 1. *Let a, b be integers with $b > 0$. Let $a = bq + r$ be the result of Euclidean division, so that $0 \leq r < b$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Suppose $d \mid a, b$, so $\gcd(a, b)$ is the largest such d. Since $r = a - qb$, we must also have $d \mid r$. Therefore, $d \mid a, b \implies d \mid b, r$. This means that $\gcd(a, b) \leq \gcd(b, r)$. Conversely, if $d \mid b, r$, then $a = bq + r$ implies that $d \mid a$. So $d \mid b, r$ implies that $d \mid a, b$, so $\gcd(b, r) \leq \gcd(a, b)$. The only way both of these inequalities is true is if $\gcd(a, b) = \gcd(b, r)$. □

The proof of this lemma illustrates another useful proof technique. If you are asked to prove that two numbers are equal, it is sometimes easiest to do so by showing that each number is larger than the other.

Example. For instance, suppose $a = 124, b = 24$. Instead of listing all the divisors of 124 and 24, we use Euclidean division to find $124 = 5 \cdot 24 + 4$, so $q = 5, r = 4$. Therefore $\gcd(124, 24) = \gcd(24, 4) = 4$.

This lemma is really useful, because it allows us to replace the computation of $\gcd(a, b)$ by the computation of $\gcd(b, r)$ for the cost of one Euclidean division. The advantage to this replacement is that we can always select $a > b$ (we'll just assume $a > 0$; if $a < 0$, replace a with $|a|$), so that b, r are smaller numbers than a, b. If we are lucky, r will be really small and we will be able to compute b, r via inspection or brute force.

But even if we aren't lucky, so that b, r are still somewhat large, we can just repeat this process! That is, we can divide b by r with remainder, to get something like $b = q_2 r + r_2$, where $0 \leq r_2 < r$, and then $\gcd(b, r) = \gcd(r, r_2)$. So we can continually replace the calculation of a gcd of a pair of integers with the calculation of the gcd of a pair of smaller integers at the cost of one Euclidean division. This process, where we repeatedly calculate Euclidean divisions to help us calculate a gcd, is called the *Euclidean algorithm*. Let's look at an example.

Example. Compute the gcd of $a = 994$ and $b = 399$ using the Euclidean algorithm.

We begin by doing a Euclidean division on 994 by 399:

$$994 = 399 \cdot 2 + 196.$$

So $q = 2, r = 196$. Since we'll be repeating Euclidean division, let's write $q = q_1 = 2, r_1 = 196$. So we have

$$994 = a = q_1 b + r_1 = 2 \cdot 399 + 196.$$

Remember, right now we know that $\gcd(994, 399) = \gcd(399, 196)$. However, it's not immediately obvious what $\gcd(399, 196)$ is, so let's do a Euclidean division with that pair of numbers:

$$399 = 196 \cdot 2 + 7.$$

We can rewrite this as

$$399 = b = q_2 r_1 + r_2,$$

where $q_2 = 2, r_2 = 7$. So this tells us that $\gcd(399, 196) = \gcd(196, 7)$. It might not be immediately obvious what $\gcd(196, 7)$ is, but a Euclidean division tells us that

$$196 = 7 \cdot 28 + 0,$$

so $7|196$. We can write $q_3 = 28, r_3 = 0$. Therefore, $\gcd(196, 7) = 7$, so $\gcd(994, 399) = 7$.

Altogether, it took us 3 Euclidean divisions to reach our final answer. A Euclidean division requires a fair amount of work, but not much more work than simply testing whether a number divides another number. In particular, notice that this method of calculating gcds is probably faster than trying to list all the factors of the initial two numbers 994 and 399. And if a, b are really large (like tens or hundreds of digits long), then a computer can still calculate gcds really quickly, but will take a long time (unless you are extremely lucky) to calculate all the factors of a, b.

We can formalize the Euclidean algorithm as follows. Given an initial pair of integers a, b, with $a, b > 0$, we compute their gcd using the following procedure.

(1) If $a < b$, swap a, b so that $a \geq b$.
(2) Compute q, r such that $a = bq + r$, where $0 \leq r < b$.
(3) If $r = 0$, then $b \mid a$, and $\gcd(a, b) = b$. Otherwise, replace a, b with b, r, return to step 2, and repeat. Notice that $\gcd(a, b) = \gcd(b, r)$ by Lemma 1.

This verbal description of the Euclidean algorithm looks like it could be converted to an actual computer program with little effort, and in the next programming assignment you will do just that. There are two important facts about this algorithm that we would want to verify if we wanted to be rigorous with our analysis: first, the algorithm should be correct, in that if it returns a result the result should always be the gcd of a, b, and second, the algorithm will terminate in a finite number of steps. We leave both of these verifications as exercises; for the second, a useful observation is that a strictly decreasing sequence of non-negative integers must be of finite length.