BEZOUT'S IDENTITY, EUCLIDEAN ALGORITHM

NOTES FOR MATH 422, CSUSM. SPRING 2009. PROF. AITKEN

This document assumes the reader is familiar with the basic properties of divisibility. It also assumes a few basic facts about primes.

1. Bezout's Identity

Let a and b be integers not both zero. There are eight important facts related to "Bezout's Identity":

1. There is a greatest common divisor of a and b called $\mathrm{GCD}(a, b)$.
2. There is a least positive linear combination of a and b.
3. (Bezout's Identity) These two numbers are the same: call it g.
4. All common divisors of a and b are divisors of g.
5. Conversely, all divisors of g are common divisors of a and b.
6. All linear combinations of a and b are multiples of g.
7. Conversely, all multiples of g are linear combinations of a and b.
8. If d is a common divisor, and e is a linear combination, then $d \mid e$.

In this section, we prove these results (but not in this order). Warning: the number g is of the form $ua + vb$, but u and v are not unique.

Definition 1. A *common divisor* of integers a and b is an integer that divides both a and b.

Definition 2. A *linear combination* of integers a and b is any integer of the form $ua + bv$ where $u, v \in \mathbb{Z}$.

Warning. The term *linear combination* is used in a different sense than in linear algebra. In linear algebra, u and v are not restricted to integers. If we want to be more precise, we can say *integral linear combination.*

Proposition 3. *Let a and b be integers, and let d be a common divisor of a and b. Then $d \mid ua + vb$ for all $u, v \in \mathbb{Z}$. In other words, if e is a linear combination of a and b, then $d \mid e$.*

Proof. By hypothesis, $a = kd$ and $b = ld$ for some $k, l \in \mathbb{Z}$. Thus $ua + vb = (uk + vl)d$. So $ua + vb$ is a multiple of d. □

Exercise 1. Show that every common divisor of a and b also divides $a + b$ and $a - b$.

Proposition 4. *Suppose $a, b \in \mathbb{Z}$ are not both not zero. Then there is a greatest common divisor of a and b. It is called the GCD or greatest common divisor of a and b, and is written* $\mathrm{GCD}(a, b)$. *Furthermore,* $\mathrm{GCD}(a, b) \geq 1$.

Proof. For convenience, suppose $a \neq 0$. Let S be the set of common divisors. The set S is (i) non-empty since $1 \in S$, and (ii) is bounded by $|a|$ by a property of divisibility. Thus there is a maximum d in S. Since $1 \in S$ and d is the maximum, $d \geq 1$. □

Date: Spring 2008, Spring 2009. Version of March 2, 2009.

Warning. If a and b are both zero, then all integers are common divisors of a and b, so there is no greatest.

Exercise 2. Suppose $a > 0$. Show $\mathrm{GCD}(a, 0) = a$.

Proposition 5. *Suppose $a, b \in \mathbb{Z}$ are not both zero. Then there is a least positive linear combination of a and b.*

Proof. For convenience, suppose $a \neq 0$. Let S be the set of positive linear combinations. Clearly $|a| \in S$, so S is non-empty. By the well-ordered principle, the set S has a minimum. □

Warning. If a and b are both zero, then the only linear combination is 0. Thus there is no minimum *positive* linear combination.

Lemma 6. *If a and b are not both zero, then the least positive linear combination is a common divisor of a and b.*

Proof. Let $m = ua + vb$ be the least positive linear combination. Using the quotient-remainder theorem we can write $a = qm + r$ where $0 \leq r < m$. Observe that

$$r = a - qm = a - q(ua + vb) = (1 - qu)a + (-qv)b.$$

Thus r is a non-negative linear combination as well. But m is the smallest positive linear combination. Thus r cannot be positive. Hence, $r = 0$. Therefore, $m \mid a$.

The proof that $m \mid b$ is similar. □

We are now ready for the main theorem of the section.

Theorem 7 (Bezout's Identity)**.** *If a and b are not both zero, then the least positive linear combination of a and b is equal to their greatest common divisor.*

Proof. Let m be the least positive linear combination, and let g be the GCD. Then $g \mid m$ by Proposition 3. In particular, $g \leq m$. By Lemma 6, m is a common divisor, so $g < m$ cannot hold. Thus $g = m$. □

Corollary 8. *If a and b are not both zero, then every common divisor of a and b divides $GCD(a, b)$.*

Proof. Let d be a common divisor. By the above theorem, $\mathrm{GCD}(a, b)$ is a linear combination of a and b, so $d \mid \mathrm{GCD}(a, b)$ by Proposition 3. □

Exercise 3. Show the converse: if d is a divisor of $\mathrm{GCD}(a, b)$, then it is a common divisor of a and b.

Proposition 9. *If a and b are not both zero, then every multiple of $GCD(a, b)$ is a linear combination of a and b.*

Proof. Let $g = \mathrm{GCD}(a, b)$. By Theorem 7, we can find $u, v \in \mathbb{Z}$ such that $g = ua + vb$. Let kg be a multiple of g. Then $kg = (ku)a + (kv)b$. □

Exercise 4. Show the converse: every linear combination of a and b is a multiple of their GCD.

Definition 10. Two integers a and b are said to be *relatively prime* if they are not both zero and they have GCD equal to 1.

Exercise 5. Let $a, b \in \mathbb{Z}$ be fixed integers. Show that the equation $ax + by = 1$ has a solution with $x, y \in \mathbb{Z}$ if and only if a and b are relatively prime.

Here is a nice application of the above.

Theorem 11. *Suppose that $a, b, c \in \mathbb{Z}$ are such that $c \mid ab$. If a and c are relatively prime, then $c \mid b$.*

Proof. Since a and c are relatively prime there are $u, v \in \mathbb{Z}$ such that $ua + vc = 1$. Thus $uab + vcb = b$. Since c divides the left-hand side, it must divide the right-hand side. □

Exercise 6. Show that if d is odd and d divides $2k$ then d divides k.

Exercise 7. Show that every odd common divisor of $a + b$ and $a - b$ also divides a and b.

2. Euclidean Algorithm

We will now discuss a method of computing GCDs. This method can be found in Euclid's *Elements*. It is one of the most efficient method of finding GCDs for large integers. This method also allows us to find u and v such that $ua + vb$ is the GCD of a and b.

Here is one step of the algorithm.

INPUT: Two integers (a, b) where $a \geq b > 0$.

OUTPUT: The pair (b, r) where r is the remainder when we write $a = bq + r$ with $0 \leq r < b$.

In the Euclidean algorithm, one simply repeats the above step. The output of the previous step becomes the input of the next step. This continues until a pair $(n, 0)$ is produced. Then n will be the GCD of a and b. We now give a series of lemmas showing that this procedure works.

Lemma 12. *The input pair and the output pair of a step of the Euclidean algorithm have the same GCD.*

Proof. Let S_1 be the set of common divisors of the input (a, b), and let S_2 be the set of common divisors of the output (b, r). Recall that $a = bq + r$, so $r = a - bq$.

Let $d \in S_1$. Then $d \mid a$ and $d \mid b$. Also $d \mid r$ since $r = 1 \cdot a + (-q)b$ is a linear combination. Thus $d \mid r$ and $d \mid b$. So $d \in S_2$.

Let $d \in S_2$. Then $d \mid r$ and $d \mid b$. But $a = qb + 1 \cdot r$ is a linear combination. Thus $d \mid a$ as well. Thus $d \in S_1$.

We now see that $S_1 = S_2$. The maximums of these sets must be the same, so the GCDs agree. □

Proposition 13. *The initial input (a, b) and the final output $(n, 0)$ have the same GCD. Thus the GCD of a and b is n.*

Proof. By the previous lemma, the GCD does not change as we replace each input by the corresponding output. Thus the GCD will remain constant throughout the process. The final output will have the same GCD as the initial input. By an earlier exercise, $(n, 0)$ has GCD equal to n. □

Proposition 14. *The Euclidean algorithm is guaranteed to terminate. In other words, a pair of the form $(n, 0)$ will eventually be produced.*

Proof. Fix a and b. Let S be the set of all second coordinates that appear as outputs as we perform the Euclidean algorithm starting with (a, b). For instance $r \in S$, where r is the remainder of dividing a by b. By the well-ordering principle the set S has a minimum m. Since $m \in S$, there is an n such that (n, m) occurs as the output of some step. If $m \neq 0$ then we must perform a step where (n, m) is the input. The new output will be (m, r) where r the remainder. Since $r < m$ and $r \in S$, we get a contradiction. We conclude that $m = 0$. So $(n, 0)$ is the output. □

Now we know that the Euclidean algorithm can be used to compute the GCD of the initial pair. By keeping track of the quotients at each step there is a method of writing the GCD as a linear combination of the initial pair. This follows from the following analysis:

Let (a, b) be a pair of integers that occurs as the input of a step in the Euclidean algorithm. Suppose the output is (b, r). Finally, suppose that we have a linear combination

$$k = ub + vr.$$

Then k is also a linear combination of (a, b). In fact,

$$k = ub + vr = ub + (a - bq)r = va + (u - qr)b.$$

Recall that eventually we get an output $(n, 0)$ where n is the GCD. Then $n = u \cdot n + v \cdot 0$ where $u = 1$ and $v = 0$ (but you can use any other value of v if you wish). The above formula shows a way to form n as a linear combination of the prior pair. By tracing back through all the steps, we reach a linear combination of the initial input that equals n.

Exercise 8. The above discussion is very general and a bit abstract. Illustrate the above discussion with a few examples.

Remark. You can apply the Euclidean algorithm to positive real numbers as well, but it is not guaranteed to stop. In fact, if the initial pair is $(a, 1)$ then it stops if and only if a is rational (and the result will be $1/d$ where d is the denominator of a). In general, it stops if and only if (a, b) are commensurable. On the other hand, comparing the diagonal a of a square (or pentagon) to the side b, there is a geometric argument that the algorithm keeps going forever. This is likely a way in which the Greeks discovered incommensurables.

The Euclidean algorithm for real numbers is related to the theory of continued fractions, which is a rich and fascinating area of number theory.

3. Prime Divisors

Theorem 15. *If $n > 1$ is composite, then n has a prime divisor p such that $p^2 \leq n$.*

Remark. Another way to say this is that a composite integer $n > 1$ has a prime divisor p with $p \leq \sqrt{n}$. So if an integers $n > 1$ is not divisible by any prime $p \leq \sqrt{n}$, we can conclude that n must be a prime. This idea can be used with the Sieve of Eratosthenes to come up with a list of primes less than N as long as N is not too big. (See class notes).

Proof. If n is composite, then $n = ab$ where $a > 1$ and $b > 1$. For convenience, suppose $a \leq b$. Let p be a prime divisor of a. Thus $p \leq a \leq b$. So

$$p^2 \leq a^2 \leq ab = n.$$

Since $p \mid a$ and $a \mid n$ we have $p \mid n$. □