Math 2710

Sep 16-20

Characterization of the gcd

Proposition: (2.29, page 34) Suppose $b \neq 0$. An integer d is the greatest common divisor of a and b if and only if

- $d \geq 0$
- d is a common divisor of a and b
- If r is a common divisor of a and b, then $r|d$.

Proof: First suppose that these three conditions are true. Then d is a common divisor, and by Proposition 2.1 (iv), if r is any other common divisor of a and b, then $r|d$ so $|r| \leq d$. So d is the greatest common divisor.

Now suppose d is the greatest common divisor of a and b. Then $d \geq 0$ and d is a common divisor, so we just need to check the third condition. By the extended euclidean algorithm there are x and y so that $ax + by = d$. By Proposition 2.1 (ii), any common divisor of a and b divides $ax + by = d$, as we wanted to show.

Least common multiple

Definition: A common multiple of two integers a and b, with $b \neq 0$, is any integer m such that $a|m$ and $b|m$. The **least common multiple** of a and b is the smallest positive integer which is a common multiple of a and b.

Theorem: The lcm of a and b is |ab/g| where g is the gcd of a and b.

Proof: We can assume a and b are non-negative as this does not affect the lcm. Because g divides both a and b, we have $ab/g = a(b/g) = b(a/g)$ so ab/g is an integer and it is a common multiple of a and b. Now let t be any common multiple of a and b. Find x and y so that $ax + by = g$. Then $tax + tby = tg$. Since t is a common multiple of a and b, we have tax and tby are both multiples of ab. So $tax + tby = abs$ for some integer s. We conclude that $t = (ab/g)s$, so that t is a multiple of ab/g. This means $t \geq (ab/g)$ so ab/g must be the least common multiple.

Linear Diophantine Equations

A *diophantine equation* is an equation where the variables are restricted to integer values.

A linear diophantine equation in one variable is of the form

$$ax = b$$

where a and b are integers and we want x to be an integer. Clearly this has a solution exactly when $a|b$.

Linear Diophantine Equations in 2 variables

A linear diophantine equation in two variables is an equation of the form

$$ax + by = c$$

where a, b, and c are integers.
Solving such an equation means finding *integers* x and y that satisfy the condition.

Theorem on Linear Diophantine Equations

Theorem:

- The linear diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)|c$.
- If x_0, y_0 is one solution to the equation, and x and y is any other solution, then there exists an integer n so that

$$x = x_0 + n\frac{b}{d} \text{ and } y = y_0 - n\frac{a}{d}$$

Proof of Main Theorem on Linear Diophantine Equations

1. If $ax + by = c$ has a solution, then $\gcd(a, b)$ must divide c. (This is Proposition 2.1 (ii))$.
2. If $\gcd(a, b)$ divides c, then there are x and y such that $ax + by = c$. To find such x and y, write $c = \gcd(a, b)n$. Use Euclid's algorithm to find x and y with $ax + by = \gcd(a, b)$. Then $anx + bny = n\gcd(a, b) = c$. So nx and ny are a solution to the original equation.

Proof continued

3. If (x, y) and (x', y') are two solutions to $ax + by = c$, then

$$a(x - x') + b(y - y') = 0 \text{ so } a(x - x') = b(y' - y).$$

Divide both sides of this equation by $d = \gcd(a, b)$ to get

$$\frac{a}{d}(x - x') = \frac{b}{d}(y - y') \tag{1}$$

Remember that $\gcd(a/d, b/d) = 1$. (This is Proposition 2.27 (ii)) At the same time, a/d divides the left side of this equality, so it must divide the right side. By Proposition 2.28, this means that a/d divides $y - y'$ so $y - y' = (a/d)m$ for some integer m. Also, b/d divides $x - x'$ so $x - x' = (b/d)m'$. Therefore

$$\frac{a}{d}\frac{b}{d}m' = \frac{a}{d}\frac{b}{d}m$$

so $m = m'$. In other words, $x' = x - \frac{b}{d}m$ and $y' = y + \frac{a}{d}m$ for some $m \in \mathbb{Z}$.

4. So far we know that any two solutions are related like (x, y) and (x', y') for SOME m. But in fact any m works because

$$a(x - \frac{b}{d}m) + b(y + \frac{a}{d}m) = ax + by - \frac{ab}{d}m + \frac{ab}{d}m = ax + by = c.$$

This concludes the proof of the main theorem.