Math 406 Section 3.3: The Greatest Common Divisor

1. **Introduction:** We defined the gcd earlier. Now we will look at some properties. Some of these are fairly intuitive and some are not, but all are useful.

2. **Theorem:** If $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

   Note: This makes intutive sense. When we divide out the common stuff there's nothing common left.

   Proof: Suppose $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$. Suppose $\alpha \mid (a/d)$ and $\alpha \mid (b/d)$. Then $\alpha x = a/d$ and $\alpha y = b/d$ for $x, y \in \mathbb{Z}$. Then $a = \alpha x d$ and $b = \alpha y d$ and so αd divides both a and b and so $\alpha d \leq d$. Thus $\alpha = 1$. $\mathcal{QED}$

   Corollary: If a and $b \neq 0$ are integers then $\exists p, q \in \mathbb{Z}$ with $a/b = p/q$ and $\gcd(p, q) = 1$.

   Note: All this is saying is that we can reduce a fraction until there are no common terms remaining.

   Proof: Set $p = a/\gcd(a, b)$ and $q = b/\gcd(a, b)$. $\mathcal{QED}$

3. **Theorem:** For integers a, b, c we have $\gcd(a, b) = \gcd(a, b + ca)$.

   Note: This makes sense. Adding multiples of one integer to the other does't change any of the common divisors.

   Proof: If $\alpha \mid a$ and $\alpha \mid b$ then $\alpha \mid (b + ca)$. Thus any divisor of both a, b is a divisor of both $a, b + ca$.

   Suppose $\alpha \mid a$ and $\alpha \mid (b + ca)$ then $\alpha \mid ((b + ca) - ca)$ so $\alpha \mid b$. Thus any divisor of both $a, b + ca$ is a divisor of both a, b.

   Since both pairs have the same set of divisors they certainly have the same greatest common divisor. $\mathcal{QED}$

4. **Definition:** For integers a, b a *linear combination* of a and b is an expression of the form $\alpha a + \beta b$ for $\alpha, \beta \in \mathbb{Z}$.

5. **Theorem:** For integers a, b, not both 0, the smallest positive linear combination of a and b equals $\gcd(a, b)$.

   Note: The adjective are important here. What this is saying is that the *greatest* common divisor is the *smallest* positive linear combination. For example $\gcd(15, 35) = 5$ and $5 = 1(35) + (-2)15$ as a linear combination, moreover there's no way to get a smaller positive linear combination.

   Proof: Suppose d is the smallest positive linear combination of a and b. We claim it is the greatest common divisor. Write:

   $$d = \alpha a + \beta b$$

   By the division algorithm we have:

   $$a = qd + r \text{ with } 0 \leq r < d$$

   Then we have:

   $$r = a - qd = a - q(\alpha a + \beta b) = a - q\alpha a - q\beta b = (1 - q\alpha)a - (q\beta)b$$

   Therefore r is also a linear combination of a and b but $0 \leq r < d$ so $r = 0$ since d is smallest. Therefore $a = qd$ and so $d \mid a$.

   Similarly $d \mid b$.

   So now we know that d is a common divisor of both a and b but why is it the greatest common divisor? Suppose $c \mid a$ and $c \mid b$. Then $c \mid (\alpha a + \beta b)$ so $c \mid d$ so $c \leq d$. Thus d is in fact the greatest. $\mathcal{QED}$

Note: This theorem is insanely useful. The reason is that without it we know that the gcd exists but we have no real way of getting ahold of it to work with it. Now we do because we know it's a linear combination of the two integers.

Corollary: If a and b are relatively prime then $\exists \alpha, \beta \in \mathbb{Z}$ with $\alpha a + \beta b = 1$.

Proof: Obvious. $\mathcal{QED}$

6. **Theorem:** If $a, b \in \mathbb{Z}^+$ then the set of linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

   Proof: First we show that every linear combination of a and b is a multiple of $\gcd(a, b)$. Let $x = \alpha a + \beta b$. Since $\gcd(a, b)$ divides both a and b it divides x and so x is a multiple of $\gcd(a, b)$.

   Second we show that every multiple of $\gcd(a, b)$ is a linear combination of a and b. We know that $\gcd(a, b) = \alpha a + \beta b$ and so clearly every multiple looks like $m\gcd(a, b) = (\alpha m)a + (\beta m)b$ and is a linear combination.

   $\mathcal{QED}$

7. **Theorem:** If $a, b \in \mathbb{Z}$ not both 0 then some $d \in \mathbb{Z}^+$ is in fact $\gcd(a, b)$ if and only if both of the following hold:

   - $d \mid a$ and $d \mid b$
   - If $c \mid a$ and $c \mid b$ then $c \mid d$.

   Note: This basically says that not only is every other divisor less than $\gcd(a, b)$ but it divides $\gcd(a, b)$.

   Proof: Suppose $d = \gcd(a, b)$. We'll show it has these properties. Of course $d \mid a$ and $d \mid b$ since it's a common divisor. Suppose $c \mid a$ and $c \mid b$. Since $d = \alpha a + \beta b$ for $\alpha, \beta \in \mathbb{Z}$ we have $c \mid d$.

   Next we'll show that if some d has these properties it must be the gcd. Since $d \mid a$ and $d \mid b$ it's obviously a common divisor. Why is it greatest? If c is some other common divisor then since $c \mid a$ and $c \mid b$ we know $c \mid d$ and so $c \leq d$. $\mathcal{QED}$