Notes for 5 Feb (Tuesday)

1 The road so far...

1. Proved the division theorem and the fundamental theorem of arithmetic.
2. Defined gcd (by the way, the definition of gcd makes sense even for negative integers). Proved Euclid's algorithm and Bezout's identity.

2 Number theory - The basics

As a corollary, if a, b are coprime, then $ax + by = 1$ for some integers a, b.
Here are consequences of Bezout's identity (can also be proven easily using the fundamental theorem of arithmetic).

1. If e divides a, b then e divides $gcd(a, b)$. Indeed, $a = eu, b = ev$. Thus, $d = eux + evy = e(ux + vy)$.
2. If a divides bc and a, b are coprime, then a divides c. (This gives another proof of the fundamental theorem of arithmetic.) Indeed, $ax + by = 1$ and $bc = ak$. Thus, $c = bcy + acx = a(ky + cx)$.
3. For every a, b, m, $gcd(ab, m)$ divides $gcd(a, m)gcd(b, m)$. If a and b are coprime, then $gcd(a, m)gcd(b, m) = gcd(ab, m)$. (Once again this is clear from the fundamental theorem.) Indeed, $d_1 = ax_1 + my_1$, $d_2 = bx_2 + my_2$. Thus, $d_1 d_2 = abz_1 + mz_2$.
   Suppose a, b are coprime. Then so are $gcd(a, m)$ and $gcd(b, m)$. Note that $gcd(ab, m)$ is divisible by $gcd(a, m)$. Write $gcd(ab, m) = gcd(a, m)e$. Now $gcd(b, m)$ also divides $gcd(ab, m)$. Therefore, $gcd(b, m)$ divides e. This means that $gcd(ab, m) = gcd(a, m)gcd(b, m)f$. By the previous part, $f = 1$.

The point of Bezout's identity is to solve linear Diophantine equations (polynomial equations with integer coefficients solved for integers). By the way, one of Hilbert's famous problems was to decide when a given Diophantine equation has a solution. This problem is "undecidable", i.e., there is no algorithm that does the job.

Theorem 1. *Given integers a, b, e, there are integers m and n with $am + bn = e$ iff $gcd(a, b)$ divides e.*

Proof. Assume that a, b, e are non-negative integers. (The other cases will be dealt with in your HW.) If $gcd(a, b)$ divides e, then $e = kgcd(a, b) = k(ax + by)$ by Bezout and hence we are done.
Conversely, if $am + bn = e$, then any divisor of a, b divides e. Hence, so does their gcd. □

Once we find one solution to $am + bn = e$, all the other solutions are of the form $m + x, n + y$ where $ax + by = 0$. Now we have the following easy lemma.

Lemma 2.1. *Let $d = gcd(a, b)$. Then the general solution of $ax + by = 0$ is $x = \frac{bk}{d}$ and $y = -\frac{ak}{d}$ for any integer k.*

Proof. Note that $\frac{a}{d}x = -\frac{b}{d}y$. Since $\frac{a}{d}, \frac{b}{d}$ are coprime, y is divisible by $\frac{a}{d}$. Hence, $y = \frac{ak}{d}$ and likewise for x. □

Given two integers a, b we say that c is a common multiple if $c = ar$ and $c = bs$ for two integers r, s. The set of common multiples is non-empty (because ab is in it) and hence has a least element that we call $lcm(a, b)$. Here is an important lemma.

Lemma 2.2. *Assume that a, b are natural numbers with one of them > 0.*

1. *$lcm(a, b) = \frac{ab}{gcd(a,b)}$.*
2. *$lcm(a, b)$ divides every common multiple of a and b.*

Proof. In the unique prime factorisation of a, b let a_i, b_i be the exponent of the ith prime p_i. Then $l = \Pi_i p^{max(a_i,b_i)}$ is a common multiple. If $c = ar, c = bs$ is any common multiple, then by the same easy proposition that a divides b iff $a_i \leq b_i \ \forall\ i$, we see that $c_i \geq a_i, b_i$ and hence $c_i \geq max(a_i, b_i)$. Therefore $l = lcm(a, b)$ and the second part of the lemma is proved.
Since we know that $gcd(a, b) = \Pi_i p_i^{min(a_i,b_i)}$, and $max(a_i, b_i) + min(a_i, b_i) = a_i + b_i \ \forall\ i$ we are done with the first part. □

Obviously it is far more effiicient to calculate the lcm using the above formula than the prime factorisation.

Here is an important theorem (seemingly obvious) about primes.

Theorem 2. *(Euclid) There are infinitely many primes.*

Proof. Suppose there are only n primes $p_1, \ldots, p_n$. Consider $p_1 p_2 \ldots p_n + 1$. This number is not divisible by any of the p_i. This observation is a contradiction to the fundamental theorem of arithmetic. □

We shall not prove the following theorem but it is obviously quite important.

Theorem 3. *(The Prime Number Theorem) Let $\pi(x)$ be the number of primes $\leq x$. Then $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$.*

It follows as a corollary that for large n, there is a prime number between n and $2n$. This is called Bertrand's postulate. More interestingly, one wants to know what the error in $\pi(x) \sim \frac{x}{\ln(x)}$ is. It turns out that getting a precise form for the error is equivalent to the Riemann hypothesis !