Notes for 6 Feb (Wednesday)

1 The road so far...

1. Proved some corollaries of Bezout's identity (like the relationship between $gcd(ab, m)$ and $gcd(a, m)gcd(b, m)$.
2. Solved linear Diophantine equations.
3. Defined lcm and found a formula for it.
4. Proved that the number of primes is infinite.

2 Modular arithmetic

How does one create a nice password ? (Hint: Take your current password and tweak it by "adding 1 to every letter".) These considerations lead us (among other things) to modular arithmetic. Basically, we want to do "clock arithmetic", i.e., $3:00 + 11$ hours is $2:00$.

Def : Two integers a, b are said to be congruent modulo a positive natural number $m \geq 2$ iff $a = b + xm$ for some integer x. They are written as $a \equiv b \mod m$. Here is an important property.

Lemma 2.1. *Let $m \geq 2$ be a natural number. Then every n is uniquely congruent modulo m to some number r in $S = \{0, 1, 2 \ldots, m-1\}$.*

Proof. By the division theorem, $n = mq + r$ for a unique r. Therefore, $n \equiv r \mod m$. If $n \equiv t \mod m$ for a $t \in S$, then $n = mq_1 + t$ and hence by uniqueness of the remainder, $t = r$. □

Generalising the above lemma to integers, such an r is called a least non-negative resiude modulo n. Likewise, it is easy to prove that

Lemma 2.2. *Two numbers are congruent modulo m iff their least non-negative residues are equal.*

The point of this relation of being congruent is that

Theorem 1. *Fix a natural $m \geq 2$. Then define a relation on $\mathbb{Z}$ as $a \sim b$ if $a \equiv b \mod m$. This relation is an equivalence relation.*

Proof. This theorem follows trivially from the equality of the least non-negative residues. □

Much more interestingly, this relation respects multiplication and addition.

Lemma 2.3. *Fix an integer $m \geq 2$. For all integers, a, b, c, a', b', c', k such that $a \equiv a'$ mod m and $b \equiv b'$ mod$m$. Then,*

1. $ka \equiv ka'$
2. $a + b \equiv a' + b'$
3. $ab \equiv a'b'$.

Proof. We prove only the third part because the rest are similar. Note that $a = a' + q_1 m$ and $b = b' + q_2 m$. Hence $ab = a'b' + m(q_1 q_2 m + a' + b')$. □

Unfortunately, the cancellation law does not work. For instance, $0 = 2.3 \ mod \ 6 = 2 \ mod \ 6 \ . \ 3 \ mod \ 6$. We shall return to this issue later on. Here is a useful and easy proposition.

Lemma 2.4. *Suppose $a \equiv b$ mod m.*

1. *If d divides m, then $a \equiv b$ mod d.*
2. *For all naturals e, $a^e \equiv b^e$ mod m.*

The point of modular arithmetic is to make many divisibility calculations easy.

1. Suppose we want 6^{37} *mod* 13. Now $6^2 \equiv 36 \equiv -3$, $6^6 \equiv (6^2)^3 \equiv -27 \equiv -1$. Thus $6^36 \equiv (6^6)^6 \equiv 1$ and $6^{37} \equiv 6$.
2. A number a is divisible by
   (a) 3 iff the sum of digits is so : $a = \sum a_i 10^i$. Thus, $a \equiv \sum a_i \ mod \ 3$.
   (b) 9 iff the sum of digits is so : Similar to 3.
   (c) 11 iff the alternating sum of digits is so : $a \equiv \sum a_i (-1)^i$.

We have a useful proposition.

Proposition 2.1. *If $a \equiv b$ mod r and $a \equiv b$ mod s then $a \equiv b$ mod $lcm(r, s)$.*

Proof. $(a - b) = rc$ and $(a - b) = sd$. Thus $a - b$ is divisible by the lcm of r, s. □

Here is an example : Claim : $2^{340} \equiv 1 \ mod \ 341$. The point is that $341 = 11.31$. Also, $2^5 = 32 \equiv -1 \ mod \ 11$ and $1 \ mod \ 31$. So $(2^5)^{68} \equiv 1$ modulo $11, 31$. Thus by the proposition we are done.
Finally, we have the following useful proposition about cancellation.

Theorem 2. *If $ra \equiv rb$ mod m then $a \equiv b$ mod $\frac{m}{gcd(r,m)}$.*

Proof. Note that $r(a - b) = cm$ meaning $\frac{r}{gcd(m,r)}(a - b) = c\frac{m}{gcd(r,m)}$ and hence $a - b$ is divisible by $\frac{m}{gcd(r,m)}$ (because it is coprime to $\frac{r}{gcd(m,r)}$). □

As a special case,

Proposition 2.2. *If r, m are coprime, then $ra \equiv rb \ mod \ m$ implies that $a \equiv b \ mod \ m$.*

Now we are in a position to solve congruence equations. There are two kinds : Solve for an integer x given a, b, m such that

1. $x + a \equiv b \ mod \ m$. This equation is easy : $x \equiv (b - a) \ mod \ m$.

2. $ax \equiv b \ mod \ m$. This cannot always be solved. ($2x \equiv 3 \ mod \ 6$ cannot have a solution.)

   Proposition 2.3. *$ax \equiv b \ mod \ m$ is solvable iff $gcd(a.m)$ divides b.*

   Proof. Indeed, $ax = b + qm$ iff $gcd(a, m)$ divides b by solving the linear Diophantine equation. □

   Example : Solve $10x \equiv 14 \ mod \ 18$. This equation has a solution because $gcd(10, 18) = 2$ divides 14. Now, following the extended Euclidean algorithm we get $10.2 - 18 = 2$ and hence $10.14 - 18.7 = 14$. Thus $x = 14$. (Actually, $x = 5$ also works.)

A special case is as follows.

Proposition 2.4. *If $gcd(a, m) = 1$, then $ax \equiv 1 \ mod \ m$ has a unique solution modulo m.*

Proof. It has a solution. If x, y are solutions, then $a(x-y) \equiv 0 \ mod \ m$. Since $gcd(a, m) = 1$, we can cancel a on both sides and get $x \equiv y \ mod \ m$. □

Also, if $gcd(a, m) = 1$, $ax \equiv b \ mod \ m$ has a unique solution modulo m for all b. Like in the case of Diophantine equations, the solutions of $ax \equiv 0$ are $x = \frac{km}{gcd(a,m)}$.

Next we take the fact that the equivalence relation $\equiv$ respects addition and multiplication more seriously. Essentially, we want to study arithmetic on the equivalence classes. Before we do so, here are two case studies :

1. Suppose we consider all even numbers to be a single entity and likewise odd. Then, we can define addition as $even + odd = odd + even = odd$, $even + even = even$, $odd + odd = even$. Moreover, multiplication is $even.odd = odd.even = even$, $even.even = even$, $odd.odd = odd$. It is easy to check that addition and multiplication behave well with each other (distributivity, associativity, etc).

2. Let's try to play the same game by considering "positive", "negative", and "zero" as single entities. The problem here is that *positive* + *negative* is ambiguous (it really depends on what the positive and negative numbers actually are, not just their signs).