Day 13

Friday June 8, 2012

1 Motivating Example: Modular Arithmetic

We are going to define a very useful equivalence relation that you have problem seen before. First we need some background however:

Lemma 1. *Fix $n > 0$, and $a, b, c \in \mathbb{Z}$. If $a + b$ is divisible by n and a is divisible by n then b is divisible by n.*

Proof. Suppose that $a+b$ and a are divisible by n. Then we get k and l in the integers such that $a+b = kn$ and $a = ln$ Substituting, we get $ln + b = kn$, ie. we have $b = n(k - l)$, which of course means b is divisible by n. □

Definition 1. We say $\exists! x \centerdot \varphi(x)$ to stand for "there exists a unique x such that $\varphi(x)$"; that is there is an x, and it is the only one with that property. To express this using the notation we already know:

$$(\exists! x \centerdot \varphi(x)) \iff (\exists x \centerdot (\varphi(x) \wedge (\forall y \centerdot \varphi(y) \rightarrow x = y)))$$

That is, there is an x that satisfies the property, and if there were any other y that satisfies it, then it is the same as x

Theorem 1 (Division Algorithm)**.**

$$\forall d \in \mathbb{Z}^+ \centerdot \forall n \in \mathbb{Z} \centerdot \exists! q, r \in \mathbb{Z} \centerdot ((n = dq + r) \wedge (0 \leq r < d))$$

Proof. Fix $d \in \mathbb{Z}^+$. Our strategy will be to show that there is a q and an r and then show they must be unique.

We will prove the statement for $n \in \mathbb{N}$; it is not hard to extend this to all $n \in \mathbb{Z}$, and you can think about why it is true.

We do many base cases in one step: for any $n < d$, we can be done instantly as we can take $q = 0$ and $r = n$. This obviously satisfies the properties.

So, for our induction hypothesis, let n be an arbitrary natural such that $n \geq d$. Assume that we can get integers q_m and r_m for all $m < n$ such that $m = dq_m + r_m$ and $0 \leq r_m < d$.

Now, we seek to show it's true for n. Well, consider $n - d$. As $n \geq d$, we know this is a natural number smaller than n. Thus we get q_{n-d} and r_{n-d} by our induction hypothesis. So $0 \leq r_{n-d} < d$ and $n - d = dq_{n-d} - r_{n-d}$. Adding d to both sides, we get $n = d(q_{n-d} + 1) - r_{n-d}$. So $q = q_{n-d} + 1$ and $r = r_{n-d}$ work.

Thus by induction it is true for all $n \in \mathbb{N}$.

Now we show uniqueness. Suppose we had two sets of q's and r's that satified this property. Then we would have

$$q_1 d + r_1 = n = q_2 + r_2$$

for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ where $0 \leq r_1 < d$ and $0 \leq r_2 < d$.

Then $(q_1 - q_2)d + (r_1 - r_2) = 0$. First we argue that $r_1 - r_2$ must be 0. d divides the right hand side (anything divides 0), and it divides the $(q_1 - q_2)d$. Thus by the lemma, it divides $r_1 - r_2$. Some work with the inequalities show that $-d < r_1 - r_2 < d$.

But of course there is only one number between $-d$ and d that is divisible by d: namely 0. So $r_1 - r_2 = 0$, so $r_1 = r_2$.

Thus we have $(q_1 - q_2)d = 0$. As $d \in \mathbb{Z}^+$, we have $d \neq 0$, and so $q_1 - q_2 = 0$, so $q_1 = q_2$. □

So we know given a divisor d, and a number n there is a unique quotient and remainder!

Definition 2. Fix $n \in \mathbb{Z}^+$. Define an relation $\sim_n$ on $\mathbb{Z}$ by

$$a \sim_n b \iff a \text{ and } b \text{ have the same remainder when you divide by } n$$

This is clearly an equivalence relation.

Theorem 2. *The relation $\sim_n$ has exactly n many equivalence classes.*

Proof. To show it has exactly n many we will show

- It has n many (lower bound)
- It has at most n many (upper bound)

To show it has n many, note that $0, 1, \ldots, n-1$ all have distinct remainders when divided by n.

To show it has at most n many, note that we are restricting the remainder r to be between 0 (inclusive) and n (exclusive). So there are only n possible remainders, so there must n. ☐

Remark 1. So, the equivalence classes look like all the numbers which have the same remainder when you divide by n. Here is the equivalence classes for $n = 3$.

$$[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2]_3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

Definition 3. Instead of saying $[i]_n = [j]_n$ we usually write

$$i \equiv j \mod n$$

Lemma 2. *If $a \sim_n b$ if and only if there is q such that $a = b + nq$.*

Proof. ($\Rightarrow$) Let the remainder of a and b be r. Then $a = q_a n + r$ and $b = q_b n + r$. So $r = b - q_b n$. So $a = (q_a - q_b)n + b$.

($\Leftarrow$) Suppose $a = b + nq$ for some q. Then write $a = q_a n + r_a$ and $b = q_b n + r_b$ from division algorithm. Then

$$q_a n + r_a = q_b n + r_b + nq$$

rearranging terms we get

$$n(q_a - q_b - q) = r_b - r_a$$

As in proof of division algorithm, $-n < r_b - r_a < n$, and it is divisible by n as left hand side is. So the difference must be 0, so $r_b = r_a$.

☐

Definition 4. We define an operation on equivalence classes:

$$[a]_n + [b]_n = [a + b]_n$$

Theorem 3. *The above notation makes sense; that is for any $x \in [a]_n$ and any $y \in [b]_n$ we have that $x + y \in [a + b]_n$*

Proof. Take $x \in [a]_n$ and any $y \in [b]_n$. By the above lemma $x = qn + a$ and $y = pn + b$. then $x + y = n(p+q) + a + b$. This shows that $x + y \sim_n a + b$ by the reverse direction of the lemma, so $x + y \in [a + b]_n$. ☐

Definition 5. We define an operation on equivalence classes:

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

Theorem 4. *The above notation makes sense; that is for any $x \in [a]_n$ and any $y \in [b]_n$ we have that $x \cdot y \in [a \cdot b]_n$.*

Proof. Exercise. ☐

So we can add, multiply.

Question 1. Can we subtract?

Answer 1. Yes, because we can add by $[-1]_n$ times the number, which is subtracting.

Question. In general, can we divide?

First let's make sense of what division is.

Definition 6. When you divide, you are really multiply by its inverse. The **inverse** of a number a is a number b such that $a \cdot b = 1$.

So, it is better to rephrase the question:

Question 2. In general, working mod n, does every number have an inverse?

Answer 2. Work $\mod 4$, and imagine 2 had an inverse x. Then we'd have

$$2x \equiv 1 \mod 4$$

Can you see why this cannot happen?

The rest of class will be spent answering the question: when can we find inverses. Let's do a little exploration first. Finding an inverse for a mod n would amount to solving the equation:

$$ax \equiv 1 \mod n$$

We have already shown above, this amount to solving the following arithmetic equation:

$$ax = 1 + bn$$

Or rewriting:

$$ax + bn = 1$$

This is called a **linear Diophantine equation**. So, our entire question of when inverses exist can be changed to: when can we solve linear Diophantine equations.

Definition 7. If n and m are integers then the $\gcd(n, m)$ is the largest number that divides both n and m.

Example 1. $\gcd(10, 5) = 5$, since 5 is the largest number that divides them both.
$\gcd(15, 9) = 3$ since 3 is the largest number that divides them both.
$\gcd(7, 10) = 1$ since 1 is the largest number that divides them both. In this case when the gcd is 1, we say they are **coprime** or **relatively prime**

Theorem 5.

$$ax + by = c \textit{ has a solution} \iff \gcd(a, b) \mid c$$

Proof. ($\Rightarrow$) Suppose that $ax + by = c$ has a solution. Let $d = \gcd(a, b)$. Then $a = q_a d + r_a$ and $b = q_b d + r_b$. So clearly $d \mid c$ as d divides the lefthand side.

($\Leftarrow$) This direction is a bit longer, and would take up too much class time. For more information, see a basic number theory textbook; it is called Bézout's Lemma ☐

Theorem 6. *Every* $[a]_n \neq [0]_n$ *has an inverse if and only if* n *is prime*

Proof. ($\Rightarrow$). Suppose that every a has has an inverse, and for contradiction suppose n was not prime. As n is not prime, $n = q \cdot p$ where $q, p \neq 1$. By assumption, p has an inverse: notate it p^{-1}. Then $p \cdot p^{-1} \equiv 1 \mod n$. Multiplying both sides by q we get $q \cdot p \cdot p^{-1} \equiv q \mod n$ As $n = q \cdot$, the left hand side is 0. So $q \equiv 0 \mod n$, but this means $n \mid q$, which of course is a contradiction as $n = q \cdot p$

($\Leftarrow$). From everything we said, finding an inverse amount to solving a Diophantine equation. $\gcd(n, a) = 1$ is n is prime and n doesn't divide a (can you see why?), thus we can solve the necessary Diophantine Equation. ☐