Geoffrey Parker - grp352
HW 22: 4.13 - 4.16
M328K
April 12th, 2012

4.13 Theorem. *Let p be a prime and let a be an integer not divisible by p; that is, $(a, p) = 1$. Then $\{a, 2a, 3a, \ldots, pa\}$ is a complete residue system modulo p.*

Proof. Let p be a prime and let a be an integer not divisible by p; that is, $(a, p) = 1$. Let $S = \{a, 2a, 3a, \ldots, pa\}$. Let i and j be arbitrary natural numbers with $1 \leq j < i \leq p$. Since $p \nmid a$, then by theorem 2.26 $(a, p) = 1$. Also, since $0 < j < i < p$, $0 < i - j < p$. So $p \nmid i - j$ and by 2.26 again $(p, i - j) = 1$. Then by theorem 2.29 $(p, a(i - j)) = 1$ and by 2.26 $p \nmid a(i - j)$. Expanding this, we get $p \nmid ai - aj$, which means $ai \not\equiv aj \pmod{p}$. Now we have shown that S has p elements and that all elements of S are pairwise incongruent modulo p. Therefore by theorem 3.17 S is a complete residue system modulo p. □

4.14 Theorem. *Let p be a prime and let a be an integer not divisible by p. Then*

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Proof. Let p be a prime and let a be an integer not divisible by p. Let $S = \{a, 2a, \ldots, pa\}$. By theorem 4.13 S is a complete residue system modulo p, which means all elements of S are pairwise incongruent modulo p. This means that each element of S must be congruent modulo p to a *distinct* element of the canonical complete residue system modulo p. Note that since by theorem 1.6 $p \mid pa$, we have $p \mid pa - 0$ and $pa \equiv 0 \pmod{p}$. Therefore each element of $T = \{a, 2a, \ldots (p-1)a\}$ is congruent to a distinct element of $R = \{1, 2, \ldots (p-1)\}$.

Now we will show by induction that the product of the elements of T is congruent modulo p to the product of the elements of R. We will name the elements of T and R as $t_1, t_2, \ldots, t_{p-1}$ and $r_1, r_2, \ldots, r_{p-1}$ respectively such that $t_1 \equiv r_1 \pmod{p}, t_2 \equiv r_2 \pmod{p}, \ldots, t_{p-1} \equiv r_{p-1} \pmod{p}$.

As our base case, $t_1 \equiv r_1 \pmod{p}$ by definition.

Our inductive hypothesis is that there exists an integer k such that $1 \leq k < p-1$ and $t_1 \cdot t_2 \cdot \ldots \cdot t_k \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_k \pmod{p}$.

For our inductive step, since $t_1 \cdot t_2 \cdot \ldots \cdot t_k \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_k \pmod{p}$ and $t_{k+1} \equiv r_{k+1}$ then by theorem 1.14 $t_1 \cdot t_2 \cdot \ldots \cdot t_{k+1} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{k+1} \pmod{p}$.

Therefore $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$.

□

4.15 Theorem (Fermat's Little Theorem, Version I)**.** *If p is a prime and a is an integer relatively prime to p, then $a^{(p-1)} \equiv 1 \pmod{p}$.*

Proof. Let p be prime and a be an integer relatively prime to p. Let $t = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$. Then by theorem 4.14 $a^{p-1}t \equiv t \pmod{p}$. Using the definition of congruece, we obtain $p \mid a^{p-1}t - t$, or $p \mid t(a^{p-1} - 1)$. So by theorem 2.27 $p \mid t$ or $p \mid a^{p-1} - 1$. By our lemma, $p \nmid t$. Therefore $p \mid a^{p-1} - 1$, or $a^{(p-1)} \equiv 1 \pmod{p}$.

Lemma: If p is a prime number then $p \nmid 1 \cdot 2 \cdot \ldots \cdot (p-1)$.
Let p be a prime number. We will show by induction that $p \nmid 1 \cdot 2 \cdot \ldots \cdot (p-1)$.

As our base case, consider $p \nmid 1$. Then $(p, 1) = 1$.

Our induction hypothesis is that there exists some k where $1 \leq k < p-1$ and $(p, 1 \cdot 2 \cdot \ldots \cdot k) = 1$.

For induction step, we know that $(p, 1 \cdot 2 \cdot \ldots \cdot k) = 1$. Also, since p is prime and $k+1 < p$ we know that $(p, k+1) = 1$. Therefore by theorem 2.29 $(p, 1 \cdot 2 \cdot \ldots \cdot k \cdot k+1) = 1$.

Now that we have shown that $(p, 1 \cdot 2 \cdot \ldots \cdot (p-1)) = 1$, we know by theorem 2.26 that $p \nmid 1 \cdot 2 \cdot \ldots \cdot (p-1)$. □

4.16 Theorem (Fermat's Little Theorem, Version II)**.** *If p is a prime and a is* any *integer, then* $a^p \equiv a \pmod{p}$.

Proof. Let p be a prime and a be any integer. Consider two cases:

Case 1: $p \mid a$. In this case, since $p \mid a$ then by theorem 1.6 $p \mid a \cdot a^{p-1}$, or $p \mid a^p$. So by theorem 1.2 $p \mid a^p - p$ and by the definition of congruence $a^p \equiv a \pmod{p}$.

Case 2: $p \nmid a$. In this case, theorem 4.15 states that $a^{(p-1)} \equiv 1 \pmod{p}$. So by theorem 1.14 $a^{(p-1)}a \equiv 1a \pmod{p}$, or equivalently $a^p \equiv a \pmod{p}$. □