Geoffrey Parker - grp352
HW 25: 4.36 - 4.42
M328K
April 26th, 2012

4.36 Theorem. *Let p be a prime and let a be an integer such that $1 \leq a < p$. Then there exists a unique natural number b less than p such that $ab \equiv 1 \pmod{p}$.*

Proof. Let p be a prime and let a be an integer such that $1 \leq a < p$. Then by theorem 4.13 $S = \{a, 2a, \ldots, pa\}$ is a complete residue system modulo p. So by definition of complete residue systems, one, being an integer, is congruent modulo p to exactly one element of S, call it t. So $t = ab$ where $b \leq p$ is a natural number. However $ap \equiv 0 \pmod{p}$ so b cannot be p. Therefore there exists a unique natural number b less than p such that $ab \equiv 1 \pmod{p}$. □

4.37 Exercise. *Let p be a prime. Show that the natural numbers 1 and $p-1$ are their own inverses modulo p.*

Solution.
$1 \cdot 1 = 1$ and $1 \equiv 1 \pmod{p}$.
$(p-1)(p-1) = p^2 - 2p + 1$. And since $p^2 \equiv 0 \pmod{p}$ and $2p \equiv 0 \pmod{p}$, we know $p^2 - 2p + 1 \equiv 1 \pmod{p}$. □

4.38 Theorem. *Let p be a prime and let a and b be integers such that $1 < a, b < p-1$ and $ab \equiv 1 \pmod{p}$. Then $a \neq b$.*

Proof. Let p be a prime and let a and b be integers such that $1 < a, b < p - 1$ and $ab \equiv 1 \pmod{p}$. Assume by way of contradiction that $a = b$. Then $aa \equiv 1 \pmod{p}$ and $p \mid aa - 1$ or equivalently $p \mid (a+1)(a-1)$. So by theorem 2.27 $p \mid a+1$ or $p \mid a - 1$. However, since $1 < a < p - 1$ both of these are natural numbers less than p, so p cannot divide either. Therefore we have a contradiction and have shown that $a \neq b$. □

4.39 Exercise. *Find all pairs of numbers a and b in $\{2, 3, \ldots, 11\}$ such that $ab \equiv 1 \pmod{13}$.*

Solution. 2, 7; 3, 9; 4, 10; 5, 8; 6, 11 □

4.40 Theorem. *If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p$.*

Proof. Let p be a prime larger than 2. Let S be the set of numbers $\{2, 3, 4, \ldots, (p-2)\}$. Note that each element of S is coprime with p. By theorem 4.36 each element a of S has some natural number $b < p$ such that $ab \equiv 1 \pmod p$. But b cannot be 1 because that would imply that $p \mid a - 1$. And if $b = p - 1$ then $p \mid ap - a$, and since $p \mid ap$ then by theorem 1.1 $p \mid a$. Since $1 < a < p - 1$, neither of these can be true, so b must be an element of the set S. And by theorem 4.38 $a \neq b$. So we can break the set S into n distinct a, b pairs where $ab \equiv 1 \pmod p$ and $|S| = 2n$. Then $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p$ can be rewritten as $a_1 b_1 a_2 b_2 \ldots a_n b_n$. Since each of these pairs is congruent modulo p to one, the entire product is congruent modulo p to one. Therefore $2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod p$. $\square$

4.41 Theorem (Wilson's Theorem)**.** *If p is a prime, then $(p-1)! \equiv -1 \pmod p$.*

Proof. Let p be prime. Note that $(p-1)! = 1(2 \cdot 3 \cdot \ldots \cdot p-2)(p-1)$. By theorem 4.40 $(2 \cdot 3 \cdot \ldots \cdot p - 2) \equiv 1 \pmod p$. So $(p-1)! \equiv p - 1 \pmod p$. And because $p \mid p$, also $p \mid p - 1 - (-1)$, so by the definition of congruence $p - 1 \equiv -1 \pmod p$. Therefore by theorem 1.11 $(p-1)! \equiv -1 \pmod p$. $\square$

4.42 Theorem (Converse of Wilson's Theorem)**.** *If n is a natural number such that $(n-1)! \equiv -1 \pmod n$, then n is prime.*

Proof. Let n be a natural number with $(n-1)! \equiv -1 \pmod n$. Because $p \mid p$, also $p \mid p - 1 - (-1)$, so by the definition of congruence $n - 1 \equiv -1 \pmod n$ and $(n-1)! \equiv n - 1 \pmod n$. And by 2.32 $(n-1, n) = 1$, so by theorem 4.3 $((n-1)!, n) = 1$. Assume by way of contradiction that n is composite. Then by definition of comosite there exist natural numbers a and b where $1 < a, b < n$ and $n = ab$. So $a \mid n$. However, by the definition of factorial $a \mid (n-1)!$. So a must divide $((n-1)!, n)$, which means that this gcd cannot be 1. Therefore we have a contradiction, so n must be prime. $\square$