Geoffrey Parker - grp352
HW 23: 4.27, 4.31 - 4.35
M328K
April 24th, 2012

4.27 Question. *The numbers* 1, 5, 7, *and* 11 *are all the natural numbers less than or equal to* 12 *that are relatively prime to* 12, *so* $\phi(12) = 4$.

1. *What is* $\phi(7)$*?*
2. *What is* $\phi(15)$*?*
3. *What is* $\phi(21)$*?*
4. *What is* $\phi(35)$*?*

Answer. $\phi(7) = 6; \phi(15) = 8; \phi(21) = 12; \phi(35) = 24$ □

4.31 Theorem. *Let* n *be a natural number and let* $x_1, x_2, \ldots, x_{\phi(n)}$ *be the distinct natural numbers less than or equal to* n *that are relatively prime to* n. *Let* a *be a non-zero integer relatively prime to* n *and let* i *and* j *be different natural numbers less than or equal to* $\phi(n)$. *Then* $ax_i \not\equiv ax_j \pmod{n}$.

Proof. Let n be a natural number and let $x_1, x_2, \ldots, x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let a be a non-zero integer relatively prime to n and let i and j be different natural numbers less than or equal to $\phi(n)$. Assume by way of contradiction that $ax_i \equiv ax_j \pmod{n}$. So by theorem 4.5, because $(a, n) = 1$, $x_i \equiv x_j \pmod{n}$. However, since x_i and x_j are less than n, they are elements of the canonical complete residue system modulo n. So by the definition of complete residue sytstems $x_i \not\equiv x_j \pmod{n}$ and we have a contradiction. Therefore $ax_i \not\equiv ax_j \pmod{n}$. □

4.32 Theorem (Euler's Theorem)**.** *If a and n are integers with $n > 0$ and $(a, n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let a and n be integers with $n > 0$ and $(a, n) = 1$. Let x_1, x_2, ..., $x_{\phi(n)}$ be the distinct natural numbers less than or equal to n that are relatively prime to n. Let $S = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\}$. Then each element ax_i of S must be congruent modulo n to some element y_i of the canonical complete residue system modulo n. Because $(n, x_i) = 1$ and $(n, a) = 1$ theorem 2.29 says $(n, ax_i) = 1$. And by theorem 4.3 $(y_i, n) = 1$) So the set of y's is just the set of x's with possibly different indicies.

Now we will show by induction that $a^{\phi(n)}x_1x_2 \cdots x_{\phi(n)} \equiv y_1y_2 \cdots y_{\phi(n)} \pmod{n}$ and $(y_1y_2 \cdots y_{\phi(n)}, n) = 1$.
As a base case, consider $\phi(n) = 1$. In this case $ax_1 \equiv y_1 \pmod{n}$ and $(x_1, n) = 1$ by definition.
Our induction hypothesis is that there exists some k where $1 \leq k < \phi(n)$,
$a^k x_1x_2 \cdots x_k \equiv y_1y_2 \cdots y_k$, and $(y_1y_2 \cdots y_k, n) = 1$.
Now given that $ax_{k+1} \equiv y_{k+1}$ by definition of y_{k+1} theorem 1.14 says that
$a^{k+1}x_1x_2 \cdots x_{k+1} \equiv y_1y_2 \cdots y_{k+1}$. And because $(y_1y_2 \cdots y_k, n) = 1$ and $(y_{k+1}, n) = 1$, we know by theorem 2.29 that $(y_1y_2 \cdots y_{k+1}, n) = 1$.

Now because the set of x's is the same as the set of y's the products of the elements of the sets are the same. We will call this product t, and we have just shown that $a^{\phi(n)}t \equiv t \pmod{n}$ and $(t, n) = 1$. Therefore by theorem 4.5 $a^{\phi(n)} \equiv 1 \pmod{n}$. $\square$

4.33 Corollary (Fermat's Little Theorem)**.** *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 a prime and a be an integer relatively prime to p. Then by Euler's Theorem $a^{\phi(p)} \equiv 1 \pmod{p}$. However, since p is prime, every natural number less than p is coprime with p, meaning that $\phi(p) = p-1$. Therefore $a^{p-1} \equiv 1 \pmod{p}$. $\square$

4.34 Exercise. *Compute each of the following without the aid of a calculator or computer.*

1. $12^{49} \pmod{15}$.

2. $139^{112} \pmod{27}$.

Solution.

1. First, $12^{49} \equiv 0 \pmod 3$ and $\phi(5) = 4$. So $12^4 \equiv 1 \pmod 5$ and $12^{49} \equiv 12^1 \equiv 2 \pmod 5$. Then we have $12^{49} \equiv 12 \pmod 3$ and $12^{49} \equiv 12 \pmod 5$, so by theorem 4.21 $12^{49} \equiv 12 \pmod{15}$

2. $27 = 3^3$ and $3 \nmid 139$ so $(27, 139) = 1$. The natural numbers coprime to 27 are those which 3 does not divide. So $\phi(27) = 26 - 8 = 18$. Then Euler's Theorem says $139^{18} \equiv 1 \pmod n$, and $112 = 6 \cdot 18 + 4$, which gives us:

$$139^{112} \equiv (139^{18})^6 \cdot 139^4 \equiv 139^4 \pmod{27}$$

   And since $139 = 5 \cdot 27 + 4$, $139 \equiv 4 \pmod{27}$. Then by theorem 1.18 $139^4 \equiv 4^4 \pmod{27}$. Therefore $139^{112} \equiv 16 \pmod{27}$.

□

4.35 Exercise. *Find the last digit in the base* 10 *representation of the integer* 13^{474}.

Solution. This is the same as $13^{474} \pmod{10}$. Note that $(13, 10) = 1$ and $\phi(10) = 4$. So by Euler's Theorem $13^4 \equiv 1 \pmod{10}$. And $474 = 4 \cdot 118 + 2$, so:

$$13^{474} \equiv 13^{4 \cdot 118 + 2} \equiv (13^4)^{118} \cdot 13^2 \equiv 1 \cdot 13^2 \equiv 169 \equiv 9 \pmod{10}$$

□