116 - Number Theory
Spring 2007

Homework 6 - Euler's Function

Name: _____
Instructor: Travis Kelm

Some Modular Inverse Problems

1. **Modular Inverses:** Prove that a positive integer t has an inverse mod m if and only if $\gcd(t, m) = 1$.

   Solution: We can prove both directions at once. Suppose that t has an inverse modulo m. Denote this inverse by k. Thus $tk \equiv 1 \pmod{m}$. This occurs if and only if $tk = 1 + cm$ for some $c \in \mathbb{Z}$. But that is equivalent to $tk + (-c)m = 1$, which means 1 is a linear combination of t and m. This means that $\gcd(t, m) = 1$. □

2. **Modular Division:** Suppose that $ta \equiv tb \pmod{m}$. Prove that if $\gcd(t, m) = 1$ then $a \equiv b \pmod{m}$. (In other words, you can "cancel" the t from both sides.)

   Solution: If $\gcd(t, m) = 1$, then by the previous problem, t has a modular inverse (call it k). By multiplying both sides of $ta \equiv tb \pmod{m}$ by k, the ts go away leaving $a \equiv b \pmod{m}$ as desired. □

3. **Rel Primeness with mod Glasses:** Prove that if $\gcd(a, m) = 1$ and if $a \equiv b \pmod{m}$ then $\gcd(b, m) = 1$ as well.

   Solution: Assume $\gcd(a, m) = 1$. Thus by the first problem a has an inverse mod m (call it k). Thus $ka \equiv 1 \pmod{m}$. But since $a \equiv b \pmod{m}$ we must have $ka \equiv kb \pmod{m}$ which means that $kb \equiv 1$ as well. Thus b has a modular inverse as well, so the first problem dictates that $\gcd(b, m) = 1$ as desired. □

Section 7.1 - Euler's Function

4. **Exercise 6:** Find all positive solutions to the equation $\phi(n) = 12$.

   Solution: There are four solutions to $\phi(n) = 12$. They are

   - $n = 28$
   - $n = 42$
   - $n = 21$
   - $n = 36$

   We describe how to prove this by analyzing several cases as detailed below.

   Using the formula derived in class, if $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ then $\phi(n) = 12$ means that

   $$12 = p_1^{t_1 - 1}(p_1 - 1)p_2^{t_2 - 1}(p_2 - 1) \cdots p_k^{t_k - 1}(p_k - 1)$$

   On account of the $p_i - 1$ terms in the expression, the only primes p_i in n must be such that $p_i - 1$ divides 12. Thus the only primes possible in n are $2, 3, 5$, and 7. So assume that $n = 2^a 3^b 5^c 7^d$ where $0 \leq a, b, c, d$ so that

   $$12 = 2^{a-1}(1)3^{b-1}(2)5^{c-1}(4)7^{d-1}(6) \tag{1}$$

   where the $p^{j-1}(p - 1)$ term is present only if the p occurs in the prime factorization of n.

   Note that if $d > 1$ then $7|12$ a contradiction, thus $d = 0, 1$. Likewise, if $c > 1$ then $5|12$ which can't happen, thus $c = 0, 1$. Finally, note that $b \leq 2$ lest $9|12$ and $a \leq 3$ lest $8|12$.

   [Case I: Assume d = 1] If $d = 1$ then equation (1) must contain $7^{1-1}(6)$ and exactly one factor of 2. Thus $c = 0$, lest we have a factor of 4. To get the factor of two we could have

   - $a = 2$ and $b = 0$ OR

- $a = 1$ and $b = 1$ OR
- $a = 0$ and $b = 1$

These three cases give us the following values for n:

- $n = 28$
- $n = 42$
- $n = 21$

One can verify that each of these is a solution to $\phi(n) = 12$.

[**Case II: Assume c = 1**] If $c = 1$ then equation (1) must contain $5^{1-1}(4)$, so all we need is a single factor of 3. As observed we must have that $d = 0$. Also if $b \neq 0$ then equation (1) will contain a factor of 2 which we don't want. So the factor of three must come from $2^{a-1}(1)$ which is never equal to three. Thus we conclude $c \neq 1$ so that n has no factor of 5.

[**Case III: Assume d = 0, b = 2**] If $b = 2$ then equation (1) must contain $3^{2-1}(2)$ so all we need is a single factor of 2. This comes from setting $a = 2$. Thus $n = 2^2 3^2$ should be a solution to $\phi(n) = 12$.

[**Case IV: Assume d = 0, b = 1**] If $b = 1$ then equation (1) must contain $3^{1-1}(2)$ so we need a factor of 6 or factors of 2 and 3. Moreover these factors must come from the $2^{a-1}(1)$ term since we are assuming that $b = 1, c = 0$, and $d = 0$. Since there is no way to get a 6 or a 3 from $2^{a-1}(1)$ we must conclude that this case cannot occur.

[**Final Case: Assume d = 0, b = 0**] Here we are assuming that $b = c = d = 0$ hence $n = 2^a$. By equation (1) this means that $12 = 2^{a-1}$. Clearly this is impossible, thus there are no solutions in this case.

Conclusion: There are four solutions to $\phi(n) = 12$. They are

- $n = 28$
- $n = 42$
- $n = 21$
- $n = 36$ □

5. Exercise 8: Show that there is no solution to the equation $\phi(n) = 14$.
Solution: Assume that $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ is the prime factorization of n. Using the formula derived in class, if then $\phi(n) = 14$ means that

$$14 = p_1^{t_1-1}(p_1 - 1)p_2^{t_2-1}(p_2 - 1) \cdots p_k^{t_k-1}(p_k - 1)$$

On account of the $p_i - 1$ terms in the expression, the only primes p_i in n must be such that $p_i - 1$ divides 14. Thus the only primes possible in n are 2 and 3. This means that $n = 2^a 3^b$ where $0 \leq a, b$ so that

$$14 = 2^{a-1}(1)3^{b-1}(2) \tag{2}$$

where the $p^{j-1}(p-1)$ term is present only if the p occurs in the prime factorization of n.

Note that if $b > 1$ then $3|14$ a contradiction, thus $b = 0, 1$. But if $b = 1$ then equation (2) becomes $14 = 2^{a-1}3^{1-1}2$ Which implies that $2^{a-1} = 7$ which is impossible. Thus $b = 0$.

But if $b = 0$ then equation (2) becomes $14 =^{a-1}$ which once again is impossible. Thus there can be no solution to the equation $\phi(n) = 12$. □

6. Exercise 15: Show that if n is a positive integer, then

$$\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd;} \\ 2\phi(n) & \text{if } n \text{ is even} \end{cases}$$

Solution: Assume that $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ is the prime factorization of n. Using the formula derived in class, we have that

$$\phi(n) = p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1)\cdots p_k^{t_k-1}(p_k-1)$$

If n is odd, then none of the p_is are equal to 2, thus the prime factorization of $2n$ is

$$2p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

So by our formula

$$\phi(2n) = 2^{(1-1)}(1)p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1)\cdots p_k^{t_k-1}(p_k-1) = 2\phi(n)$$

as desired.

If n is even then n contains a factor of two so we might as well assume that $p_1 = 2$ so that $n = 2^a p_2^{t_2} \cdots p_k^{t_k}$ is the prime factorization of n. So by our tired and true formula

$$\phi(n) = 2^{a-1}(1)p_2^{t_2-1}(p_2-1)\cdots p_k^{t_k-1}(p_k-1)$$

Observe then that the prime factorization of $2n$ is $2n = 2^{a+1} p_2^{t_2} \cdots p_k^{t_k}$ which means that our favorite formula says

$$\phi(2n) = 2^{(a+1-1)}(1)p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1)\cdots p_k^{t_k-1}(p_k-1) = 2\phi(n)$$

as desired. □

7. Exercise 26: Show that if the equation $\phi(n) = k$ has exactly one solution, then $36|n$.

Solution: We'll prove the contrapositive. Suppose that $\phi(n) = k$ and that $36 \nmid n$. We'll show that there is some other number m such that $\phi(m) = k$. As usual let $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ be the prime factorization of n. This then means that

$$k = \phi(n) = p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1)\cdots p_k^{t_k-1}(p_k-1)$$

First note that if n is odd, then Exercise 15 shows that $\phi(2n) = k$ so we are done.

Thus we should assume that n is even. So we may assume that $p_1 = 2$ giving us $n = 2^a p_2^{t_2} \cdots p_k^{t_k}$. Notice that if $a = 1$ then $n/2 = p_2^{t_2} \cdots p_k^{t_k}$ and our favorite formula reveals that $\phi(n) = \phi(n/2)$.

So now let us assume that $a \geq 2$. If n has no factor of 3, then the number $n' = 2 \cdot 3 p_2^{t_2} \cdots p_k^{t_k}$ is different than n, yet you can compute that $\phi(n') = \phi(n)$ as well.

So finally let us assume that $p_2 = 3$ so that $n = 2^a 3^b \cdots p_k^{t_k}$ where $a \geq 2$ and $b \geq 1$. Check that we can't have $b \geq 2$ because we assumed that $36 \nmid n$. Thus $b = 1$ so $n = 2^a \cdot 3 \cdots p_k^{t_k}$. So consider now the number $\hat{n} = 2^{a+1} \cdots p_k^{t_k}$ (take a 3 but add a 2). You should see that $\phi(\hat{n}) = \phi(n)$ as desired.

That's it, we've exhausted all the cases. We've shown that so long as $36 \nmid n$ then there is some other number m such that $\phi(n) = \phi(m)$.

[You should note that the statement in this exercise is not an *if and only if*. To see this note that $\phi(36) = 12$ but $\phi(13) = 12$ as well. You might ask yourself, what is the smallest integer n such that n is the unique solution to the equation $\phi(x) = \phi(n)$?] □

8. Exercise 27: Show that if $k > 0$ then $\phi(n) = k$ has only finitely many solutions.

Solution: As always let $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ be the prime factorization of n. Using the formula derived in class, we have that

$$\phi(n) = p_1^{t_1-1}(p_1 - 1)p_2^{t_2-1}(p_2 - 1)\cdots p_k^{t_k-1}(p_k - 1) \qquad \text{thus} \tag{3}$$

$$k = p_1^{t_1-1}(p_1 - 1)p_2^{t_2-1}(p_2 - 1)\cdots p_k^{t_k-1}(p_k - 1) \tag{4}$$

Since k is an integer, there are only a finite number of primes that divide k, thus only a finite number of possibilities for the p_i. Moreover, given any prime divisor p of k, there is some integer t such that $p^t > k$ and thus $p^t \not| k$. This means that for each possible p_i in equation (4) there are only finitely many possibilities for the exponent $t_i - 1$. It follows that there are only finitely many solutions to equation (4). □