

Math 322 Fall 2017  
Number Theory HW 7 Solutions  
Due Friday, October 27

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

(★) **Starred Problem:** Show that if  $n$  is odd, then  $\phi(4n) = 2\phi(n)$ .

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Show that 1387 is a pseudoprime but not a strong pseudoprime to the base 2.

**Solution:** We first want to compute  $2^{1386} \pmod{1387}$ . We can compute this directly, or we can observe that  $2^{18} \equiv 1 \pmod{1387}$ , and then compute that  $2^{1386} = (2^{18})^{77} \equiv 1^{77} \equiv 1 \pmod{1387}$ . Thus 1387 is a pseudoprime to the base 2.

Now we apply Miller's test. We compute

$$2^{1386/2} = 2^{693} = (2^{18})^{38} \cdot 2^9 \equiv 2^9 \equiv 512 \pmod{1387}.$$

Thus  $2^{1386/2} \not\equiv \pm 1 \pmod{1387}$  and thus 1387 fails the Miller test for the base 2. So 1387 is not a strong pseudoprime to the base 2, and is also not prime.

2. Let  $m$  be a natural number. Find a reduced residue system modulo  $2^m$ .

**Solution:** One reduced residue system modulo  $2^m$  is the set of all numbers which are relatively prime to  $2^m$  and less than  $2^m$ . A number  $d$  is relatively prime to  $2^m$  if and only if  $d$  is odd. thus a reduced residue system modulo  $2^m$  is

$$\{1, 3, 5, 7, \dots, 2^m - 1\} = \{n \in \mathbb{N} : (n, 2) = 1, n < 2^m\} = \{2n + 1 : 0 \leq n < 2^{m-1}\}.$$

3. Use Euler's theorem to find the last decimal digit of:

(a)  $3^{1000}$

**Solution:** We know  $\phi(10) = 4$  so  $3^{1000} = (3^4)^{250} \equiv 1 \pmod{10}$ , so the last decimal digit of  $3^{1000}$  is 1.

(b)  $7^{999,999}$

**Solution:** We know  $\phi(10) = 4$  so  $7^{999,999} = (7^4)^{249,999} \cdot 7^3 \equiv 7^3 \equiv 3 \pmod{10}$ .

(c) Let  $n$  be a natural number. Prove that  $\phi(n) = n - 1$  if and only if  $n$  is prime.

**Solution:** Suppose  $n$  is prime. Then if  $n \nmid d$  we know that  $(n, d) = 1$ , and thus every number less than  $n$  is relatively prime to  $n$ . Since  $(n, n) = n > 1$ , there are  $n - 1$  numbers  $\leq n$  and relatively prime to  $n$ .

Conversely, suppose  $\phi(n) = n - 1$ . Then  $n > 1$  since if  $n = 1$  then  $\phi(n) = 1 \neq n - 1$ . Then  $(n, n) = n > 1$ , so if there are  $n - 1$  numbers  $\leq n$  and relatively prime to  $n$  this means that every number less than  $n$  is relatively prime to  $n$ . Thus  $n$  can have no factors except itself and 1, so  $n$  is prime by definition.

4. Let  $a, b$  be relatively prime natural numbers. Show that  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ .

**Solution:** By Euler's theorem, we know that  $a^{\phi(b)} \equiv 1 \pmod{b}$  and  $b^{\phi(a)} \equiv 1 \pmod{a}$ . But clearly  $a^{\phi(b)} \equiv 0 \pmod{a}$  and  $b^{\phi(a)} \equiv 0 \pmod{b}$ , so we have  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a}$  and  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{b}$ . Then by the Chinese Remainder Theorem, we have  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ .

5. Let  $c_1, c_2, \dots, c_{\phi(m)}$  be a reduced residue system modulo  $m$ , where  $m > 2$ . Show that  $c_1 + c_2 + \dots + c_{\phi(m)} \equiv 0 \pmod{m}$ .

**Solution:**

First notice that, as with our proof of Euler's theorem in class, we know that the set  $\{c_1, c_2, \dots, c_{\phi(m)}\}$  has exactly one representative from every equivalence class modulo  $m$  that is relatively prime to  $m$ . Thus if  $R = \{r_1, r_2, \dots, r_{\phi(m)}\}$  is the reduced residue system of integers which are  $\leq m$  and relatively prime to  $m$ , we know that

$$c_1 + c_2 + \dots + c_{\phi(m)} \equiv r_1 + r_2 + \dots + r_{\phi(m)} \pmod{m}.$$

So we just need to prove the result for this particular reduced residue system.

We observe that if  $(r_i, m) = 1$ , then  $(m - r_i, m) = 1$ , so every element of  $R$  has an additive inverse modulo  $m$  that is also in  $R$ . Further, suppose that  $r_i \equiv -r_i \pmod{m}$ ; then  $m \mid 2r_i$  and since  $m \neq 2$  this implies that  $(m, r_i) > 1$ , which is a contradiction, so each element has a distinct additive inverse. Thus we can uniquely pair each element with its additive inverse, and we have

$$r_1 + r_2 + \dots + r_{\phi(m)} \equiv (r_1 - r_1) + (r_2 - r_2) + \dots \equiv 0 \pmod{m}.$$

6. Determine whether each of the following functions is multiplicative, completely multiplicative, or neither.

(a)  $f(n) = 0$

**Solution:** Completely multiplicative, since  $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$ .

(b)  $\gcd(n, k)$  for some fixed integer  $k$ .

**Solution:** Multiplicative. We see it is not completely multiplicative since  $\gcd(4, 2) = 2 \neq 2 \cdot 2 = \gcd(2, 2) \cdot \gcd(2, 2)$ .

To prove that it's multiplicative: fix  $k$  and suppose  $(m, n) = 1$ . Suppose  $d|mn, k$ . Then we can write  $d = d_1d_2$  where  $d_1|m, k$  and  $d_2|n, k$ . Thus  $\gcd(mn, k) \leq \gcd(m, k) \cdot \gcd(n, k)$ .

Conversely, suppose  $d_1|m, k$  and  $d_2|n, k$ . Then  $d_1d_2|mn, k$ , and since  $(m, n) = 1$  we know that  $d_1d_2|k$ . Thus  $\gcd(m, k)\gcd(n, k) \leq \gcd(mn, k)$ . Therefore  $\gcd(mn, k) = \gcd(m, k)\gcd(n, k)$  if  $(m, n) = 1$ .

(c)  $\log(n)$  **Solution:** Not multiplicative:  $\log(6) = \log(2) + \log(3) \neq \log(2)\log(3)$ .

7. Find all numbers  $n$  with  $\phi(n) = 16$ , and prove that you have found them all.

**Solution:** Suppose  $\phi(n) = 16$ . Suppose  $p$  is a prime factor of  $n$ , then  $\phi(p)|16$ , so  $p-1$  is equal to 2,4,8,16, so  $p$  must be 3,5, or 17. Further if any prime has an exponent higher than 1, the prime must divide  $\phi(p) = 16$ , so 3, 5, and 17 have exponent at most 1.

We now divide this into a bunch of cases. First suppose  $n = 2^a3^b5^c17$ . Then if  $b$  or  $c$  is equal to 1,  $\phi(n) > 16$ , so we reduce to the case where  $n = 2^a \cdot 17$ . Then if  $a > 0$ , we have  $16 = \phi(n) = 2^{a-1}(2-1)17^0(17-1) = 2^{a-1} \cdot 16$  and thus  $a = 1$  and  $n = 34$ . If  $a = 0$  then  $n = 17$  and we can compute  $\phi(n) = 16$ .

Now suppose  $17 \nmid n$ . We have four cases. Suppose  $n = 2^a$ . Then  $16 = \phi(n) = 2^{a-1}(2-1)$  and thus  $a = 5$  and  $n = 32$ .

Suppose  $n = 2^a \cdot 3$ . We don't need to consider the case  $a = 0$  since  $\phi(3) \neq 16$ . Then  $16 = \phi(n) = 2^{a-1} \cdot 2 = 2^a$ , so  $a = 4$  and  $n = 48$ .

Suppose  $n = 2^a \cdot 5$ . We don't need to consider the case  $a = 0$ . Then  $16 = \phi(n) = 2^{a-1} \cdot 4 = 2^{a+1}$ . So  $a = 3$  and  $n = 40$ .

Finally, suppose  $n = 2^a \cdot 3 \cdot 5$ . Again we don't need to consider  $a = 0$ . Then  $16 = \phi(n) = 2^{a-1} \cdot 2 \cdot 4 = 2^{a+2}$ . So  $a = 2$  and  $n = 60$ .

So we conclude that if  $\phi(n) = 16$ , then  $n \in \{17, 32, 34, 40, 48, 60\}$ .