

## Selected Solutions

**Sect 3.4, #8:** Show that if  $GCD(a, 561) = 1$ , then  $a^{80} \equiv 1 \pmod{561}$ .

**Proof:** Notice that  $561 = 3 \cdot 11 \cdot 17$ . We will look at  $a^{80}$  modulo each of these factors and use the Chinese Remainder Theorem to get a congruence modulo their product.

Observe that since  $(a, 561) = 1$  we have  $(a, 3) = (a, 11) = (a, 17) = 1$ . Then by Euler's theorem,

$$\begin{aligned} a^2 &\equiv 1 \pmod{3} \implies (a^2)^{40} = a^{80} \equiv 1 \pmod{3} \\ a^{10} &\equiv 1 \pmod{11} \implies (a^{10})^8 = a^{80} \equiv 1 \pmod{11} \\ a^{16} &\equiv 1 \pmod{17} \implies (a^{16})^5 = a^{80} \equiv 1 \pmod{17}. \end{aligned}$$

Therefore, we must solve the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{11} \\ x &\equiv 1 \pmod{17} \end{aligned}$$

By the Chinese Remainder Theorem, there is a unique solution modulo 561. Notice that  $x = 1$  works. This means that,  $a^{80} \equiv 1 \pmod{561}$ .

**Comments:** You must explain why the three congruences imply that  $a^{80} \equiv 1 \pmod{561}$ . It is a little deceptive since everything is a 1. Consider the following system:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 5 \pmod{11} \\ x &\equiv 14 \pmod{17} \end{aligned}$$

The Chinese Remainder Theorem tells you there is a unique solution modulo 561. However, it is not immediately obvious what that unique solution is, and it is not possible to just multiply the right hand sides to get it (that is,  $x \equiv 140 \pmod{561}$  doesn't work).

**Sect 3.5, #3:** Show that if  $n$  is even,  $\phi(2n) = 2\phi(n)$ .

**Proof:** Since  $n$  is even, we can write  $n = 2^a \cdot b$ , where  $b$  is odd. Then since  $(2^a, b) = 1$ , we can use the multiplicativity of  $\phi$  to get

$$\begin{aligned} 2\phi(n) &= 2\phi(2^a \cdot b) \\ &= 2 \cdot \phi(2^a) \cdot \phi(b) \\ &= 2 \cdot 2^{a-1} \cdot \phi(b) \\ &= 2^a \cdot \phi(b) \\ &= \phi(2^{a+1}) \cdot \phi(b) \\ &= \phi(2^{a+1} \cdot b) \\ &= \phi(2n) \end{aligned}$$

**Comments:** It is not enough to say that  $n = 2k$  for some  $k$ . The problem arises when you try to apply the multiplicativity of  $\phi$ . It is not always true that  $\phi(4k) = \phi(4) \cdot \phi(k)$ .

**Web Problem #1:** Show that if  $p > 5$  is prime, then  $(p-1)! + 1$  has (at least) two distinct prime factors.

**Proof:** By Wilson's Theorem, we know that  $(p-1)! \equiv -1 \pmod{p}$ , so that  $p \mid (p-1)! + 1$ . We will prove the result by contradiction. Suppose that  $p$  is the only prime factor of  $(p-1)! + 1$ , so that for some integer  $k \geq 1$ ,

$$(p-1)! + 1 = p^k.$$

We can rewrite this equation as

$$(p-1)! = p^k - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + 1),$$

and after dividing out the  $p-1$ , this leaves

$$(p-2)! = p^{k-1} + p^{k-2} + \cdots + 1.$$

Consider this equation modulo  $p-1$ . Since  $p > 5$  is prime,  $p-1 > 4$  is composite, so by last week's homework we know that  $(p-2)! \equiv 0 \pmod{p-1}$ . Notice that  $p \equiv 1 \pmod{p-1}$ . Thus,

$$\begin{aligned} 0 &\equiv \underbrace{1^{k-1} + 1^{k-2} + \cdots + 1}_{k \text{ terms}} \pmod{p-1} \\ &\equiv k \pmod{p-1} \end{aligned}$$

So we have  $k = (p-1) \cdot i$  for some  $i \geq 1$ . In particular, we know that  $k \geq p-1$ .

We will now derive a contradiction using some very crude estimates:

$$\begin{aligned} 1 &= p^k - (p-1)! \\ &\geq p^{p-1} - (p-1)! \\ &= (p-1)! \left( \frac{p^{p-1}}{(p-1)!} - 1 \right) \\ &= (p-1)! \left( \frac{p}{p-1} \cdot \frac{p}{p-2} \cdots \frac{p}{1} - 1 \right) \\ &> (p-1)! (1 \cdot 1 \cdots p-1) \\ &> (5-1)! \cdot (5-1) \\ &= 96. \end{aligned}$$

Since  $1 > 96$  is false, we have a contradiction. Therefore, there must be at least two distinct prime factors.

**Comment:** There was some confusion about whether the problem meant *exactly* two distinct prime factors or *at least* two distinct prime factors. You could have emailed for clarification or simply worked out a couple examples on a computer:

$$6! + 1 = 721 = 7 \cdot 103$$

$$10! + 1 = 3628801 = 11 \cdot 329891$$

$$12! + 1 = 479001601 = 13^2 \cdot 2834329$$

$$16! + 1 = 20922789888001 = 17 \cdot 61 \cdot 137 \cdot 139 \cdot 1059511$$

**Web Problem #2a:** Find all  $n$  such that  $\phi(n) = 3$ .

**Proof 1:** We can write out the prime factorization as  $n = p_1^{a_1} \cdots p_k^{a_k}$ . Then since  $\phi$  is a multiplicative function, we want to find all  $n$  such that

$$\begin{aligned} 3 &= \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \\ &= (p_1^{a_1-1})(p_1 - 1) \cdots (p_k^{a_k-1})(p_k - 1) \end{aligned}$$

Therefore, we must choose the primes and their powers so that  $(p_i - 1) \mid 3$  and  $p_i^{a_i-1} \mid 3$ . The first condition can only be satisfied by  $p = 2$ . But if  $p = 2$ , then the second condition cannot be met. Therefore, there are no  $n$  such that  $\phi(n) = 3$ .

**Proof 2:** As in the first proof, we have

$$3 = (p_1^{a_1-1})(p_1 - 1) \cdots (p_k^{a_k-1})(p_k - 1).$$

Notice that if any  $p_i > 2$ , the product will be even. So the only prime allowed is  $p = 2$ . But if  $a > 1$ , then the product  $p^{a-1}(p - 1) = 2^{a-1}$  will be even. So the only possibility is  $n = 2^1$ , but this has  $\phi(n) = 1$ .

**Web Problem #2b:** Find all  $n$  such that  $\phi(n) = 4$ .

**Proof:** Starting as in problem #2a, we get

$$4 = (p_1^{a_1-1})(p_1 - 1) \cdots (p_k^{a_k-1})(p_k - 1).$$

So we must pick the primes and their powers so that  $(p_i - 1) \mid 4$  and  $p_i^{a_i-1} \mid 4$ . The first condition gives three possibilities:  $p_1 = 2, p_2 = 3, p_3 = 5$ . We will work systematically starting with the largest prime.

If  $a_3 \geq 2$ , then  $\phi(n) \geq \phi(5^2) = 20$ , which is too large. So we must have  $a_3 = 0$  or  $a_3 = 1$ . If  $a_3 = 1$ , then we write  $n = 5m$  with  $(5, m) = 1$ , so that  $\phi(n) = 4\phi(m)$ . The only way we get the required value is if  $\phi(m) = 1$ . There are only two integers  $m$  such that  $\phi(m) = 1$ , and they are  $m = 1$  and  $m = 2$ . Therefore, two possible values of  $n$  are  $n = 5$  and  $n = 10$ .

If  $a_3 = 0$ , then we are down to two primes. If  $a_2 \geq 2$ , then  $\phi(n) \geq \phi(3^2) = 6$ , which is too large. So  $a_2 = 0$  or  $a_2 = 1$ . If  $a_2 = 1$ , then we write  $n = 2^{a_1} \cdot 3$ , so that  $\phi(n) = \phi(2^{a_1}) \cdot \phi(3) = 2_1^a$ . We want this to equal 4, so we must have  $a_1 = 2$ . This shows that  $n = 12$  is another possibility.

Finally, if  $a_3 = 0$ , then  $n = 2^{a_1}$ . We can immediately compute that  $\phi(n) = 2^{a_1-1}$ . Since we want this to equal 4, we take  $a_1 = 3$ . This gives  $n = 8$  as the final possibility.

So the values of  $n$  such that  $\phi(n) = 4$  are  $n = 5, 8, 10, 12$ .