

## Math 4150 Homework 3 Solutions

### Problem 10.3

(a) Let  $a$  be such that  $\gcd(a, 561) = 1$ . By Fermat's theorem, we have  $a^2 \equiv 1 \pmod{3}$ ,  $a^{10} \equiv 1 \pmod{11}$ , and  $a^{16} \equiv 1 \pmod{17}$ . Raising each of these congruences to an appropriate power we get  $a^{560} \equiv 1 \pmod{3}$ ,  $a^{560} \equiv 1 \pmod{11}$ , and  $a^{560} \equiv 1 \pmod{17}$ . Thus  $a^{560} - 1$  is divisible by 3, 11, and 17. Since these three numbers are relatively prime, then  $a^{560} - 1$  is divisible by their product, which is 561. Thus  $a^{560} \equiv 1 \pmod{561}$ . Since  $a$  was arbitrary, this shows that 561 is a Carmichael number.

(b) Searching for Carmichael numbers is very difficult if you just know the definition. The next two are 1105 and 1729. It is a difficult theorem that there are infinitely many Carmichael numbers. This was proved in 1994, and had been an open question for a long time before that.

### Problem 11.2

(a) Suppose first there is an odd prime  $p$  dividing  $m$ . Then we can write  $m = p^k n$  for some  $n$  which is not divisible by  $p$ . By multiplicativity of the phi function, we obtain  $\varphi(m) = (p^k - p^{k-1})\varphi(n) = p^{k-1}(p-1)\varphi(n)$ . In particular  $\varphi(m)$  is divisible by  $p-1$ , which is even. Therefore  $\varphi(m)$  is even. Now, if there is no odd prime dividing  $m$ , then  $m$  is a power of 2, say  $m = 2^s$ . Since  $m \geq 3$ , then  $s \geq 2$ . In this case we have  $\varphi(m) = 2^s - 2^{s-1} = 2^{s-1}$ , which is divisible by 2. Thus  $\varphi(m)$  is even.

(b) We claim that  $\varphi(m)$  is divisible by 4 unless  $m = 2$  or  $m = 4$ , or  $m = 2p^d$ ,  $m = p^d$  for some odd prime  $p$  and  $d \geq 1$ , where  $p \equiv 3 \pmod{4}$ . To see this, suppose first that  $m$  is a power of 2,  $m = 2^s$ . Then  $\varphi(m) = 2^{s-1}$ , which is divisible by 4 unless  $s \leq 2$ . This gives the exceptions  $m = 2$  and  $m = 4$ . Next, suppose  $m$  is divisible by exactly one odd prime  $p$ , so that  $m = 2^s p^d$  for some  $s \geq 0$  and  $d \geq 1$ . If  $s = 0$  then  $\varphi(m) = p^{d-1}(p-1)$ . This is not divisible by 4 if  $p \equiv 3 \pmod{4}$ . Now if  $s \geq 1$ , then  $\varphi(m) = 2^{s-1}(p-1)p^{d-1}$ . The only way this is not divisible by 4 is if  $p-1$  is not divisible by 4 and  $s = 1$ . This gives the exception  $m = 2p^d$  with  $p \equiv 3 \pmod{4}$ . Finally, suppose  $m$  is divisible by at least two odd primes  $p$  and  $q$ . Then  $\varphi(m)$  is

divisible by  $(p-1)(q-1)$ , which is clearly a multiple of 4. Thus there are no more exceptions.

**Problem 11.5** The three parts of the problem are similar, so we solve only part (a) to illustrate the method.

(a) From the first congruence, we are looking for a solution to  $x = 3 + 7y$ . Substituting this expression for  $x$  into the second congruence, we obtain  $3 + 7y \equiv 5 \pmod{9}$ , or  $7y \equiv 2 \pmod{9}$ . This is equivalent to solving the equation  $7y + 9z = 2$ . In general you should use the methods of chapter 8 to solve this kind of equation, but in this case one solution is obvious:  $y = -1, z = 1$ . We then have  $x = 3 + 7(-1) = -4$ . You should check that this is in fact a solution to the system of congruences.

**Problem 11.7** Let  $e$  denote the number of eggs in the unfortunate farmer's truck. Then we have  $e \equiv 0 \pmod{7}$ , and also  $e - 1$  is divisible by 2, 3, 4, 5, and 6. Equivalently,  $e - 1$  is divisible by 3, 4, and 5, and is therefore divisible by  $3 \cdot 4 \cdot 5 = 60$ . Thus  $e = 60x + 1$  for some  $x$ . We can then reformulate the problem as follows: find the smallest nonnegative value of  $x$  such that  $60x + 1 \equiv 0 \pmod{7}$ . This is equivalent to  $60x \equiv 6 \pmod{7}$ . Since  $\gcd(6, 7) = 1$ , this is equivalent to  $10x \equiv 1 \pmod{7}$ . Starting with  $x = 1$  and trying the first few values we find the smallest solution is  $x = 5$ . Therefore the smallest possible number of eggs is  $60(5) + 1 = 301$ .

**Problem 16.1** We do only part (a) to illustrate the method.

(a) Write 13 as a sum of powers of 2:  $13 = 2^3 + 2^2 + 1$ . Now successively square 5 modulo 23:  $5^2 = 25 \equiv 2 \pmod{23}$ ,  $5^4 \equiv 4 \pmod{23}$ ,  $5^8 \equiv 16 \pmod{23}$ . Therefore  $5^{13} \equiv 16 \cdot 4 \cdot 5 \pmod{23} \equiv 21 \pmod{23}$ .