Math 255 - Spring 2017
Answers to selected suggested problems
Problems between March 1 and April 12 (Exam 2)

Please note: If there are any typos, please post about them on Piazza. The latest corrections to the solutions will be available there.

Section 5.2

10. (a) Using the Corollary, if p is a prime $a \equiv a^p \equiv b^p \equiv b \pmod{p}$

11. (a) Each term in the sum is congruent 1 modulo p, so this is $(p-1)\cdot 1 \equiv -1 \pmod{p}$

    (b) The sum is congruent to $1+2+\cdots+(p-1) = \frac{p(p-1)}{2}$. Since p is odd, 2 divides $p-1$ so $\frac{p(p-1)}{2} = pk$ for k an integer, and is therefore congruent to 0 modulo p.

14. Use the Chinese Remainder Theorem to consider the congruence first modulo p and then modulo q.

Section 5.3

1. (a) Similar to Homework 6, problem 1, the case for $p = 23$.

3. The pairs are $(2,12), (3,8), (4,6), (5,14), (7,10), (9,18), (11,21), (13,16), (15,20), (17,19)$

9. To prove the hint, replace each even integer a with the odd integer $-(p-a) \equiv a \pmod{p}$. Collecting the negative signs, this will give a factor of $(-1)^{(p-1)/2}$.

11. In the proof of Theorem 5.5, it says that

$$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2,$$

so the answer they are looking for is

$$\pm\left(\frac{p-1}{2}\right)!$$

When $p = 29$, this is 12 and 17, and when $p = 37$ this is 6 and 31.

Section 6.1

2. We have $12378 = 2 \cdot 3 \cdot 2063$ and $3054 = 2 \cdot 3 \cdot 509$ so $\gcd(12378, 3054) = 6$ and $\operatorname{lcm}(12378, 3054) = 2 \cdot 3 \cdot 509 \cdot 2053 = 6300402$.

12. (a) Recall that if $n = p_1^{k_1} \dots p_r^{k_r}$ with $k_i \geq 1$, then $\tau(n) = (k_1+1)\cdots(k_r+1)$. Note that we cannot have $k_i + 1 = 1$, because $k_i \neq 0$. Therefore if $\tau(n) = 10$, then either n is divisible by one prime with $k_1 = 9$ or n is divisible by two primes with $k_1 = 1$ and $k_2 = 4$. Therefore n is of the form p^9 for p prime or of the form $p_1 p_2^4$, for p_1 and p_2 distinct primes. The smallest integer for which $\tau(n) = 10$ is $48 = 3 \cdot 2^4$.

17. See Homework 6 # 4 (a) plus the proof in class that $f(n) = n$ is multiplicative.

19. Similar to Homework 6 # 4 (a)

Section 6.2

1. (a) One of n, $n+1$, $n+2$, $n+3$ must be divisible by $4 = 2^2$.

Section 7.2

1. $\varphi(1001) = 720$, $\varphi(5040) = 1152$, $\varphi(36000) = 9600$.

7. (b) First note that if p is any prime, then

$$1 - \frac{1}{p} \geq 1 - \frac{1}{2} = \frac{1}{2},$$

because $p \geq 2$.
Then if $n = p_1^{k_1} \dots p_r^{k_r}$ with $k_i \geq 1$, then

$$\begin{aligned} \phi(n) &= n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\ &\geq n\left(\frac{1}{2}\right)^r = \frac{n}{2^r} \end{aligned}$$

Section 7.3

3. For each $n = 5, 7, 8, 9, 13$ separately, show that $a^{15} \equiv a^3 \pmod{n}$. For $n = 5$, this follows from $a^5 \equiv a \pmod{5}$ (Corollary on page 88) then cube both sides. For $n = 7$, Corollary again then square both sides and multiply both sides by a. For $n = 13$, Corollary once more then multiply both sides by a^2. For $n = 8$ you must do a even and a odd separately and the argument is similar to Homework 8 # 2. Finally for $n = 9$ you must do $\gcd(a, 3) = 1$ separately from $\gcd(a, 3) = 3$; when $\gcd(a, 3) = 1$, $a^7 \equiv a \pmod{9}$ then square and multiply both sides by a.

5. Do m and n separately then Chinese Remainder Theorem. We do it for m, it is exactly the same for n: $m^{\phi(n)} \equiv 0 \pmod{m}$ since $\phi(n) \geq 1$ and $n^{\phi(m)} \equiv 1 \pmod{m}$ since $\gcd(m, n) = 1$.

7. See the solutions to Quiz 18.

Section 8.1

1. (a) 2 has order 8, 3 has order 16 and 5 has order 16 (so 3 and 5 are primitive roots of 17 but 2 is not)

   (b) 2 has order 18, 3 has order 18 and 5 has order 9 (so 2 and 3 are primitive roots of 19 but 5 is not)

   (c) 2 has order 11, 3 has order 11 and 5 has order 22 (so 5 is a primitive root of 23 but 2 and 3 are not)

2. (a) If the order of a^h were smaller then the order of a would be smaller.

   (b) $x = a^k$ is such that $x^2 \equiv 1 \pmod{p}$, but since p is a prime this quadratic equation only has solutions $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$. If x were $1 \pmod{p}$, then the order of a would be k, not $2k$.

3. Let $m = 2^n - 1$. Then $2^n \equiv 1 \pmod{m}$ but no smaller power of 2 is 1 modulo m, because if say 2^k for $1 \leq k < m$ were 1 modulo m, then m would divide $2^k - 1$, but $0 < 2^k - 1 < 2^n - 1 = m$ which is a contradiction. Therefore 2 has order n modulo $m = 2^n - 1$. By Theorem 8.1, this means that n divides $\varphi(2^n - 1)$.

   (b) The orders are 4, 2, 4, 4, 2, 4, and 2 respectively, whereas $\phi(15) = 8$.

11. (a) 10 only has two primitive roots and they are 3 and 7.

    (b) $\varphi(17) = 16$, so by Theorem 8.3 3^h has order 16 if and only if $\gcd(h, 16) = 1$. Therefore the other primitive roots are $3^3 \equiv 10 \pmod{17}$, $3^5 \equiv 5 \pmod{17}$, $3^7 \equiv 11 \pmod{17}$, $3^9 \equiv 14 \pmod{17}$, $3^{11} \equiv 7 \pmod{17}$, $3^{13} \equiv 12 \pmod{17}$, and $3^{15} \equiv 6 \pmod{17}$.

Section 8.4

1. The primitive roots of 13 are 2, $2^5 \equiv 6 \pmod{13}$, $2^7 \equiv 11 \pmod{13}$ and $2^{11} \equiv 7 \pmod{13}$. Using brute force (i.e. computing all of the powers of these primitive roots until we get 5), we have that $\log_2 5 \equiv \log_6 5 \equiv 9 \pmod{12}$ and $\log_{11} 5 \equiv \log_7 5 \equiv 3 \pmod{12}$.

3. (a) $x \equiv 3, 5, 14, 12 \pmod{17}$

   (b) $x \equiv 5 \pmod{17}$

   (c) $x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$

   (d) $x \equiv 1 \pmod{16}$

8.4

#3 a) $x \equiv 3^k \bmod 17$ $\quad x^{12} \equiv 3^{12k} \bmod 17$

$13 \equiv 3^4 \bmod 17$

$$3^{12k} \equiv 3^4 \bmod 17$$

$\Rightarrow 12k \equiv 4 \bmod 16$ $\quad \gcd(12,16) = 4$

$\Rightarrow 3k \equiv 1 \bmod 4$

$\Rightarrow k \equiv 3 \bmod 4$

$\Rightarrow k \equiv 3, 7, 11, 15 \bmod 16$

So $x \equiv 10, 11, 7, 6 \bmod 17$

b) $x \equiv 3^k \bmod 17$ $\quad x^5 \equiv 3^{5k} \bmod 17$

$8 \equiv 3^{10} \bmod 17$

$10 \equiv 3^3 \bmod 17$

$$3^{10} \cdot 3^{5k} \equiv 3^3 \bmod 17$$

$$5k + 10 \equiv 3 \bmod 16$$

$$5k \equiv -7 \bmod 16$$

$$k \equiv 5 \bmod 16$$

So $x \equiv 5 \bmod 17$

c) $x \equiv 3^k \mod 17$ $\quad x^8 \equiv 3^{8k} \mod 17$

$9 \equiv 3^2 \mod 17$

$8 \equiv 3^{10} \mod 17$

$$3^2 \cdot 3^{8k} \equiv 3^{10} \mod 17$$

$$8k+2 \equiv 10 \mod 16$$

$$8k \equiv 8 \mod 16 \quad \gcd(8,16)=8$$

$$k \equiv 1 \mod 2$$

$$k \equiv 1, 3, 5, 7, 9, 11, 13, 15 \mod 16$$

$$x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \mod 17$$

d) Because 7 is also a primitive root of 17 we can do

$$7^x \equiv 7 \mod 17$$

$$\Rightarrow \quad x \equiv 1 \mod 16$$

If it were not this would not work!

Example: $9^x \equiv 9 \mod 17$

$$\Rightarrow x \equiv 1 \mod 8$$

since 9 has order 8 not 16.