Math 255 - Spring 2018
Homework 12 Solutions

1. By Theorem 2 of Section 10, if there is a with order $m-1$ modulo m, then $m-1$ divides $\phi(m)$. In particular, this means that on the one hand $m-1 \leq \phi(m)$.

   On the other hand, recall that $\phi(m)$ is the number of units in $\mathbb{Z}/m\mathbb{Z}$. This set contains m elements, and one of them is 0, which is never a unit. From this it follows that in any case $\phi(m) \leq m-1$.

   We conclude that in this particular situation, $\phi(m) = m-1$, or in other words every element $1, 2, \ldots, m-1$ is relatively prime to m. If m is composite, then there is d with $1 < d < m$ and d divides m. In that case d is not relatively prime to m. Therefore, for every element $1, 2, \ldots, m-1$ to be relatively prime to m, it must be the case that m has no divisor other than 1 and itself, and so m is prime.

2. We first note that if g is a primitive root of p, then g is a unit modulo p by definition. Therefore, by Theorem 5 of Section 10 there is k an integer (in fact $1 \leq k \leq \phi(p) = p-1$) with $g \equiv h^k \pmod{p}$, since h is also a primitive root of p.

   We now apply Lemma 1 of Section 10: $g \equiv h^k \pmod{p}$ has order $p-1$, since it is a primitive root of p, and therefore it follows that $(k, p-1) = 1$. Suppose now for a contradiction that k were even. In that case, since $p-1$ is also even (recall that p is odd), it would be the case that $(k, p-1) \geq 2$. Therefore k must be odd.

3. Recall that to show that $a+1$ has order 6, we must show not only that $(a+1)^6 \equiv 1 \pmod{p}$, but also that no smaller power of $a+1$ is congruent to 1 modulo p.

   However, it still pays to begin by showing that $(a+1)^6 \equiv 1 \pmod{p}$, for reasons that we will explain later. So we begin by showing that. Recall throughout that since a has order 3 modulo p, we have that $a^3 \equiv 1 \pmod{p}$. We also note that per the hint, since $a \not\equiv 1 \pmod{p}$ (we know that is not the case since 1 has order 1 modulo p, and a has order 3) we have that $a^2 + a + 1 \equiv 0 \pmod{p}$. Therefore we can compute

$$\begin{aligned}
(a+1)^6 &\equiv a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1 \pmod{p} \\
&\equiv 1 + 6a^2 + 15a + 20 + 15a^2 + 6a + 1 \pmod{p} \\
&\equiv 21a^2 + 21a + 22 \pmod{p} \\
&\equiv 21(a^2 + a + 1) + 1 \pmod{p} \\
&\equiv 1 \pmod{p}.
\end{aligned}$$

   As we remarked above, this does not conclude the proof, since a smaller power of $a+1$ could be congruent to 1 modulo p. However, we did acquire the following knowledge: By Theorem 1, since $(a+1)^6 \equiv 1 \pmod{6}$, it follows that the order of $a+1$ divides 6. Therefore it can only be 1, 2, 3 or 6. If we can eliminate the possibilities 1, 2 and 3, the result will follow.

We first consider the possibility that $a+1$ has order 1 modulo p. If that were the case, then $a+1 \equiv 1 \pmod{p}$, and we would have $a \equiv 0 \pmod{p}$, which is not a unit modulo p. Therefore a could not have order 3 modulo p (the order of a number modulo m is only defined if this number is a unit) and so $a+1$ does not have order 1 modulo p.

We now consider the possibility that $a+1$ has order 2 modulo p. In that case we would have $(a+1)^2 \equiv a^2+2a+1 \equiv a^2+a+1+a \equiv a \equiv 1 \pmod{p}$. (Here we used that $a^2+a+1 \equiv 0 \pmod{p}$ again.) But $a \not\equiv 1 \pmod{p}$, so this is not possible.

Finally we consider the possibility that $a+1$ has order 3 modulo p. But that is not possible since $(a+1)^3 \equiv a^3+3a^2+3a+1 \equiv 1+3(a^2+a+1)-3+1 \equiv -1 \pmod{p}$, and if p is odd, then $1 \not\equiv -1 \pmod{p}$.

Therefore $a+1$ must have order 6 modulo p.

4. (a) We consider two cases: Either n is divisible by an odd prime, or n is not divisible by an odd prime.

   If n is divisible by an odd prime, say p, write $n = p^e m$, with $(p,m) = 1$. Then we have

$$\begin{aligned}\phi(n) &= \phi(p^e)\phi(m) \\ &= (p^e - p^{e-1})\phi(m).\end{aligned}$$

   We note that $p^e - p^{e-1}$ is the difference of two odd numbers (if p is odd and $e \geq 1$, then so are p^e and p^{e-1}) and therefore $p^e - p^{e-1} \equiv 1 - 1 \equiv 0 \pmod{2}$. In other words, $p^e - p^{e-1}$ is even, and a product of an even number and an integer is even, so $\phi(n)$ is even.

   If n is not divisible by an odd prime, then n is only divisible by even primes, but there is only one even prime. It follows that $n = 2^e$ for some $e \geq 2$ (remember that $n > 2$). In that case

$$\begin{aligned}\phi(n) = \phi(2^e) &= 2^e - 2^{e-1} \\ &= 2(2^{e-1} - 2^{e-2}),\end{aligned}$$

   and $2^{e-1} - 2^{e-2}$ is an integer since $e \geq 2$. Therefore $\phi(n)$ is even in this case as well.

   (b) We show the existence of such an a by exhibiting it: If $a \equiv -1 \pmod{n}$, then $(a,n) = 1$. Furthermore, if $n > 2$, then $a \equiv -1 \not\equiv 1 \pmod{n}$, so a does not have order 1 modulo n. However, $a^2 \equiv (-1)^2 \equiv 1 \pmod{n}$, so a has order 2. By Theorem 2 of Section 10, the order of $a \equiv -1 \pmod{n}$ divides $\phi(n)$, and therefore $\phi(n)$ is even.

5. Let g be a primitive root of m. In this case, by Theorem 5, we have

$$\prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} a \equiv \prod_{i=1}^{\phi(m)} g^i \pmod{m}.$$

By exponent laws and using the formula $\sum_{i=1}^{\phi(m)} i = \frac{\phi(m)(\phi(m)+1)}{2}$, we therefore have

$$\prod_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} a \equiv g^{\frac{\phi(m)(\phi(m)+1)}{2}} \pmod{m}.$$

Now if $m = 2$, then $\phi(m) = 1$ and this product is $g \pmod 2$. Since g is a primitive root of 2, it must be that $g \equiv 1 \pmod 2$, but $1 \equiv -1 \pmod 2$, so the result follows.

Consider now $m > 2$. By problem 4, $\phi(m)$ is then even and $\phi(m) + 1$ is odd. In particular, $\frac{\phi(m)}{2}$ is an integer, and we can write

$$g^{\frac{\phi(m)(\phi(m)+1)}{2}} \equiv (g^{\phi(m)+1})^{\phi(m)/2} \equiv g^{\phi(m)/2} \pmod{m},$$

since $g^{\phi(m)} \equiv 1 \pmod m$.

If we are willing to use Problem 2 of Homework 11, we are now done, since $g^{\phi(m)/2} \not\equiv 1 \pmod m$, because g is a primitive root of m and $\phi(m)/2$ is less than $\phi(m)$, the order of g. Therefore $g^{\phi(m)/2} \equiv -1 \pmod m$, and the claim is proved.

We can also obtain the result without appealing to our earlier work by showing directly that $g^{\phi(m)/2} \equiv -1 \pmod m$. By Theorem 5 of Section 10, because -1 is a unit modulo m, there is an integer k with $1 \leq k \leq \phi(m)$ with $-1 \equiv g^k \pmod m$. Then $1 \equiv (-1)^2 \equiv g^{2k} \pmod m$. It follows that $2k \equiv 0 \pmod{\phi(m)}$, and since $\phi(m)$ is even, we can divide all the way through by 2 to obtain the equation $k \equiv 0 \pmod{\phi(m)/2}$. In other words k is divisible by $\phi(m)/2$. In the range $1 \leq k \leq \phi(m)$, this forces $k = \phi(m)/2$ or $k = \phi(m)$, but we know that $k \neq \phi(m)$, since $g^{\phi(m)} \equiv 1 \pmod m$ but $g^k \equiv -1 \pmod m$. Therefore, if $-1 \equiv g^k \pmod m$ then $k = \phi(m)/2$, and $g^{\phi(m)/2} \equiv -1 \pmod m$.