Math 255 - Spring 2017
Homework 8 Solutions

1. If $n = 2$ then the product contains only the element 1 and we are done. Therefore we now let $n > 2$. By definition for each $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, there is $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

$$aa^{-1} \equiv 1 \pmod{n}.$$

We divide the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ into two sets: The first set has $a^{-1} \not\equiv a \pmod{n}$, and the second set has $a^{-1} \equiv a \pmod{n}$. Since each element of $(\mathbb{Z}/n\mathbb{Z})^\times$ must be in one set or the other, we have that

$$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a = \prod_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^\times \\ a^{-1} \not\equiv a \pmod{n}}} a \cdot \prod_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^\times \\ a^{-1} \equiv a \pmod{n}}} a.$$

We compute each product separately.

To compute the first product, we claim that the elements of the first set above can be split up into pairs (a, b) with $ab \equiv 1 \pmod{n}$ and $a \not\equiv b \pmod{n}$. Indeed, if $ab \equiv 1 \pmod{n}$, then b is none other than the unique element $a^{-1} \pmod{n}$. We claim that if a is in the first set, then a^{-1} is also in the first set, and therefore appears in the first product. If a belongs to the first set, then $a^{-1} \not\equiv a \pmod{n}$. Then because $(a^{-1})^{-1} \equiv a \pmod{n}$, it is also the case that a^{-1} is not congruent to its inverse (which is a), so a^{-1} is also in the first set. This shows that the pairs (a, b) do partition the first set in a unique and well-defined way, and since the product of many factors of 1 is 1, we have

$$\prod_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^\times \\ a^{-1} \not\equiv a \pmod{n}}} a \equiv 1 \pmod{n}.$$

Now we consider the second product. The argument above will not work since each element a does not appear twice. Instead, we claim that the elements of the second set can be split up into pairs (a, b) with $b \equiv -a \pmod{n}$. First, we notice that given a, $-a \pmod{n}$ is unique and different from a since $n \neq 2$. Secondly, we claim that if a is in the second set, then $-a$ is also in the second set. Indeed, if $a^{-1} \equiv a \pmod{n}$, then $a^2 \equiv 1 \pmod{n}$ and $(-a)^2 \equiv 1 \pmod{n}$ as well. Therefore $-a$ is also in the second set. This proves that these pairs do partition the second set in a unique and well-defined way. We now notice that in this case, $ab \equiv -1 \pmod{n}$, since $b \equiv -a \pmod{n}$ so

$$ab \equiv a(-a) \equiv -a^2 \equiv -1 \pmod{n}.$$

Therefore, the second product is a product of a certain number of factors of -1, and

$$\prod_{\substack{a \in (\mathbb{Z}/n\mathbb{Z})^\times \\ a^{-1} \equiv a \pmod{n}}} a \equiv \pm 1 \pmod{n},$$

depending on whether we can make an even or an odd number of pairs (a, b). This completes the proof.

We take this opportunity to note that later in the semester we will learn how to find all solutions to the equation $x^2 \equiv 1 \pmod{n}$. If $f(n)$ is the number of solutions of this equation, then $f(n)$ is even, and

$$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a \equiv (-1)^{f(n)/2} \pmod{n}.$$

In particular if n is prime, then $f(n) = 2$ and $\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a = (n-1)!$ and we recover Wilson's Theorem.

2. Since the divisors of 10 are $1, 2, 5$ and 10, if a is any integer then the possibilities for $\gcd(a, 10)$ are also $1, 2, 5$ and 10. We tackle each of these possibilities in turn, and show that in each case $a^{4n+1} \equiv a \pmod{10}$, which is equivalent to saying that a^{4n+1} and a have the same last digit.

   Suppose first that $\gcd(a, 10) = 1$. Then by Euler's Theorem, $a^{\varphi(10)} \equiv 1 \pmod{10}$. Since
$$\varphi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4,$$
   this means that $a^4 \equiv 1 \pmod{10}$. Raising both sides to the nth power for n a positive integer, we get $a^{4n} \equiv 1 \pmod{10}$. Now multiplying both sides by a, we get $a^{4n+1} \equiv a \pmod{10}$, and we are done.

   Suppose now that $\gcd(a, 10) = 2$. As a consequence, we have that $a \equiv 0 \pmod{2}$ (since 2 divides a) and $\gcd(a, 5) = 1$ (since 5 is prime and it does not divide a; if 5 divided a then 10 would divide a and we would have $\gcd(a, 10) = 10$, not 2). This suggests that we should consider the congruence of a^{4n+1} modulo 2 and 5 separately, and use the Chinese Remainder Theorem. We first note that if 2 divides a, then 2 also divides a^{4n+1} for any positive integer n. Therefore $a^{4n+1} \equiv 0 \equiv a \pmod{2}$. To compute $a^{4n+1} \pmod{5}$, we note that $\varphi(5) = 4$, so $a^4 \equiv 1 \pmod{5}$, and by the same argument used above, $a^{4n+1} \equiv a \pmod{5}$. Now we have that $a^{4n+1} \equiv a \pmod{2}$ and $a^{4n+1} \equiv a \pmod{5}$, and so by the Chinese Remainder Theorem, since 2 and 5 are relatively prime, it follows that $a^{4n+1} \equiv a \pmod{10}$.

   Let's move on now to the case of $\gcd(a, 10) = 5$. By a similar argument as above since 2 is also prime, we have as a consequence that $a \equiv 0 \pmod{5}$ and $\gcd(a, 2) = 1$. With the same argument as above, 5 also divides a^{4n+1} so $a^{4n+1} \equiv a \equiv 0 \pmod{5}$. On the other hand, since a is odd, we have $a \equiv 1 \pmod{2}$, and raising both sides to the $(4n+1)$th power gives $a^{4n+1} \equiv 1 \equiv a \pmod{2}$. Since $a^{4n+1} \equiv a \pmod{2}$ and $a^{4n+1} \equiv a \pmod{5}$ in this case as well, we can conclude with the Chinese Remainder Theorem that $a^{4n+1} \equiv a \pmod{10}$.

   The last case is $\gcd(a, 10) = 10$, or in other words the case that 10 divides a. In that case $a \equiv 0 \pmod{10}$ and raising both sides to the power of $4n + 1$ gives $a^{4n+1} \equiv 0 \equiv a \pmod{10}$, which is what we needed to prove.

3. First, for the order of a to be defined modulo n, it must be the case that $\gcd(a, n) = 1$. Therefore by Euler's Theorem $a^{\varphi(n)} \equiv 1 \pmod{n}$. Since the order of a is the least positive integer k such that $a^k \equiv 1 \pmod{n}$, it follows therefore that $n - 1 \leq \varphi(n)$.

   Now, recall that $\varphi(n)$ is the number of units in $\mathbb{Z}/n\mathbb{Z}$. Since 0 is never a unit and $\mathbb{Z}/n\mathbb{Z}$ contains n elements, there are always at most $n-1$ units in $\mathbb{Z}/n\mathbb{Z}$. In other words, for all n, $\varphi(n) \leq n - 1$.

   Putting together our two inequalities, we have that for the n we are considering, $\varphi(n) = n-1$. This means that every element of $\mathbb{Z}/n\mathbb{Z}$ except for 0 is a unit, or in other words that every integer ℓ with $1 \leq \ell \leq n-1$ is relatively prime to n. In particular, the only divisor of n that is strictly less than n is 1. As we have shown in class, this is equivalent to saying that n is prime.