Math 255 - Spring 2018
Homework 11 Solutions

1. The last two digits of any positive integer is the least residue of this integer modulo 100. Therefore we essentially want to compute $2018^{2018} \pmod{100}$. Since 100 is not a prime, we cannot use Fermat's Little Theorem. Furthermore, 100 and 2018 are not relatively prime (2 divides both of them) so we cannot apply Euler's Theorem directly. However, we can still finesse something by factoring 100 into its prime-power factors. In other words, we will compute $2018^{2018} \pmod{4}$ and $2018^{2018} \pmod{25}$.

   We begin with $2018^{2018} \pmod{4}$. Again we note that $(4, 2018) = 2 \neq 1$, so we cannot apply Euler's Theorem. Still this is not such a big deal, because arithmetic modulo 4 is simple. Indeed, $2018 \equiv 2 \pmod{4}$, so we are interested in computing $2^{2018} \pmod{4}$. Here we notice that already $2^2 \equiv 0 \pmod{4}$, and $2^{2018} = 2^2 \cdot 2^{2016}$. Therefore, $2^{2018} \equiv 0 \pmod{4}$, since it is certainly divisible by 4.

   We now turn our attention to $2018^{2018} \pmod{25}$. This time, $(2018, 25) = 1$, so we can apply Euler's Theorem. We have that $\phi(25) = 25 - 5 = 20$, so $2018^{20} \equiv 1 \pmod{25}$. Since we have that $2018 = 20 \cdot 100 + 18$, it follows that $2018^{2018} \equiv 2018^{18} \pmod{25}$. Furthermore, since $2018 \equiv 18 \pmod{25}$, we conclude that $2018^{2018} \equiv 18^{18} \pmod{25}$.

   This is not super easy to compute, but it is certainly possible:

$$\begin{aligned} 18^{18} &= (18^2)^9 \\ &\equiv ((-7)^2)^9 \pmod{25} \\ &\equiv 49^9 \pmod{25} \\ &\equiv (-1)^9 \pmod{25} \\ &\equiv -1 \equiv 24 \pmod{25}. \end{aligned}$$

   Therefore, we now know that $2018^{2018} \equiv 0 \pmod{4}$ and $2018^{2018} \equiv 24 \pmod{25}$. The unique number, modulo 100, that is both $0 \pmod{4}$ and $24 \pmod{25}$ is in fact 24 itself. (We can see this either using the Chinese Remainder Theorem, or in the following quick way: There are four lifts of $24 \pmod{25}$ to $\mathbb{Z}/100\mathbb{Z}$: $24, 49, 74$ and 99. Only one of these is $0 \pmod{4}$ (actually, note that there is one that is $0 \pmod{4}$, one that is $1 \pmod{4}$, one that is $2 \pmod{4}$ and one that is $3 \pmod{4}$; that is a consequence of the Chinese Remainder Theorem), and that is $24 \pmod{100}$).

   Therefore the last two digits of 2018^{2018} are 24. This agrees with Homework 10 in which we showed that the last digit was 4.

2. We first handle the case of $n = 2$ separately, for reasons that will only become clear much later. Since the only element of $(\mathbb{Z}/2\mathbb{Z})^\times$ is 1, the product is 1.

   Now let $n \geq 3$. To solve this problem, we will partition this product into two:

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

and consider each product separately.

The first product is 1, by an argument similar to the one used in the proof of Wilson's Theorem. Indeed, consider the set

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

We have that the following additional two facts are true about the elements of S:

- If $a \in S$, then $a^{-1} \in S$ as well. This follows because $(a^{-1})^{-1} \equiv a \pmod{n}$.
- If $a, b \in S$ and $a \not\equiv b \pmod{n}$, then $a^{-1} \not\equiv b^{-1} \pmod{n}$. This is because if $a^{-1} \equiv b^{-1} \pmod{n}$, then

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

Therefore, the elements of S can be partitioned into pairs (a, a^{-1}), by which we mean that both elements of the pair belong to S, each element of S belongs to one and only one pair, and no pair contains two identical element. Since the product of each pair is 1, and 1 raised to an arbitrary exponent is 1, the first product is 1.

We now turn our attention to the second product. We will use a similar argument, except this time since $a \equiv a^{-1} \pmod{n}$, we must modify the pairs (because our old pairs would just be singletons here). Let

$$T = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a \equiv a^{-1} \pmod{n}\}.$$

We now show that this set can be partitioned into pairs $(a, -a)$. We follow an approach similar to the one we used for the set S. To help us, we note that $a \equiv a^{-1} \pmod{n}$ if and only if $a^2 \equiv 1 \pmod{n}$ (this is true because we can multiply both sides by a, and a is a unit in $\mathbb{Z}/n\mathbb{Z}$ by assumption). The following three facts are true:

- For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $a \not\equiv -a \pmod{n}$. This is because if it were, then we would have $2a \equiv 0 \pmod{n}$, but since $(a, n) = 1$, this forces $2 \equiv 0 \pmod{n}$ or n divides 2. This is not the case since $n \geq 3$.
- If $a \in T$, then $-a \in T$ as well. This follows because $(-a)^2 \equiv a^2 \equiv 1 \pmod{n}$.
- If $a, b \in T$ and $a \not\equiv b \pmod{n}$, then $-a \not\equiv -b \pmod{n}$. This is because -1 is a unit modulo n.

Therefore, the elements of T can be partitioned into pairs $(a, -a)$, where again we mean that no pair contains two identical elements, both elements of the pair belong to T, and each element belongs to one and only one pair.

The product of each such pair is

$$a \cdot (-a) \equiv -a^2 \equiv -1 \pmod{n},$$

(we recall that if $a \in T$, then $a^2 \equiv 1 \pmod{n}$), and therefore the second product is either 1 or -1, depending on how many pairs are contained in the set T.

Therefore we have

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

3. (a) We have that

$$\begin{aligned} \phi(n) &= n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \\ &= pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \\ &= (p-1)(q-1). \end{aligned}$$

(b) We are now in the situation where we know that $n = pq$ for distinct primes p and q, and we know the value of $\phi(n) = (p-1)(q-1)$. Expanding $\phi(n)$, we get

$$\phi(n) = pq - p - q + 1 = n - (p+q) + 1.$$

Therefore, we have that

$$p + q = n - \phi(n) + 1,$$

and since we know n and $\phi(n)$, we know $p + q$.

(c) We have that

$$x^2 - (p+q)x + n = x^2 - (p+q) + pq = (x-p)(x-q).$$

Therefore, knowing n and $\phi(n)$ we can get $p+q$, and therefore the polynomial $x^2 - (p+q)x + n$. From there, we can use the quadratic formula to compute the two roots of this polynomial, and get p and q. (Actually, in real life Newton's method would be a much faster and easier way to get p and q, especially since it converges quickly and we know *a priori* that the roots are integers.)

(d) We apply the algorithm. First we have that if $4399 = pq$, then

$$p + q = n - \phi(n) + 1 = 4399 - 4264 + 1 = 136.$$

Then we form the polynomial $x^2 - (p+q)x + n$, which here is

$$x^2 - 136 + 4399.$$

Using the quadratic formula, we have that the roots of this polynomial are

$$\begin{aligned}\frac{136 \pm \sqrt{136^2 - 4 \cdot 4399}}{2} &= \frac{136 \pm \sqrt{18496 - 4 \cdot 17596}}{2} \\ &= \frac{136 \pm \sqrt{900}}{2} \\ &= \frac{136 \pm 30}{2}.\end{aligned}$$

We therefore get that

$$p = \frac{136 - 30}{2} = \frac{106}{2} = 53$$

and

$$q = \frac{136 + 30}{2} = \frac{166}{2} = 83,$$

and from this it follows that

$$4399 = 53 \times 83.$$

4. (a) Since there are natural maps

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ a &\mapsto a,\end{aligned}$$

and

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto a,\end{aligned}$$

given by "reducing more," (these are the maps we discussed in class before discussing lifting) there is also a natural map

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto (a, a),\end{aligned}$$

given by reducing a modulo m in the first factor and reducing a modulo n in the second factor. Using the Chinese Remainder Theorem, we can prove that this map is a bijection. (We can use CRT since $(m, n) = 1$.)

We first show that it is surjective. This is because by CRT any pair of congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ corresponds to an element $x \equiv c \pmod{mn}$. Here by "correspond" we mean exactly that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$, and therefore any pair $(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has a preimage in $\mathbb{Z}/mn\mathbb{Z}$ under this map.

Secondly, this map is injective, because any pair of congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ corresponds to a **unique** element $x \equiv c \pmod{mn}$. Therefore there cannot be c_1 and $c_2 \in \mathbb{Z}/mn\mathbb{Z}$ that map to the same pair $(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, or this would violate the uniqueness in the statement of CRT.

Therefore, the map we gave above is a bijection. (In fact, we could show more, it is a ring homomorphism.)

We now show that if we restrict both sides to the units, the map is still well-defined and surjective. In other words, $a \in \mathbb{Z}/mn\mathbb{Z}$ is a unit if and only if both $a \in \mathbb{Z}/m\mathbb{Z}$ and $a \in \mathbb{Z}/n\mathbb{Z}$ are units.

In the first direction, if $a \in \mathbb{Z}/mn\mathbb{Z}$ is a unit, then $(a, mn) = 1$, and therefore $(a, m) = 1$ and $(a, n) = 1$. (This can be shown by contradiction; if either of these statements were not true, then the common divisor of a and m or of a and n would also be a common divisor of a and mn.) This shows that the map is still well-defined after restricting the domain and codomain.

In the second direction, if $a \in \mathbb{Z}/m\mathbb{Z}$ and $a \in \mathbb{Z}/n\mathbb{Z}$ are both units, then $a \in \mathbb{Z}/mn\mathbb{Z}$ is also a unit. Indeed, suppose that p is a prime that divides both a and mn (so that $(a, mn) \neq 1$). Then p divides mn and therefore p divides m or n, from which it follows that p divides either (a, m) or (a, n), a contradiction. This shows that the map remains surjective after restricting the domain, because each element of the image still has a preimage.

Note that we do not need to show that the restriction to units is injective, as the restriction of an injective map is always injective.

In conclusion, the map

$$\begin{aligned}(\mathbb{Z}/mn\mathbb{Z})^\times &\to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \\ a &\mapsto (a, a),\end{aligned}$$

is a bijection.

(b) This is now easy: Because both sets are finite, a bijection between them establishes that the sets are the same size. $\phi(mn)$ is the size of $(\mathbb{Z}/mn\mathbb{Z})^\times$, and by definition of the Cartesian product, the set $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ has size $\phi(m)\phi(n)$.