Math 255 - Spring 2018
Homework 10 Solutions

1. Here 26 is not a prime, so we may not use Fermat's Little Theorem directly. However, if we can compute the least residue of $2018^{2018} \pmod 2$ and $2018^{2018} \pmod{13}$ (and those are primes so maybe we'll get to use Fermat's Little Theorem), then using the Chinese Remainder Theorem we will be able to obtain the least residue of $2018^{2018} \pmod{26}$.

   First we notice that $2018 \equiv 0 \pmod 2$, so $2018^{2018} \equiv 0^{2018} \equiv 0 \pmod 2$.

   Next, we consider $2018^{2018} \pmod{13}$. We can apply Fermat's Little Theorem since $(2018, 13) = 1$. We first note that $2018 = 12 \times 168 + 2$ and $2018 = 13 \times 155 + 3$, so that $2018 \equiv 3 \pmod{13}$. Therefore we have

$$\begin{aligned} 2018^{2018} &\equiv 3^{12\times 168+2} \pmod{13} \\ &\equiv (3^{12})^{168} \cdot 3^2 \pmod{13} \\ &\equiv 1^{168} \cdot 9 \pmod{13} \\ &\equiv 9 \pmod{13} \end{aligned}$$

   Therefore, $2018^{2018} \equiv 0 \pmod 2$ and $2018^{2018} \equiv 9 \pmod{13}$. It might be clear that $22 \pmod{26}$ satisfies both these congruences, and therefore $2018^{2018} \equiv 22 \pmod{26}$, but if that is not clear, we can use the Chinese Remainder Theorem algorithm.

   Here M_1 and x_1 don't matter since $a_1 = 0$, and $M_2 = 2$ and $x_2 \equiv 2^{-1} \equiv 7 \pmod{13}$. Therefore

$$\begin{aligned} 2018^{2018} &\equiv 0 + 9 \cdot 2 \cdot 7 \pmod{26} \\ &\equiv 126 \pmod{26} \\ &\equiv 22 \pmod{26}. \end{aligned}$$

2. Here we begin by noting that the last digit of 2018^{2018} is the least residue of 2018^{2018} modulo 10. Sadly, once again 10 is not a prime, so we cannot use Fermat's Little Theorem. But as in problem 1, if we can figure out $2018^{2018} \pmod 2$ and $2018^{2018} \pmod 5$, then using the Chinese Remainder Theorem we will obtain $2018^{2018} \pmod{10}$, and therefore the last digit.

   Again we have $2018 \equiv 0 \pmod 2$, so $2018^{2018} \equiv 0^{2018} \equiv 0 \pmod 2$.

   Next, we consider $2018^{2018} \pmod 5$. We can apply Fermat's Little Theorem since $(2018, 5) = 1$. We have $2018 \equiv 3 \pmod 5$ and $2018 = 4 \times 504 + 2$, so

$$\begin{aligned} 2018^{2018} &\equiv 3^{4\times 504+2} \pmod 5 \\ &\equiv (3^4)^{504} \cdot 3^2 \pmod{13} \\ &\equiv 1^{504} \cdot 9 \pmod{13} \\ &\equiv 4 \pmod 5 \end{aligned}$$

Therefore, $2018^{2018} \equiv 0 \pmod 2$ and $2018^{2018} \equiv 4 \pmod 5$. It might be clear that 4 (mod 10) satisfies both these congruences, and therefore the last digit of 2018^{2018} is 4. Of course, if that is not clear, we can use the Chinese Remainder Theorem algorithm, which we leave to the reader.

(Note that this is cool, because 2018^{2018} is a number with more than 6,500 digits! That we can compute the last one without computing the whole giant number is neat.)

3. By Wilson's Theorem, we have that

$$(p-1)! \equiv -1 \pmod p.$$

We also note that

$$\begin{aligned}(p-1)! &= (p-3)!(p-2)(p-1) \\ &\equiv (p-3)!(-2)(-1) \pmod p \\ &\equiv 2(p-3)! \pmod p.\end{aligned}$$

Therefore

$$2(p-3)! \equiv -1 \pmod p.$$

From this we easily conclude that

$$2(p-3)! + 1 \equiv 0 \pmod p.$$

4. We note that $437 = 19 \times 23$; it is not a prime! Therefore we will do as in problems 1 and 2, and consider 18! modulo 19 and modulo 23 separately. The Chinese Remainder Theorem will allow us to get the answer we want at the end.

Since 19 is prime, a straightforward application of Wilson's Theorem tells us that $18! \equiv -1 \pmod{19}$.

To compute $18! \pmod{23}$, we will also use Wilson's Theorem, but we will have to work a little bit harder. Wilson's Theorem gives us that

$$22! \equiv -1 \pmod{23}.$$

Similarly to problem 3, we have

$$\begin{aligned}22! &= 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \\ &\equiv 18! \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \pmod{23} \\ &\equiv 18! \cdot 24 \pmod{23} \\ &\equiv 18! \pmod{23}.\end{aligned}$$

Therefore we have

$$18! \equiv 22! \equiv -1 \pmod{23}.$$

In conclusion, $18! \equiv -1 \pmod{19}$ and $18! \equiv -1 \pmod{23}$. Therefore, the Chinese Remainder Theorem tells us that the only class modulo 437 that satisfies both these congruences is $-1 \pmod{437}$. (By uniqueness, since $-1 \equiv -1 \pmod{19}$ and $-1 \equiv -1 \pmod{23}$.) Therefore we have

$$18! \equiv -1 \equiv 436 \pmod{437}.$$

5. (a) We notice that we can write

$$f(n) = \sum_{d|n}(d+1) = \sum_{d|n} d + \sum_{d|n} 1 = \sigma(n) + d(n).$$

Therefore using Theorems 1 and 2 we have, if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power factorization of n, that

$$f(n) = (e_1+1)(e_2+1)\cdots(e_k+1) + \left(\frac{p_1^{e_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{e_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_k^{e_k+1}-1}{p_k-1}\right)$$

(b) We do not expect f to be multiplicative; while a product or quotient of multiplicative functions is multiplicative, a sum or a difference is not, because addition doesn't play that well with multiplication. Another reason why we do not expect f to be multiplicative is that in the formula we got above, we cannot split up $f(n)$ into a product of functions of $p_i^{e_i}$, there is a pesky sum in the middle.

Indeed we may disprove the statement by giving a single counter-example: We have that $(3,4) = 1$ and

$$\begin{aligned} f(3 \cdot 4) = f(12) &= (1+1) + (2+1) + (3+1) + (4+1) + (6+1) + (12+1) \\ &= 2+3+4+5+7+13 \\ &= 34, \end{aligned}$$

but

$$\begin{aligned} f(3) &= (1+1) + (3+1) \\ &= 2+4 \\ &= 6, \end{aligned}$$

and

$$\begin{aligned} f(4) &= (1+1) + (2+1) + (4+1) \\ &= 2+3+5 \\ &= 10. \end{aligned}$$

And we see that

$$f(12) \neq f(3)f(4),$$

despite the fact that $(3,4) = 1$. Therefore f is not multiplicative.

6. (a) We have

$$\begin{aligned} 10! &\equiv -1 \pmod{11} \\ 9!1! &\equiv 1 \pmod{11} \\ 8!2! &\equiv -1 \pmod{11} \\ 7!3! &\equiv 1 \pmod{11} \\ 6!4! &\equiv -1 \pmod{11} \\ 5!5! &\equiv 1 \pmod{11} \end{aligned}$$

(b) We can guess the following theorem: Let p be a prime. Then

$$(p-1-i)!i! \equiv (-1)^{i+1} \pmod{p}.$$

The proof is:

$$\begin{aligned} (p-1-i)!i! &\equiv (-1)^i(-1)^i(p-1-i)!i! \pmod{p} \\ &\equiv (-1)^i(p-1-i)!(-1)^i i! \pmod{p} \\ &\equiv (-1)^i(p-1-i)!(-1)(-2)\dots(-i+1)(-i) \pmod{p} \\ &\equiv (-1)^i(p-(i+1))!(p-1)(p-2)\dots(p-(i-1))(p-i) \pmod{p} \\ &\equiv (-1)^i(p-1)! \pmod{p} \\ &\equiv (-1)^i(-1) \pmod{p} \\ &\equiv (-1)^{i+1} \pmod{p}, \end{aligned}$$

where in the first step we have used that $(-1)^i(-1)^i = ((-1)^i)^2 = 1$.