Math 255 - Spring 2017
Homework 6 Solutions

1. If we show that

$$18! \equiv -1 \pmod{19}$$
$$18! \equiv -1 \pmod{23}$$

then we can apply the Chinese Remainder Theorem: Let $x = 18!$. Then assuming that

$$x \equiv -1 \pmod{19}$$
$$x \equiv -1 \pmod{23}$$

then there is a unique equivalence class modulo 437 that satisfies both of these conditions. We claim that this equivalence class is $x \equiv -1 \pmod{437}$. Indeed, if $x = -1 + 437k$ for $k \in \mathbb{Z}$, then $x = -1 + 19(23k)$ and $x = -1 + 23(19k)$, so $x \equiv -1 \pmod{19}$ and $x \equiv -1 \pmod{23}$. Therefore $x \equiv -1 \pmod{437}$ fits the bill, and by the Chinese Remainder Theorem this solution is unique and so there is nothing further to do.

We now tackle the two congruences: By Wilson's Theorem, since 19 is prime, we have that $18! \equiv -1 \pmod{19}$.

Again by Wilson's Theorem, since 23 is prime, we have that $22! \equiv -1 \mod 23$. On the other hand,

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

since $24 \equiv 1 \pmod{23}$. Therefore we have

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

and our proof is now complete.

2. Let n be composite. Then there is $d_1|n$ with $1 < d_1 < n$. Let $d_2 = \frac{n}{d_1}$. We consider two cases:

Case 1: Suppose that $d_1 \neq d_2$. Note that $1 < d_2 < n$ also, since $1 < d_1 < n$ implies $1 > \frac{1}{d_1} > \frac{1}{n}$, and multiplying all sides by n, which is positive, gives $n > \frac{n}{d_1} > 1$. Since both d_1 and d_2 are strictly between 1 and n and they are unequal, they both appear, separately, in the product $(n-1)!$. Therefore $d_1 d_2$ divides $(n-1)!$, or in other words n divides $(n-1)!$, so $(n-1)! \equiv 0 \pmod{n}$.

Case 2: Suppose now that $d_1 = d_2$. For simplicity write $d = d_1 = d_2$. In that case $n = d^2$ and since $n \geq 6$ (the case of $n = 4$ is excluded, and we will tackle it later), this means that $d \geq 3$.

Let $1 < k < d$ be an integer. Such a k exists since $d \geq 3$. Then $1 < kd < n$: Indeed on the one hand both $1 < k$ and $1 < d$ so $1 < kd$. On the other hand, $k < d$, so $kd < d^2 = n$. Also $kd \neq d$, since $k \neq 1$.

Since both d and kd are strictly between 1 and n and they are unequal, they both appear, separately, in the product $(n-1)!$. By the same argument as above, $(kd)d = kd^2 = kn$ divides $(n-1)!$. Since n divides kn, n divides $(n-1)!$ and $(n-1)! \equiv 0 \pmod{n}$.

We now see why $n = 4$ must be excluded: In that case the only possible d with $1 < d < n$ is $d = 2$. We are therefore forced to apply Case 2, but since d is too small, there is no integer k with $1 < k < 2$, so the argument breaks down. Indeed,

$$3! = 1 \cdot 2 \cdot 3 = 6 \equiv 2 \pmod{4},$$

and $3!$ is not 0 modulo 4.

We also note that Case 2 is necessary in this proof: If p is a prime and $n = p^2$, then the only divisor d with $1 < d < n$ is p. This shows that we cannot assume that we can always find a pair of divisors d_1, d_2 with $1 < d_1, d_2 < n$ and $d_1 \neq d_2$.

3. Since $\tau(n)$ is the number of divisors of n, to bound it above we will use the following ideas: We will take the set of divisors of n and split it up into pairs (d_1, d_2) with $d_1 d_2 = n$. We will then show that there cannot be more than $\sqrt{n}$ such pairs. Therefore $\tau(n) \leq 2\sqrt{n}$.

   We first tackle the splitting up of divisors into pairs: For any $d_1 | n$, let $d_2 = \frac{n}{d_1}$. Then d_2 also divides n, since $n = d_1 d_2$. Furthermore, for each d_1 there is a unique such d_2, and if $d_1 \neq d_1'$, then $d_2 \neq d_2'$. Therefore, each divisor of n appears exactly once in one of the pairs (d_1, d_2) obtained in this manner, except for one exception: The pair (d, d) when $n = d^2$. In that case the divisor $d = \sqrt{n}$ appears twice.

   Therefore we have

$$2 \cdot \#\{\text{distinct pairs } (d_1, d_2) \text{ with } d_1 d_2 = n\} = \begin{cases} \tau(n) & \text{if } n \text{ is not a square,} \\ \tau(n) + 1 & \text{if } n \text{ is a square.} \end{cases}$$

   In any case,

$$\tau(n) \leq 2 \cdot \#\{\text{distinct pairs } (d_1, d_2) \text{ with } d_1 d_2 = n\}.$$

   We now show that $\#\{\text{distinct pairs } (d_1, d_2) \text{ with } d_1 d_2 = n\} \leq \sqrt{n}$. Without loss of generality, we assume that all of the pairs are such that $d_1 \leq d_2$. We claim that in this case, $d_1 \leq \sqrt{n}$: Indeed suppose that $d_1 > \sqrt{n}$. Then $d_2 > \sqrt{n}$ also since $d_2 \geq d_1$. Then $n = d_1 d_2 > (\sqrt{n})^2 = n$, a contradiction. So $d_1 \leq \sqrt{n}$.

   We have that

$$\#\{\text{distinct pairs } (d_1, d_2) \text{ with } d_1 d_2 = n\} = \#\{\ d_1 | n \text{ with } d_1 \leq \sqrt{n}\},$$

   since instead of counting the pairs we might as well just count their first element.

   Then we have

$$\begin{aligned} \#\{\ d_1 | n \text{ with } d_1 \leq \sqrt{n}\} &\leq \#\{\ d_1 \text{ an integer with } d_1 \leq \sqrt{n}\} \\ &\leq \sqrt{n}. \end{aligned}$$

   The first inequality is because the set of positive divisors of n that are less than or equal to $\sqrt{n}$ is contained in the set of positive integers that are less than or equal to $\sqrt{n}$, therefore its cardinality has to be smaller. The second inequality is because there are always exactly $\lfloor a \rfloor$ (where $\lfloor \cdot \rfloor$ is the floor function) positive integers that are less than or equal to a, and $\lfloor a \rfloor \leq a$ by definition.

   Putting everything together, we have

$$\begin{aligned} \tau(n) &\leq 2 \cdot \#\{\text{distinct pairs } (d_1, d_2) \text{ with } d_1 d_2 = n\} \\ &\leq 2\sqrt{n}, \end{aligned}$$

   which is what we we trying to prove.

4. (a) Let $g(n) = (f(n))^k$, and let n, m be positive integers with $\gcd(m,n) = 1$. Then we have

$$\begin{aligned} g(mn) &= (f(mn))^k \\ &= (f(m)f(n))^k \\ &= (f(m))^k(f(n))^k \\ &= g(m)g(n), \end{aligned}$$

since f is multiplicative.

(b) Since τ is multiplicative, so is τ^3 by part (a). By Theorem 6.4, so is F.

(c) Since τ is multiplicative, so is $\sum_{d|n} \tau(d)$ by Theorem 6.4. By part (a), so is G.

(d) Since f and g are multiplicative, $f(1) = g(1) = 1$. (Let f be multiplicative. $\gcd(n,1) = 1$ for all n, so $f(n) = f(1 \cdot n) = f(1)f(n)$. Since $f(n) = f(n)$, this forces $f(1) = 1$.)

Now let $n > 1$ and write $n = p_1^{k_1} \dots p_r^{k_r}$ for the factorization of n into primes. Note that if $i \neq j$, $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$. Therefore we have

$$\begin{aligned} f(n) &= f(p_1^{k_1}) \dots f(p_r^{k_r}) \\ &= g(p_1^{k_1}) \dots g(p_r^{k_r}) \\ &= g(n). \end{aligned}$$

The first equality is because f is multiplicative and all of the prime powers are relatively prime, the second equality is by assumption and the last equality is because g is multiplicative.

Therefore $f(n) = g(n)$ for all n.

(e) By parts (b) and (c), F and G are multiplicative. Therefore by part (d) it is enough to show that $F(p^k) = G(p^k)$ for all primes p and all $k \geq 1$ to obtain the result.

(Please turn over.)

We have

$$
\begin{aligned}
G(p^k) &= \left(\sum_{d|p^k} \tau(d)\right)^2 \\
&= \left(\sum_{j=0}^{k} \tau(p^j)\right)^2 && \text{since the divisors of } p^k \text{ are } p^j,\ j=0,\ldots,k \\
&= \left(\sum_{j=0}^{k} (j+1)\right)^2 && \text{since } \tau(p^j) = j+1 \\
&= \left(\sum_{j=1}^{k+1} j\right)^2 && \text{by reindexing} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{since } \sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)^2(k+2)^2}{4}
\end{aligned}
$$

and also

$$
\begin{aligned}
F(p^k) &= \sum_{d|p^k} (\tau(d))^3 \\
&= \sum_{j=0}^{k} (\tau(p^j))^3 && \text{since the divisors of } p^k \text{ are } p^j,\ j=0,\ldots,k \\
&= \sum_{j=0}^{k} (j+1)^3 && \text{since } \tau(p^j) = j+1 \\
&= \sum_{j=1}^{k+1} j^3 && \text{by reindexing} \\
&= \frac{(k+1)^2(k+2)^2}{4} && \text{since } \sum_{j=1}^{k+1} j^3 = \frac{(k+1)^2(k+2)^2}{4}.
\end{aligned}
$$

This last formula can be shown by induction.
Since $F(p^k) = G(p^k)$ for all primes p and all $k \geq 1$, it follows that $F(n) = G(n)$ for all $n \geq 1$.