Problem 1 (15pts) A few computations:

(a–5pts) Supply two distinct solutions to the system:

\[ 2x \equiv 2 \pmod{3} \]
\[ 3x \equiv 2 \pmod{4} \]
\[ 3x \equiv 2 \pmod{5} \]

You need not simplify

Solution. We can use

\[ x = 2 \cdot 2 \cdot 4^2 \cdot 5^2 + 3 \cdot 2 \cdot 3^2 \cdot 5^2 + 3 \cdot 2 \cdot 3^3 \cdot 4 \]

as a first solution. Another solution is

\[ x = 2 \cdot 2 \cdot 4^2 \cdot 5^2 + 3 \cdot 2 \cdot 3^2 \cdot 5^2 + 3 \cdot 2 \cdot 3^4 \cdot 4 + 3 \cdot 4 \cdot 5. \]

(b–5pts) What are the last two digits of \(3^{883}\)?

Solution. The last two digits are the remainder upon division by 100. Now \(\phi(100) = \phi(2^2 \cdot 5^2) = (4 - 2)(25 - 5) = 40\), and \(\gcd(3, 100) = 1\), so \(3^{40} \equiv 1 \pmod{100}\) by Euler’s Theorem. Thus

\[ 3^{883} = (3^{40})^{22} \cdot 3^3 \equiv 1 \cdot 27 \pmod{100}. \]

Of course we know that if \(a \equiv b \pmod{n}\) and \(0 \leq b < n\), then the remainder upon division of \(a\) by \(n\) is \(b\). Thus the remainder upon division by 100 is 27, that is, the last two digits are 27.

(c–5pts) Let \(p\) be an odd prime. What is the remainder upon division of \(5^p(p - 2)!\) by \(p\)?

Solution. We know by Fermat’s Little theorem that \(5^p \equiv 5 \pmod{p}\) and \((p - 1)! \equiv (p - 1)(p - 2)! \equiv (p - 1)(-1) \equiv (-1)(-1) = 1 \pmod{p}\) by Wilson’s theorem, so \(5^p(p - 2)! \equiv 5 \pmod{p}\) and thus the remainder is 2 if \(p = 3\), 0 if \(p = 5\), and 5 otherwise.
**Problem 2** (10pts) Suppose that $7 \nmid a$. Prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7. Fermat.

*Solution.* Since $7 \nmid a$, we know that $a^3 \equiv 1 \pmod{7}$, that is, $7 \mid (a^3 - 1) = (a^3 + 1)(a^3 - 1)$. But 7 is prime and we proved long ago that if $p$ prime divides $ab$ then $p \mid a$ or $p \mid b$. Thus 7 divides $a^3 + 1$ or $a^3 - 1$ as required.

**Problem 3** (10pts) Prove the converse of Wilson’s theorem, that is, prove that if $(n-1)! \equiv -1 \pmod{n}$ for $n > 1$, then $n$ is prime. Suppose not. Then there is $2 \leq d \leq n - 1$ such that $d \mid n$, and . . . .

*Solution.* Suppose that $2 \leq d \leq (n-1)$ such that $d \mid n$. Then $d \mid n \mid (n-1)! + 1$ and since $d \leq n - 1$ certainly $d \mid (n-1)! = 1 \cdot 2 \cdot (d-1) \cdot (d) \cdot (d+1) \cdots (n-1)$. It follows that $d$ divides any linear combination of $(n-1)!$ and $(n-1)! + 1$, that is, that $d \mid 1$, a contradiction since $d \geq 2$.

**Problem 4** (10pts) Suppose that $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ where the $p_i$ are distinct odd primes and the $\alpha_i \in \mathbb{N}_{>0}$. Prove that $2^r \mid \phi(n)$.

*Solution.* Recall that given an odd $p$ prime and $\alpha \in \mathbb{N}_{>0}$, $\phi(p^\alpha) = p^\alpha - p^{\alpha - 1} = p^{\alpha-1}(p-1)$. Of course $p - 1$ is even, so we can write $\phi(p^\alpha) = 2 \cdot \beta_p$ where $\beta_p$ is the natural number $p^{\alpha-1}\frac{p-1}{2}$. Finally we recall that $\phi$ is multiplicative. Thus

$$
\phi(n) = \phi \left( \prod_{i=1}^{r} p_i^{\alpha_i} \right) = \prod_{i=1}^{r} \phi(p_i^{\alpha_i}) = \prod_{i=1}^{r} 2\beta_{p_i} = 2^r \prod_{i=1}^{r} \beta_{p_i},
$$

where $\prod_{i=1}^{r} \beta_{p_i}$ is a product of natural numbers. It is thus apparent that $2^r \mid \phi(n)$ as required.

**Problem 5** (20pts) Let $F$ be the number theoretic function such that $F(n) = 1$ if $n = 1$, and $F(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = (-1)^t$ if $n > 1$, (where the $p_i$ are distinct primes and the $\alpha_i \in \mathbb{N}_{>0}$ as usual).

(a–10pts) Prove that $F$ is multiplicative.

*Solution.* Suppose that $m, n \in \mathbb{N}_{>0}$ such that $\gcd(m, n) = 1$. We need to show that $F(mn) = F(m)F(n)$. If $m = 1$ then

$$
F(mn) = F(1 \cdot n) = 1 \cdot F(n) = F(n) = F(m)F(n)
$$

and similarly for the $n = 1$ case so we suppose that $m, n > 1$.

By the Fundamental Theorem of Arithmetic, we can write $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for distinct primes $p_1, \ldots, p_r$ and $\alpha_1, \ldots, \alpha_r \in \mathbb{N}_{>0}$, and $n = q_1^{\beta_1} \cdots q_t^{\beta_t}$ for distinct primes $q_1, \ldots, q_t$ and $\beta_1, \ldots, \beta_t \in \mathbb{N}_{>0}$. Since the $\gcd(m, n) = 1$, it follows that $\{p_1, \ldots, p_r\} \cap \{q_1, \ldots, q_t\} = \emptyset$. Thus

$$
mn = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_t^{\beta_t}
$$

is a product of $r + t$ distinct primes with nonzero coefficients, that is $F(mn) = (-1)^{r+t}$. Of course

$$
F(m) = F(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = (-1)^r,
$$

and

$$
F(n) = F(q_1^{\beta_1} \cdots q_t^{\beta_t}) = (-1)^t,
$$

so $F(mn) = (-1)^{r+t} = (-1)^r(-1)^t = F(m)F(n)$ as required.
(b–10pts) Suppose that $F(n) = \sum_{d \mid n} \lambda(d)$ for another number theoretic function $\lambda$. Compute $\lambda(100)$.

Solution. We use Möbius inversion. So $\lambda(100) = \sum_{d \mid 100} \mu(d)F(100/d)$. Recall that

$$\mu(d) = \begin{cases} 
1 & \text{if } d = 1 \\
0 & \text{if there is prime } p \text{ such that } p^2 \mid d \\
(-1)^r & \text{if } d = p_1 \cdots p_r \text{ for distinct primes } p_1, \ldots, p_r.
\end{cases}$$

In particular, the only interesting divisors of $100 = 2^2 \cdot 5^2$ are $1, 2, 5, 10$, and $\mu(1) = 1, \mu(2) = \mu(5) = -1, \mu(2 \cdot 5) = 1$. Thus

$$\lambda(100) = \sum_{d \mid 100} \mu(d)F(100/d) = \mu(1)F(100/1) + \mu(2)F(100/2) + \mu(5)F(100/5) + \mu(10)F(100/10) = F(2^2 \cdot 5^2) - F(2 \cdot 5^2) - F(2^2 \cdot 5) + F(2 \cdot 5).$$

By definition

$$F(2^2 \cdot 5^2) = F(2 \cdot 5^2) = F(2^2 \cdot 5) = F(2 \cdot 5) = (-1)^2 = 1,$$

so $\lambda(100) = 1 - 1 - 1 + 1 = 0$. \qed

Problem 6 (10pts) Given $n \in \mathbb{N}_{>0}$, a reduced set of residues modulo $n$ is a set of $\phi(n)$ integers $\{a_1, \ldots, a_{\phi(n)}\}$ such that $a_i \not\equiv a_j \pmod{n}$ for $1 \leq i < j \leq n$ and $\gcd(a_i, n) = 1$ for all $1 \leq i \leq \phi(n)$. In class we would have said that $\{a_1, \ldots, a_n\}$ is equivalent modulo $n$ to $\{m \in \{1, \ldots, n\} \mid \gcd(m, n) = 1\}$. We have frequently used (and you may freely use below) that if $\{a_1, \ldots, a_r\}$ is equivalent modulo $n$ to $\{b_1, \ldots, b_r\}$, then $a_1 \cdots a_r \equiv b_1 \cdots b_r \pmod{n}$.

So suppose that $p$ is prime and $\{a_1, \ldots, a_{\phi(p)}\}$ is a reduced set of residues modulo $p$. What is the remainder upon division of $a_1 \cdots a_{\phi(p)}$ by $p^2$?

Solution. Of course if $p$ is prime then $\phi(p) = p - 1$, and $\{m \in \{1, \ldots, p\} \mid \gcd(m, p) = 1\} = \{1, \ldots, (p-1)\}$. Thus (using the usual argument described above) $a_1 \cdots a_{p-1} \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \equiv -1 \equiv (p-1) \pmod{p}$ (where the second to last congruence is Wilson’s theorem). We conclude that the remainder upon division of $a_1 \cdots a_{p-1}$ by $p$ is $p - 1$. (We again used that if $a \equiv b \pmod{n}$ and $0 \leq b < n$, then the remainder upon division of $a$ by $n$ is $b$, as in Problem 1b). \qed