Math 342 Tutorial
June 4, 2025

Question 1. **(a)** What is the remainder of when 5^{100} is divided by 7? **(b)** What is the remainder when $18!$ is divided by 437?

(a) $5^{100} = 5^{(16)(6)}5^4 \equiv 5^4 \equiv 2 \pmod 7$.

(b) We have $437 = 23 \cdot 19$. By Wilson's Theorem

$$-1 \equiv 22! \equiv 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv (-1)(-2)(-3)(-4)18! \equiv 18! \pmod{23}.$$

and

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

But then $-1 \equiv 18! \pmod{19 \cdot 23}$, i.e. $-1 \equiv 18! \pmod{437}$.

Question 2. Show that if p is an odd prime, then $2(p-3) \equiv -1 \pmod p$.

By Wilson's Theorem,

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

Question 3. Show that if n is a composite integer with $n \neq 4$, then $(n-1)! \equiv 0 \pmod n$.

If n is composite, then $n = ab$ with $1 < a \leqq b < n$. If the only proper factorzation of n is as $n = a^2$, then a must be a prime number.

For the first case, assume $n = ab$ with $a \neq b$. Then both a, b divide $(n-1)!$ by definition, hence also $n \mid (n-1)!$. If $n = p^2$ for some prime p, then since $n > 4$ in this case, it is also true that $2p < n$ (why?). But then p, $2p \mid (n-1)!$, hence $2n \mid (n-1)!$ so that $n \mid (n-1)!$ as $n \mid 2n$.

Question 4. Show that $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$.

For k such that $1 \leqq k < p$, we have that $k^{p-1} \equiv 1 \pmod p$. So,

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv \underbrace{1 + 1 + \cdots + 1}_{p-1} \equiv p - 1 \equiv -1 \pmod p.$$

Question 5. **(a)** Let p be a prime, and let $n_1, \ldots, n_k$ $(k > 1)$ be integers between 0 and p inclusive such that $n_1 + \cdots + n_k = p$ Show that $\binom{p}{n_1,\ldots,n_k} \equiv 0 \pmod p$ whenever each $n_i < p$. **(b)** Show that $(x_1 + \cdots + x_n)^{p^e} \equiv x_1^{p^e} + \cdots + x_n^{p^e} \pmod p$. **(c)** Show that $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p$ in two ways.

(a) The proof is by induction on k. Let $k = 2$. Then $\binom{p}{n_1,n_2} = \binom{p}{n_1}$ since $n_2 = p - n_1$. The assumption that each n_1, $n_2 < p$ means in particular that $0 < n_1 < p$. For simplicity, write $n = n_1$. Then

$$\binom{p}{n} = \frac{p(p-1)\cdots(p-n+1)}{n!}.$$

Since $(p,\, n!) = 1$, we must have that

$$\frac{(p-1)\cdots(p-n+1)}{n!}$$

is an integer. Hence, $\binom{p}{n} \equiv 0 \pmod{p}$. This shows the base case.
Next, assume that $k \geqq 2$ and the result holds for this given k. Let $n_1, \ldots, n_{k+1}$ be nonnegative integers such that $\sum_{i=1}^{k} n_i = p$ and each $n_i < p$. If $n_{k+1} = 0$, then

$$\binom{p}{n_1, \ldots,\, n_{k+1}} = \binom{p}{n_1, \ldots,\, n_k} \equiv 0 \pmod{p}$$

by the inductive hypothesis. If $n_{k+1} > 0$, then

$$\binom{p}{n_1, \ldots,\, n_{k+1}} = \binom{p}{n_{k+1}}\binom{p - n_{k+1}}{n_1, \ldots, n_k} \equiv 0 \pmod{p}$$

by the base case. The result now follows by mathematical induction.

(b) The proof is by double induction. The base case $e = 0$ and $n = 1$ is trivially true. Also trivial is the first inductive step that if $e = 0$, and if the result holds for a given $n \geqq 1$ with $e = 0$, it also holds for $n+1$. Next, let $e \geqq 0$ be given, and assume the result holds for all $n \geqq 1$ with this given e. Then

$$\begin{aligned} (x_1 + \cdots x_n)^{p^{e+1}} &\equiv ((x_1 + \cdots + x_n)^{p^e})^p \\ &\equiv (x_1^{p^e} + \cdots + x_n^{p^e})^p \\ &\equiv \sum_{\substack{n_1,\ldots,n_k \\ n_1+\cdots+n_k=p}} \binom{p}{n_1, \ldots, n_k} (x_1^{n_1} \cdots x_k^{n_k})^{p^e} \\ &\equiv x_1^{p^{e+1}} + \cdots + x_n^{p^{e+1}} \pmod{p} \end{aligned}$$

by the inductive hypothesis and part (a). The result now follows from induction.

(c) If p is even the result is trivial. So assume p is odd. By Fermat's Little Theorem, $1^p + 2^p + \cdots + (p-1)^p \equiv \frac{p(p-1)}{2} \pmod{p}$. Since p is odd, $\frac{p-1}{2}$ is an integer, hence the sum is divisible by p. By part (b) instead, we have that $1^p + 2^p + \cdots + (p-1)^p \equiv (1+2+\cdots+(p-1))^p \equiv (\frac{p(p-1)}{2})^p \equiv 0^p \equiv 0 \pmod{p}$.

Question 6. **(a)** Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. **(b)** Show that if p is prime, then $p \mid (a^p + (p-1)!a)$. **(c)** Show that if p is an odd prime, then $1^2 3^2 \cdots (p-4)^2(p-2)^2$ is equivalent to $(-1)^{(p+1)/2}$ modulo p.

(a) We have that $(p,\, q) = 1$. By Fermat's Little Theorem,

$$1 \equiv p^{q-1} \equiv p^{q-1} + q^{p-1} \pmod{q}.$$

Similarly,

$$1 \equiv q^{p-1} \equiv q^{p-1} + p^{q-1} \pmod{p}.$$

Hence,

$$p^{q-1} + q^{p-1} \pmod{pq}.$$

(b) Observe, $a^p + (p-1)!a \equiv a(1 + (p-1)!) \equiv 0 \pmod{p}$. The first congruence is by Fermat's Little Theorem; the second by Wilson's Theorem.

(c) We have

$$\begin{aligned} 1^2 3^3 \cdots (p-4)^2(p-2)^2 &= (1 \cdot 1)(3 \cdot 3) \cdots (p-4)(p-4)(p-2)(p-2) \\ &= (-1)^{(p-1)/2}(1)(-1)(3)(-3) \cdots (p-4)(4-p)(p-2)(2-p) \end{aligned}$$

$$= (-1)^{(p-1)/2}(1)(p-1)(3)(p-3)\cdots(p-4)4(p-2)2.$$

Since the odd positive integers less than p are $1,\ 3, \ldots,\ p-4,\ p-2$, and the even positive integers less than p are $2,\ 4, \ldots,\ p-3,\ p-1$, we have that

$$\begin{aligned} 1^2 3^3 \cdots (p-4)^2(p-2)^2 &= (-1)^{(p-1)/2}(p-1)! \\ &\equiv (-1)^{(p-1)/2}(-1) \\ &\equiv (-1)^{(p+1)/2} \pmod{p} \end{aligned}$$

by Wilson's Theorem.

The questions 7 and 9 each show by elementary means that ϕ is a multiplicative arithmetical function (your textbook contains a third). Next week, we will derive an algebraic proof using the Chinese Remainder Theorem. Many of the results you are learning via elementary means admit more natural interpretations in more general algebraic settings. We will see that the main properties of the Euler Totient Function are easier understood in this more general setting.

Question 7. **(a)** Suppose that $(m,\ m') = 1$, and that a runs through a complete system of residues modulo m, and that a' runs through a complete system of integers modulo m'. Show that $a'm + am'$ runs through a complete set of residues modulo mm'. **(b)** Show that ϕ is multiplicative, that is, if $(m,\ m') = 1$, then $\phi(mm') = \phi(m)\phi(m')$.

(a) There are mm' numbers $a'm + am'$. If

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \pmod{mm'}$$

then $a_1m' \equiv a_2m' \pmod{m}$, hence $a_1 \equiv a_2 \pmod{m}$. Similarly, $a_1' \equiv a_2' \pmod{m'}$. Thus, the mm' such numbers are all incongruent and form a complete set of residues mod mm'.

(b) Let $a,\ a',\ m,\ m'$ be as in part (a). If $(a'm+am',\ mm') = 1$, then $(a'm+am',\ m) = 1 = (a'm+am',\ m')$ which in turn implies that $(am',\ m) = 1 = (a'm,\ m)$ so that $(a,\ m) = 1 = (a',\ m')$ since $(m,\ m') = 1$. We can also transpose this argument. Thus, the $\phi(mm')$ integers of the form $a'm + am'$ coprime to mm' are in bijective correspondence with the $\phi(m)\phi(m')$ ordered pairs $(a,\ a')$ of integers with $(a,\ m) = 1$ and $(a',\ m') = 1$. Thus, $\phi(mm') = \phi(m)\phi(m')$, as desired.

Given two arithmetical functions f and g, we define their Dirichlet product $f * g$ as $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$. The function ι is defined by $\iota(n) = \lfloor \frac{1}{n} \rfloor$. We call ι the arithmetic identity.

Question 8. Let f and g be two arithmetical functions. Show the following. **(a)** $f * g = g * f$. **(b)** $(f * g) * h = f * (g * h)$. **(c)** $f * \iota = \iota * f = f$. **(d)** g is the arithmetic inverse of f if $f * g = \iota$. Show the arithmetic function f has an inverse if and only if $f(1) \neq 0$. Show that if f has an arithmetic inverse, then it is unique. **(e)** If h is the arithmetic inverse of g, then $(f * g) * h = f$. **(f)** If f and g are multiplicative, then so is $f * g$.

(a) Let n be given. As d ranges over the divisors n/d ranges over the conjugate pairs. Hence,

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right)g(d) = (g * f)(n).$$

(b) We have

$$((f * g) * h)(n) = \sum_{d|n} (f * g)(d)h\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \left(\sum_{d'|d} f(d') g\left(\frac{d}{d'}\right) \right) h\left(\frac{n}{d}\right)$$

$$= \sum_{\substack{d|n \\ d'|d}} f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d}\right).$$

Note that we are just summing over all triples $a,\ b,\ c$ such that $abc = n$. Therefore, we can write this as

$$\sum_{\substack{d|n \\ d'|d}} f(d') g\left(\frac{d}{d'}\right) h\left(\frac{n}{d}\right) = \sum_{\substack{d|n \\ d'|d}} g(d') h\left(\frac{d}{d'}\right) f\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \left(\sum_{d'|d} g(d') h\left(\frac{d}{d'}\right) \right) f\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} (g * h)(d) f\left(\frac{n}{d}\right)$$

$$= ((g * h) * f)(n)$$

$$= (f * (g * h))(n).$$

(c) Observe

$$(f * \iota)(n) = \sum_{d|n} \iota(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \left\lfloor \frac{1}{d} \right\rfloor f\left(\frac{n}{d}\right) = f(n).$$

(d) Note that $(f * g)(1) = \iota(1)$ reduces to $f(1)g(1) = 1$. So if $f(1) = 0$, then f admits no arithmetic inverse. If $f(1) \neq 0$, then $g(1)$ is uniquely determined as $g(1) = 1/f(1)$. Next, assume we have determined the values $g(k)$ for $k < n$ in such a way that $(f * g)(k) = \iota(k)$. We need to solve $(f * g)(n) = \iota(n)$, i.e.,

$$0 = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = f(1)g(n) + \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right)$$

But then $g(n)$ is uniquely determined as

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right)$$

This shows at once existence and uniqueness.

(e) $(f * g) * h = f * (g * h) = f * \iota = f$.

(f) Suppose that $(m,\ n) = 1$. There the divisors d od mn are in bijective correspondence with pairs $(a,\ b)$ such that $a \mid m$ and $b \mid n$; in particular, d factors uniquely as $d = ab$ with $a \mid m$ and b min n. Then further $(a,\ b) = 1$ and $(m/a, n/b) = 1$.
Let $h = f * g$ where f and g are multiplicative. Then

$$h(mn) = \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{a|m \\ b|n}} f(ab) g\left(\frac{mn}{ab}\right)$$

$$
\begin{aligned}
&= \sum_{\substack{a|m\\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\
&= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right)\\
&= h(n)h(m),
\end{aligned}
$$

as required.

The Möbius function $\mu(n)$ is defined as follows: $\mu(1) = 1$; if $n = p_1^{e_1}\cdots p^{e_k}$, then $\mu(n) = (-1)^k$ if $e_1 = \cdots = e_k = 1$; $\mu(n) = 0$ otherwise.

Question 9. Show the following. **(a)** μ is multiplicative. **(b)** $\sum_{d|n}\mu(d) = \lfloor\frac{1}{n}\rfloor$. **(c)** Show that ϕ is multiplicative using part (b). [Hint: Argue that you can write $\phi(n) = \sum_{k=1}^{n}\lfloor\frac{1}{(n,\,k)}\rfloor$]

(a) If $(m,\,n) = 1$, then mn has square factors if and only if m or n does. If n has square factors, then $\mu(n) = 0$ so that $\mu(mn) = 0 = 0\mu(m) = \mu(n)\mu(m)$. Similarly, if m has square factors, then again $\mu(mn) = \mu(m)\mu(n) = 0$. If $m = n = 1$, then $\mu(mn) = \mu(1) = 1 = 1\cdot 1 = \mu(1)\mu(1) = \mu(n)\mu)m$. If $m = 1$ and $n = p_1\cdots p_k$, then $\mu(mn) = \mu(n) = 1\mu(n) = \mu(m)\mu)n$. Similarly, if $n = 1$ and $m = q_1\cdots q_\ell$, then $\mu(mn) = \mu(m)\mu(n)$. If $n = p_1\cdots p_k$ and $m = q_1\cdots q_\ell$, then $\mu(mn) = \mu(p_1\cdots p_k q_1\cdots q_\ell) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \mu(n)\mu(m)$.

(b) When $n = 1$, we have $\mu(1) = 1 = \lfloor\frac{1}{1}\rfloor$. Let $n > 1$ and write $n = p_1^{e_1}\cdots p_k^{e_k}$. In the sum $\sum_{d|n}\mu(d)$, the only nonzero terms are $d = 1$ and d a product of distinct primes. Thus,

$$
\begin{aligned}
\sum_{d|n}\mu(d) &= 1 + \sum_{p|n}\mu(p) + \sum_{\substack{p_i,p_j|n\\ i<j}}\mu(p_1p_2) + \cdots\\
&= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0.
\end{aligned}
$$

This shows that indeed $\sum_{d|n}\mu(d) = \lfloor\frac{1}{n}\rfloor$.

(c) Observe that

$$
\phi(n) = \sum_{\substack{k=1\\ (k,\,n)=1}}^{n} 1 = \sum_{k=1}^{n}\left\lfloor\frac{1}{(k,\,n)}\right\rfloor.
$$

From part (b), we then have that

$$
\begin{aligned}
\phi(n) = \sum_{k=1}^{n}\left\lfloor\frac{1}{(k,\,n)}\right\rfloor &= \sum_{k=1}^{n}\sum_{d|(k,\,n)}\mu(d) = \sum_{k=1}^{n}\sum_{\substack{d|k\\ d|n}}\mu(d)\\
&= \sum_{d|n}\sum_{q=1}^{n/d}\mu(d) = \sum_{d|n}\mu(d)\frac{n}{d} = (\mu * \mathrm{id})(n)
\end{aligned}
$$

where $id(m) = m$ for each $m \in \mathbf{N}$. Since id is trivially multiplicative, and since μ is multiplicative by part (a), we have that $\phi = \mu * \mathrm{id}$ is multiplicative by Question 8(f).

Question 10. Show the following properties of ϕ.

(a) $\phi(p^e) = p^e - p^{e-1}$ for every prime p and $e > 0$.

(b) If $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.

(c) $\phi(mn) = \phi(m)\phi(n)d/\phi(d)$ where $d = (n,\, m)$.

(d) $a \mid b$ implies $\phi(a) \mid \phi(b)$.

(e) $\phi(n)$ is even for $n \geqq 3$. Moreover, if n has r distinct odd prime factors, then $2^r \mid \phi(n)$.

(a) The only divisors of p^e are $1,\, p,\, p^2, \ldots,\, p^e$. The integers at most p^e coprime to p^e are then $2, \ldots, p-1, p-2, \ldots, p^2-1, \ldots$. There are $p^{e-1}(p-1) = p^e - p^{e-1}$, i.e., $\phi(p^e) = p^e - p^{e-1}$.

(b) Observe

$$\begin{aligned}\phi(n) = \phi(p_1^{e_1} \cdots p_k^{e^k}) &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p^{e_1} \cdots p_k^{e_k}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),\end{aligned}$$

as required.

(c) The prime divisors of mn are either prime divisors of m or n. If they are prime divisors of both, then they divide $d = (m,\, n)$. Then

$$\frac{\phi(mn)}{mn} = \prod_{p|mn}\left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m}\left(1 - \frac{1}{p}\right)\prod_{p|n}\left(1 - \frac{1}{p}\right)}{\prod_{p|d}\left(1 - \frac{1}{p}\right)} = \frac{\frac{\phi(m)}{m}\frac{\phi(n)}{n}}{\frac{\phi(d)}{d}}$$

which suffices to show the result.

(d) We are given $b = ac$. If $a = b$ or $b = c$, the result is trivial. Hence, assume $1 < a,\, c < b$. From part (c), we have

$$\phi(b) = \phi(ac) = \phi(a)\phi(c)\frac{(a,\, c)}{\phi((a,\, c))} = (a,\, c)\phi(a)\frac{\phi(c)}{\phi((a,\, c))}.$$

Now we use induction. The result is trivial for $b = 1$. Suppose $b > 1$ and the result holds for all smaller positive integers. Then it holds for c, i.e., $(a,\, c) \mid c$ so that $\phi((a,\, c)) \mid \phi(c)$. Hence, the right-hand-side is a multiple of $\phi(a)$, so that $\phi(a) \mid \phi(b)$.

(e) For $n = p_1^{e_1} \cdots p_k^{e_k}$, we have

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = \frac{n}{\prod_{p|n} p}\prod_{p|n}(p-1).$$

If there are r odd prime divisors of n, then there are r even factors $p - 1$ in $\phi(n)$. Thus, $2^r \mid \phi(n)$.

An integer a is a quadratic residue mod the odd prime p if there is a solution x to $x^2 \equiv q \pmod{p}$. The integer a is a quadratic nonresidue mod p if there is no such x. The Legendre symbol $(\frac{a}{p})$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p. \end{cases}$$

Question 11. **(a)** Show that if a is a quadratic residue mod the odd prime p, then there are exactly two incongruent solutions. **(b)** Show that $(p-1)!$ is congruent to $-\left(\frac{a}{p}\right)a^{(p+1)/2}$ modulo p.

(a) We are given that $x^2 \equiv \pmod p$ for some x. Suppose there is another such solution y, i.e., $y^2 \equiv a \pmod p$. Then $x^2 - y^2 = (x+y)(x-y) \equiv 0 \pmod p$. Therefore, either either $p \mid x+y$ or $p \mid x-y$. In the first case $y \equiv -x \pmod p$; in the second, $y \equiv x \pmod p$. This shows there are at most two incongruent solutions. To see there are at least 2 solutions, note that $(-x)^2 \equiv a \pmod p$ whenever $x^2 \equiv a \pmod p$.

(b) If a is a quadratic residue and suppose $0 \leqq x_1 < p$ is such that $x_1^2 = a \pmod p$. We group x_1 and $p - x_1 \equiv -x_1$ together. For every other residue representative x, there is a associate x' to x for which $xx' =\equiv a \pmod p$. There are $(p-3)/2$ such pairings. Now $x_1(-x_1) \equiv -a$ and $xx' \equiv a$. Thus $(p-1)! \equiv (-a)a^{(p-3)/2} \equiv -a^{(p-1)/2} \pmod p$.

If a is a quadratic nonresidue, then each nonzero residue x can be uniquely paired with a residue x' such that $xx' \equiv a \pmod p$. There are $(p-1)/2$ such pairings, hence $(p-1)! \equiv a^{(p-1)/2} \pmod p$.

Putting things together, we have that

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{(p-1)/2} \pmod p.$$