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?

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

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

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

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.

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.

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 $\phi(mm') = \phi(m)\phi(m')$.

Given two arithmetical functions f and g, we define their Dirichlet product $f * g$ as $(f * g)(n) = \sum_{d|n} f(n)g(\frac{n}{d})$. 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 $f * g$.

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

Question 10. Show the following properties of ϕ.

(a) $\phi(p^e) = p^e - p$ 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 $2^r \mid \phi(n)$.

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 at most two incongruent solutions. **(b)** Show that $(p-1)!$ is congruent to $-\left(\frac{a}{p}\right) a^{(p+1)/2}$ modulo p.