CSE 547: Homework Three

Amirhossein Najafizadeh

Semester: Fall 2024
SBU ID: 116715544
Email: Amirhossein.Najafizadeh@stonybrook.edu

Question 1

1). 4.32

Fermat's Little Theorem:

$$n^{p-1} \equiv 1 \pmod{m}$$

Euler's Theorem; let n and m be integers such that $\gcd(n, m) = 1$. Then:

$$n^{\phi(m)} \equiv 1 \pmod{m}$$

where $\phi(m)$ is Euler's totient function.

Consider the set of integers $S = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ that are coprime to m. Multiplying each element by n, we get the set $T = \{na_1, na_2, \ldots, na_{\phi(m)}\}$. Since multiplication by n permutes the elements of S modulo m, the products of the elements in both sets are congruent modulo m:

$$a_1 a_2 \cdots a_{\phi(m)} \equiv (na_1)(na_2) \cdots (na_{\phi(m)}) \pmod{m}$$

This simplifies to:

$$a_1 a_2 \cdots a_{\phi(m)} \equiv n^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \pmod{m}$$

Since all a_i are coprime to m, we can cancel them out:

$$1 \equiv n^{\phi(m)} \pmod{m}$$

Thus, **Euler's Theorem** is proved.

Question 2

2). 4.33

If $f(m)$ and $g(m)$ are multiplicative functions, then the function

$$h(m) = \sum_{d \mid m} f(d) g(m/d)$$

is also multiplicative.

To show that $h(m)$ is multiplicative, we need to prove that for any coprime integers m and n, the following holds:

$$h(mn) = h(m)h(n)$$

Since f and g are multiplicative, for any divisors $d_1 \mid m$ and $d_2 \mid n$, we have:

$$f(d_1d_2) = f(d_1)f(d_2)$$
$$g\left(\frac{mn}{d_1d_2}\right) = g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)$$

Consider the divisors of mn. Any divisor $d \mid mn$ can be uniquely expressed as $d = d_1d_2$, where $d_1 \mid m$ and $d_2 \mid n$. Thus, we can write:

$$h(mn) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1d_2)g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right)$$

Using the multiplicativity of f and g, this becomes:

$$h(mn) = \sum_{d_1 \mid m} f(d_1)g\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} f(d_2)g\left(\frac{n}{d_2}\right)$$

This shows:

$$h(mn) = h(m)h(n).$$

Therefore, $h(m)$ is multiplicative.

Question 3

3). 4.47

If $n^{m-1} \equiv 1 \pmod{m}$ and $n^{(m-1)/p} \not\equiv 1 \pmod{m}$ for all primes p such that $p \mid (m-1)$, then m is prime.

Assume for contradiction that m is composite. Then $m = ab$ for some integers $1 < a, b < m$. Consider the order of $n \mod m$, denoted as d. By definition, d is the smallest positive integer such that $n^d \equiv 1 \pmod{m}$.

From the condition $n^{m-1} \equiv 1 \pmod{m}$, it follows that $d \mid (m-1)$. For each prime divisor p of $(m-1)$, we have $n^{(m-1)/p} \not\equiv 1 \pmod{m}$, implying that d does not divide any proper divisor of $(m-1)$. Thus, the order d must be exactly $m-1$. This means the powers $n^k \mod m$ for $1 \leq k < m$ are distinct.

If $m = ab$, then by *Fermat's Little Theorem*, for any integer coprime to a prime factor of m, the order should divide a smaller number than $m-1$. This contradicts our finding that the order is exactly $m-1$.

Therefore, our assumption that m is composite must be false. Hence, m is prime.

Question 4

4). 5.14

Prove identity (5.25) by negating the upper index in *Vandermonde's convolution* (5.22). Then show that another negation yields (5.26).

Vandermonde's Convolution (5.22):

$$\sum_k \binom{r}{m+k}\binom{s}{n-k} = \binom{r+s}{m+n}, \quad \text{integers } m, n \tag{1}$$

Identity (5.25):

$$\sum_{k<l} \binom{l-k}{m}\binom{s}{k-n}(-1)^k = (-1)^{l+m}\binom{s-m-1}{l-m-n}, \quad \text{integers } l, m, n \geq 0 \tag{2}$$

Identity (5.26):

$$\sum_{0\leq k<l} \binom{l-k}{m}\binom{q+k}{n} = \binom{l+q+1}{m+n+1}, \quad \text{integers } l, m \geq 0, \text{ integers } n \geq q \geq 0 \tag{3}$$

We are going to start with *Vandermonde's convolution*:

$$\sum_k \binom{r}{m+k}\binom{s}{n-k} = \binom{r+s}{m+n} \tag{4}$$

First we negate the upper index r:

$$\sum_k \binom{-l}{m+k}\binom{s}{n-k} \tag{5}$$

Then we are going to use the identity for negative binomial coefficients:

$$\binom{-l}{m+k} = (-1)^{m+k}\binom{l+m+k-1}{m+k} \tag{6}$$

After that, we substitute into the sum:

$$\begin{aligned} &= \sum_k (-1)^{m+k}\binom{l+m+k-1}{m+k}\binom{s}{n-k} \\ &= (-1)^m \sum_k (-1)^k \binom{l+m+k-1}{m+k}\binom{s}{n-k} \end{aligned}$$

Finally, this matches identity (5.25):

$$(-1)^{l+m}\sum_{k<l} \binom{l-k}{m}\binom{s}{k-n} = (-1)^{l+m}\binom{s-m-1}{l-m-n} \tag{7}$$

Now to show that another negation yields (5.26), first we negate the upper index s:

$$\sum_k (-1)^m(-1)^k\binom{l+m+k-1}{m+k}\binom{-q}{n-k} \tag{8}$$

Then we are going to use the identity for negative binomial coefficients:

$$\binom{-q}{n-k} = (-1)^{n-k}\binom{q+n-k-1}{n-k} \tag{9}$$

After that, we substitute into the sum:

$$\begin{aligned} &= (-1)^m \sum_k (-1)^k (-1)^{n-k} \binom{l+m+k-1}{m+k}\binom{q+n-k-1}{n-k} \\ &= (-1)^{m+n} \sum_k (-1)^k \binom{l+m+k-1}{m+k}\binom{q+n-k-1}{n-k} \end{aligned}$$

Then this matches identity (5.26):

$$\sum_{0\le k<l} \binom{l-k}{m}\binom{q+k}{n} = \binom{l+q+1}{m+n+1} \tag{10}$$

Thus, by negating the indices as described, we have proven identities (5.25) and (5.26).

Question 5

5). 5.16

We want to evaluate the sum:

$$S = \sum_{k=0}^{\infty} \binom{2a}{a+k}\binom{2b}{b+k}\binom{2c}{c+k}(-1)^k$$

for nonnegative integers a, b, and c.

To solve this, we use a combinatorial identity involving binomial coefficients and alternating series. The identity is:

$$\sum_{k=0}^{n} \binom{n}{k}\binom{m+k}{k}(-1)^k = \binom{m}{n}$$

First, consider the sum of the first two binomial coefficients:

$$\sum_{k=0}^{\infty} \binom{2a}{a+k}\binom{2b}{b+k}(-1)^k = \binom{a+b}{a}$$

Next, apply the identity to the result with the third binomial coefficient:

$$\sum_{k=0}^{\infty} \binom{a+b}{a+k}\binom{2c}{c+k}(-1)^k = \binom{a+b+c}{a+b}$$

Thus, the evaluated sum is:

$$S = \binom{a+b+c}{a+b}$$

Question 6

6). 5.37

To prove the identities involving factorial powers as an analog to the binomial theorem, we need to show:

$$
\begin{aligned}
(x+y)^{\underline{n}} &= \sum_{k=0}^{n} \binom{n}{k} x^{\underline{k}} y^{\underline{n-k}} \\
(x+y)^{\overline{n}} &= \sum_{k=0}^{n} \binom{n}{k} x^{\overline{k}} y^{\overline{n-k}}
\end{aligned}
$$

where $x^{\underline{k}}$ and $x^{\overline{k}}$ represent falling and rising factorial powers, respectively.

The falling factorial power $x^{\underline{k}}$ is defined as:

$$x^{\underline{k}} = x(x-1)(x-2)\cdots(x-k+1)$$

The rising factorial power $x^{\overline{k}}$ is defined as:

$$x^{\overline{k}} = x(x+1)(x+2)\cdots(x+k-1)$$

For both identities, we can use combinatorial arguments similar to those used in the binomial theorem.

Combinatorial Argument, consider a set of size n. The term $x^{\underline{k}}$ corresponds to choosing k elements from this set and arranging them in a sequence, which is equivalent to permutations. The term $y^{\underline{n-k}}$ does the same for the remaining elements. **Binomial Coefficient**, the binomial coefficient $\binom{n}{k}$ counts the number of ways to choose k elements from a set of size n.

Combinatorial Argument, similarly, for rising factorials, consider sequences where each element can be chosen with replacement, allowing for repetition. This corresponds to combinations with repetition. **Binomial Coefficient**, again, $\binom{n}{k}$ counts the ways to choose elements with repetition allowed.

These identities are extensions of the binomial theorem using factorial powers, which count permutations and combinations in different contexts. The proofs rely on understanding how these factorial powers relate to combinatorial selections and arrangements. This approach demonstrates that these identities hold for all nonnegative integers n, providing an analog to the classical binomial theorem.

Question 7

7).

For any non-negative integer n ($n \geq 0$), prove that the following expression is an integer:

$$(\frac{1}{5})n^5 + (\frac{1}{3})n^3 + (\frac{7}{15})n$$

We will use *mathematical induction* to prove that the expression is an integer for all non-negative integers n. When $n = 0$, the expression evaluates to 0, which is an integer. Assume the expression is an integer for some $k \geq 0$. We need to prove it's also an integer for $k + 1$.
Let $P(k)$ represent the expression for $n = k$:

$$P(k) = (1/5)k^5 + (1/3)k^3 + (7/15)k$$

Now, let's calculate $P(k + 1) - P(k)$:

$$\begin{aligned} P(k+1) - P(k) &= [(1/5)(k+1)^5 + (1/3)(k+1)^3 + (7/15)(k+1)] \\ &\quad -[(1/5)k^5 + (1/3)k^3 + (7/15)k] \\ = [(1/5)(k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) &+ (1/3)(k^3 + 3k^2 + 3k + 1) + (7/15)(k + 1)] \\ &\quad -[(1/5)k^5 + (1/3)k^3 + (7/15)k] \\ &= k^4 + 2k^3 + k^2 + 1 \end{aligned}$$

This difference is always an integer for any non-negative integer k. Since $P(k)$ is assumed to be an integer, and the difference $P(k+1)-P(k)$ is an integer, $P(k+1)$ must also be an integer. By the principle of *mathematical induction*, we have proved that the expression is an integer for all non-negative integers n.

When n is negative, the expression is not guaranteed to be an integer. The term $(7/15)n$ will always be a fraction for any non-zero integer n, positive or negative. For odd negative integers, n^3 and n^5 will be negative, potentially creating fractions that don't cancel out with the $(7/15)n$ term. For even negative integers, n^3 and n^5 will be positive, but again, the fractions may not cancel out completely.
For $n = -1$:

$$(1/5)(-1)^5 + (1/3)(-1)^3 + (7/15)(-1) = -1/5 - 1/3 - 7/15 = -11/15$$

This is clearly not an integer. Therefore, the conclusion that the expression is always an integer does not hold for negative integers.

Question 8

8).

Let a, b, x, y, and v be integers. We want to prove that:

$$\gcd(a, b) \leq \gcd(xa + yb, ua + vb)$$

Let $d = \gcd(a, b)$. By definition, d is the largest integer that divides both a and b. Since d divides both a and b, we can express a and b as:

$$a = k_1 d \quad \text{and} \quad b = k_2 d, \quad \text{where } k_1 \text{ and } k_2 \text{ are integers}$$

Now, let's consider the expression $xa + yb$:

$$\begin{aligned} xa + yb &= x(k_1 d) + y(k_2 d) \\ &= d(xk_1 + yk_2) \end{aligned}$$

Similarly, for $ua + vb$:

$$\begin{aligned} ua + vb &= u(k_1 d) + v(k_2 d) \\ &= d(uk_1 + vk_2) \end{aligned}$$

Now we can see that d is a common divisor of both $xa+yb$ and $ua+vb$. By the definition of GCD, we know that:

$$\gcd(xa + yb, ua + vb) \geq d$$

Since we defined d as $\gcd(a, b)$ in step 1, we can rewrite the inequality as:

$$\gcd(xa + yb, ua + vb) \geq d = \gcd(a, b)$$

Question 9

B1).

Find all non-negative integer pairs (a, b) that satisfy both of the following conditions:

$$\gcd(a, b) = 10$$
$$\text{lcm}(a, b) = 100$$

Approach using GCD & LCM Relationship: We start with the fundamental theorem $\gcd(a, b) \times \text{lcm}(a, b) = a \times b$.

Substituting the given values $10 \times 100 = a \times b$ which simplifies to: $a \times b = 1000$. We need to find factor pairs of 1000 where both factors are multiples of 10 (since gcd = 10). The possible factor pairs are: (10, 100), (20, 50), (50, 20), and (100, 10).

Prime Factorization Approach: We know that $\gcd(a, b) = 10 = 2 \times 5$ and $\text{lcm}(a, b) = 100 = 2^2 \times 5^2$.

Let $a = 2^x \times 5^y$ and $b = 2^z \times 5^w$, where x, y, z, w are non-negative integers. For $\gcd(a, b) = 10$:

$$\min(x, z) = 1$$
$$\min(y, w) = 1$$

For $\text{lcm}(a, b) = 100$:

$$\max(x, z) = 2$$
$$\max(y, w) = 2$$

The possible combinations are:

$$(x, y, z, w) \in \{(1, 1, 2, 2), (1, 2, 2, 1), (2, 1, 1, 2), (2, 2, 1, 1)\}$$

These correspond to the pairs:

$$(a, b) \in \{(10, 100), (20, 50), (50, 20), (100, 10)\}$$