CSE 547: Homework Two

Amirhossein Najafizadeh

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

Question 1

1). 2.22

Let's review Lagrange's identity first:

$$\sum_{1\le j<k\le n}(a_jb_k-a_kb_j)^2=(\sum_{k=1}^{n}{a_k}^2)(\sum_{k=1}^{n}{b_k}^2)-(\sum_{k=1}^{n}a_kb_k)^2$$

First we are going to prove Lagrange's identity, after that we are going find an identity for the more general double sum. We are going to expand each part of the equation, then combine everything to together.

$$(I)\ (\sum_{i=1}^{n}a_ib_i)^2=\sum_{i=1}^{n}\sum_{j=1}^{n}a_ib_ia_jb_j=\sum_{i=1}^{n}{a_i}^2{b_i}^2+2\sum_{1\le i<j\le n}(a_ib_ia_jb_j)$$

$$(II)\ (\sum_{i=1}^{n}{a_i}^2)(\sum_{i=1}^{n}{b_i}^2)=\sum_{i=1}^{n}{a_i}^2{b_i}^2+\sum_{1\le i<j\le n}({a_i}^2{b_j}^2+{a_j}^2{b_i}^2)$$

$$(III)\ -\sum_{1\le i<j\le n}(a_ib_j-a_jb_i)^2=-\sum_{1\le i<j\le n}({a_i}^2{b_j}^2-2a_ib_ia_jb_j+{a_j}^2{b_i}^2)$$

$$\begin{aligned}(II)+(III)\ &\sum_{i=1}^{n}{a_i}^2{b_i}^2+\sum_{1\le i<j\le n}({a_i}^2{b_j}^2+{a_j}^2{b_i}^2)-\sum_{1\le i<j\le n}({a_i}^2{b_j}^2-2a_ib_ia_jb_j+{a_j}^2{b_i}^2)\\&=\sum_{i=1}^{n}{a_i}^2{b_i}^2+2\sum_{1\le i<j\le n}a_ib_ia_jb_j\end{aligned}$$

Since we have $I=II+III$; it proves Lagrange's identity.

$$(\sum_{i=1}^{n}a_ib_i)^2=(\sum_{i=1}^{n}{a_i}^2)(\sum_{i=1}^{n}{b_i}^2)-\sum_{1\le i<j\le n}(a_ib_j-a_jb_i)^2$$

$$\sum_{1\le i<j\le n}(a_ib_j-a_jb_i)^2=(\sum_{i=1}^{n}{a_i}^2)(\sum_{i=1}^{n}{b_i}^2)-(\sum_{i=1}^{n}a_ib_i)^2$$

Now we are going to use it to find an identity for this summation:

$$S = \sum_{1\leq j<k\leq n} ((a_jb_k - a_kb_j)(A_jB_k - A_kB_j))$$

According to Lagrange's identity we have for a, b, A, B:

$$(\sum_{i=1}^{n} a_ib_i)(\sum_{i=1}^{n} A_iB_i) = (\sum_{i=1}^{n} a_iA_i)(\sum_{i=1}^{n} b_iB_i) - \sum_{1\leq j<k\leq n} (a_jb_k - a_kb_j)(A_jB_k - A_kB_j)$$

$$\sum_{1\leq j<k\leq n} (a_jb_k - a_kb_j)(A_jB_k - A_kB_j) = (\sum_{i=1}^{n} a_iA_i)(\sum_{i=1}^{n} b_iB_i) - (\sum_{i=1}^{n} a_ib_i)(\sum_{i=1}^{n} A_iB_i)$$

Question 2

3). 4.16

First of all, let's take a look at Euclid's theorem:

$$E_n = \prod_{i=1}^{n} p_i + 1 \text{ where } p_i \text{ is the } i\text{th prime number}$$

Now we are going to find a recursive definition for Euclid's numbers:

$$E_{n+1} = \prod_{i=1}^{n+1} p_i + 1$$

$$E_{n+1} = p_{n+1} \prod_{i=1}^{n} p_i + 1$$

$$E_{n+1} = E_n \times p_{n+1} + 1$$

$$\Rightarrow E_n = E_{n-1} \times p_n + 1$$

$$E_n = E_1 \dots E_{n-1} + 1$$

Now we are going to work on the sum of the reciprocals of the first n Euclid number.

$$S_n = \sum_{i=0}^{n} \frac{1}{E_i}$$

$$= \frac{1}{E_1} + \cdots + \frac{1}{E_n}$$

$$= 1 - \frac{1}{E_1 \dots E_n} = 1 - \frac{1}{E_{n+1} - 1}$$

Question 3

4). 4.24

Let's express n in base p:

$$n = d_kp^k + d_{k-1}p^{k-1} + \cdots + d_0$$

$$\text{The sum of the digits is: } \nu_p(n) = d_k + d_{k-1} + \cdots + d_0$$

Let $e_p(n!)$ represent the sum of the digits of $n!$ in base p, and $\nu_p(n!)$ represent the highest power of p dividing $n!$

$$e_p(n!) = \text{sum of the digits of } n! \text{ in base } p$$
$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$
$$\nu_p(n) = \text{sum of the digits of } n \text{ in base } p$$

The term $\nu_p(n)$ adjusts the total count of digits by accounting for the contributions from the factors of p in n. Now the term $\frac{\nu_p(n)}{p-1}$ represents how many full sets of p are in n. Consider the contribution of a digit d in position m in base p. The contribution of this digit to $e_p(n!)$ is:

$$d \cdot (p^m + p^{m-1} + \cdot + p^0) = d \cdot \frac{p^{m+1} - 1}{p - 1}$$

This formula arises from the geometric series for summing powers of p. The sum of the digits of $n!$ in base p can be expressed as:

$$e_p(n!) = n - \frac{\nu_p(n)}{p - 1}$$

Where n is the total number of digits and $\nu_p(n)$ counts how many times p divides into n.

Question 4

5). 4.26

We have a tree called Stern-Brocot tree. The idea is to start with the two fractions $(\frac{0}{1}, \frac{1}{0})$ which are 0 and ∞. Then its going to repeat the following operation as many times:

$$\text{Insert } \frac{m + m‘}{n + n‘} \text{ between two adjacent fractions } \frac{m}{n} \text{ and } \frac{m‘}{n‘}$$

In this tree, if $\frac{m}{n}$ and $\frac{m‘}{n‘}$ are consecutive fractions at any stage of the construction, we have:

$$m‘n - mn‘ = 1$$

This relation is true initially $(1.1 - 0.0 = 1)$; and when we insert a new mediant $\frac{m+m‘}{n+n‘}$, the new cases that need to be checked are:

$$(m + m‘)m - m(n + n‘) = 1$$
$$m‘(n + n‘) - (m + m‘)n‘ = 1$$

Both of these equations are equivalent to the original condition that they replace. Therefore the given rule is invariant at all stages of the construction. Furthermore, if $\frac{m}{n} < \frac{m‘}{n‘}$ and if all values are nonnegative, we can say that:

$$\frac{m}{n} < \frac{m + m‘}{n + n‘} < \frac{m‘}{n‘}$$

A mediant fraction isn't halfway between its progenitors, but it does lie somewhere in between. Therefore the construction preserves order, and we couldn't possibly get the same fraction in two differenct places.

Now our $g(n)$ is a sub-tree of Stern-Brocot tree. When considering $g(n)$, it includes fractions $\frac{m}{n}$ such that $mn \leq N$. $g(n)$ includes only those fractions with specific constraints on ther numerators and denominators. As we navigate the Stern-Brocot tree, each level of the tree represents fractions with increasing denominators and numerators. The condition $mn \leq N$ restricts this traversal to a certain range, forming a sub-tree of fractions that adhere to this rule. In this sub-tree, if $\frac{m}{n}$ precedes $\frac{m‘}{n‘}$, they maintain the property $m‘n - mn‘ = 1$ because they are generated from the mediants of adjacent fractions in the tree.

Question 5

6). 4.30

Let $n_1, n_2, \ldots, n_k$ be pairwise coprime integers, and let $a_1, a_2, \ldots, a_k$ be any integers. Then there exists an integer x such that:

$$x \equiv a_i \mod n_i \quad \text{for } i = 1, 2, \ldots, k$$

Moreover, this solution x is unique modulo N, where $N = n_1 n_2 \cdots n_k$. We define $N = n_1 n_2 \cdots n_k$ and for each i, let:

$$N_i = \frac{N}{n_i}$$

Since the n_i are pairwise coprime, N_i is also coprime to n_i for each i.

By Bézout's identity, there exist integers b_i such that:

$$N_i b_i \equiv 1 \mod n_i$$

Therefore, for each i, we can write:

$$x_i = a_i N_i b_i$$

Now, we can construct x as follows:

$$x = \sum_{i=1}^{k} x_i = \sum_{i=1}^{k} a_i N_i b_i$$

We will show that this x satisfies the congruences.

For any j:

$$x \equiv \sum_{i=1}^{k} a_i N_i b_i \mod n_j$$

Notice that $N_i \equiv 0 \mod n_j$ for all $i \neq j$, so:

$$x \equiv a_j N_j b_j \mod n_j$$

Since $N_j b_j \equiv 1 \mod n_j$, we have:

$$x \equiv a_j \mod n_j$$

This shows that x satisfies all the congruences.
Now that we proved there is an answer, we are going to prove that it is unique.
Suppose there are two solutions x_1 and x_2 such that:

$$x_1 \equiv a_i \mod n_i \quad \text{and} \quad x_2 \equiv a_i \mod n_i \quad \text{for all } i$$

Then:

$$x_1 - x_2 \equiv 0 \mod n_i$$

for all i. Let $d = x_1 - x_2$. This implies d is divisible by each n_i. Since the n_i are pairwise coprime, d is divisible by their product N:

$$d \equiv 0 \mod N$$

Hence, $x_1 \equiv x_2 \mod N$, proving the uniqueness of the solution modulo N.

Question 6

7). 4.38

First let's take a look at the equation:

$$\gcd((a^n - b^n), (a^m - b^m)) = a^{\gcd(n,m)} - b^{\gcd(n,m)}$$
$$a \perp b, a > b, 0 \leq m < n$$

Now we are going to check some lemmas before proving the equation. First, we know that:

$$\gcd(a, b) = \gcd(a, b - k \times a)$$

Next, we have a polynomial identity for $a^n - b^n$:

$$(a^n - b^n) = (a - b)(a^{n-1}b^0 + \cdots + a^0b^{n-1})$$

So let's assume that $r = n \mod m$. As the polynomial identity displayed, we can have:

$$(a^n - b^n) = (a^m - b^m)(a^{n-m}b^0 + \cdots + a^rb^{n-m-r}) + b^{m\lfloor \frac{n}{m} \rfloor}(a^r - b^r)$$

Now, we are going replace this in the first equation:

$$\gcd((a^m - b^m), (a^m - b^m)(a^{n-m}b^0 + \cdots + a^rb^{n-m-r}) + b^{m\lfloor \frac{n}{m} \rfloor}(a^r - b^r))$$
$$= \gcd((a^m - b^m), b^{m\lfloor \frac{n}{m} \rfloor}(a^r - b^r))$$

Since we have $a \perp b$, it means that $b^{m\lfloor \frac{n}{m} \rfloor}$ has no common factors in this equation. So we are going to remove it and have:

$$\gcd((a^n - b^n), (a^m - b^m)) = \gcd((a^m - b^m), (a^r - b^r)) \text{ where } r = n \mod m$$

If we continue this approach, we can go until we reach $\gcd(m, n)$. Since the next number after that will be zero, we can prove the validation of our equation:

$$\gcd((a^n - b^n), (a^m - b^m)) = \gcd((a^m - b^m), (a^r - b^r)) \text{ where } r = n \mod m$$
$$\ldots = \gcd((a^{\gcd(m,n)} - b^{\gcd(m,n)}, 0) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$$

Question 7

9).

If we have $m \mid n$ (meaning that n can be divided by m), then n should be divided by all prime factors of n.

$$m = {p_1}^{a_1} \times {p_2}^{a_2} \ldots \times {p_k}^{a_k}$$
$$m \mid n \Rightarrow {p_1}^{a_1} \times {p_2}^{a_2} \ldots \times {p_k}^{a_k} \mid n$$
$${p_1}^{a_1} \mid n \wedge {p_2}^{a_2} \mid n \ldots \wedge {p_k}^{a_k} \mid n$$

In this problem, we can write number six as its prime factors 2×3. Therefore, we need need to prove that:

$$2 \mid n \times (n+1) \times (n+2) \wedge 3 \mid n \times (n+1) \times (n+2)$$

Since 2 and 3 are coprime, then we can prove each of them individually. Let's start with 2:

$$\text{if } n \equiv 0 \mod 2 \to n \times (n+1) \times (n+2) \equiv 0 \mod 2$$
$$\text{if } n \equiv 1 \mod 2 \to n+1 \equiv 2 \equiv 0 \mod 2 \to n \times (n+1) \times (n+2) \equiv 0 \mod 2$$

To say it in simple words, for each real number as N, one of the two N or $N+1$ is divided by 2. As for 3:

$$\text{if } n \equiv 0 \mod 3 \to n \times (n+1) \times (n+2) \equiv 0 \mod 3$$
$$\text{if } n \equiv 1 \mod 3 \to n+2 \equiv 3 \equiv 0 \mod 3 \to n \times (n+1) \times (n+2) \equiv 0 \mod 3$$
$$\text{if } n \equiv 2 \mod 3 \to n+1 \equiv 3 \equiv 0 \mod 3 \to n \times (n+1) \times (n+2) \equiv 0 \mod 3$$

To say it in simple words, for each real number as N, one of the three N, $N+1$, or $N+2$ is divided by 3. Now we can say:

$$2 \mid n \times (n+1) \times (n+2) \wedge 3 \mid n \times (n+1) \times (n+2)$$
$$6 \mid n \times (n+1) \times (n+2)$$

Question 8

10).

Let's say we have a and b, first we rewrite them as their prime factors:

$$a = {p_1}^{e_1} {p_2}^{e_2} \ldots {p_k}^{e_k}$$
$$b = {p_1}^{f_1} {p_2}^{f_2} \ldots {p_k}^{f_k}$$

Now we are going to compute $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ with these values:

$$\gcd(a, b) = {p_1}^{\min(e_1, f_1)} {p_2}^{\min(e_2, f_2)} \ldots {p_k}^{\min(e_k, f_k)}$$
$$\operatorname{lcm}(a, b) = {p_1}^{\max(e_1, f_1)} {p_2}^{\max(e_2, f_2)} \ldots {p_k}^{\max(e_k, f_k)}$$
$$\gcd(a, b) \times \operatorname{lcm}(a, b) = \prod_{i=1}^{k} {p_i}^{\min(e_i, f_i) + \max(e_i, f_i)}$$

Now we know that $\min(a, b) + \max(a, b) = a + b$, therefore we have:

$$\begin{aligned}\gcd(a, b) \times \operatorname{lcm}(a, b) &= \prod_{i=1}^{k} {p_i}^{e_i+f_i} \\ &= \prod_{i=1}^{k} {p_i}^{e_i} {p_i}^{f_i} \\ &= \prod_{i=1}^{k} {p_i}^{e_i} \times \prod_{i=1}^{k} {p_i}^{f_i} = a \times b\end{aligned}$$