Homework 1

Wenye Xiong 2023533141

March 7, 2024

1 Problem 1

Assume the statement is false. This means there exists a real number x and a positive integer n such that:

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \neq \left\lfloor \frac{x}{n} \right\rfloor$$

$n > 0$ and $x - 1 < \lfloor x \rfloor < x$, so we can write:

$$\left\lfloor \frac{x-1}{n} \right\rfloor < \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor < \left\lfloor \frac{x}{n} \right\rfloor$$

Both of the left and right hand side of the equation are integers, and $n > 1$, so we have the only choice:

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor - 1$$

Substituting this back into the original inequality, we get:

$$\left\lfloor \frac{x}{n} \right\rfloor \neq \left\lfloor \frac{x}{n} \right\rfloor - 1$$

This is a contradiction, so the original statement is true.

2 Problem 2

Assume that gcd(a,b)=1 and gcd(a,c)=1. Then we have:

$$ax + by = 1$$
$$au + cv = 1$$

x,y,u,v are all integers.

Multiplying the first equation with cv, we get:

$$acvx + bcyv = cv$$

Add both sides of the equation with au, we get:

$$acvx + bcyv + au = cv + au$$

Which means:

$$a(cvx + u) + bc(yv) = 1$$

So we have gcd(a,bc)=1 because as c,v,x,u,y,v are all integers, cvx+u,yv are also integers.

So we have proved that if gcd(a,b)=1 and gcd(a,c)=1, then gcd(a,bc)=1.

Next we will prove that if gcd(a,bc)=1, then gcd(a,b)=1 and gcd(a,c)=1.

Assume that gcd(a,bc)=1, then we have:

$$ax + bcy = 1$$

We know that x,c,y are all integers, so we can write the equation as:

$$ax + b(cy) = 1 ,$$

where x,cy are integers.

So we have gcd(a,b)=1.

Similarly, we can prove that gcd(a,c)=1 by writing the equation as:

$$ax + c(by) = 1 \qquad ,$$

where x,by are integers.

So we have proved if gcd(a,bc)=1, then gcd(a,b)=1, gcd(a,c)=1

In conclusion, we have proved that gcd(a,b)=1 and gcd(a,c)=1 if and only if gcd(a,bc)=1.

3 Problem 3

$\alpha = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$

Here's the proof:
The first term $\left\lfloor \frac{n}{p} \right\rfloor$ appears since we want to count the number of terms less than n and are multiples of p. We first assume that each of these contributes one p to n!

But then when we consider multiples of p^2, we are not multiplying just one p but two of these p to the product. So we now count the number of multiple of p^2 less than n and add them.

This is captured by the second term $\left\lfloor \frac{n}{p^2} \right\rfloor$. Repeat this to account for higher powers of p less than n, and we have $\alpha = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$
I can write the sum from 1 to infinity because the terms after $\left\lfloor \frac{n}{p^{log_p n}} \right\rfloor$ are all 0

4 Problem 4

Assume that there exists a x such that we can find a n where $x^7 = n$ and $x \notin \mathbb{Z}^+$.

And since x is a rational number, we can write x as $\frac{a}{b}$, where a and b are both positive integers and gcd(a,b)=1

So we have $\frac{a^7}{b^7} = n$

Which means a^7 and b^7 share a common factor b^7

This obviously contradicts with the fact that gcd(a,b)=1, according to the FTA. So if x is a rational number and exists $n \in \mathbb{Z}^+$, then $x \in \mathbb{Z}^+$

5 Problem 5

Because we have $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$ and $a \equiv b \pmod{n}$, we can easily find that n divides a-b

Let's define $\sum_{i=0}^{k} c_i a^i$ as S_a and $\sum_{i=0}^{k} c_i b^i$ as S_b

Then we have $S_a - S_b = \sum_{i=0}^{k} c_i(a^i - b^i)$

We can factor out a-b from the right hand side of the equation, and we get:

$S_a - S_b = (a-b)\sum_{i=0}^{k} c_i(a^{i-1} + a^{i-2}b + ... + b^{i-1})$

As we have proved that n divides a-b, we can write a-b as $n \times m$

So we have $S_a - S_b = n \times m \times \sum_{i=0}^{k} c_i(a^{i-1} + a^{i-2}b + ... + b^{i-1})$

Which means $S_a - S_b$ is divisible by n. So we have proved that $S_a \equiv S_b$ (mod n)

6 Problem 6

Multiplying $u^2 + uv + v^2$ with $u - v$, we get $u^3 - v^3$

So we have $u^3 - v^3 \equiv 0 \pmod 9$

Assume that u and v are not equal after mod 3:

If $u \in [0]_3$ and $v \notin [0]_3$, then $u^3 - v^3 \equiv v^3 \equiv 2$ or $1 \pmod 3$. The same when $v \in [0]_3$ and $u \notin [0]_3$

If $u \in [1]_3$ and $v \in [2]_3$, then $u^3 - v^3 \equiv 2 \pmod 3$
Or if $u \in [2]_3$ and $v \in [1]_3$, then $u^3 - v^3 \equiv 1 \pmod 3$

None of these cases can satisfy the original equation, so we have proved that $u \equiv v \pmod 3$.

Assume that $u, v \in [1]_3$, then we can write u,v as $3k + 1, 3l + 1$

Substituting these into the original equation, we get:

$(3k + 1)^2 + (3k + 1)(3l + 1) + (3l + 1)^2 \equiv 0 \pmod 9$
Unfolding the equation, we get:,

$$9k^2 + 9k + 9l^2 + 9l + 9kl + 3 \equiv 0 \pmod 9$$

Which is always false, so we have proved that $u, v \in [1]_3$ is not a solution.

Next, consider the case where $u, v \in [2]_3$, then we can write u,v as $3k+2, 3l+2$

Substituting these into the original equation, we get:

$(3k+2)^2+(3k+2)(3l+2)+(3l+2)^2 \equiv 0 \pmod 9$, Unfolding the equation, we get:

$$9k^2 + 18k + 9l^2 + 18l + 9kl + 12 \equiv 0 \pmod 9$$

Which is always false, so we have proved that $u, v \in [2]_3$ is not a solution.

Then consider the last case where $u, v \in [0]_3$, then we can write u,v as $3k, 3l$

Substituting these into the original equation, we get:

$(3k)^2 + (3k)(3l) + (3l)^2 \equiv 0 \pmod 9$, Unfolding the equation, we get:

$$9k^2 + 9kl + 9l^2 \equiv 0 \pmod 9$$

Which is always true, so we have proved that $u, v \in [0]_3$ is a solution.

In conclusion, we have proved that $u, v \in [0]_3$ is the only solution.