Homework 1

Wenye Xiong 2023533141

March 26, 2024

1 Problem 1

$n_1 = 13, n_2 = 17, n_3 = 19, n_4 = 23$, these are all prime numbers.

So we let $n = n_1 n_2 n_3 n_4 = 13 \times 17 \times 19 \times 23 = 96577$.

Then we let $N_1 = n/n_1 = 96577/13 = 7429$, $N_2 = n/n_2 = 96577/17 = 5681$, $N_3 = n/n_3 = 96577/19 = 5083$, $N_4 = n/n_4 = 96577/23 = 4199$.

Using the Extended Euclidean Algorithm, we can find $s_1, t_1, s_2, t_2, s_3, t_3, s_4, t_4$ such that $s_1 n_1 + t_1 N_1 = 1$, $s_2 n_2 + t_2 N_2 = 1$, $s_3 n_3 + t_3 N_3 = 1$, $s_4 n_4 + t_4 N_4 = 1$.

We get: $s_1 = 1143, t_1 = -2$; $s_2 = -2005, t_2 = 6$; $s_3 = -535, t_3 = 2$; $s_4 = 1278, t_4 = -7$.

So the one solution is:
$b = b_1 N_1 t_1 + b_2 N_2 t_2 + b_3 N_3 t_3 + b_4 N_4 t_4 = b_1 \cdot 7429 \cdot (-2) + b_2 \cdot 5681 \cdot 6 + b_3 \cdot 5083 \cdot 2 + b_4 \cdot 4199 \cdot (-7) = -14858 b_1 + 34086 b_2 + 10166 b_3 - 29393 b_4$.

Then $x \in \mathbb{Z}$ is a solution iff $x \equiv b \pmod{96577}$. That is $[b]_{96577}$

2 Problem 2

The first equation requires that $x = 6t + b_1$.

Take this into the second equation, we get $6t + b_1 \equiv b2 \pmod{15}$.

So $6t \equiv b_2 - b_1 \pmod{15}$.

Since $gcd(6, 15) = 3$, it is clear that $3|b_2 - b_1$.

Under this condition, let's solve the problem:

The first equation requires that $x = 6t_1 + b_1$., while the second equation requires that $x = 15t_2 + b_2$.

So $6t_1 + b_1 = 15t_2 + b_2$.

And we get: $6t_1 - 15t_2 = b_2 - b_1$. Because $3|b_2 - b_1$, we can write it as: $2t_1 - 5t_2 = \frac{b_2 - b_1}{3}$.

Using the Extended Euclidean Algorithm, we can find s, t such that $2s - 5t = 1$. The answer is $s = 3, t = 1$

So one solution is:

$$t_1 = 3 \cdot \frac{b_2 - b_1}{3} = b_2 - b_1, t_2 = \frac{b_2 - b_1}{3}, x = 6b_2 - 5b_1$$

Then $x \in \mathbb{Z}$ is a solution iff $x \equiv 6b_2 - 5b_1 \pmod{30}$. That is $[6b_2 - 5b_1]_{30}$

3 Problem 3

To prove $x \star y = xyxy + 2$made (G,) an Abelian Group, we need to prove the following four properties:

1. Closure: Both x and y are greater than 1, so we know that $x \star y = xy - (x + y) + 1 + 1 = (x - 1) \cdot (y - 1) + 1$ is also greater than 1. So $x \star y$ is in G.

2. Associativity: Let x, y, z be three elements in G, $(x \star y) \star z = ((x-1) \cdot (y-1) + 1) \star z = ((x-1) \cdot (y-1) + 1 - 1) \cdot (z-1) + 1 = (x-1) \cdot ((y-1) \cdot (z-1) + 1 - 1) + 1 = x \star (y \star z)$.

3. Identity: Let e = 2, then $x \star e = x \star 2 = 2x - (x + 2) + 2 = x$, $e \star x = 2 \star x = 2x - (x + 2) + 2 = x$.

4. Inverse: Let $x \in G$, $x^{-1} = 1 + \frac{1}{x-1}$, then $x \star x^{-1} = x \star (1 + \frac{1}{x-1}) = x \cdot (1 + \frac{1}{x-1}) - (x + 1 + \frac{1}{x-1}) + 2 = 2 = e$.
We have $x^{-1} = 1 + \frac{1}{x-1}$. And since $x > 1$, it is clear that x^{-1} is also in G.

5. Commutativity: Let x, y be two elements in G, $x \star y = xy - (x + y) + 2 = yx - (y + x) + 2 = y \star x$.

So (G,) is an Abelian Group.

4 Problem 4

$\mathbb{Z}_{23}^*$ is a multiplicative Abelian group of order 22, so for any $a \in \mathbb{Z}_{23}^*$, $a^{22} = 1$.

Thus the order of any element in that group must divide 22, so all orders must be 1, 2, 11, or 22.

To find the generator, we are looking for an element whose order is 22.

To find them, we need only compute the second and 11th powers of each element modulo 23; when neither is 1, we have found an element of order 22.

These are not generators:
1 (of cause)
2 ($2^{11} \equiv 1 \pmod{23}$)
3 ($3^{11} \equiv 1 \pmod{23}$)
4 ($4^{11} \equiv 1 \pmod{23}$)
6 ($6^{11} \equiv 1 \pmod{23}$)
8 ($8^{11} \equiv 1 \pmod{23}$)
9 ($9^{11} \equiv 1 \pmod{23}$)
12 ($12^{11} \equiv 1 \pmod{23}$)
13 ($13^{11} \equiv 1 \pmod{23}$)
16 ($16^{11} \equiv 1 \pmod{23}$)
18 ($18^{11} \equiv 1 \pmod{23}$)
22 ($22^2 \equiv 1 \pmod{23}$)

In conclusion, these are the generators of $\mathbb{Z}_{23}^*$: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

$f(X) = X^5 + 2X^4 + 5X^3 + 3X^2 + 12X + 18$

For this problem, I couldn't come up with a better solution, so I wrote a program in cpp to find the roots. Here's the code.

```
#include <bits/stdc++.h>
using namespace std;
int poly(int x)
{
```

```
    return pow(x, 5) + 2 * pow(x, 4) + 5 * pow(x, 3) + 3 * pow(x, 2 ) +
        12 * x + 18;
}
int main()
{
    for (int i = 1; i <= 23; i++)
    {
        if (poly(i) % 23 == 0)
        {
            cout << i << " is a root of the polynomial" << endl;
        }
    }
    return 0;
}
```

The roots of this polynomial are 3, 11, 16, 17, 20.

5 Problem 5

According to the definition of order, o(a) is the least integer greater than 0 such that $a^{o(a)} = 1$. To prove that $o(a)|k$, let's suppose that there is a postive integer k such that $a^k = 1$ and $o(a) \nmid k$.

Then we can write k as $k = o(a)q + r$, where $0 < r < o(a)$.

So $a^k = a^{o(a)q+r} = (a^{o(a)})^q \cdot a^r = 1^q \cdot a^r = a^r$.

Since $a^k = 1$, we have $a^r = 1$.

But $0 < r < o(a)$, which contradicts the definition of order.

So $o(a)|k$.

For a multiplicative Abelian Group G, G = 1,2,3,...,m, and for any $i \neq j$, $aa_i \neq aa_j$.

So $aa_1 \cdot aa_2 \cdot aa_3 \cdot ... \cdot aa_m = a_1a_2....a_m$.
Thus $a^m = 1$. Together with the previous result, the order of any group element must be a divisor of the group's order.

6 Problem 6

According to the definition of order, o(a) is the least integer greater than 0 such that $a^{o(a)} = 1$ and o(b) is the least integer greater than 0 such that $b^{o(b)} = 1$.

Let $m = o(a), n = o(b)$. Consider $(ab)^{mn}$, we have $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1$. That means $o(ab)|mn$

Consider an integer l such that $(ab)^l = 1$

Then we have $a^l b^l = 1$, which means $a^l = b^{-l}$ since $a^l b^l b^{-l} = 1 \cdot b^{-l}$

So $a^{nl} = b^{-nl} = (b^n)^{-l} = 1$, which means $o(a)|nl$ as we have proved in Problem 5.

Because $gcd(o(a), o(b)) = 1$, we have $o(a)|l$. And similarly, we get $o(b)|l$

Because $gcd(o(a), o(b)) = 1$, so $mn|l = o(ab)$ and with $o(ab)|mn$. In general, $o(ab) = o(a) \cdot o(b)$

So $o(ab) = o(a) \cdot o(b)$.