Homework 5

Wenye Xiong 2023533141

April 2, 2024

1 Problem 1

We need to find all integers i such that g^i is a generator of $\mathbb{Z}_p^*$, where $p = 107$ and $g = 2$.

First, we know that the order of $\mathbb{Z}_p^*$ is $p - 1 = 106$.

Then, we know that the order of g^i is $\frac{106}{gcd(i,106)}$.

So, g^i is a generator of $\mathbb{Z}_p^*$ iff $gcd(i, 106) = 1$.
That is all odd integer i such that $1 \leq i \leq 106$ except 53.

To verify my provement, I wrote a program.

```
#include <bits/stdc++.h>
using namespace std;
int powmod(int a, int b, int m)
{
    int res = 1;
    while (b--)
    {
        res = (res * a) % m;
    }
    return res;
}
bool isgenerator(int g, int p)
{
    set<int> s;
    for (int i = 1; i < p; i++)
    {
```

```
        s.insert(powmod(g, i, p));
    }
    return s.size() == p - 1;
}
int main()
{
    for (int i = 1; i <= 106; i++)
    {
        if (isgenerator(powmod(2, i, 107), 107))
        {
            cout << i << endl;
        }
    }
    return 0;
}
```

According to the result of the program, we can see that all the integers i such that g^i is a generator of $\mathbb{Z}_p^*$ are:
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 55 57 59 61 63 65 67 69 71 73 75 77 79 81 83 85 87 89 91 93 95 97 99 101 103 105

2 Problem 2

We know that the order of $\mathbb{Z}_p^*$ is $p-1=2q$.
The order of a generator a of $\mathbb{Z}_p^*$ is also $2q$, which means that the smallest integer l to satisfy $a^l=1$ is 2q.

For g^i, because $\frac{(p-1)\cdot i}{gcd(i,p-1)} \geq (p-1)$, so $(g^i)^{\frac{p-1}{gcd(i,p-1)}} = g^{i\cdot\frac{p-1}{gcd(i,p-1)}} = g^{ik}$, where k is an integer no less than 1.

So, $(g^i)^{\frac{p-1}{gcd(i,p-1)}} = 1$, that means the order of g^i is no greater than $\frac{p-1}{gcd(i,p-1)}$.

So, g^i is a generator of $\mathbb{Z}_p^*$ only if $gcd(i,p-1)=1$.

Then let's prove that if $gcd(i,2q)=1$, then g^i is a generator of $\mathbb{Z}_p^*$.

Suppose that we can find an integer m such that g^m is not a generator but $gcd(m,p-1)=1$.

Take n as the least integer to satisfy $(g^m)^n=1$.

Also, because $(g^m)^{(p-1)}=1$, we have $n|(p-1)$. Which means n is 2 or q.

We have $g^{m\cdot n}=1$, which means $m\cdot n$ is a multiple of p-1.

Because $gcd(m,p-1)=1$, and n can only be 2 or q, so mn can only be a multiple of 2 or a multiple q, but not a multiple of 2q, which is p-1. And this is just a contradiction.

So we have proved that g^i is a generator of $\mathbb{Z}_p^*$ iff $gcd(i,2q)=1$.

Of all the integers i such that $1 \leq i \leq 2q$, the number of integers i that satisfy $gcd(i,2q)=1$ is $\phi(2q)$, which is $q-1$.

So the number of generators of $\mathbb{Z}_p^*$ is $q-1$.

3 Problem 3

```
p=1797693134862315907729305190789024733617976978942306572734300811577326758055009
6313270847732240753602112011387987139335765878976881441662249284743063947412437776
789342486548527630221960124609411945308295208500576883815068234246288147391311054
0827237163350510684586298239947245938479716304835356329624227998859

A=1129835751630026189475896666667354281816845178451448750969029100664347239526230
1660339321250121412739990882322349247872597126604275489279817778126751282160747054
528305947268903473131302761986422868846643825832755204543759020379063550672860377
47990211270498725719832545069939211537187397967692960974047174481O8

B=1117727678052102394963651916915168810433949881962970620138536466745747434010427
3644732888615642962919269160152639836608801273674945462668628146757920567508446198
949451329462406607413724791303733004048727534691325334573342976778190097710268718
53784116601471902964123133033215335861025521234574995637892553213669

a=0
b=0
for i in range(1, 10000):
    if pow(3, i, p) == A:
        a = i
        print(i)
        break

for i in range(1, 10000):
    if pow(3, i, p) == B:
        b = i
        print(i)
        break

print(pow(A, b, p))
print(pow(B, a, p))
```

The result: a = 9385, b = 3083
The output of Alice and Bob is 108281127834534623810417078020561498665963920722439039409874596727792606753195226630990803887709039825462505249924203502002076243274206123001706208026653029057500457776843481258274843650075907186383731879368899673093247226552949922258154109141050722107250459531050193524575407729955089783156991072473983501282

4 Problem 4

For x in $[1, 2]$, $f(x) = 10^{1/(x-1)}$, that makes up $[10, +\infty)$

For x in $(5, 6]$, let $f(6) = 8 - \frac{1}{2}, f(6 - 2^{-n}) = 8 - 2^{-n-1}, n = 1, 2, 3, ...$

$f(x) = x + 2$, for all other $x \in (5, 6]$ And we have constructed a bijection between $(5, 6]$ and $(7, 8)$

Now our mission is to construct a bijection between $[3, 4)$ and $(9, 10)$.

Let $f(3) = 9 + \frac{1}{2}, f(3 + 2^{-n}) = 9 + 2^{-n-1}, n = 1, 2, 3, ...$

$f(x) = x + 6$, for all other $x \in [3, 4)$

Then we can see that $f(x)$ is a bijection between $[1, 2] \cup [3, 4) \cup (5, 6]$ and $(7, 8) \cup (9, \infty)$

5 Problem 5

Suppose that $|(a_1, a_2, a_3, ...) : a_i \in 1, 2, 3\ for\ all\ i = 1, 2, 3, ...| = |\mathbb{Z}^+|$
Denote $(a_1, a_2, a_3, ...) : a_i \in 1, 2, 3\ for\ all\ i = 1, 2, 3, ...$ as S, then we have a bijection between f: $\mathrm{Z}^+ \to S$.

f(1) = $\mathrm{a}_{11}, a_{12}, a_{13}, ...$
$f(2) = a_{21}, a_{22}, a_{23}, ...$
$f(3) = a_{31}, a_{32}, a_{33}, ...$

...
$f(n) = a_{n1}, a_{n2}, a_{n3}, ...$

Then we let $a_i = 1$ if $a_{ii} \neq 1$, $a_i = 2$ if $a_{ii} = 1$.

Obviously, set s = a1, a2, a3, . . . is in S, but has no preimage in $\mathrm{Z}^+, since$s $\neq f(i)$ for every i = 1,2,3,...n. That means f can't be a bijection

So $|(a_1, a_2, a_3, ...) : a_i \in 1, 2, 3\ for\ all\ i = 1, 2, 3, ...| \neq |\mathbb{Z}^+|$.

6 Problem 6

Suppose that $|A| = k$, because $A \cap B = \emptyset$, B can only be the subsets of X taken these k elements away.

For A, the number of ways to choose k elements X is C_n^k.

For B, we want to know the number of subsets of X taken k elements away, that is a normal set with n-k elements. And the number is 2^{n-k}.

And the total number of sets A,B is just to sum up all the possibilities of k from 0 to n. But remember we also make many repeatition, since the set$\{A, B\}$ is just the same as $\{B, A\}$. So we need to divide this result by 2. But what is tricky here is the set $\{\emptyset, \emptyset\}$: we have only counted it once! So if we want the real answer, we have to add 1 before dividing 2.

So the total number of sets is $\frac{(\sum_{i=0}^{n} C_n^i 2^{n-i})+1}{2}$, which can be further simplified as $\frac{(3^n)+1}{2}$

So the final result is $\frac{(3^n)+1}{2}$