MATHEMATICAL CIPHERS

Delving into the Cryptographic Complexities of Number Theory and Abstract Algebra

Question 1

Prove that any prime number $p \equiv 1 \bmod 4$ can be expressed as the sum of two squares.

Question 1

Prove that any prime number $p \equiv 1 \bmod 4$ can be expressed as the sum of two squares.

Key points to note –

- **Every square is either 0(mod4) or 1(mod4)**
  - (2n)^2 = 4n^2 = 0(mod4)
  - (2n+1)^2 = 4n^2 + 4n + 1 = 1(mod4)
- Then what can be the sum of 2 possible squares –
  - 0 + 0 = 0(mod4) – Not a prime
  - 1 + 1 = 2(mod4) = 0(mod2) – Not a prime
  - 0 + 1 = 1(mod4) – Can be a prime

Question 1

Prove that any prime number $p \equiv 1 \bmod 4$ can be expressed as the sum of two squares.

The exact proof is complicated but if you wanna know how its done exactly –

See this link

Question 2

Solve the system of congruences:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

This is a typical **Chinese Remainder Theorem** question

- So let, x = 2mod3, ie. x = 3k+2
- Now, 3k+2 = 3mod5 => So, 3k = 1 mod 5
- So, k = 2 mod 5 => k = 5m+2
- Then, x = 3k+2 = 15m+8
- So, 15m+8 = 2 mod 7 => 15m = 1 mod7 => m = 1 mod 7 => m = 7n+1
- So, x = 15(7n+1)+8 = 105n+23
- **Hence, x = 23 mod 105**

Number Theory

Why its needed?

- **RSA cryptosystem –** relies on the difficulty of factoring large composite numbers into their prime factors.
- **Diffie-Hellman Key Exchange**: Uses modular exponentiation.
- **Digital Signature Algorithm (DSA) –** depends on the difficulty of solving the discrete logarithm problem.
- **Error detection** – Many cryptographic hash functions and error detection codes use number theoretic properties to ensure data integrity.

Cyclic Group

Let G be a finite group of order m (written multiplicatively).
Let g be in G
Consider the set { g^0, g^1, g^2, …. }
Also, g^m = g^0 = 1, so that the set has at max m elements.

If in this way, we get a set of m elements, we say **'g' is a generator for the set G.**

Discrete Logarithm Problem

- Fix cyclic group G of order m, and generator g
- We know that $\{g^0, g^1, .., g^{(m-1)}\} = G$
- For every $h \in G$, there is a unique $x \in Zm^*$ s.t. $g^x = h$
- Define (base g)logh to be this x - the discrete logarithm of h with respect to g (in the group G)

Discrete Logarithm Problem

Dlog problem in G

- given g, h compute log(g)h

And why do we use this?

- Because solving this is **hard !!**

Example 1

What is log(2)10 in the group Z(11)*?

Example 1

What is log(2)10 in the group Z(11)*?

What do we need to find?

- 'x' such that 2^x = 10mod11

What can 'x' be?

- 2^5 = 32
- and 32 = 10mod11

So x = 5;

That means -> log(2)10 = 5 in Z(11)* group.

More examples

Suppose $G = \mathbb{F}_{101}^{\times}$. Then $\log_3 37 = 24$, since $3^{24} \equiv 37 \bmod 101$.

Things to notice –

- This is a group under **multiplication**
- So, we need to find 'x' such that **3^x = 37mod101**
- x = 24
- Hence, **log(3)37 = 24**

More examples

Suppose $G = \mathbb{F}_{101}^{+}$. Then $\log_3 37 = 46$, since $46 \cdot 3 \equiv 37 \bmod 101$.

Things to notice –

- This is a group under **addition**
- So, we need to find ‘x’ such that **3*x = 37mod101**
- And **NOT** ‘x’ such that 3^x=37mod101
- x = 24
- Hence, **log(3)37 = 24**

Deffie-Hellman Problem

- Fix group G with generator g
- Define

$$DH_g(h_1, h_2) = DH(g^x, g^y) = g^{xy}$$

So, in essence, given g, h1, h2 we need to find x, y such that

x = log(g)h1 and **y = log(g)h2**

And finally, **DH(g)(h1, h2) = g^(xy)**

Example

In $\mathbb{Z}_{11}^*$, what is $\mathsf{DH}_2(5, 8)$?

Given g, h1, h2 lets first find x and y

So, x = log(2)5 => x = 4

and y = log(2)8 => y= 3

Thus, g^(xy) mod 11 = 2^(12) mod 11 = **4 mod 11**

So, DH(2)(5, 8) = 4

Computational Diffie-Hellman (CDH) Problem

Given g, h1, h2, compute DH(g)(h1, h2)

Decisional Diffie-Hellman (CDH) Problem

Given g, h1, h2, distinguish the correct DH(g)(h1, h2) from a uniform element of G

What does 'uniform' mean?
Any random pick from the set G, or more concretely, picking an element in such a way that every element is equally likely to be picked

Group selection

In cryptography, we basically choose **large prime-order groups** as it makes the computation of CDH and DDH problems touher.

Also, it might be worth recalling that in the prev meet, I discussed how **prime order groups are always cyclic.**

What's ahead?

If you are willing to go deeper in Discrete Logarithm Problem, I've linked notes from MIT that I found interesting

You can take a look at it - https://math.mit.edu/classes/18.783/2022/LectureNotes9.pdf

Let’s review what all we saw in
Number Theory

1) **Shift Cipher**
2) Some **Probability**
3) Concept of **Perfect Secrecy**
4) Moving to **Computational Secrecy**
5) **Modular Arithmetics**
6) Factoring and **Groups**
7) **Cyclic groups**
8) **Discrete Log Problems**, CDH, DDH

THANK YOU :)