BLS12-381 curve

order of curve is

es

Group theory Introduction

→ A non empty set G equipped with binary operation '$*$' is groupoid.

→ Groupoid is called quasi group.

Semigroup if binary operation '$*$' satisfies associative property

$$(a*b)*c = a*(b*c)$$

f

Monoid : If there exists identity element 'e' in G

$$e*a = a*e = a \quad \forall a \in G$$

$$0+2 = 2$$

→ semigroup $(N, \times)$ is monoid

Group :

[G1] closure: $a \in G, b \in G \Rightarrow a*b \in G \ \forall a,b \in G$

[G2] Associativity: $(a*b)*c = a*(b*c)$

[G3] Existence of identity:

$$e*a = a*e = a, \quad \forall a \in G.$$

[G4] Existence of inverse: Each element of G is invertible for every $a \in G$, there exist a^{-1} in G such that

$$a*a^{-1} = a^{-1}*a = e$$

Abelian group

$$a*b = b*a \quad \forall a,b \in G.$$

commutative under ~~multiplication~~ binary operation

Abelian group

Finite group:

Group is said to be finite if the underlying set G is a finite set and a group which is not finite is infinite group

Rings

Ring denoted $\langle R, +, * \rangle$ is set of elements with 2 binary operations called addition and multiplication

* Group + Abelian group
* closure under multiplication
* Associativity of multiplication
* Distributive law $a(b+c) = ab + ac$

$(a+b)c = ac + bc$

commutative ring: Already a Ring

$ab = ba$ for all $a, b \in R$

commutative for multiplication

Integral domain: Already a commutative ring

Multiplicative identity (M5): there is an element 1 $a1 = 1a = a$ for all $a \in R$

No zero divisors (M6): If $a, b \in R$ and $ab = 0$, then

* $a = 0$ or $b = 0$

Fields P

$\langle F, +, * \rangle$ is set of elements with two binary operation

(A1-M6) - F is an integral domain; that is F satisfies axioms A1 - A5

M7 (multiplicative inverse) ; for each a in F, except 0, there is element a^{-1} in F such that

$$a a^{-1} = (a^{-1}) a = 1$$

* Rational number
* Real
* complex

Finite field: galoi field that contains finite number of elements.

→ integer (mod p)

symbolic representation

- perfect secrecy
  ↳ something that seems equally likely.

~~$f(x) = a + b \cdot x$~~

$a - b = a + -b$

perfect secrecy proof

Let numbers be N. Given,

$a, b, v, \omega \in N$, $f(x \in N) = a + b \cdot x$

$f(v) = \omega$

$v \neq 0$

perfect secrecy for 1 degree polynomial secret sharing.

$a + b \cdot \theta = \omega$

proven by showing that exactly one b exist for each a, namely $(\omega + -a) \cdot v^{-1}$

Finite field : we donot care about "value" of numbers.

elements are irreducible polynomials.

shamir secret share

$0, 1, 2, \dots, \infty$

$\mathbb{Z}$ (zollen)

$\mathbb{Z}_{100}$ (Group of integers modulo 100)

$a + b := a + b \,\%\, 100$

finite field of numbers

$a + b := a + b \,\%\, 100$

$-a$ is represented as $100 - a$

we need a multiplicative inverse for finite field.

$a^{-1} =$

~~Q-Q~~:

why primes??

N = 10007

How to compute multiplicative inverse?

→ Discrete log problem
→ Discrete log assumption

Finite field arithmetic

GF(p^n)

Extended euclidean algorithm.

To have a multiplicative inverse

$A \times ? \equiv 1 \bmod B$

A and B must be relatively prime.

~~Upon the completion of session~~ for 3 MOD 5

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	2	~~3~~ -5	X

B) A (Q
R

~~Q = Q₁~~

$\boxed{T = T_1 - T_2 \times Q}$

B

$T = 1 - (-1) \times$

$T = 2$

short v

Roots of unity

Root of unity is complex number

$x^n = 1$

for any positive integer n, n^{th} root of uniy are complex solutionto equation $x^n=1$, there are n solution to equation

for x^4 there are 4 solutions

x^2 there are 2 solutions