21 LECTURES

Bitcoin Masterclass

Modular Arithmetic

Day 1

Objective

Understand from first principles how bitcoins are locked to keypairs

Digital signatures: ECDSA & Schnorr

modular arithmetic, finite fields, elliptic curves,
discrete log-problem, public key cryptography

Trigger warning: Math

Signatures in Bitcoin: Basic requirements

When Alice's coins are spent, we require some proof `w` that:

- Can be produced by Alice
- Can't be produced (efficiently) by anybody else
- Can be verified by everybody
- Commits to the details of the transaction

Roadmap

Algebra

- Groups
- Modular arithmetic
- (Finite) fields
- Discrete log

Elliptic curves

- EC math

ECs over finite fields

- Schnorr
- ECDSA

Algebraic groups

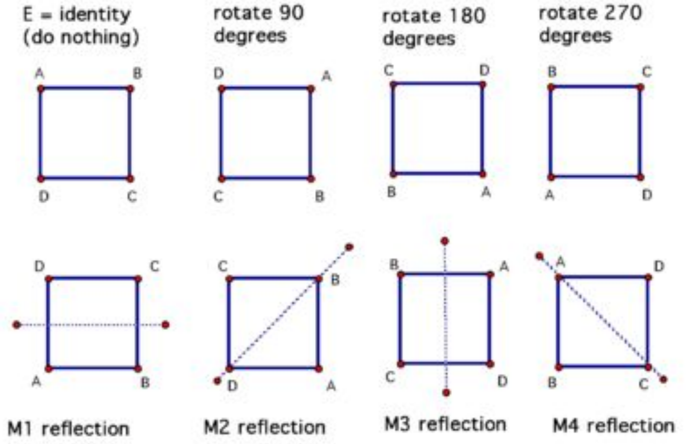
A group is a set `G` together with an operation `*` such that:

- `G is "closed" under *: a*b is in G`
- `*` is associative: `(a*b)*c = a*(b*c)`
- There exists an identity element `e: e*a = a*e = a` `(Blackboard: prove uniqueness)`
- Every element `a` has an inverse `b: a*b = b*a = e`

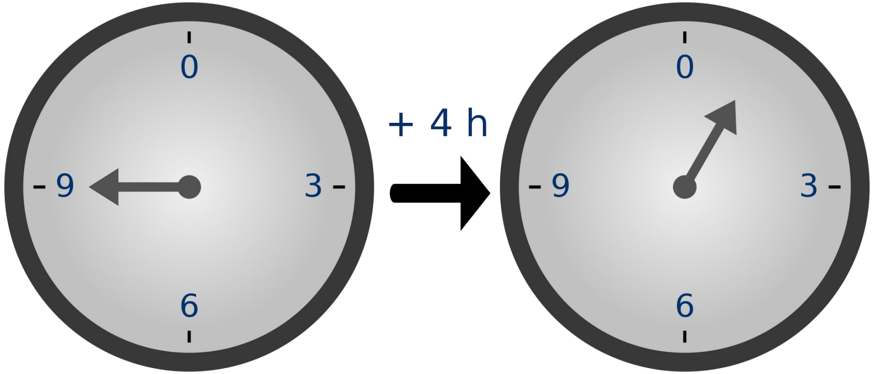
$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

+

$$\mathbb{Q} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{N}; b \neq 0 \right\}, *$$



Constructing finite groups (why?): Modular arithmetic



$$13 \equiv 1 \mod 12$$

$$a \equiv b \mod n \Rightarrow \exists k : a = k * n + b$$

Blackboard: some examples and basic properties

Two basic examples of finite modular groups

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}\text{, with addition}$$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1, 2, \ldots, n-1 \mid \text{coprime to } n\}\text{, with multiplication}$$

Why coprime?
Multiplicative inverse
a.k.a. “modular division”

Multiplication Mod 6

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Two more salient features of finite prime groups

- They are cyclic, i.e. generator `a` generates the group: `{a,a²,a³,…} = G`
  - Blackboard: Example
- Computing the multiplicative inverse is easy: Fermat's Little Theorem:
  - Blackboard: Examples

$$a^{p-1} \equiv 1 \mod p \Rightarrow a \cdot a^{p-2} \equiv 1 \mod p$$

Fields: Introducing a second group operation

- Addition, Multiplication
  - Associative, commutative, have identities
  - Distributive
- Every element has inverses, except the multiplicative inverse for the additive identity element
- Fields induce two groups

- Example: rational numbers

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathrm{GF}(p) = \{0, 1, \ldots, p-1\}$$

In a well-defined sense, this is the *only* field with p elements (“isomorphism”)

The discrete logarithm problem for finite cyclic groups

- In cyclic groups every element can be obtained by applying the group operation on the generator a certain number of times
  - Additive groups: `b = g*n (mod p)`
  - Multiplicative groups: `b = g^n (mod p)`
- Discrete log problem: Invert
  - `n = b/g (mod p)`
  - `n = log(b)` (base `g`) (naming!)
- Not all discrete log problems are hard, depends on the group and operation
  - Judge the above over GF(p)

Up next: An interesting candidate group to exploit this hardness

Roadmap

Algebra

- Groups
- Modular arithmetic
- (Finite) fields
- Discrete log

Elliptic curves

- EC math

ECs over finite fields

- Schnorr
- ECDSA

Elliptic curves

- Not ellipses
  - connected to finding arc lengths on ellipses
- Cubic equations
  - With some requirements on A, B

$$y^2 = x^3 + Ax + B$$

- Group structure
  - Line between A and B will intersect a third time