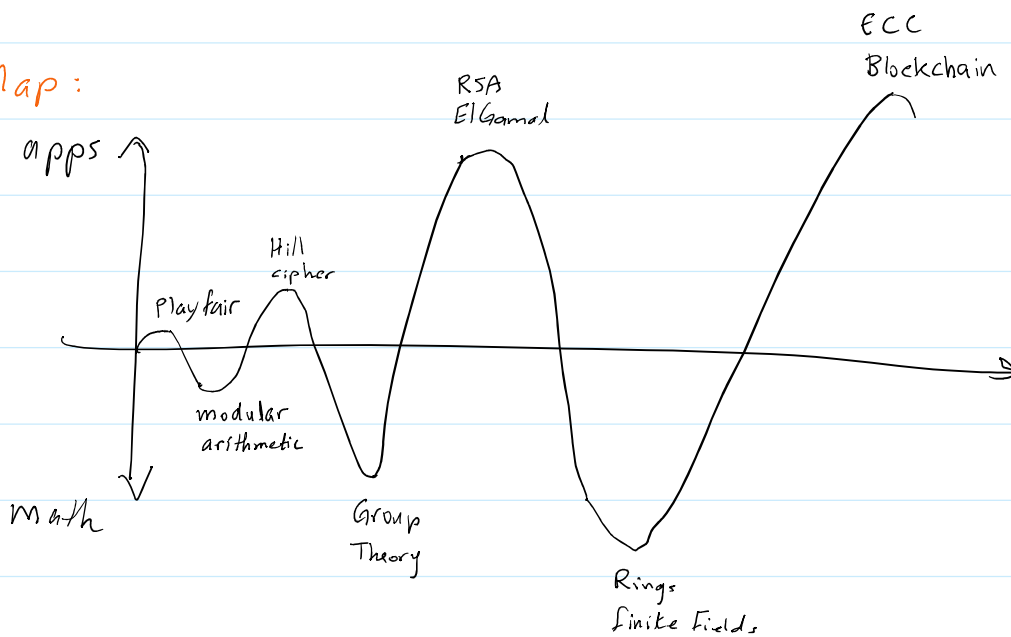


Quiz 2

Map:



1) Fermat little Theorem (FLT)

if p is prime then $\forall a$ relatively prime to p

$$a^{p-1} \equiv 1 \pmod{p}$$

e.g. $p=7$, $a=2$

$$2^6 \equiv 64 \equiv 1 \pmod{7}$$

$$2) \text{ Exer. } ① \quad 2^3 3^4 3^7 4^{661} \pmod{7}$$

$$\begin{aligned} &\equiv 2^{661} \equiv (2^6)^{110} \cdot 2^1 \\ &\equiv (1)^{110} \cdot 2^1 \\ &\equiv 2 \pmod{7} \end{aligned}$$

$$② \quad 2^2 2^6 5^6 7^9 9^{\underline{6323}} \pmod{11}$$

$$\begin{aligned} &\equiv 2^{6323} \equiv (2^{10})^{632} \cdot 2^3 \\ &\equiv 8 \pmod{11} \end{aligned}$$

3) Note:

$$\begin{array}{ccc} & A^E & \\ \text{mod } p \swarrow & & \searrow \text{mod } (p-1) \\ \equiv a^e & & \pmod{p} \end{array}$$

4) Exer $2781^{4562} \pmod{11}$

$$\begin{array}{ccc} & 2781 & \\ \text{mod } 11 \downarrow & & \searrow \text{mod } 10 \\ \equiv (-2)^2 & & \equiv 4 \pmod{11} \end{array}$$

5) e.g.

$$\begin{array}{ccc} & 2^{16} & \\ & \searrow & \\ \equiv 2^2 & & \equiv 4 \end{array} \pmod{15}$$

$\times$ 15 is not a prime

Lecture Notes on Group Theory.

§1. Groups

6) Defⁿ. Let $*$ be a binary operation, then $*$

6) Defⁿ. Let $*$ be a binary operation, then $*$ is said to be on a set A if $*$ is a function from $A \times A$ to A .

$$* : A \times A \rightarrow A$$

Here, A is closed under $*$ operation

e.g. $\mathbb{Z}$ is closed under addition

7) Defⁿ (Group)

a group $(G, \cdot)$ is a nonempty set G with a binary operation $\cdot$ on G such that:

① Closure: $\forall a, b \in G$, we have $a \cdot b \in G$

② Associative: $\forall a, b, c \in G$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

③ Identity: $\exists e \in G$ such that $\forall a \in G$

$$a \cdot e = e \cdot a = a$$

④ Inverse: $\forall a \in G$, $\exists a^{-1} \in G$, such that

$$a \cdot a^{-1} = e = a^{-1} \cdot a$$

8) e.g. $(\mathbb{Z}_{10}^*, \cdot)$ multiplicative group mod 10
 $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

$$e = 1$$

a	1	3	7	9
a^{-1}	1	7	3	9

$(\mathbb{Z}_5, +)$ the additive group modulo 5

$$e = 0, \quad \begin{array}{c|ccccc} a & 0 & 1 & 2 & 3 & 4 \\ \hline a^{-1} & 0 & 4 & 3 & 2 & 1 \end{array}$$

$(\mathbb{Z}, +)$

$$e = 0$$

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