# **Nhóm Số Học, Logarithm Rời Rạc & ECC Trong ZK-Proofs**

## **Meta Description**

Tìm hiểu toán học nền tảng của Zero-Knowledge Proofs (ZKP): nhóm số học, logarithm rời rạc & Elliptic Curve Cryptography (ECC). Vai trò trong zk-SNARKs, zk-STARKs & blockchain!

## **Key Takeaways**

✅ **Nhóm số học & Modular Arithmetic**: Cung cấp nền tảng toán học để thực hiện các phép toán trong ZKP, đảm bảo tính đóng, kết hợp, phần tử đơn vị và nghịch đảo.  
 ✅ **Logarithm rời rạc**: Bài toán tìm **x** trong phương trình **g^x = h** cực kỳ khó giải, tạo nền tảng bảo mật cho nhiều giao thức mật mã, bao gồm Schnorr Protocol.  
 ✅ **Elliptic Curve Cryptography (ECC)**: Sử dụng nhóm đường cong elliptic để tăng hiệu suất zk-SNARKs, giúp tạo các bằng chứng nhỏ gọn, nhanh chóng và an toàn hơn.  
 ✅ **Ứng dụng thực tế**: ECC được sử dụng trong Zcash, Polygon zkEVM, và Scroll để tối ưu hóa Zero-Knowledge Proofs.

## **Nhóm Số Học và Modular Arithmetic**

Nhóm số học [(**Group Theory**)](https://en.wikipedia.org/wiki/Group_theory) là một nhánh quan trọng của đại số trừu tượng, nghiên cứu các tập hợp với phép toán thỏa mãn bốn tính chất:

* **Đóng (Closure):** Kết quả của phép toán vẫn thuộc nhóm.
* **Kết hợp (Associativity):** (a \* b) \* c = a \* (b \* c) với mọi a, b, c.
* **Phần tử đơn vị (Identity):** Có một phần tử e sao cho a \* e = e \* a = a.
* **Nghịch đảo (Invertibility):** Mỗi phần tử a có phần tử nghịch đảo b sao cho a \* b = b \* a = e.

Trong [**modular arithmetic**](https://en.wikipedia.org/wiki/Modular_arithmetic) **(số học modulo)**, các phép toán thực hiện trong một phạm vi giới hạn bằng **modulus p**, nghĩa là sau khi vượt qua giá trị **p**, kết quả quay về từ đầu. Ví dụ:

5 + 7 mod 12 = 0

📌 **Ứng dụng trong ZKP**: Nhóm số học giúp đảm bảo phép toán trong ZKP có thể thực hiện hiệu quả nhưng vẫn bảo mật. Một trong những nhóm phổ biến là **Z\_p**\* (tập hợp số nguyên modulo số nguyên tố p).

🔹 **Ví dụ:** Trong **Z₁₇**\*, phần tử **3** có thể là phần tử sinh (generator), vì nó có thể tạo ra tất cả các phần tử khác khi lũy thừa theo modulo 17.

## **Logarithm Rời Rạc Và Vai Trò Trong Zero-Knowledge Proofs**

### **Logarithm Rời Rạc Là Gì?**

Logarithm rời rạc là bài toán tìm **x** sao cho:

**g^x = h**

trong một nhóm hữu hạn, với **g** là phần tử sinh (generator) và **h** là một phần tử nhóm.

Bài toán **Discrete Logarithm Problem (DLP)** rất khó giải, đặc biệt với số nguyên tố **p** lớn, tạo nền tảng bảo mật cho nhiều giao thức mật mã.

### **Ứng Dụng Logarithm Rời Rạc Trong ZKP**

Schnorr Protocol là một giao thức ZKP sử dụng logarithm rời rạc để chứng minh một người biết giá trị **x** mà không tiết lộ nó.

📌 **Ví dụ:** 1️⃣ **Người chứng minh (Prover)** có bí mật **x** và muốn chứng minh rằng họ biết **x** sao cho **g^x = h**, với **g** là phần tử sinh.  
 2️⃣ **Người chứng minh** chọn số ngẫu nhiên **k**, tính **g^k**, và gửi cho **người kiểm tra (Verifier)**.  
 3️⃣ **Người kiểm tra** gửi một thử thách ngẫu nhiên **c**.  
 4️⃣ **Người chứng minh** tính giá trị **s = k - c \* x (mod p-1)** và gửi lại.  
 5️⃣ **Người kiểm tra** kiểm tra xem:

**g^(k - c\*x) = (g^k)/h^c**

Nếu đúng, người kiểm tra tin rằng người chứng minh thực sự biết **x**, mà không cần biết giá trị cụ thể của nó.

✅ **Tính chất Zero-Knowledge được đảm bảo**, vì quá trình này không tiết lộ **x** cho bất kỳ ai.

## **Elliptic Curve Cryptography (ECC) và Ứng Dụng Trong SNARKs**

### **ECC Là Gì?**

Mật mã đường cong elliptic [(**Elliptic Curve Cryptography - ECC**)](https://en.wikipedia.org/wiki/Elliptic_curve_cryptograph) là một dạng mật mã khóa công khai sử dụng **cấu trúc đại số của đường cong elliptic** trên một trường hữu hạn. ECC có ưu điểm **bảo mật cao với kích thước khóa nhỏ**, nhờ vào bài toán **Elliptic Curve Discrete Logarithm Problem (ECDLP)**, khó giải hơn so với bài toán logarithm rời rạc trên **Z\_p**\*.

📌 **Đường cong elliptic được mô tả bởi phương trình:**

**y2=x3+ax+b**

với **a, b** là hằng số, và các điểm trên đường cong tạo thành một **nhóm hữu hạn** dưới phép cộng điểm.

### **Ứng Dụng ECC Trong zk-SNARKs**

zk-SNARKs (**Zero-Knowledge Succinct Non-Interactive Argument of Knowledge**) là một dạng Zero-Knowledge Proof không tương tác, giúp tạo **các bằng chứng nhỏ gọn, nhanh chóng**.

ECC giúp zk-SNARKs hiệu quả hơn nhờ sử dụng **cặp ghép (pairings) trên đường cong elliptic** để kiểm tra bằng chứng.

🔹 **Cặp ghép bilinear:**

**e:G1×G2​→G3**

🔹 **Ứng dụng thực tế:**

* **Zcash (ZEC):** Sử dụng zk-SNARKs để cung cấp giao dịch ẩn danh.
* **Polygon zkEVM:** Tích hợp zk-SNARKs với BLS12-381 để mở rộng Ethereum.
* **Scroll, Aztec Protocol:** Sử dụng đường cong BN254 để tăng tốc độ xác minh.

📌 **Tìm hiểu thêm về zk-SNARKs trong** [**bài viết này**](https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof#History).

## **Bảng So Sánh Tổng Quan**

| **Tiêu chí** | **Nhóm số học & Modular Arithmetic** | **Logarithm Rời Rạc** | **ECC trong SNARKs** |
| --- | --- | --- | --- |
| **Định nghĩa** | Cấu trúc toán học với phép toán modulo | Tìm **x** trong **g^x = h** | Mật mã dựa trên đường cong elliptic |
| **Vai trò trong ZKP** | Tạo nhóm hữu hạn giúp tính toán hiệu quả | Đảm bảo bảo mật nhờ độ khó DLP | Tăng hiệu suất và giảm kích thước proof trong zk-SNARKs |
| **Ví dụ cụ thể** | Nhóm **Z\_p**\* với p nguyên tố | **Schnorr Protocol** | **zk-SNARKs với BN254** |

## **Kết Luận**

Nhóm số học, logarithm rời rạc, và ECC là **nền tảng toán học quan trọng** giúp Zero-Knowledge Proofs hoạt động hiệu quả.

📌 **Tóm tắt nhanh:** ✅ **Modular Arithmetic** tạo nhóm hữu hạn, đảm bảo tính toán nhanh.  
 ✅ **Logarithm rời rạc** làm cho ZKP bảo mật bằng cách tạo ra bài toán khó giải.  
 ✅ **ECC** tối ưu hóa zk-SNARKs, giúp bằng chứng nhỏ gọn và nhanh hơn.

🚀 **Bạn muốn tìm hiểu thêm về giao thức ZKP?** Hãy đọc ngay **bài tiếp theo về Interactive vs Non-Interactive Proofs**!