

# **EECS 498/CSE 598: Zero-Knowledge Proofs**

## **Winter 2026**

### **Lecture 3**

Paul Grubbs

[paulgrub@umich.edu](mailto:paulgrub@umich.edu)

Beyster 4709

# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- Basics of groups
- Elliptic curve groups
- Pairings of elliptic curves

# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- Basics of groups
- Elliptic curve groups
- Pairings of elliptic curves

# Announcements

- Project 1 is online
- Autograder is working
- there's a new cryptocurrency called “zero knowledge proof coin”...

## Zero Knowledge Proof

Built In Protest. Designed in Proof.

The ZKP crypto presale 2026 marks the beginning, a system reset sealed in math, hype, or approval. We built it because the system was rigged, and someone had to write the counter-code.

The Zero Knowledge Proof Manifesto is not a whitepaper. It's a line in the sand. It's how we reclaim data, dismantle trust-based systems, and prove everything we stand for.



**Buy Zero Knowledge  
Proof Coin During the  
Crypto Presale 2026  
Before It Hits the Market**

[Join the Auction](#)



# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- Basics of groups
- Elliptic curve groups
- Pairings of elliptic curves

# Montgomery arithmetic (\*)

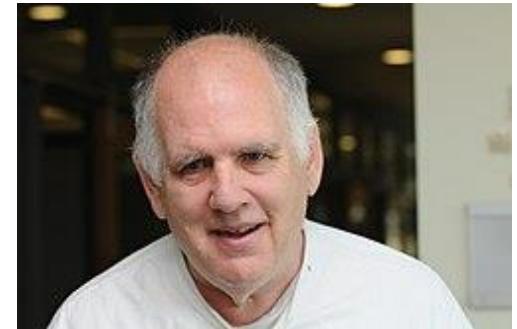
P Prime

How to do mod. arith. in code?

add mod ( $[a]_p, [b]_p$ ):

$$c \leftarrow [a]_p + [b]_p$$

$$[c]_p \leftarrow \underline{\underline{c \bmod p}}$$



Auxiliary modulus  $R > p$        $\gcd(P, R) = 1$

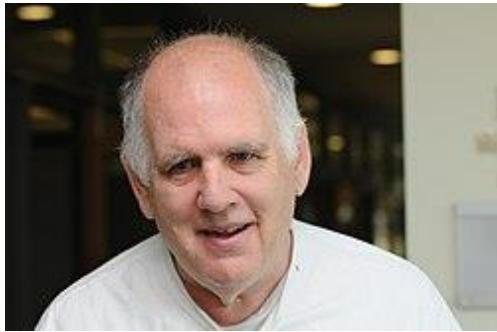
Montgomery form:

$$a \mapsto aR \bmod p$$

$$aR \bmod p + bR \bmod p = (a+b)R$$

$$(aR \bmod p)(bR \bmod p) \stackrel{?}{=} (abR)R$$

# Montgomery arithmetic (\*)



$\text{MontMul}(a', b', P, P' | R)$ :

$\{0, \dots, RP-1\} \ni T \leftarrow a'b'$

$$m \leftarrow ((T \bmod R)P') \bmod R.$$

$$t \leftarrow (T + mP)/R$$

If  $t \geq P$ :  
Ret  $t - P$

Else  
Ret  $t$

Claim:

$$t \in \{0, \dots, 2P\}$$

$$m \in \{0, \dots, R-1\} \text{ so } T + mP \in \{0, \dots, (RP-1) + (R-1)P = 2RP\}$$

$$\text{and } t \in \{0, \dots, 2P-1\}$$

$$\frac{T + mP \bmod P}{R} \equiv TR^{-1} \bmod P$$

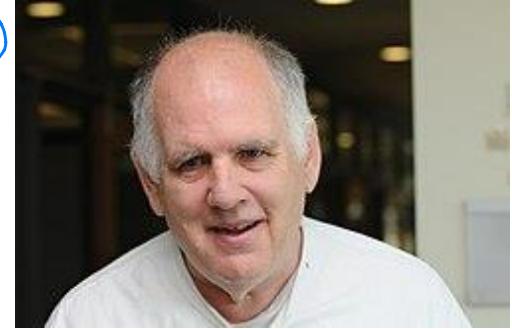
$$RP^{-1} + RP - P \\ 2RP - P - 1$$

$$2RP - P - 1$$

# Montgomery arithmetic (\*)

Claim:  $R$  divides  $T + mP$  (over  $\mathbb{Z}$ )

$$\begin{aligned} T + mP &= T + ((T \bmod R) P' \bmod R) P \\ &= T + T \cancel{(P' P)} \equiv -1 \bmod R \\ &\equiv T - T \bmod R \equiv 0 \bmod R \quad \text{Q.E.D.} \end{aligned}$$



# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- **Basics of groups**
- Elliptic curve groups
- Pairings of elliptic curves

# Algebraic groups

Let  $S$  be a set,  $\otimes: S \times S \rightarrow S$  binary operation

$(S, \otimes)$  is a group if:

- $S$  has identity  $1$   
 $a \otimes 1 \rightarrow a$  and  $1 \otimes a \rightarrow a$
- $\otimes$  associative  
 $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
- Inverses  $\forall a \in S \exists x \in S$  s.t.

$a \otimes x \rightarrow 1$  and  $x \otimes a \rightarrow 1$

- - - Order of element

$a$ 's order  $x$ :

smallest  $N$  s.t.  $x \cdot a = 1$

If  $a \otimes b = b \otimes a$ ,  
say "Abelian"

If  $\exists a$  s.t.

$\{a, a^2, \dots, a^{|S|}\} = S$   
say Cyclic

$$\text{ord}(a) \leq |S|$$

$$\text{ord}(a) \mid |S|$$

# Examples of groups

$(\mathbb{Z}, +)$

$(\mathbb{Z}_P, \times (\text{no } 0))$

Symmetries of  $\boxed{\square}$

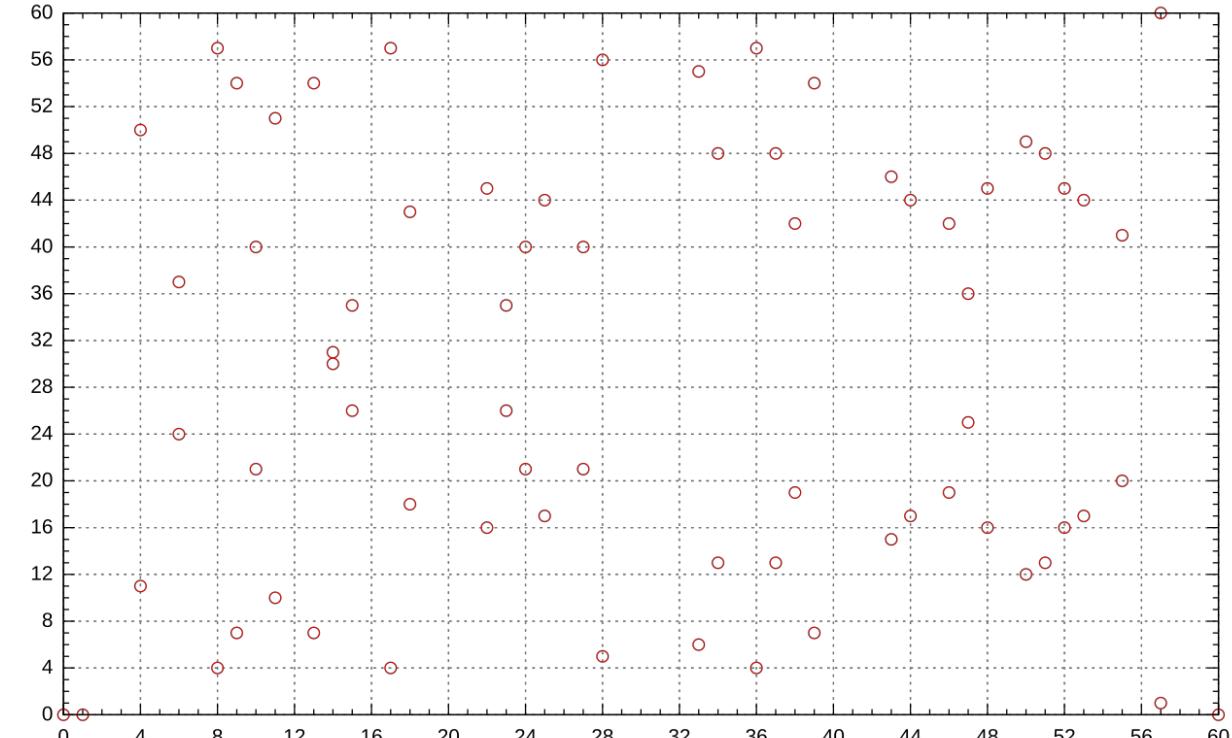
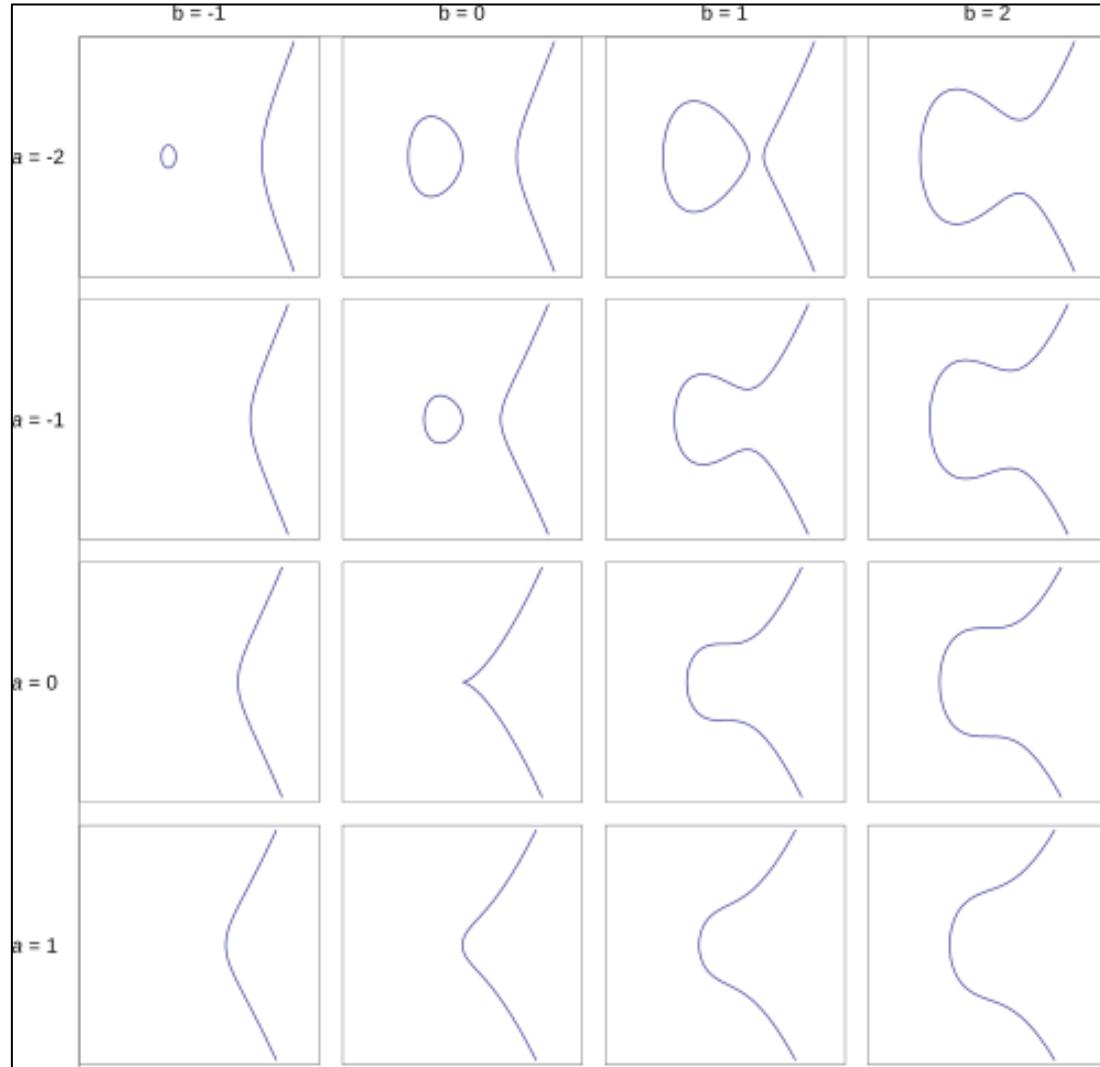
General linear group

# The discrete logarithm problem

# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- Basics of groups
- **Elliptic curve groups**
- Pairings of elliptic curves

# Elliptic curves over finite fields



$$y^2 = x^3 - x \text{ over } \mathbb{F}_{61}$$

# Elliptic curves in cryptography: a history

- Elliptic curve factorization method (Lenstra ‘86)
- mid-80s: first suggestions of EC-based cryptography, by Koblitz and Miller
- 80s-90s: initial work on efficient ECC (lots of patents by Certicom)
- 1993: MOV attack breaks supersingular curves using Weil pairing
- 2001: Identity-based encryption from the Weil pairing
- late 90s through mid-00s: initial proposals for isogeny-based cryptography
- 2011: SIDH published by Jao and de Feo
- 2022: SIDH completely broken by Castryck and Decru ☹

# Elliptic curve basics

$$a, b \in \mathbb{F}_p$$
$$4a^3 + 27b^2 \neq 0$$

Take  $\mathbb{F}_p$

Let  $\bar{E} = \{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + ax + b\}$

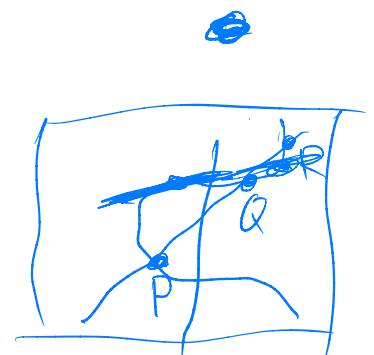
$$E = \bar{E} \cup \{\theta\}$$

$E$  is a group under "point addition"

$E/\mathbb{F}_p$  Abelian

$$P + Q = Q + P$$

$$P + (-P) = \theta$$



# Agenda for this lecture

- Announcements
- Montgomery arithmetic
- Basics of groups
- Elliptic curve groups
- Pairings of elliptic curves

# **Constructive uses of pairings**

# **Computational questions**