EECS 498/CSE 598: Zero-Knowledge Proofs
Winter 2026
Lecture 3

Paul Grubbs

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

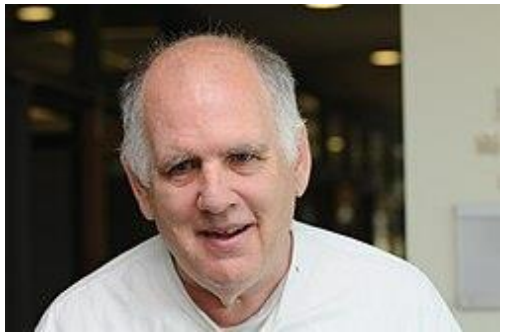
- Project 1 is online
- Autograder is working
- there's a new cryptocurrency called "zero knowledge proof coin"...

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

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

$[c]_p \leftarrow c \pmod p$

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

Montgomery form:

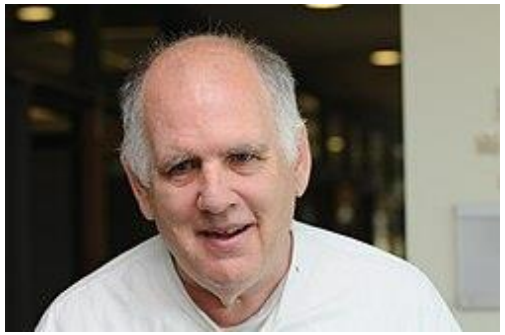
$$a \mapsto aR \bmod p$$

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

Montgomery arithmetic (*)

$(aR \bmod p)(bR \bmod p) = (abR)R$

$P \cdot P' \equiv -1 \bmod R$



MontMul(a', b', P, P', R):

$[0, \ldots RP-1]$

$T \leftarrow a'b'$

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

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

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

Else
  Ret t

Claim:

MontMul outputs $(ab)R \bmod P$:

$\frac{T + mP}{R} \to 0 \bmod p \equiv TR^{-1} \bmod P$

Claim:

$t \in [0, \ldots, 2P]$

$m \in [0, \ldots, R-1]$ so $T + mP \in [0, \ldots (RP-1) + (R-1)P \equiv 2RP]$

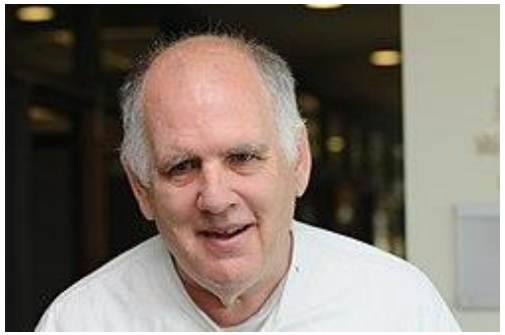
$RP-1 + RP-P$

$2RP-P-1$

and $t \in [0, \ldots, 2P-1]$

Montgomery arithmetic (*)

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



$$T + mP = T + ((T \bmod R)\, p' \bmod R)\, P$$

$$= T + TPP' \qquad \equiv -1 \bmod R$$

$$\equiv T - T \bmod R \equiv 0 \bmod R \qquad \boxtimes$$

Agenda for this lecture

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

Algebraic groups

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

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

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

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

If $\exists a$ s.t. $\{a, a^2, \ldots, a^{|S|} = a\} = S$
say cyclic

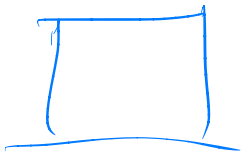
- Order of element
  a's order x:
  smallest $\mathbb{N}$ s.t. $x \cdot a = 1$

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

Examples of groups

$(\mathbb{Z}, +)$

$(\mathbb{Z}_p, \times \pmod 0)$

Symmetries of 

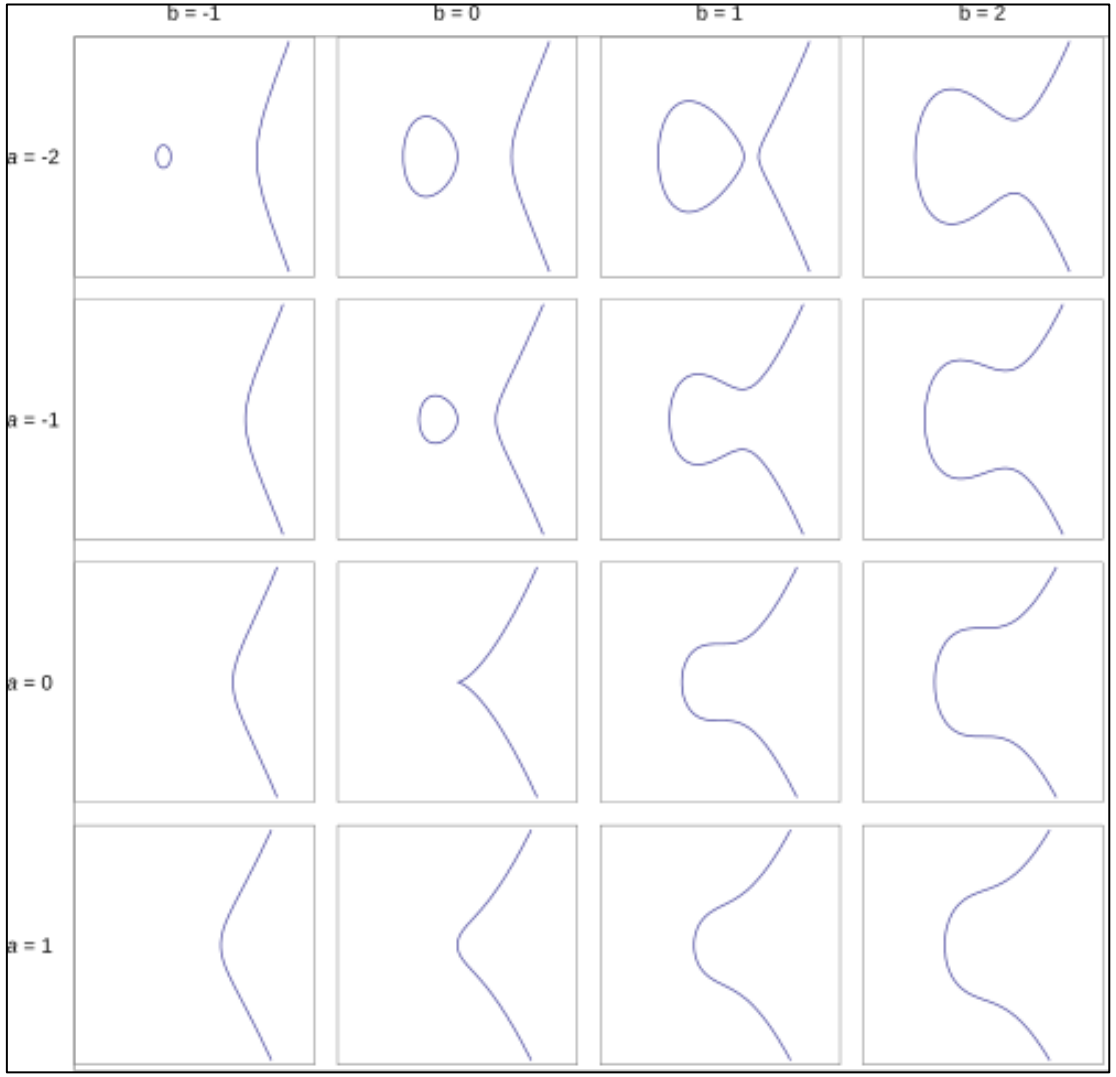
General linear group

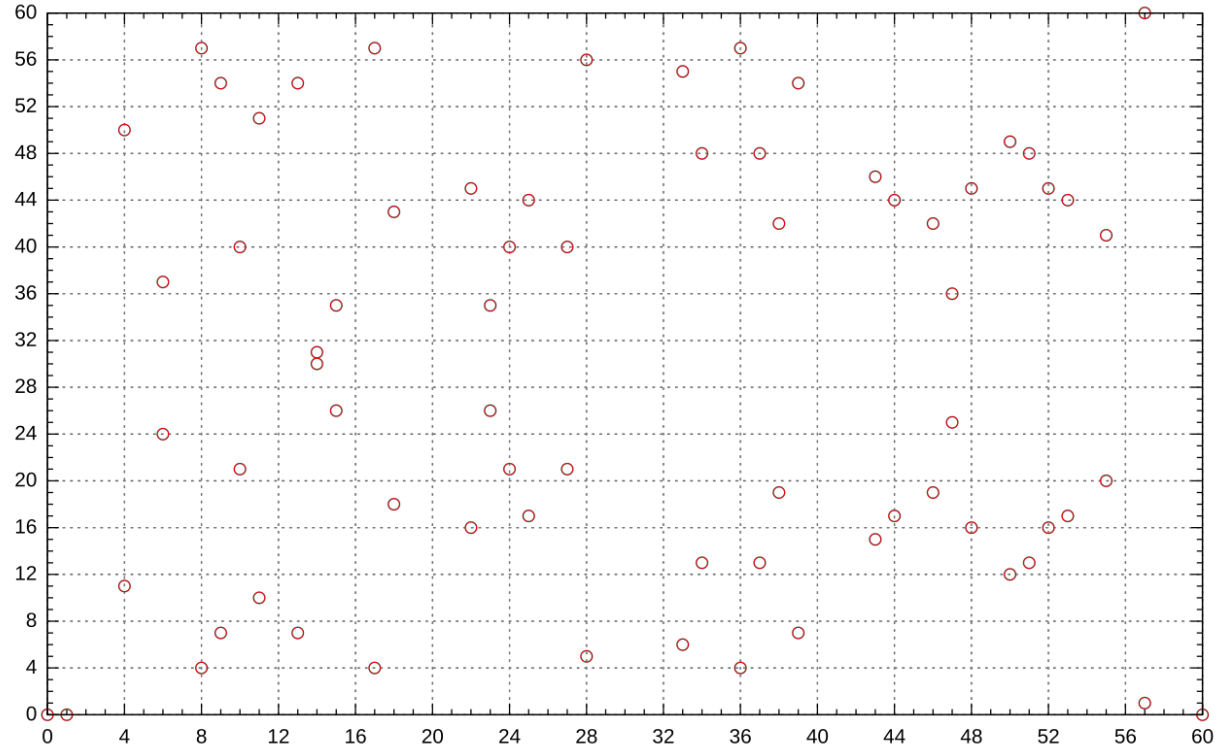
The discrete logarithm problem

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

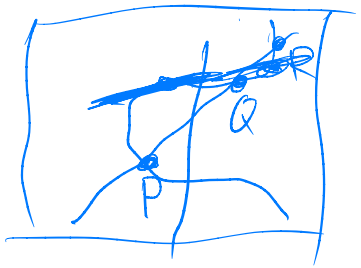
$E = \overline{E} \cup \{\mathcal{O}\}$

E is a group under "point addition"

$E/\mathbb{F}_p$ Abelian

$P + Q = Q + P$

$P + (-P) = \mathcal{O}$



Agenda for this lecture

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

Constructive uses of pairings

Computational questions