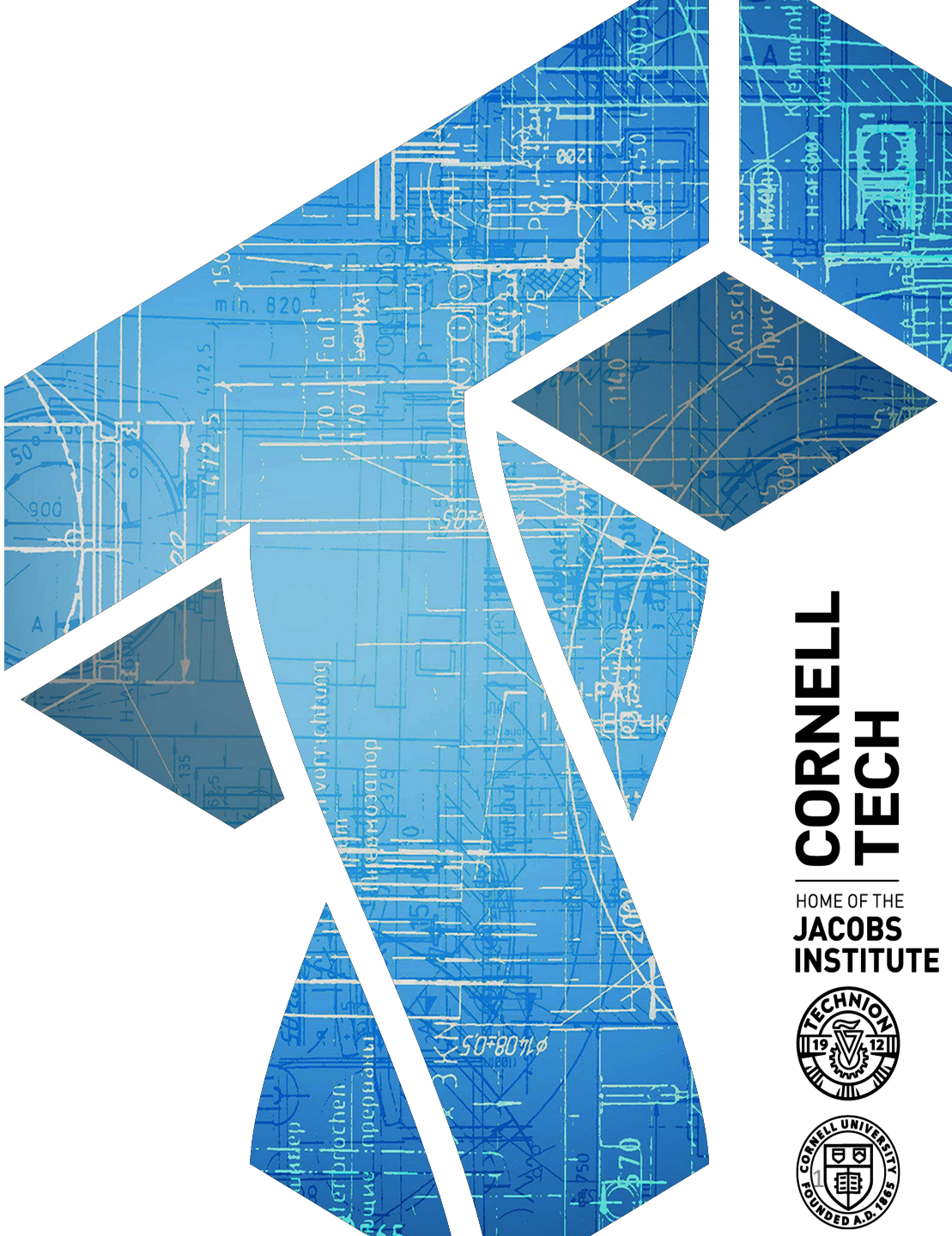
CS 5830
Cryptography



CORNELL TECH

HOME OF THE JACOBS INSTITUTE

Asymmetric crypto so far

- RSA
  - Work in $\mathbf{Z}_N^*$ for large composite N = pq
  - RSA assumption: given X^e mod N can't recover X without secret key d (assuming X is uniformly chosen)
- Discrete log problem (DLP)
  - Worked in prime-order subgroup of $\mathbf{Z}_p^*$ for prime p. g is a generator of subgroup. q is size of subgroup
  - Discrete log assumption: given g^x mod p can't recover x (assuming x is uniformly chosen)

Finite fields

- Finite field is a finite set with basic operations:
  - Addition, subtraction, multiplication, division
  - We saw GF(2^{128}) previously
- Integers modulo prime p is also a field
  - Notated F_p or GF(p) .
  - The set is {0,1,…,p-1}
    - Addition is a + b mod p
    - Multiplication is ab mod p .
- We use GF(p) for ***elliptic curves***

Elliptic curves

- Are discrete log based systems. They use a new kind of group defined relative to a finite field. We will only need curves over $\mathbf{F}_p$
- Independently suggested for cryptographic applications by Victor Miller and Neal Koblitz in 1985
- They are now the go-to state-of-art in practice

Comparison

Security level	RSA size (log N)	DLP in finite field (log p)	ECC group size (log q)
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
256	15360	15360	512

ECC has smallest secure representations and fastest performance of all asymptotic primitives we will see

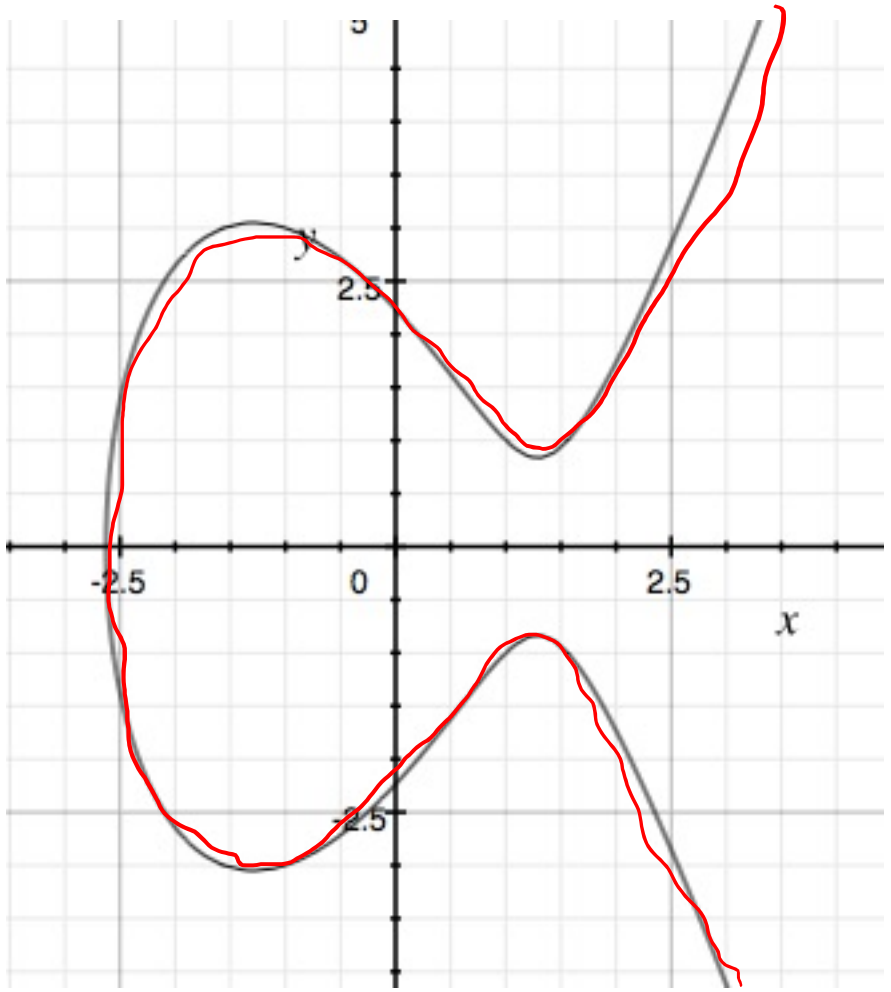
Elliptic curves

- An elliptic curve is set of x,y points in $\mathbf{F}_p$ defined by an equation

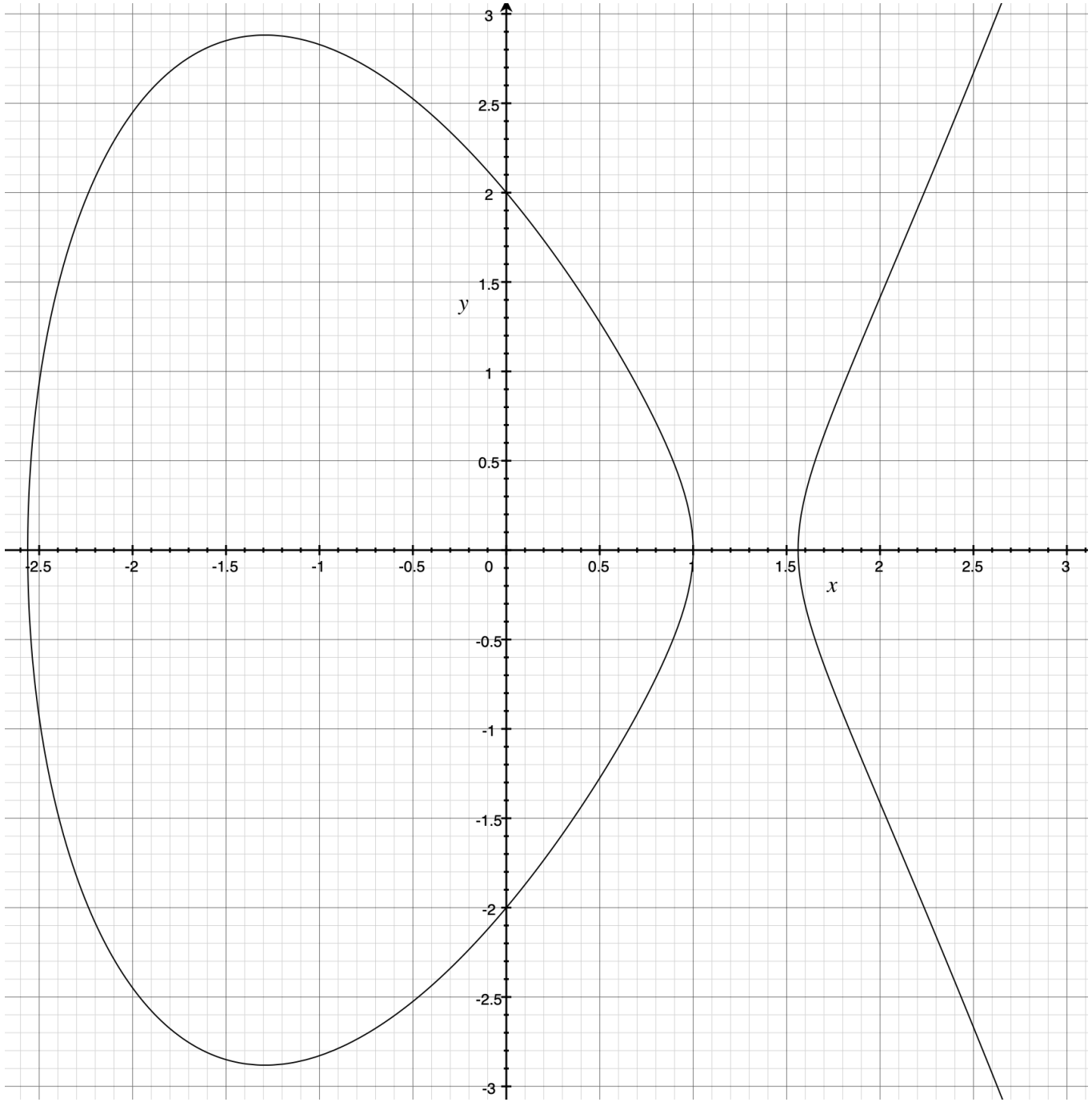
$$E = \{(x, y) \mid y^2 = x^3 + ax + b \bmod p\}$$

  a,b are fixed values also from $\mathbf{F}_p$

- Plus one special point $\mathcal{O}$ called the "point at infinity"
- Technical condition: $4a^3 + 27b^2 \neq 0$
  - Otherwise curve fails to be non-singular (no cusps or self-intersections)

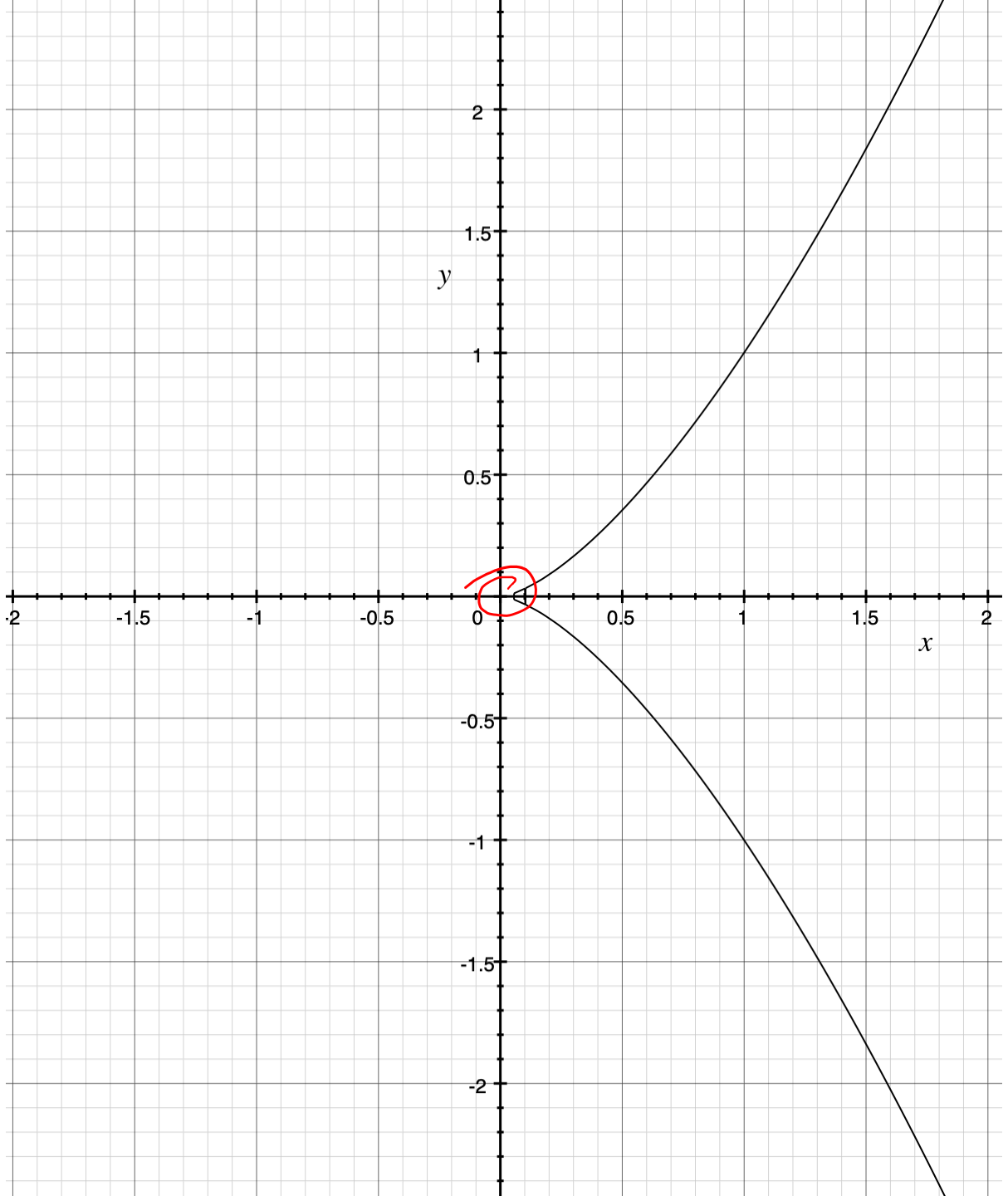


$y^2 = x^3 - 5x + 5$ (over the reals)



$y^2 = x^3 - 5x + 4$

$4a^3 + 27b^2$



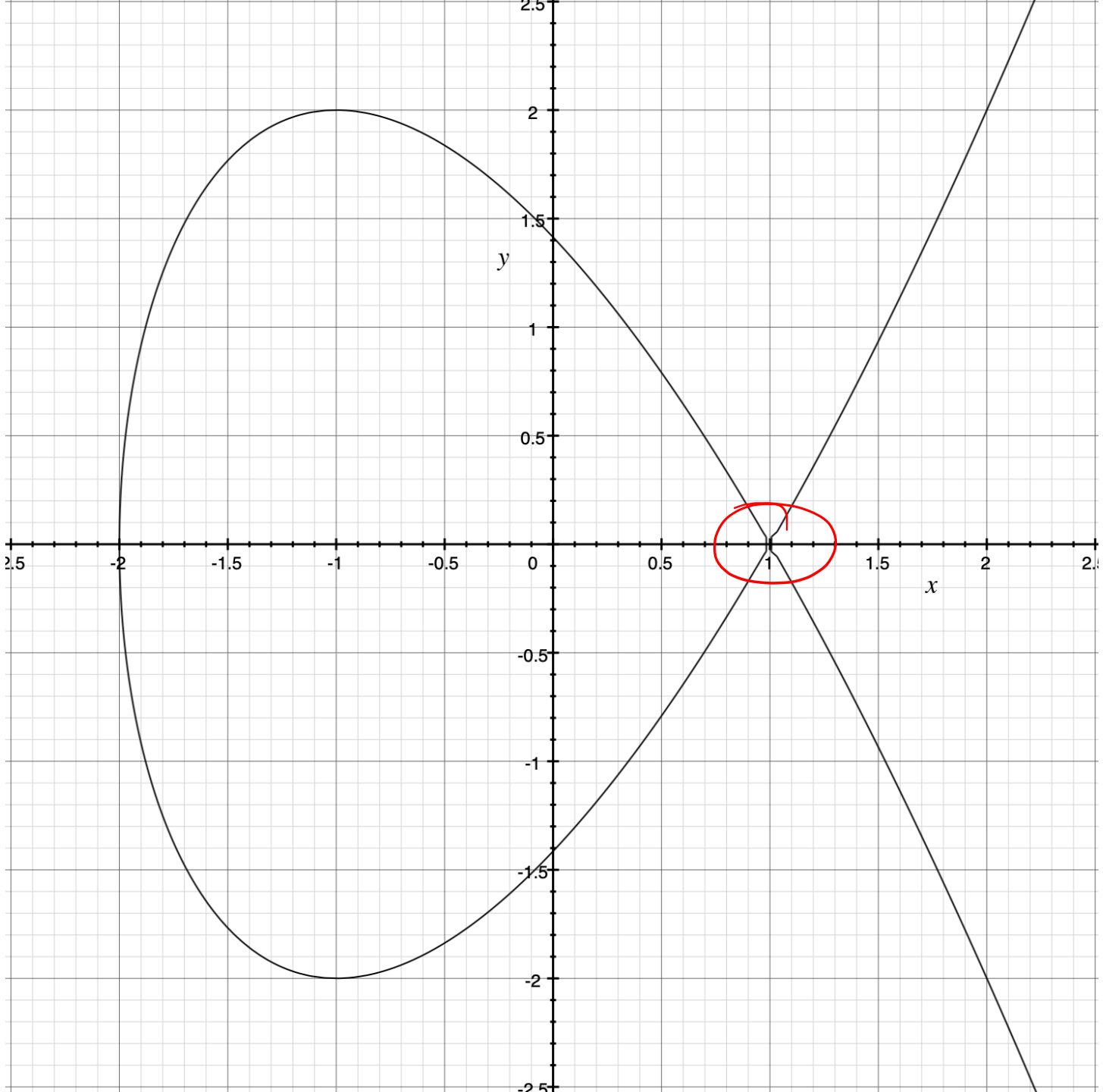
$y^2 = x^3$

$a = b = 0$

=>

Doesn't satisfy:

$4a^3 + 27b^2 \neq 0$



$y^2 = x^3 - 3x + 2$

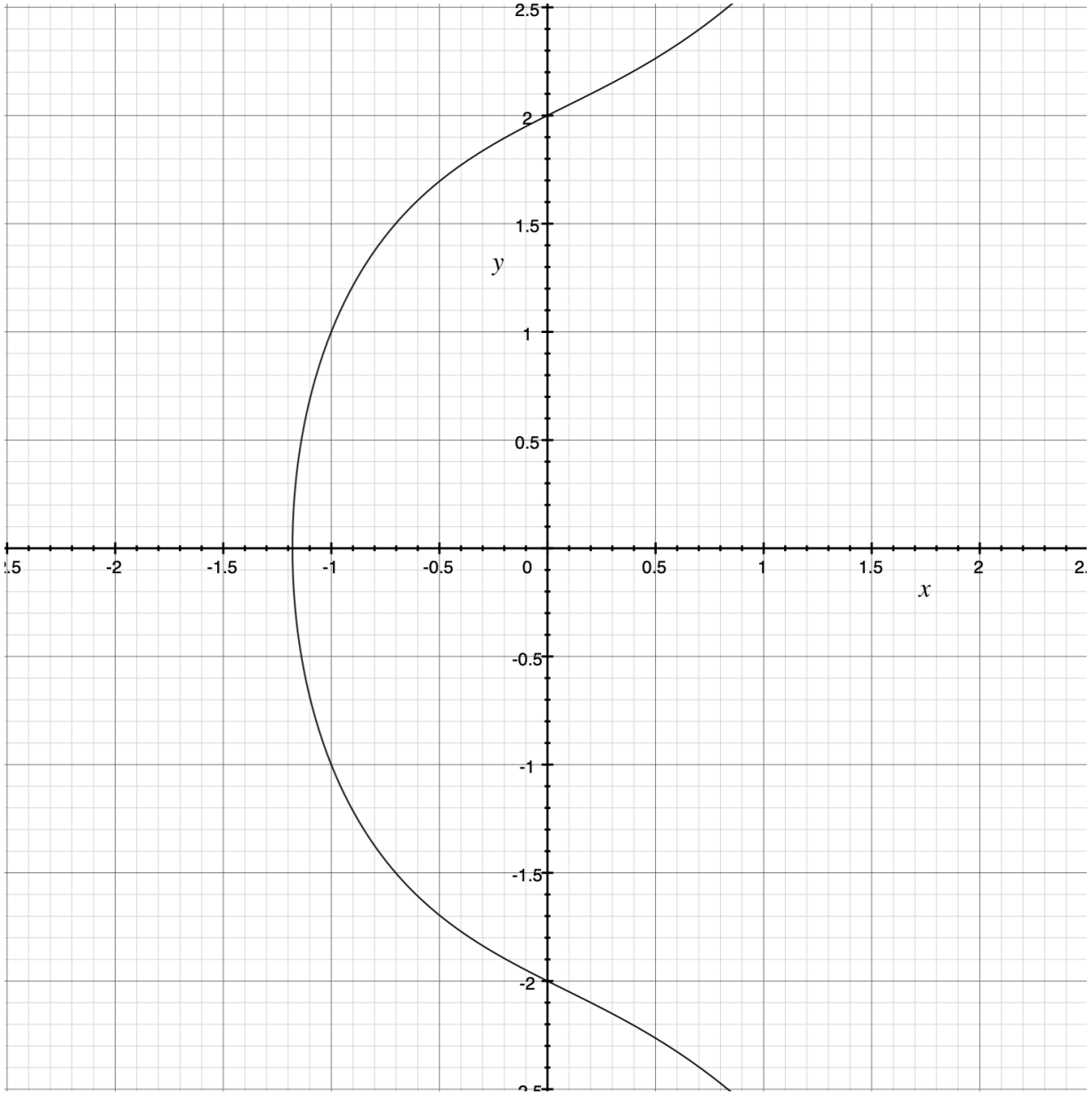
$a = -3, b = 2$

=>

Doesn't satisfy:

$4a^3 + 27b^2 \neq 0$

$-108 + 108 = 0$ ✓



$y^2 = x^3 + 2x + 4$

(over the reals)

Elliptic curves over finite field

- Can't draw pretty curve, which is just a set of points
- Example: $y^2 = x^3 + 2x + 4 \mod 5$ (i.e., over $\mathbf{F}_5$)

x	0	1	2	3	4
x^3	0	1	3	2	4
$2x$	0	2	4	1	3
4	4	4	4	4	4
y^2	4	2	1	2	1
y	2, 3		1, 4		1, 4

E has 7 points: $O, (0,2), (0,3), (2,1), (2,4), (4,1), (4,4)$

$(0,2) + (0,3) = (0,0)$

Elliptic curves as groups

Recall that a *group* is a set G along with an operation * such that (s.t.) for all a,b,c in G:

- *Closure*: a*b in G
- *Associativity*: (a*b)*c = a*(b*c)
- *Identity*: exists 1 in G s.t. 1*a = a*1 = a
- *Inverses*:

  for all a in G, there exists a^{-1} in G s.t. $a*a^{-1} = 1$

Abelian groups: a*b = b*a

Elliptic curve group operation

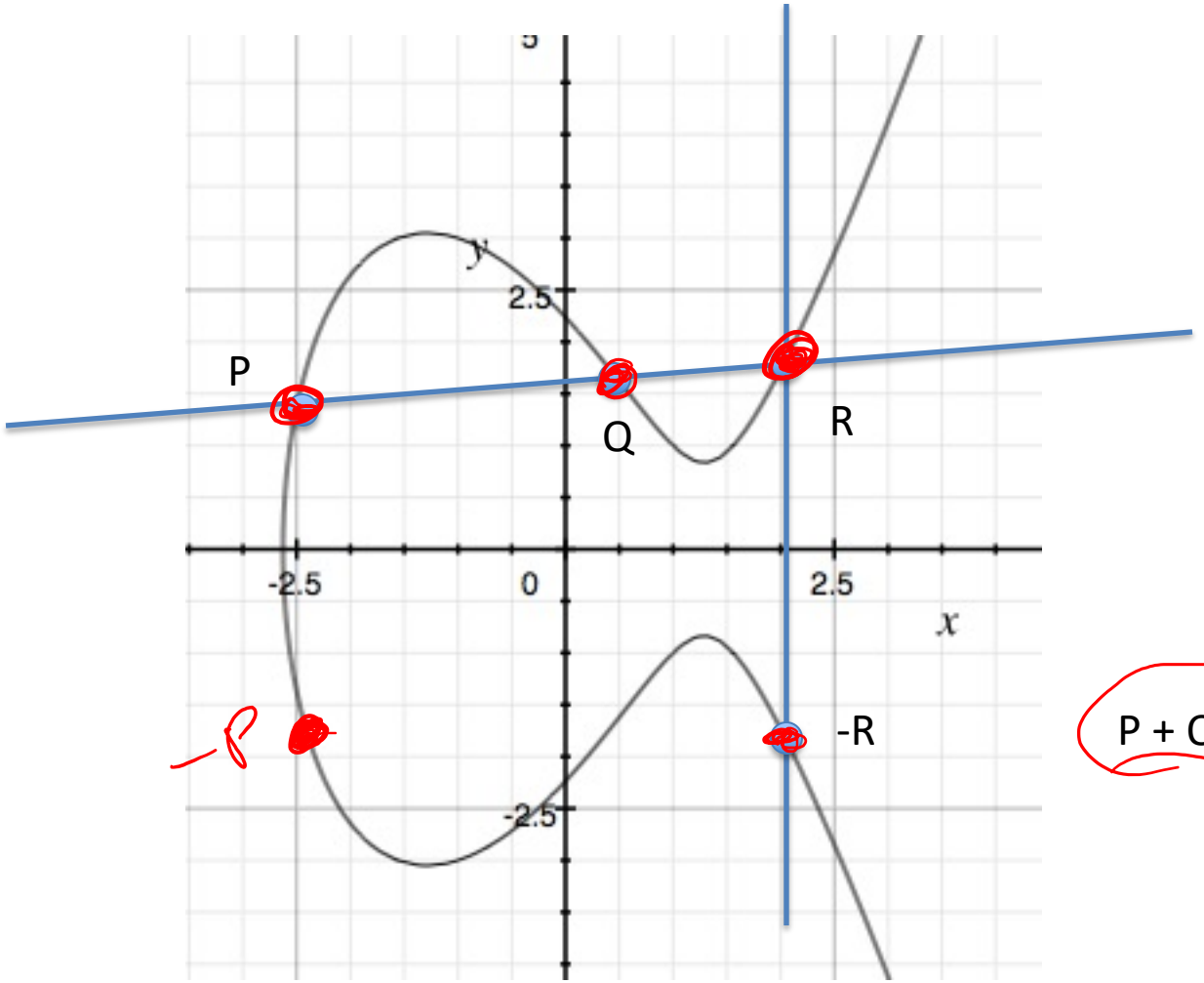
- The operation * is called “point addition” and we usually denote this P + Q for P,Q in E

- What does it mean to “add” two points

  P = (x1,y1) and Q = (x2,y2)?

$P + Q = (x1 + x2, y1 + y2)$

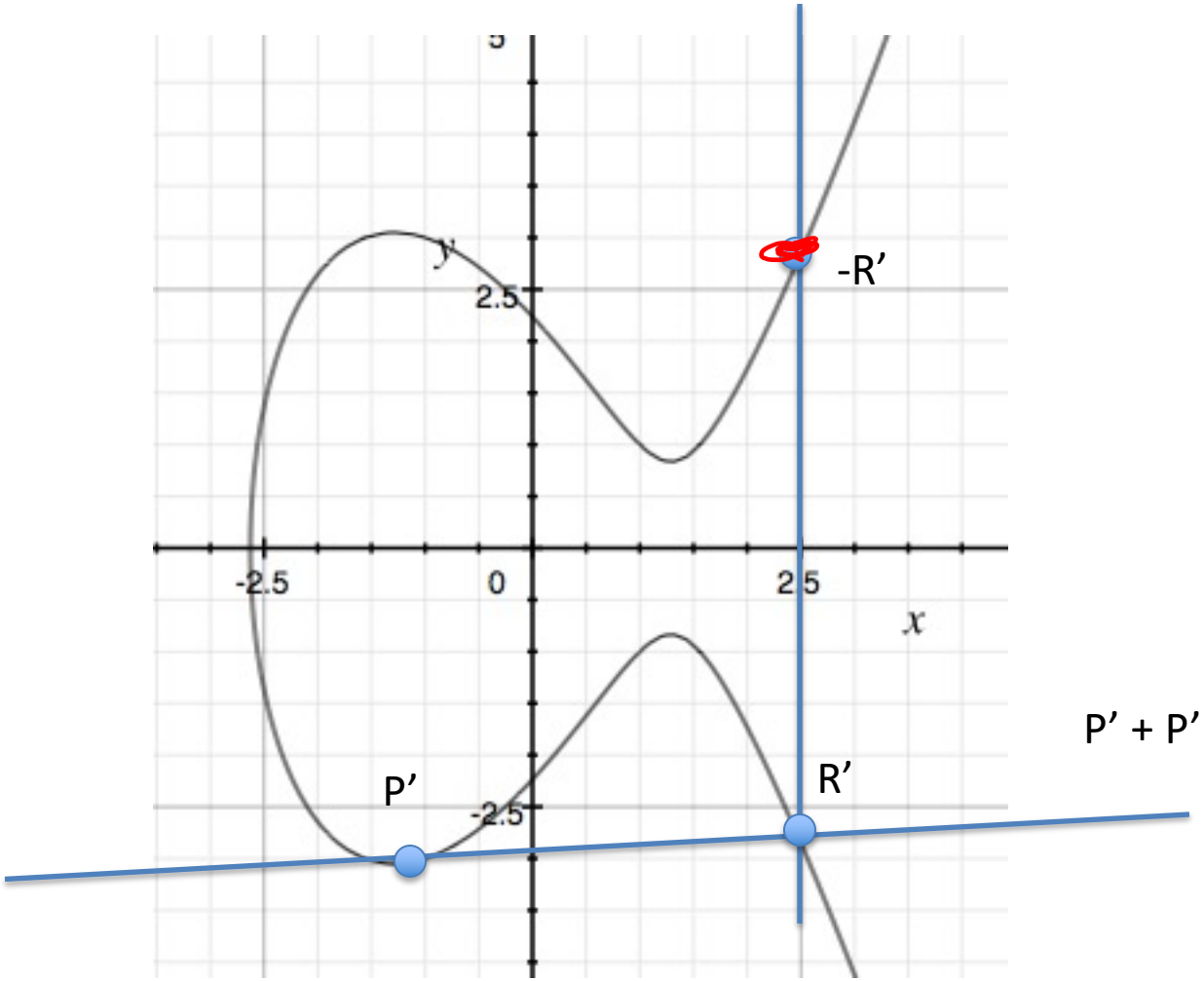
Adding two points P = (x1,y1) and Q = (x2,y2) with x1 ≠ x2



P + Q = -R

$y^2 = x^3 - 5x + 5$ (over the reals)

Adding P’ = (x1,y1) to itself

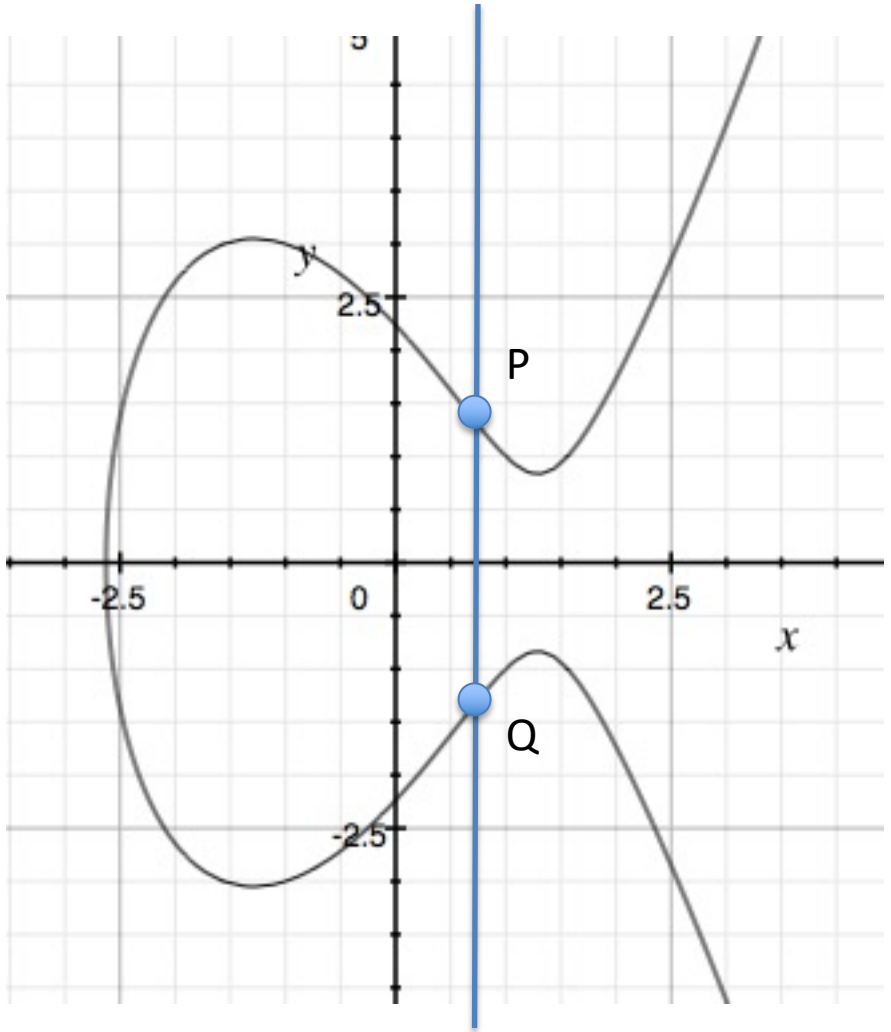


P’ + P’ = -R’

$y^2 = x^3 - 5x + 5$ (over the reals)

Point at infinity

Adding two points P = (x1,y1) and Q = (x2,y2) with x1 = x2

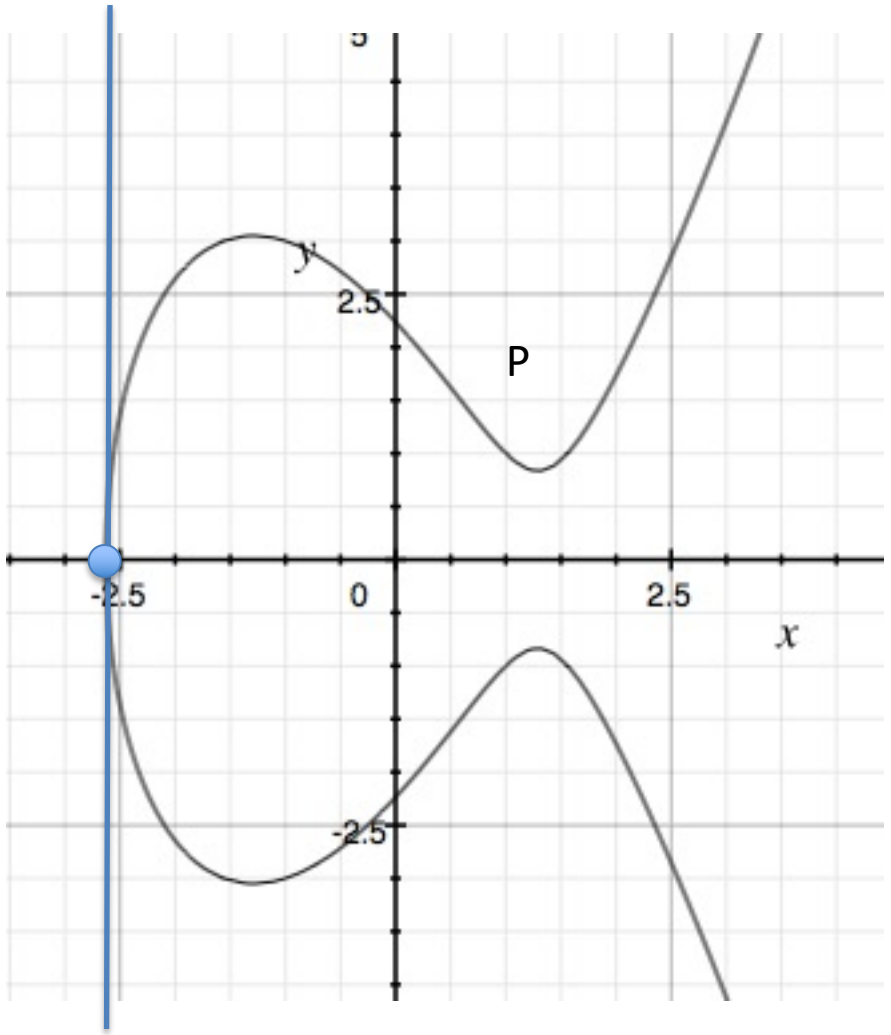


P + Q = O

Calligraphic "Oh"

$y^2 = x^3 - 5x + 5$ (over the reals)

Adding two points P = (x1,y1) and Q = (x2,y2) with x1 = x2, y1 = y2 = 0



P + P = O

$y^2 = x^3 - 5x + 5$ (over the reals)

Elliptic curve group operation

- Let $\mathcal{O}$ be the identity for the group
  - $P + \mathcal{O} = \mathcal{O} + P = P$ for any point
- Let P^{-1} be $(x,-y)$ for $P = (x,y)$
  - By definition $P + P^{-1} = \mathcal{O}$
  - $\mathcal{O}^{-1} = \mathcal{O}$
- P + Q has geometric interpretation
  - $P + Q + R = \mathcal{O}$
  - $P' + P' = -R'$

- Over finite fields same, but calculate algebraically

Elliptic curve group operation (over F_p)

- Adding P = (x1,y1) , Q = (x2,y2):
  - Slope is D = (y2-y1) / (x2-x1) mod p
- Line through P,Q is

  $y = D(x-x1) + y1 \mod p$
- Substitute in to curve equation:

  $(D(x-x1) + y1)^2 = x^3 + ax + b \mod p$
- Only three values of x satisfy equation: x1,x2 and
  - $x3 = D^2 - x1 - x2 \mod p$
  - So: $y3 = D(x3-x1) + y1 \mod p$
- Above only works for $x1 \neq x2$. P = Q case handled similarly to compute slope of tangent

Elliptic curve group operation (over F_p)

P + Q for P = (x1,y1) Q = (x2,y2)

If P = $\mathcal{O}$ then return Q

If Q = $\mathcal{O}$ then return P

If x1 = x2 and y1 = -y2 then return $\mathcal{O}$

If x1 = x2 and y1 = y2 = 0 then return $\mathcal{O}$

If x1 = x2 then $D = (3x1^2 + a)/(2y1) \bmod p$

Else $D = (y2-y1) / (x2-x1) \bmod p$

$x3 = D^2 - x1 - x2 \bmod p$

$y3 = D(x2-x1) + y1 \bmod p$

Return (x3,-y3)

Elliptic curve group operation (over F_p)

- Amazingly, point addition is a group operation
  - *Closure*: P + Q on curve for all P, Q
  - *Associativity*: P + (Q + Z) = (P + Q) + Z
  - *Abelian*: P + Q = Q + P

- Scalar multiplication nP is just adding P to itself n times
  - This is analogous to "exponentiation" in $\mathbf{Z}_p^*$
  - Can compute with double and add algorithm (same as square and multiply)
- Can pick generator P that defines cyclic subgroup of E

  { 0P, 1P, 2P, 3P,…, qP } = all points of interest on curve (could be that q = p)

  (choose so q is big prime)

don't actually use

Building elliptic curve groups

- How do we find suitable curves?
  - Pick large prime p
  - Pick values for a and b to define
    $$y^2 = x^3 + ax + b \bmod p$$
  - Determine size of group, see if it is prime (or close to prime)
- There are efficient algorithms for all this
- Short, better answer in practice: Use predefined ones
  - NIST curves such as P256. See Appendix D in https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
  - Curve25519 (defined over $p = 2^{255} - 19$)

Elliptic curve DH

Pick random x from $\mathbf{Z}_q$

$X = xP$

$K = H(xY)$

X

Y

Pick random y from $\mathbf{Z}_q$

$Y = yP$

$K = H(yX)$

Pick random x from $\mathbf{Z}_{|G|}$

$X = g^x$

$K = H(Y^x)$

X

Y

Pick random y from $\mathbf{Z}_{|G|}$

$Y = g^y$

$K = H(X^y)$

Elliptic curve DLP

- Given xP compute x
- Same as g^x compute x, just different group!

- Best known algorithm against well-chosen ECC group version runs in time $q^{0.5}$
  - Baby-step, giant-step algorithm we saw before, applied here

Other asymmetric primitives?

- ECC most secure cryptographic groups we know for DH
  - Provides 128 bit security with 256-bit group size

Two important quantum algorithms

- [Shor 1994] factors composite number N
  - Recall, fastest algorithm we can implement is NFS. Runs in time $\mathcal{O}\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$
  - Shor's algorithm gives solution using quantum circuit of size $\mathcal{O}\left((\log N)^2(\log\log N)(\log\log\log N)\right)$
  - Can be used to compute discrete logs as well

- [Grover 1996] inverts functions with quadratic speedup
  - Uses $\mathcal{O}\left(\sqrt{2^k}\right)$ to recover K from $E_K(0^n)$, for |K| = k bits
  - Double key lengths: AES-256 all good for 128 bit security

Cryptopoclypse?

Cryptographic Combiners

RegDH$_1$, PQCDH$_1$

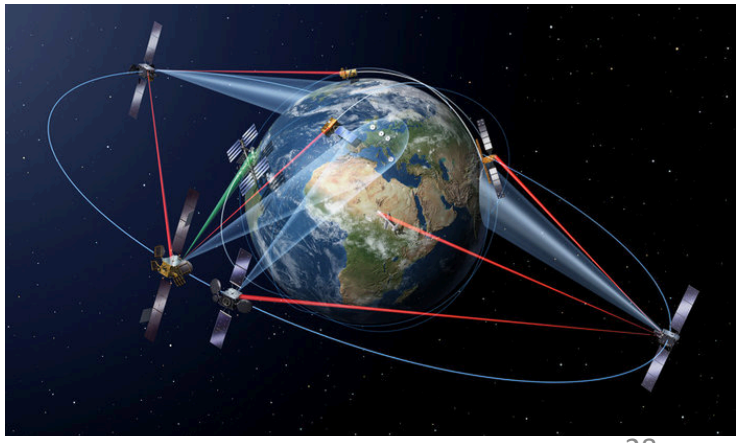
RegDH$_2$, PQCDH$_2$

- "Post-quantum crypto" (PQC)
  - Asymmetric algorithms with conjectured security against QCs
  - ***Hash-based signatures***, ***lattice-based***, code-based, non-linear systems of equations, elliptic curve isogenies
  - Gaining practical momentum:
    - NIST competition, practical variants of TLS key exchange

Picture

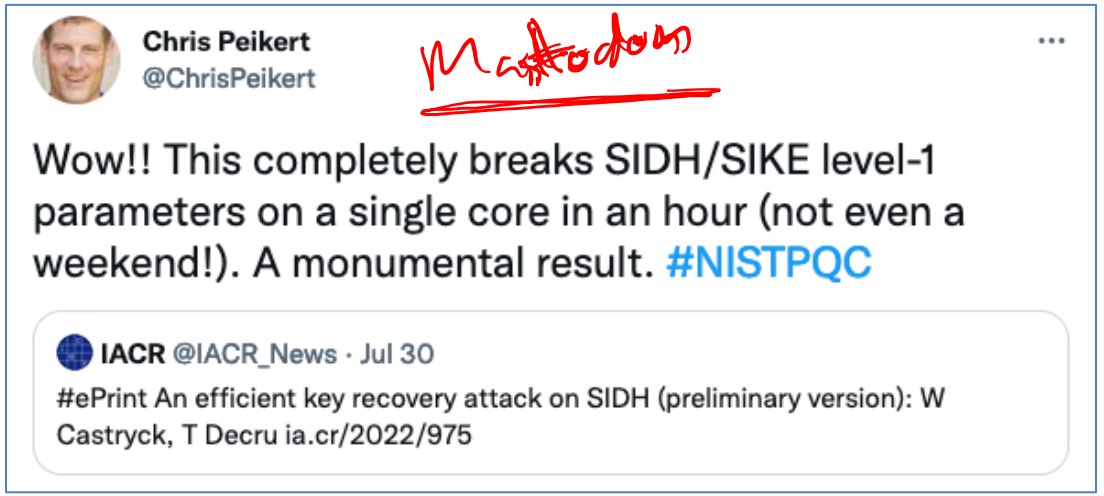
- Quantum key distribution
  - Interesting concept, but turned into snake oil
  - Run away!

Snake oil



A conjecture

"Standardized PQC cryptosystems will be broken classically before quantum computers break a non-PQC cryptosystem"



Recent supporting evidence:

- Supersingular Isogeny Diffie–Hellman key exchange [Jao, De fao 2011]
- Supersingular Isogeny Key Encapsulation (SIKE, fourth round candidate for NIST PQC competition) in 2017
- [Castryk, Decru 2022], [Maino, Martindale 2022]:
  - key recovery in one hour on a single core

Summary

- Elliptic curves are specially constructed groups where DLP is conjectured to be hard
- These are faster than RSA or DLP over $\mathbf{Z}_p^*$
- Being used widely in practice
  - EC-DSA (bitcoin)
  - TLS EC-DHE (elliptic curve ephemeral DH)
- Post-quantum crypto studies new asymmetric primitives conjectured to resist quantum computers