

An introduction to elliptic curve cryptography

Craig Costello

Workshop on Elliptic Curves

University of Sydney, 1 October 2026

Part 1: Motivation

Part 2: Elliptic curves

Part 3: Over $\mathbb{Q}$ and $\mathbb{C}$

Part 4: Elliptic curve cryptography

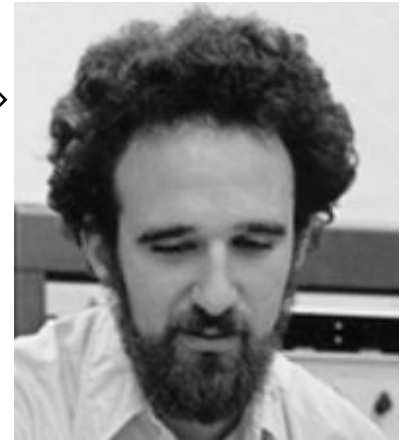
Diffie-Hellman key exchange (circa 1976)

$q = 1606938044258990275541962092341162602522202993782792835301301$

$g = 123456789$



$g^a \bmod q = 78467374529422653579754596319852702575499692980085777948593$



$560048104293218128667441021342483133802626271394299410128798 = g^b \bmod q$

$a =$

685408003627063
761059275919665
781694368639459
527871881531452

$b =$

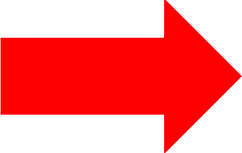
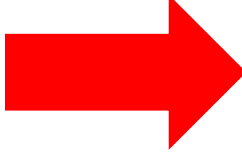
362059131912941
987637880257325
269696682836735
524942246807440

$g^{ab} \bmod q = 437452857085801785219961443000845969831329749878767465041215$

Index calculus

$$\begin{array}{l} \text{solve} \quad g^x \equiv h \pmod{p} \\ \text{e.g.} \quad 3^x \equiv 37 \pmod{1217} \end{array}$$

- factor base $p_i = \{2, 3, 5, 7, 11, 13, 17, 19\}$, $\#p_i = 8$
- Find 8 values of k where 3^k splits over p_i , i.e., $3^k \equiv \pm \prod p_i \pmod{p}$

(mod 1217)		(mod 1216)		(mod 1216)
$3^1 \equiv 3$		$1 \equiv L(3)$		$L(2) \equiv 216$
$3^{24} \equiv -2^2 \cdot 7 \cdot 13$		$24 \equiv 608 + 2 \cdot L(2) + L(7) + L(13)$		$L(3) \equiv 1$
$3^{25} \equiv 5^3$		$25 \equiv 3 \cdot L(5)$		$L(5) \equiv 819$
$3^{30} \equiv -2 \cdot 5^2$		$30 \equiv 608 + L(2) + 2 \cdot L(5)$		$L(7) \equiv 113$
$3^{34} \equiv -3 \cdot 7 \cdot 19$		$34 \equiv 608 + L(3) + L(7) + L(19)$		$L(11) \equiv 1059$
$3^{54} \equiv -5 \cdot 11$		$54 \equiv 608 + L(5) + L(11)$		$L(13) \equiv 87$
$3^{71} \equiv -17$		$71 \equiv 608 + L(17)$		$L(17) \equiv 679$
$3^{87} \equiv 13$		$87 \equiv L(13)$		$L(19) \equiv 528$

Index calculus

$$\begin{array}{ll} \text{solve} & g^x \equiv h \pmod{p} \\ \text{e.g.} & 3^x \equiv 37 \pmod{1217} \end{array}$$

$$\begin{array}{l} L(2) \equiv 216 \\ L(3) \equiv 1 \\ L(5) \equiv 819 \\ L(7) \equiv 113 \\ L(11) \equiv 1059 \\ L(13) \equiv 87 \\ L(17) \equiv 679 \\ L(19) \equiv 528 \end{array}$$

Now search for j such that $g^j \cdot h = 3^j \cdot 37$ factors over p_i

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}$$

$$\begin{aligned} L(37) &\equiv 3 \cdot L(2) + L(7) + L(11) - 16 \pmod{1216} \\ &\equiv 3 \cdot 216 + 113 + 1059 - 16 \\ &\equiv 588 \end{aligned}$$

$$\text{Subexponential complexity } L_p\left[1/3, (64/9)^{1/3}\right] = e^{\left((64/9)^{1/3} + o(1)\right)(\ln(p))^{1/3} \cdot (\ln \ln(p))^{2/3}}$$

Diffie-Hellman key exchange (circa 2016)

$$q =$$

5809605995369958062859502533304574370686975176362895236661486152287203730997110225737336044533118407251326157754980517443990529594540047121662885672187032401032111639706440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580161860200247492568448150242515304449577187604136428738580990172551573934146255830366405915000869643732053218566832545291107903722831634138599586406690325959725187447169059540805012310209639011750748760017095360734234945757416272994856013308616958529958304677637019181594088528345061285863898271763457294883546638879554311615446446330199254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$$g = 123456789$$

g^a
 $(\text{mod } q)$
 $=$

197496648183227193286262018614250555971909799762533760654008147994875775445667054218578105133138217497206890599554928429450667899476854668595594034093493637562451078938296960313488696178848142491351687253054602202966247046105770771577248321682117174246128321195678537631520278649403464797353691996736993577092687178385602298873558954121056430522899619761453727082217823475746223803790014235051396799049446508224661850168149957401474638456716624401906701394472447015052569417746372185093302535739383791980070572381421729029651639304234361268764971707763484300668923972868709121665568669830978657804740157916611563508569886847487772676671207386096152947607114559706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532605242210147489825669666012419572610049572551002200293281421876806011231076345540456724876139639963344901857872119208518550803791724

4116046620695933066832285256534418724107779992205720799935743972371563687620383783327424719396665449687938178193214952698336131699379861648113207956169499574005182063853102924755292845506262471329301240277031401312209687711427883948465928161110782751969552580451787052540164697735099369253619948958941630655511051619296131392197821987575429848264658934577688889155615145050480918561594129775760490735632255728098809700583965017196658531101013084326474277865655251213287725871678420376241901439097879386658420056919119973967264551107584485525537442884643379065403121253975718031032782719790076818413945341143157261205957499938963479817893107541948645774359056731729700335965844452066712238743995765602919548561681262366573815194145929420370183512324404671912281455859090458612780918001663308764073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$=$
 g^b
 $(\text{mod } q)$

$$a =$$

7147687166405;957187905360554739658269240518614591652354912615715297097100679170037904924330116019497881089087696131592831386326210951294944584400497488929803858493191812844757232102398716043906200617764831887545755623377085391250529236463183321912173214641346558452549172283787727566955898452199622029450892269665074265269127802446416400190259271040043389582611419862375878988193612187945591802864062679\86483957813927304368495559776413009721221824915810964579376354556165546298837778595680891578821511273574220422646379170599917677567\30420698422392494816906777896174923072071297603455802621072109220\5466273969774855343758990879608882627763290293452560094576029847\39136138876755438662247926529997805988647241453046219452761811989\97464772529088780604931795419514638292288904557780459294373052654\10485180264002079415193983851143425084273119820368274789460587100\30497747706924427898968991057212096357725203480402449913844583448

$$b =$$

655456209464694;93360682685816031704969423104727624468251177438749706128879957701\93698826859762790479113062308975863428283798589097017957365590672\8357138638957122466760949930089855480244640303954430074800250796203638661931522988606354100532244846391589786412120273772558373965\48653931285483865070903191974204864923589439190352993032676961005\08840431979272991603892747747094094858192679116146502863521484987\08623286193422239171712154568612530067276018808591500424849476686\706784051068715397706852664532638332403983747338379697022624261377163163204493828299206039808703403575100467337085017748387148822224875309641791879395483731754620034884930540399950519191679471224\05558557093219350747155777569598163700850920394705281936392411084\43600686183528465724969562186437214972625833222544865996160464558\54629937016589470425264445624157899586972652935647856967092689604\42796501209877036845001246792761563917639959736383038665362727158

Diffie-Hellman key exchange (cont.)

- Individual secret keys secure under Discrete Log Problem (DLP): $g, g^x \mapsto x$
- Shared secret secure under Diffie-Hellman Problem (DHP): $g, g^a, g^b \mapsto g^{ab}$
- Fundamental operation in DH is group exponentiation: $g, x \mapsto g^x$
... done via "square-and-multiply", e.g., $(x)_2 = (1, 0, 1, 1, 0, 0, 0, 1 \dots)$
- We are working "**mod** q ", but only with one operation: multiplication
- Main reason for fields being so big: (sub-exponential) index calculus attacks!

Elliptic-curve key exchange

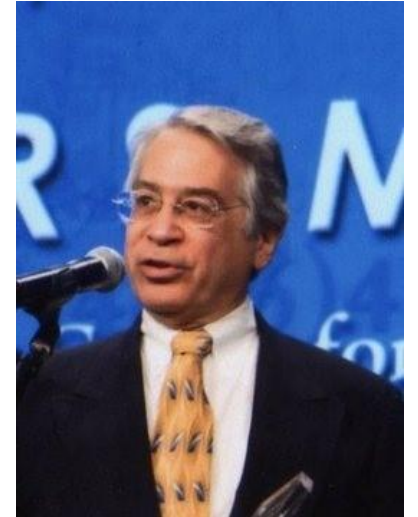
Koblitz and Miller (1985) independently proposed elliptic-curve groups.



Koblitz

$$g^a, g^b \mapsto g^{ab}$$

$$[a]P, [b]P \mapsto [ab]P$$



Miller

Fast arithmetic, with a hard discrete-logarithm problem.

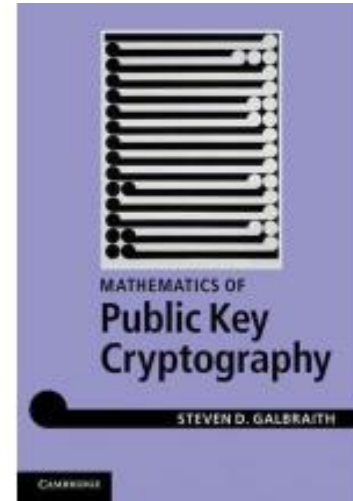
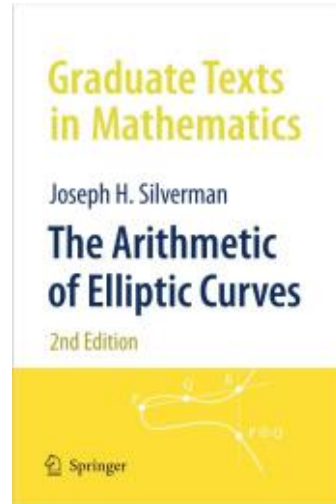
Part 1: Motivation

Part 2: Elliptic curves

Part 3: Over $\mathbb{Q}$ and $\mathbb{C}$

Part 4: Elliptic curve cryptography

Some good references



Elliptic
curves

Silverman's talk: "An Introduction to the Theory of Elliptic Curves"
<http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf>

Elliptic
curves

Sutherland's MIT course on elliptic curves:
<https://math.mit.edu/classes/18.783/2015/lectures.html>

ECC

Koblitz-Menezes: ECC: the serpentine course of a paradigm shift
<http://eprint.iacr.org/2008/390.pdf>

group $(G, +)$

can do $+$ $-$

ring $(R, +, \times)$

can do $+$ $-$ $\times$

field $(F, +, \times)$

can do $+$ $-$ $\times$ $\div$

If you've never seen an elliptic curve before....

Remember: an elliptic curve is a group defined over a field

elliptic curve group $(E, \oplus)$

can do $\oplus \ominus$

underlying field $(K, +, \times)$

can do $+$ $-$ $\times$ $\div$

operations in underlying field are used and combined to
compute the elliptic curve operation $\oplus$

Why move beyond lines and conics?

Degree 1: on the additive line, a discrete logarithm is division.

$$Q = [m]P \implies m = QP^{-1} \pmod{p}, \quad P \neq 0$$

Degree 2: conic groups return us to finite-field logarithms.

$$C_d: x^2 - dy^2 = 1, \quad d \text{ nonsquare in } \mathbb{F}_p, \quad p \neq 2$$

$$C_d(\mathbb{F}_p) \cong \{z \in \mathbb{F}_{p^2}^\times : z^{p+1} = 1\}$$

$p + 1$ points, with finite-field index-calculus attacks.

Degree three: elliptic curves

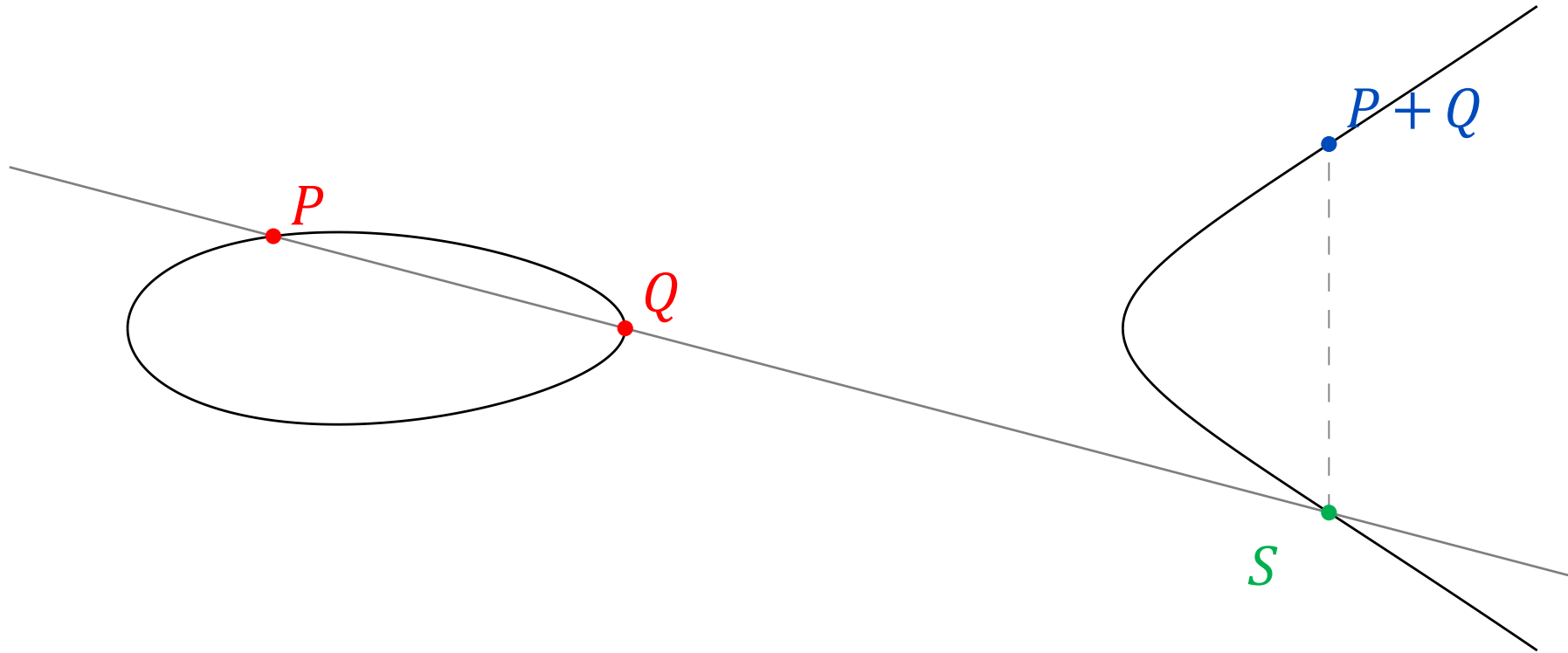
A smooth projective curve of genus 1, with a chosen K -point $\mathcal{O}$.

$$E/K: \quad y^2 = x^3 + ax + b$$



$$\text{char}(K) \neq 2, 3, \quad 4a^3 + 27b^2 \neq 0$$

Two points determine a third intersection



$$P + Q + S = O, \quad P + Q = -S$$

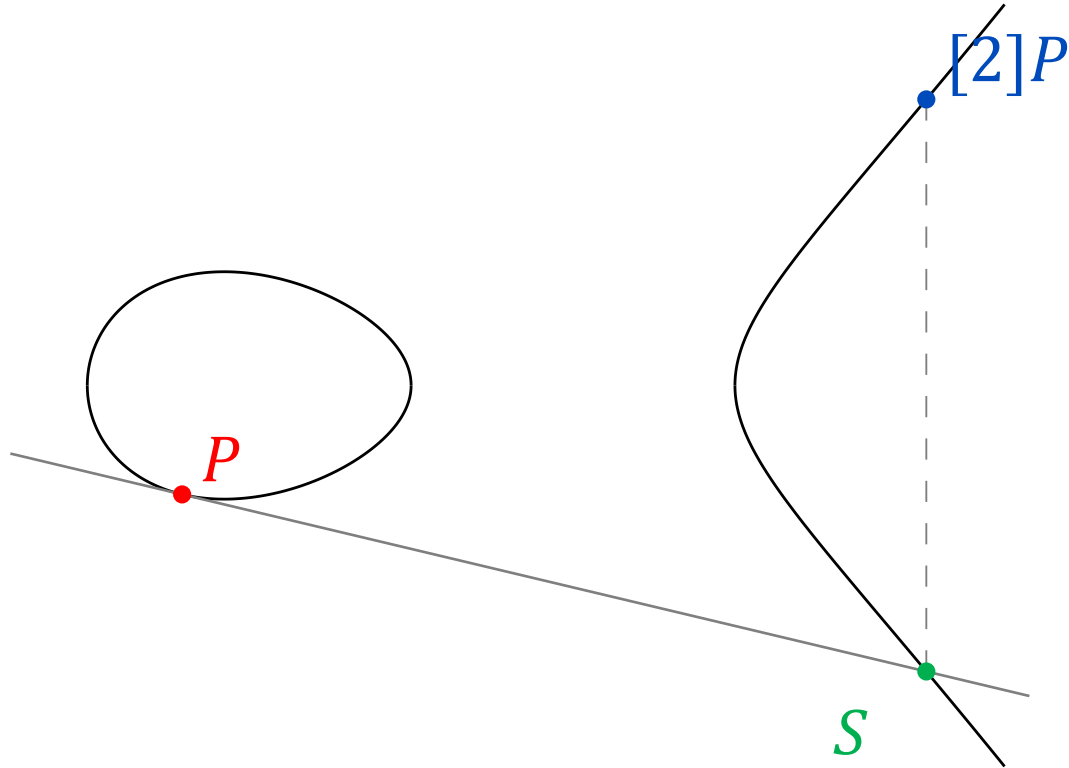
A tangent adds a point to itself

$$E: y^2 = x^3 - 2x$$

$$P = (-1, -1)$$

$$\lambda = \frac{3(-1)^2 - 2}{2(-1)} = -\frac{1}{2}$$

$$[2]P = \left(\frac{9}{4}, \frac{21}{8}\right)$$



The tangent meets the curve twice at P .

The group law in formulas

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$P \neq \pm Q$$

$$\lambda = \frac{3x_P^2 + a}{2y_P}$$

$$P = Q, \quad y_P \neq 0$$

$$R = P + Q$$

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = \lambda(x_P - x_R) - y_P$$

$$O + P = P, \quad P + (-P) = O, \quad \text{and} \quad -(x, y) = (x, -y).$$

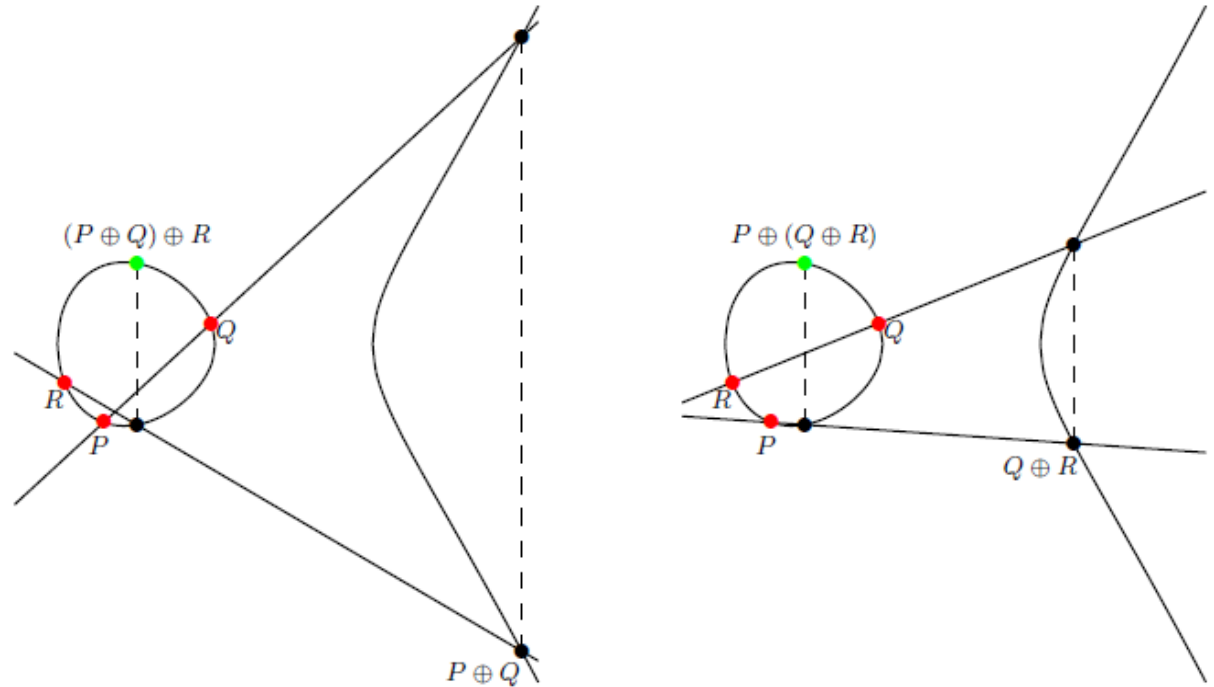
The (abelian) group axioms

- **Closure:** the third point of intersection must be in the field

- **Identity:** $E_{a,b}(K) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\infty\}$

- **Inverse:** $\ominus (x, y) = (x, -y)$

- **Associative:** a theorem



- **Commutative:** line through P and Q same as line through Q and P

Part 1: Motivation

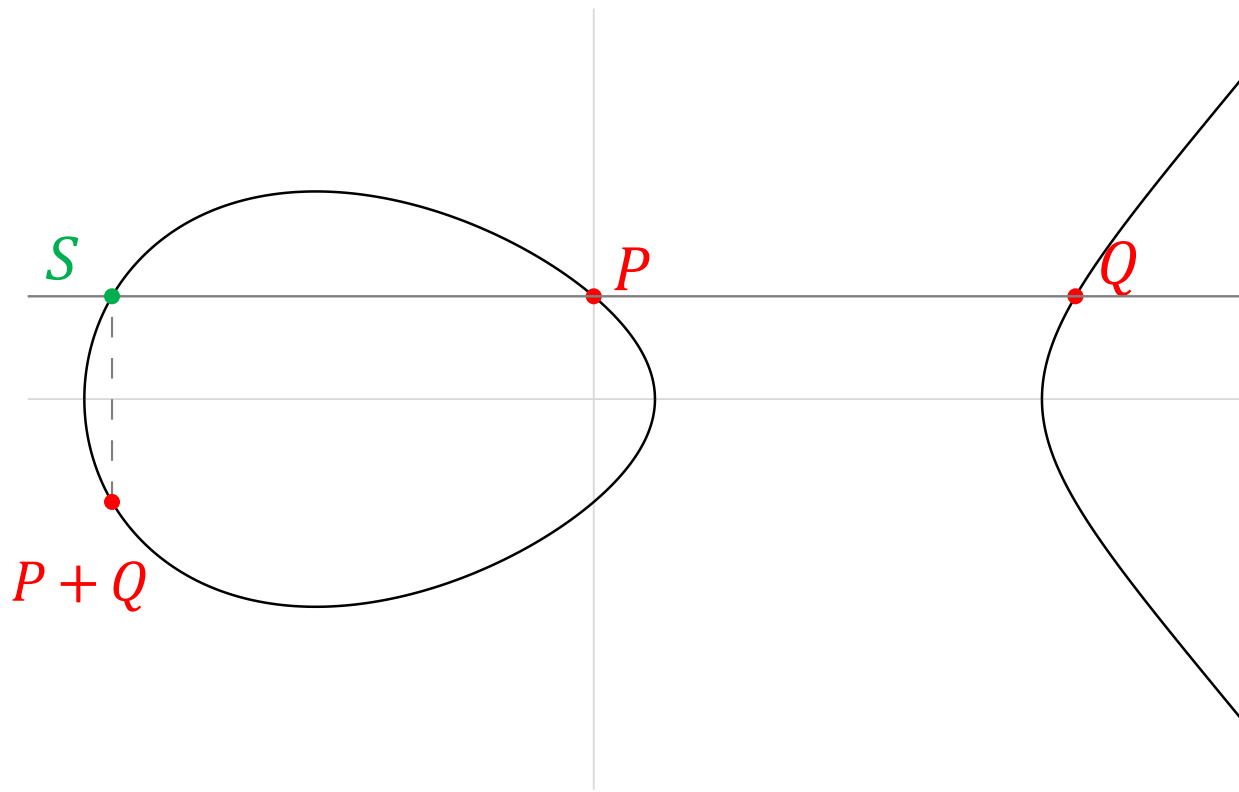
Part 2: Elliptic curves

Part 3: Over $\mathbb{Q}$ and $\mathbb{C}$

Part 4: Elliptic curve cryptography

Rational points on $E/\mathbb{Q}$

$$E: y^2 = x^3 - 4x + 1$$



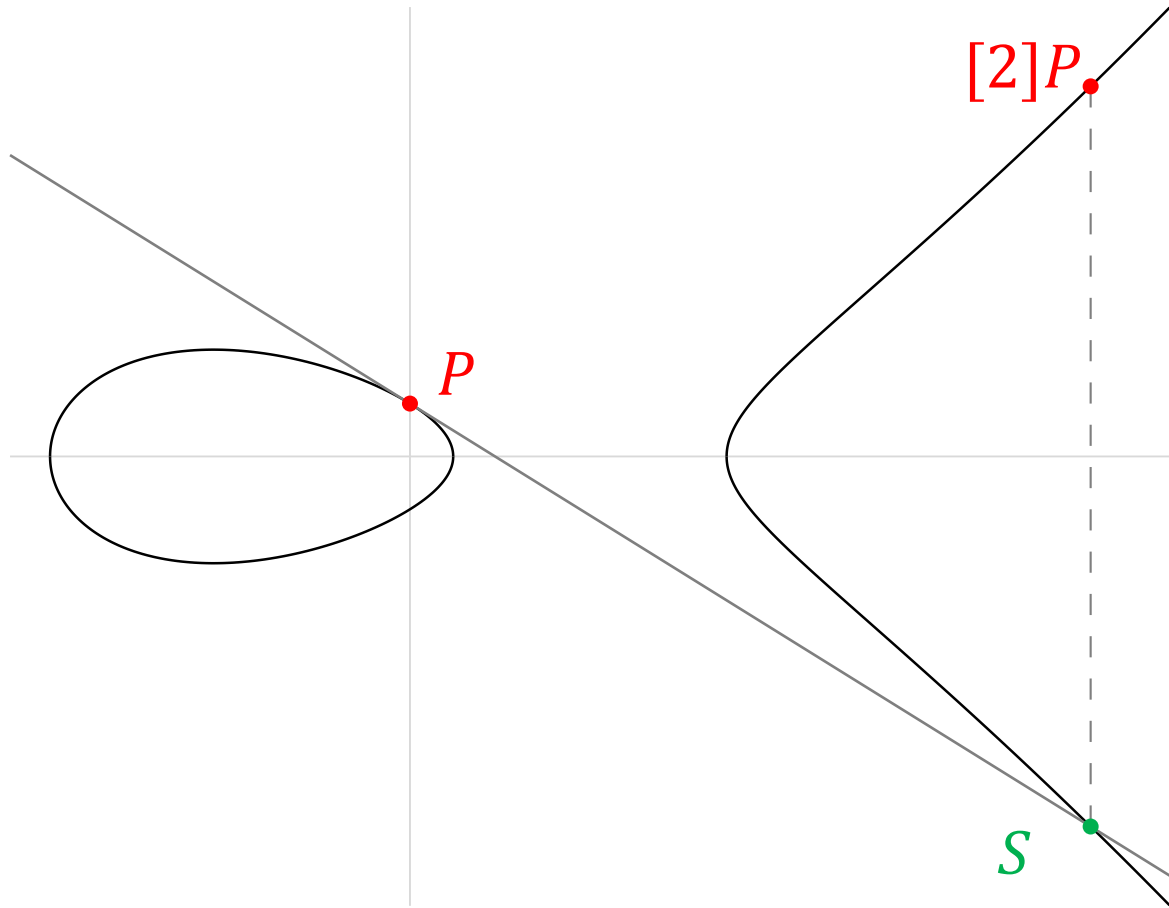
$$P = (0, 1), \quad Q = (2, 1)$$

$$y = 1$$

$$x(x - 2)(x + 2) = 0$$

$$P + Q = (-2, -1)$$

More rational points



The tangent at P is $y = 1 - 2x$

$$\lambda = \frac{3(0)^2 - 4}{2(1)} = -2$$

$$[2]P = (4, 7)$$

$$[3]P = \left(-\frac{7}{4}, \frac{13}{8}\right)$$

Mordell–Weil: a finite description

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

Torsion: $[n]T = \mathbf{O}$ for some integer $n > 0$.

Rank counts independent infinite-order generators.

$$y^2 = x^3 - 4x + 1: \quad E(\mathbb{Q}) = \mathbb{Z}P \oplus \mathbb{Z}Q$$

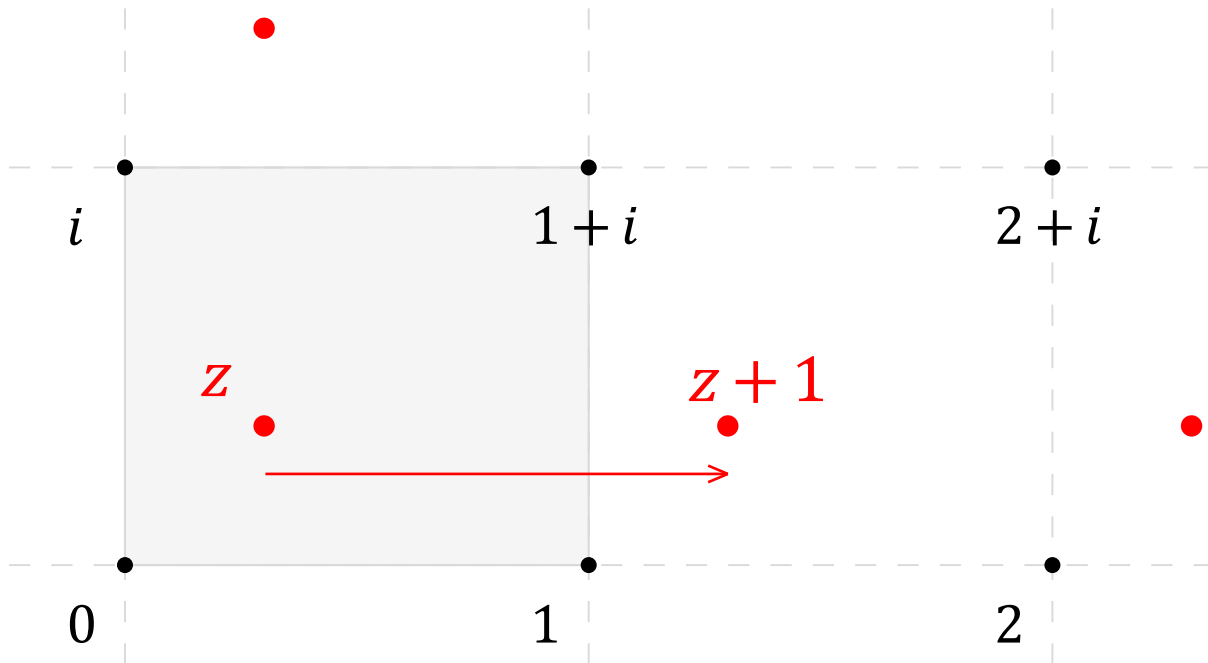
$$P = (0, 1), \quad Q = (2, 1), \quad R = [m]P + [n]Q$$

Some small ranks

Curve	Rank	Free generators
$y^2 = x^3 - x$	0	none
$y^2 = x^3 - 2$	1	(3,5)
$y^2 = x^3 - 4x + 1$	2	(0,1), (2,1)

Positive rank gives infinitely many rational points.

Elliptic curves over $\mathbb{C}$



$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

$$\omega_2/\omega_1 \notin \mathbb{R}$$

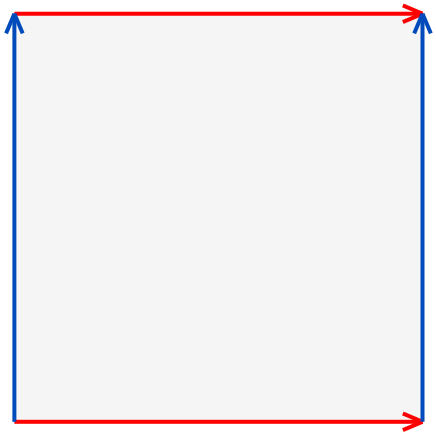
$$\Lambda = \mathbb{Z} + i\mathbb{Z}$$

$$[z] = [z+1] = [z+i]$$

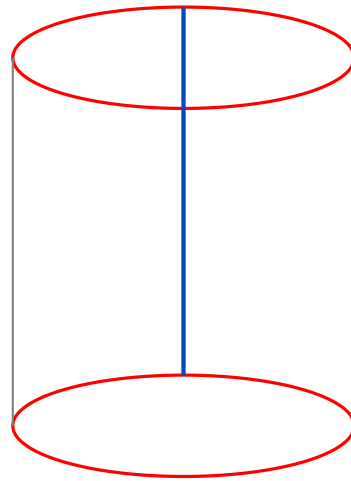
A period changes the representative, but leaves the same class.

Why the quotient is a torus

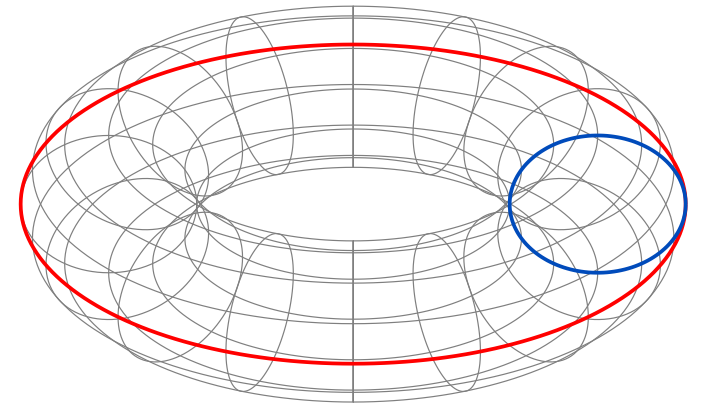
$$\mathbb{C}/(\mathbb{Z} + i\mathbb{Z}) \simeq (\mathbb{R}/\mathbb{Z})^2$$



Square



Cylinder



Torus

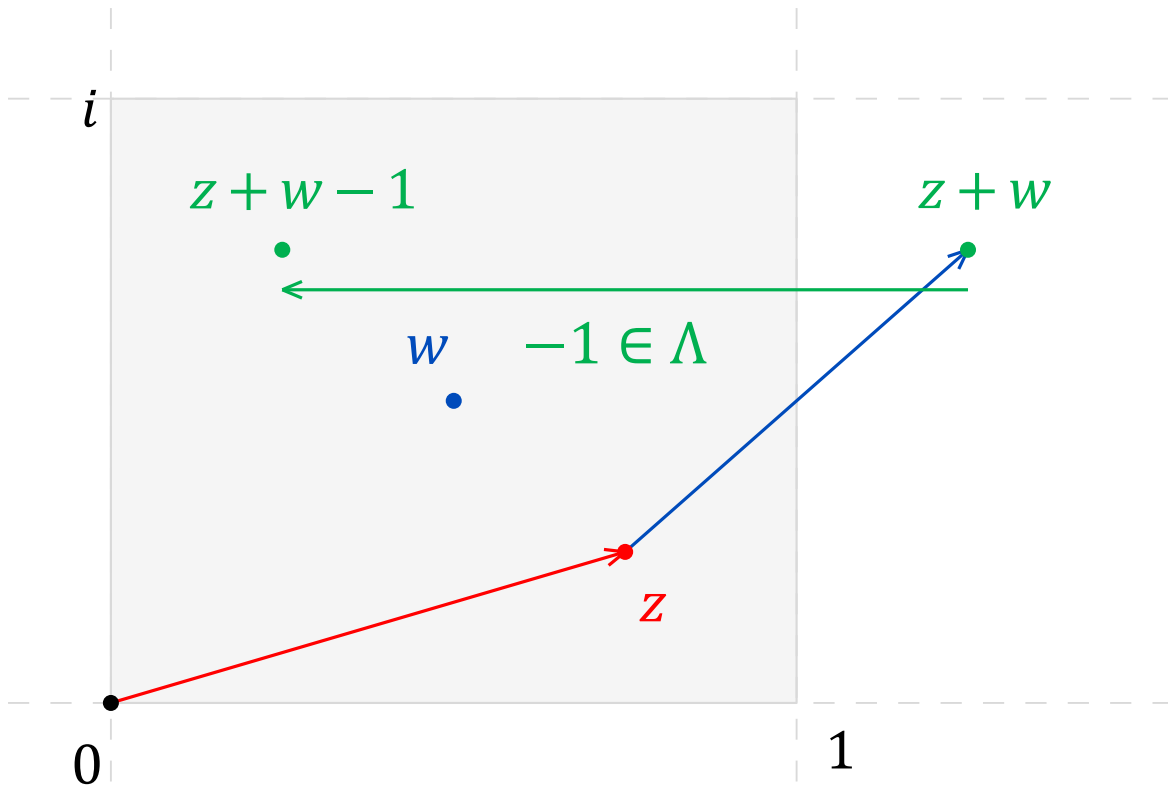
Join left and right edges, then join the circular ends.
Two real dimensions, one complex dimension.

Addition modulo a lattice

$$z = \frac{3}{4} + \frac{1}{4}i, \quad w = \frac{1}{2} + \frac{1}{2}i$$

$$z + w = \frac{5}{4} + \frac{3}{4}i$$

$$\left[\frac{5}{4} + \frac{3}{4}i \right] = \left[\frac{1}{4} + \frac{3}{4}i \right]$$



Subtracting $1 \in \Lambda$ gives the same torus point.

The Weierstrass parametrisation

The Weierstrass function $\wp$ inverts the elliptic integral.

$$\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$

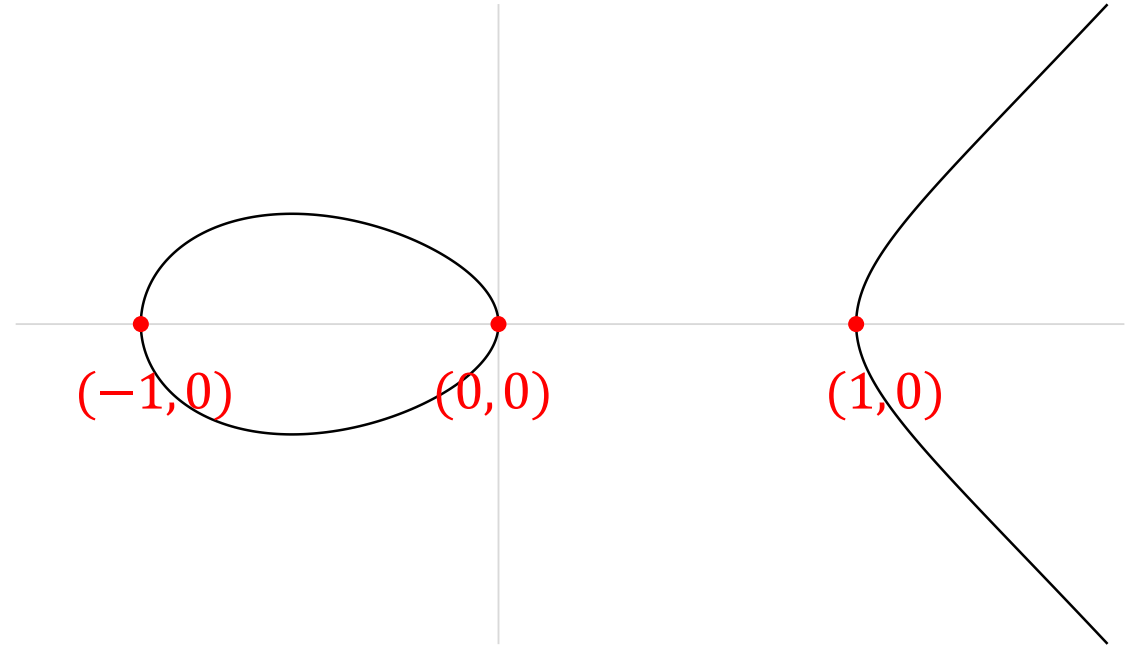
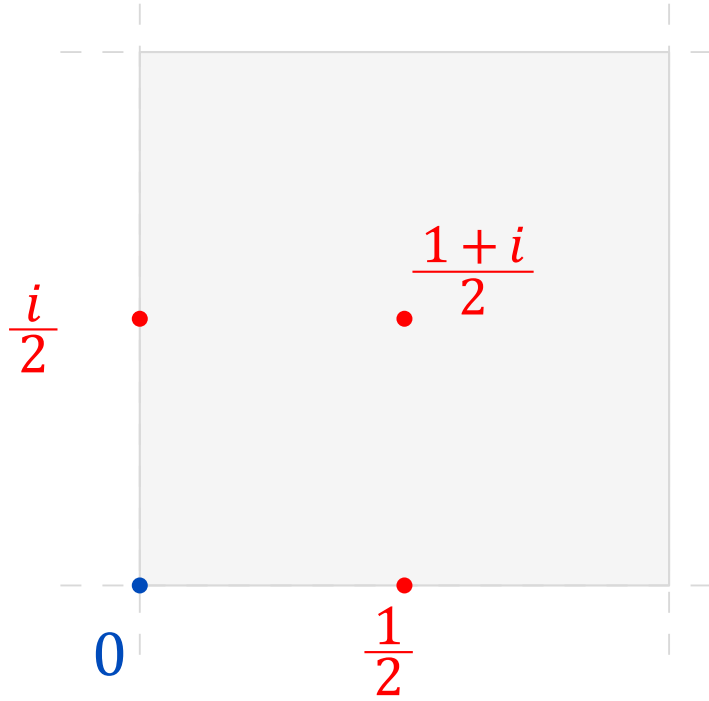
$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(u - \omega)^2} - \frac{1}{\omega^2} \right).$$

$$[z] \mapsto \left(\wp(z), \frac{\wp'(z)}{2} \right), \quad [0] \mapsto \mathcal{O}$$

$$(\wp')^2 = 4\wp^3 + 4a\wp + 4b$$

$$z(P + Q) = z(P) + z(Q) \text{ in } \mathbb{C}/\Lambda.$$

Four points killed by doubling



0 is the point at infinity.

$$E(\mathbb{C})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

For $y^2 = x^3 - x$, use a scaled square lattice.

Part 1: Motivation

Part 2: Elliptic curves

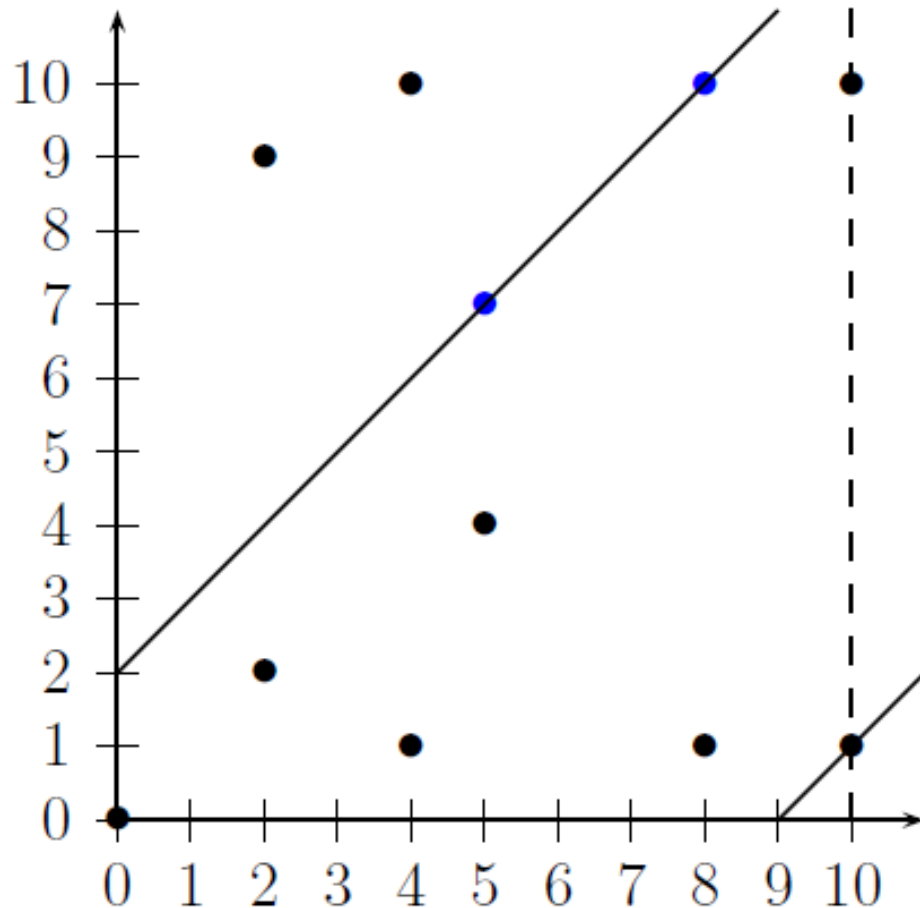
Part 3: Over $\mathbb{Q}$ and $\mathbb{C}$

Part 4: Elliptic curve cryptography

A toy example, cont.

$$E/\mathbb{F}_{11}: y^2 = x^3 - 2x$$

$$\#E = 12$$



$$(5,7) \oplus (8,10) = (10,10)$$

ECDH key exchange (1999 – nowish)

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

$$E/\mathbb{F}_p: y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ 36134250956749795798585127919587881956611106672985015071877198253568414405109)$



$a =$

89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

$[a]P = (84116208261315898167593067868200525612344221886333785331584793435449501658416, \\ 102885655542185598026739250172885300109680266058548048621945393128043427650740)$

$[b]P = (24897888184477543965151224683693228039934561265205382251606920317839692409866, \\ 39216653051315936751218517470892784660594591992540129887276696959298943554579)$

$[ab]P = (114280511058103970128405829592043166823317010363608011211277752089967665159665, \\ 38401020163043884668877143922767232804915209766578696485607981625456381538422)$

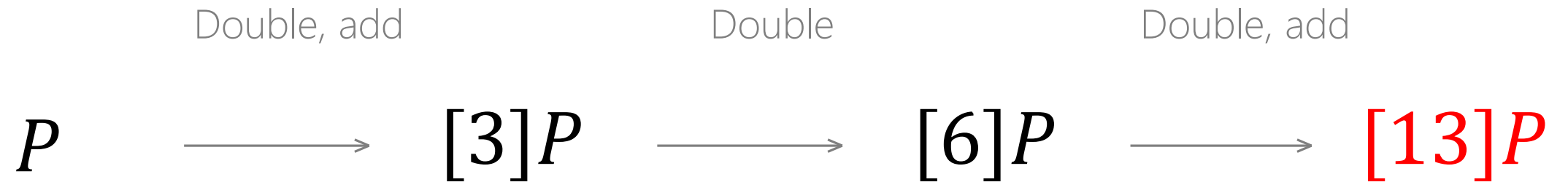


$b =$

10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

Scalar multiplication: read the bits

$$13 = (1101)_2$$



Read the bits from left to right, after the leading 1.

$$R \leftarrow [2]R, \quad R \leftarrow R + P \quad \text{if the bit is 1}$$

The field operations behind each bit

$$\lambda_{\text{DBL}} = \frac{3x^2 + a}{2y}$$

$$\lambda_{\text{ADD}} = \frac{y_Q - y_P}{x_Q - x_P}$$

Bits	1	0	1
Work	<i>D, A</i>	<i>D</i>	<i>D, A</i>

Field inversions cost time. Secret-dependent work may leak bits.

Projective coordinates

$$(X:Y:Z) \sim (cX:cY:cZ), \quad c \in K^\times$$

$$x = X/Z, \quad y = Y/Z \quad (Z \neq 0)$$

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

$$O = (0:1:0)$$

The all-zero triple is forbidden.

Doubling without an inversion

$$W = 3X^2 + aZ^2$$

$$X' = 2YZ(W^2 - 8Y^2XZ)$$

$$Y' = W(12Y^2XZ - W^2) - 8Y^4Z^2$$

$$Z' = 8Y^3Z^3$$

No inversion. Handle $[2]O = O$ separately.

One inversion at the end

Use the same bit algorithm in projective coordinates.

$$(X_R:Y_R:Z_R) = [k](X_P:Y_P:Z_P)$$

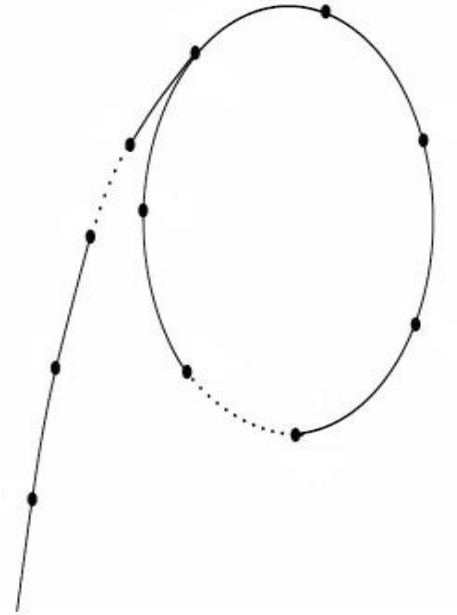
$$Z_R \neq 0: \quad z = Z_R^{-1}$$

$$(x_R, y_R) = (X_R z, Y_R z)$$

If $Z_R = 0$, the answer is O .

ECDLP security and Pollard's rho algorithm

- ECDLP: given $P, Q \in E(\mathbb{F}_p)$ of prime order N , find k such that $Q = [k]P$
- Pollard'78: compute pseudo-random $R_i = [a_i]P + [b_i]Q$ until we find a collision $R_i = R_j$ with $b_i \neq b_j$, then $k = (a_j - a_i)/(b_i - b_j)$
- Birthday paradox says we can expect collision after computing $\sqrt{\pi N/2}$ group elements R_i , i.e., after $\approx \sqrt{N}$ group operations.
So 2^{128} security needs $N \approx 2^{256}$
- The best known ECDLP algorithm on (well-chosen) elliptic curves remains generic, i.e., elliptic curves are as strong as is possible



Index calculus on elliptic curves?

[Miller, 85] : “it is extremely unlikely that an index calculus [...] will ever be able to work”

Consider $E/\mathbb{F}_{1217}$: $y^2 = x^3 - 3x + 139$

$$\#E(\mathbb{F}_{1217}) = 1277$$

$$P = (3,401) \text{ and } Q = (192,847)$$

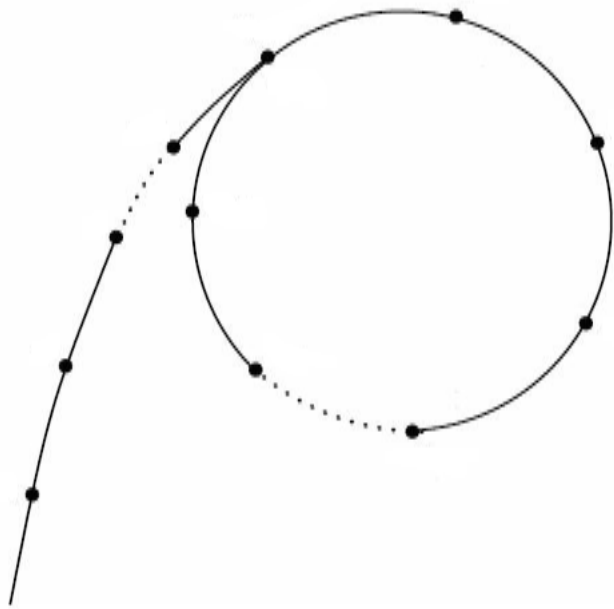
ECDLP: find k such that $[k]P = Q$

Regardless of factor base, can't efficiently decompose elements!

e.g., factor base $R_i = \{(3,401), (5,395), (7,73), (11,252), (13,104), (19,265)\}$

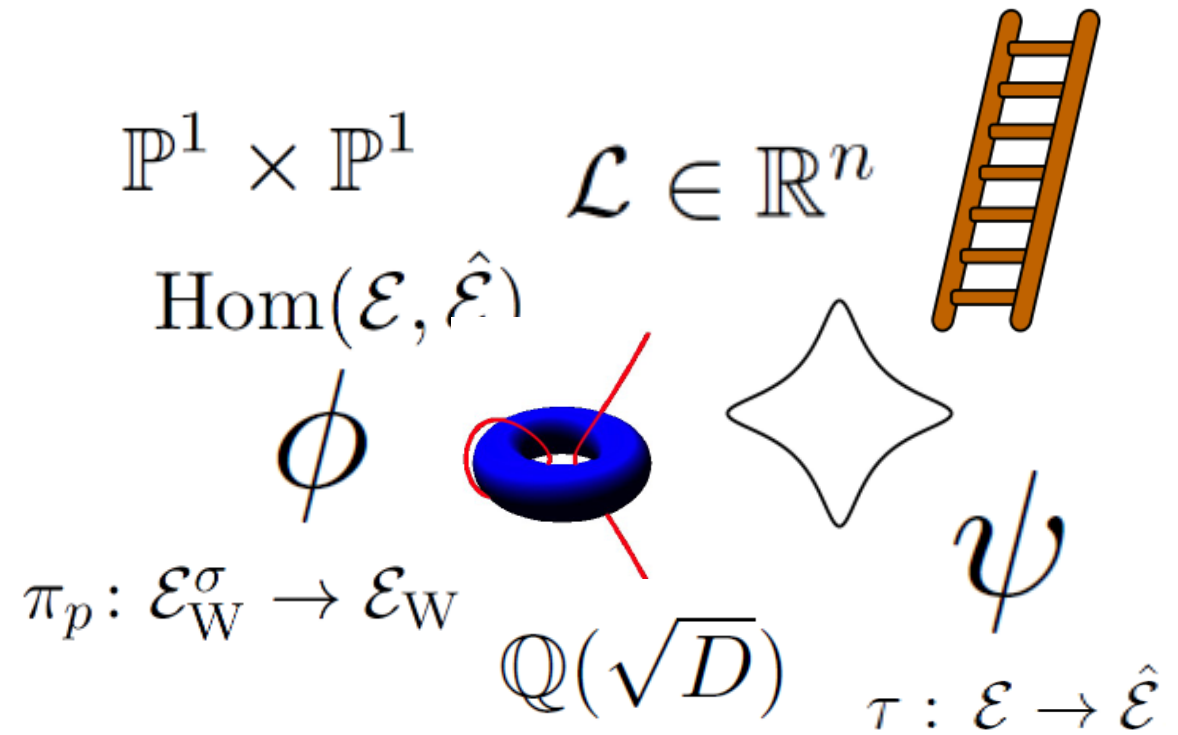
Writing $S = \sum [k_i]R_i$ involves solving discrete logarithms, compare this to integers **mod** p where we lift and factorise over the integers

Elliptic curves: the best of both worlds



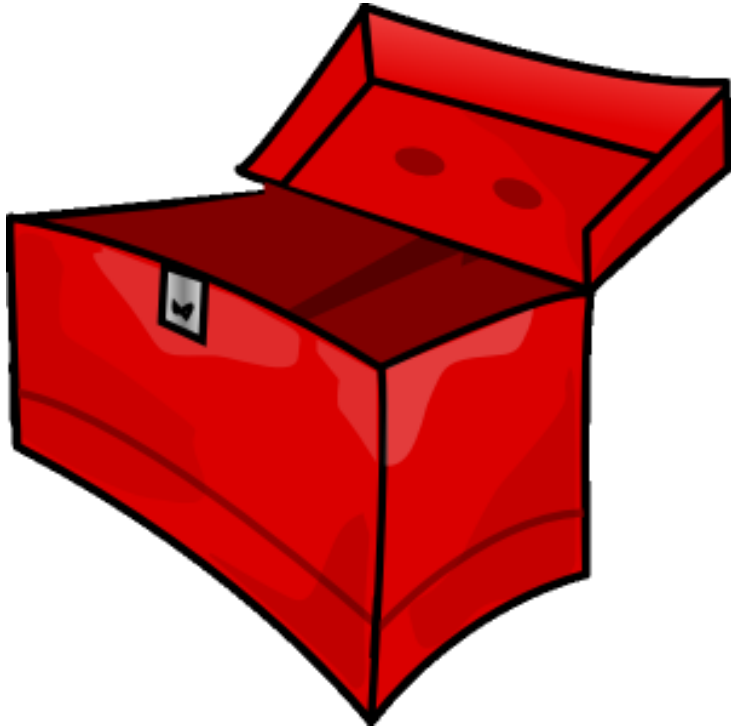
attacker: generic

vs.



us: not generic

ECC is the best of both worlds



attacker's toolbox

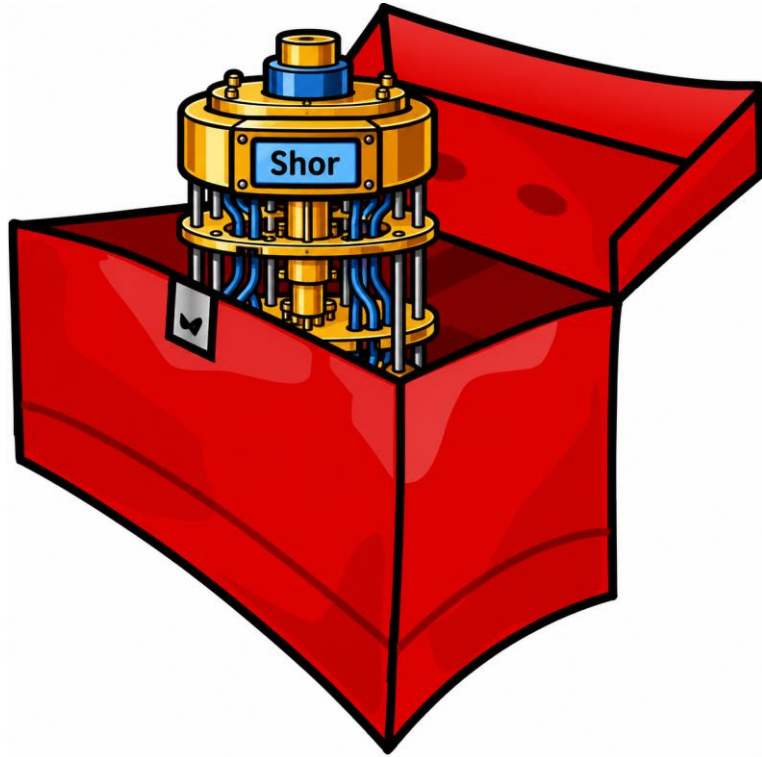
vs.



our toolbox

Quantum computers change the problem

Shor's algorithm gives the attacker a new tool.



attacker's toolbox



our toolbox

A sufficiently large fault-tolerant quantum computer solves the DLP.

From objects to maps

Today: elliptic curves and their groups of points.

$$\varphi: E \longrightarrow E'$$

$$\varphi(P + Q) = \varphi(P) + \varphi(Q), \quad \varphi(O) = O'$$

$$[2]: E \longrightarrow E, \quad P \longmapsto [2]P$$

Tomorrow's (isogeny) talk: maps between elliptic curves.

Questions?