

# Elliptic Nets

## How To Catch an Elliptic Curve

**Kate Stange**

**Brown University Graduate Student Seminar  
February 7, 2007**

<http://www.math.brown.edu/~stange/>

# Timeline

**Circa 4000 B.C.**  
pre-Colombian  
farmers discover  
potato

**1573**

Potato results in  
birth of Caravaggio<sup>1</sup>

**February 7, 2004**

Inventor of Poutine dies  
of pulmonary disease

**Last spring**

A cute potato  
named George  
is born

**July 12 2005**

Sonja Thomas wins  
\$2500 by eating 53  
potato skins in 12  
minutes

**Now**

That samosa  
you are eating  
is George

<sup>1</sup>The Potato Fan Club: <http://tombutton.users.btopenworld.com/>

# **Part I: Elliptic Curves are Groups**

# Elliptic Curves

In general,

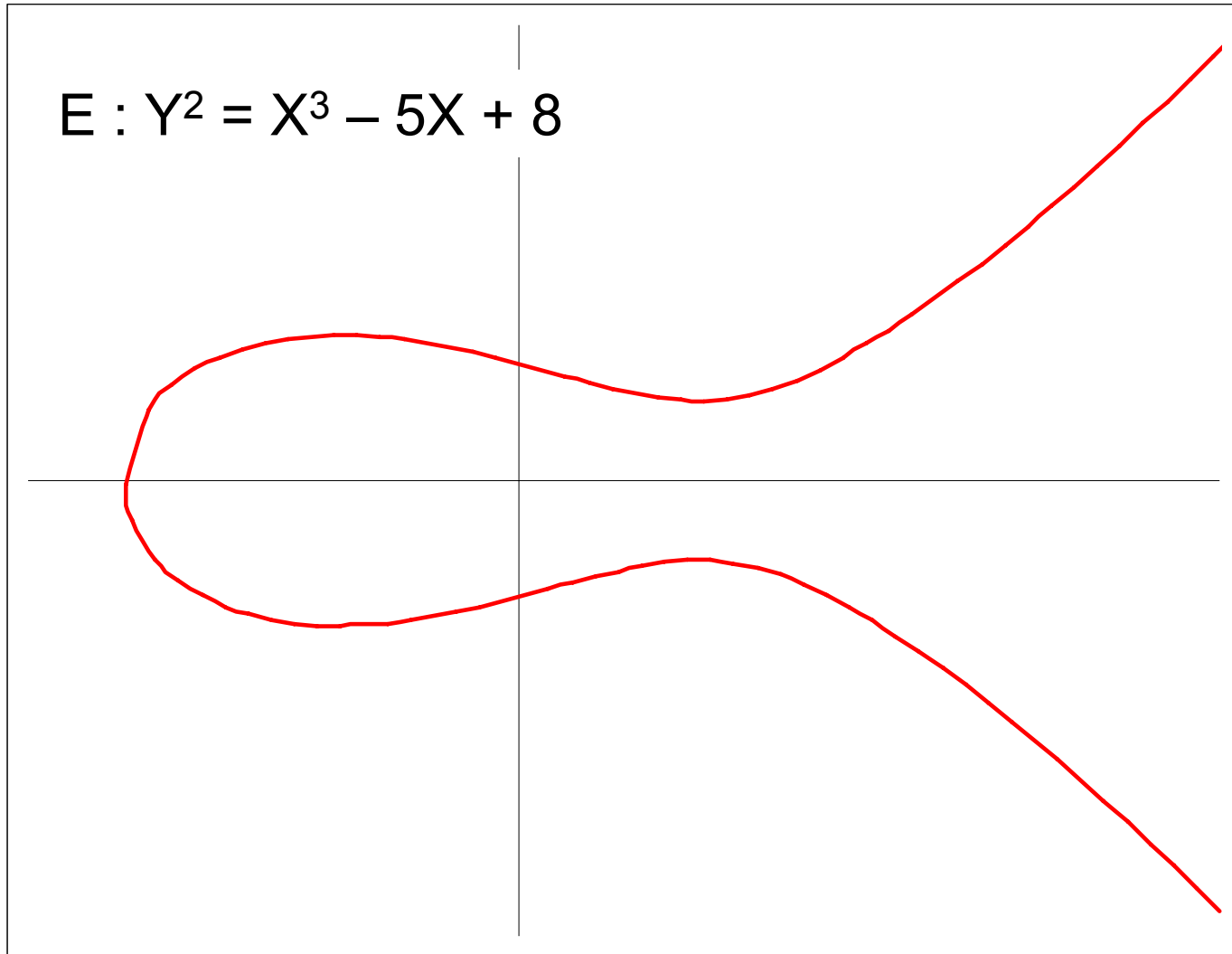
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

For people like us,

$$y^2 = x^3 + Ax + B$$

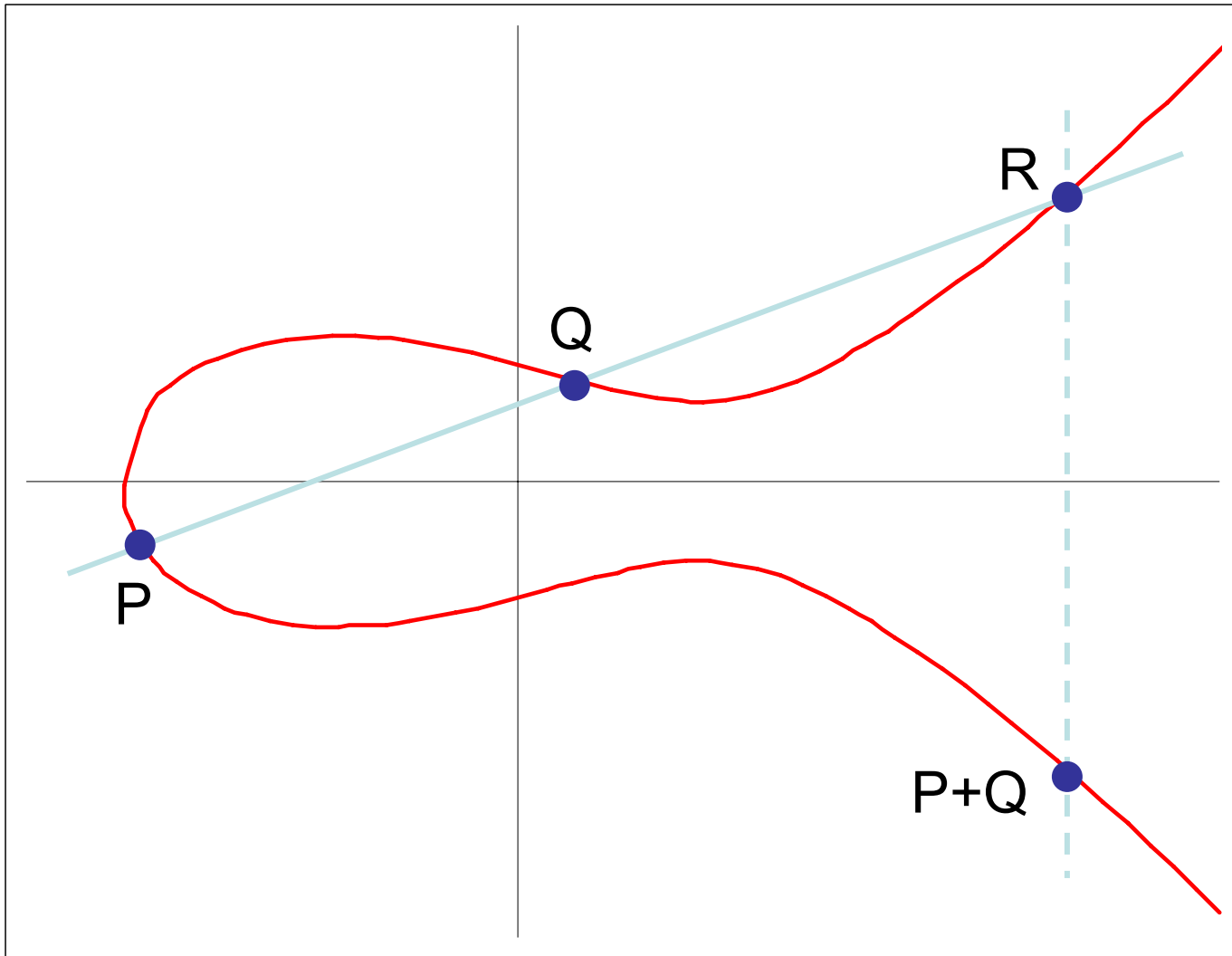
(Us regular folks, who might enjoy characteristic  $\neq 2, 3$  or an occasional python boot.)

# A Typical Elliptic Curve E



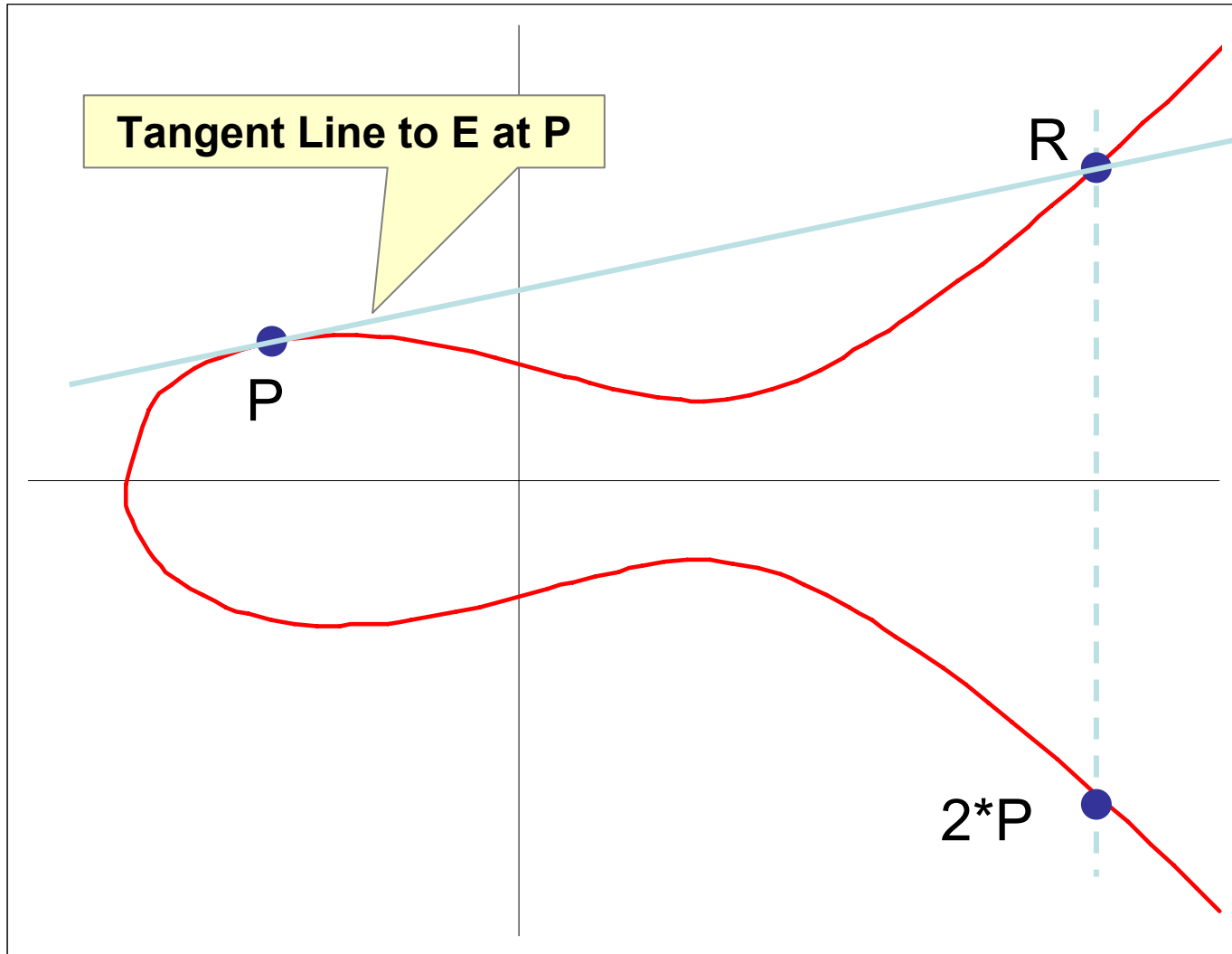
The lack of shame involved in the theft of this slide from Joe Silverman's website should make any graduate student proud.

# Adding Points P + Q on E



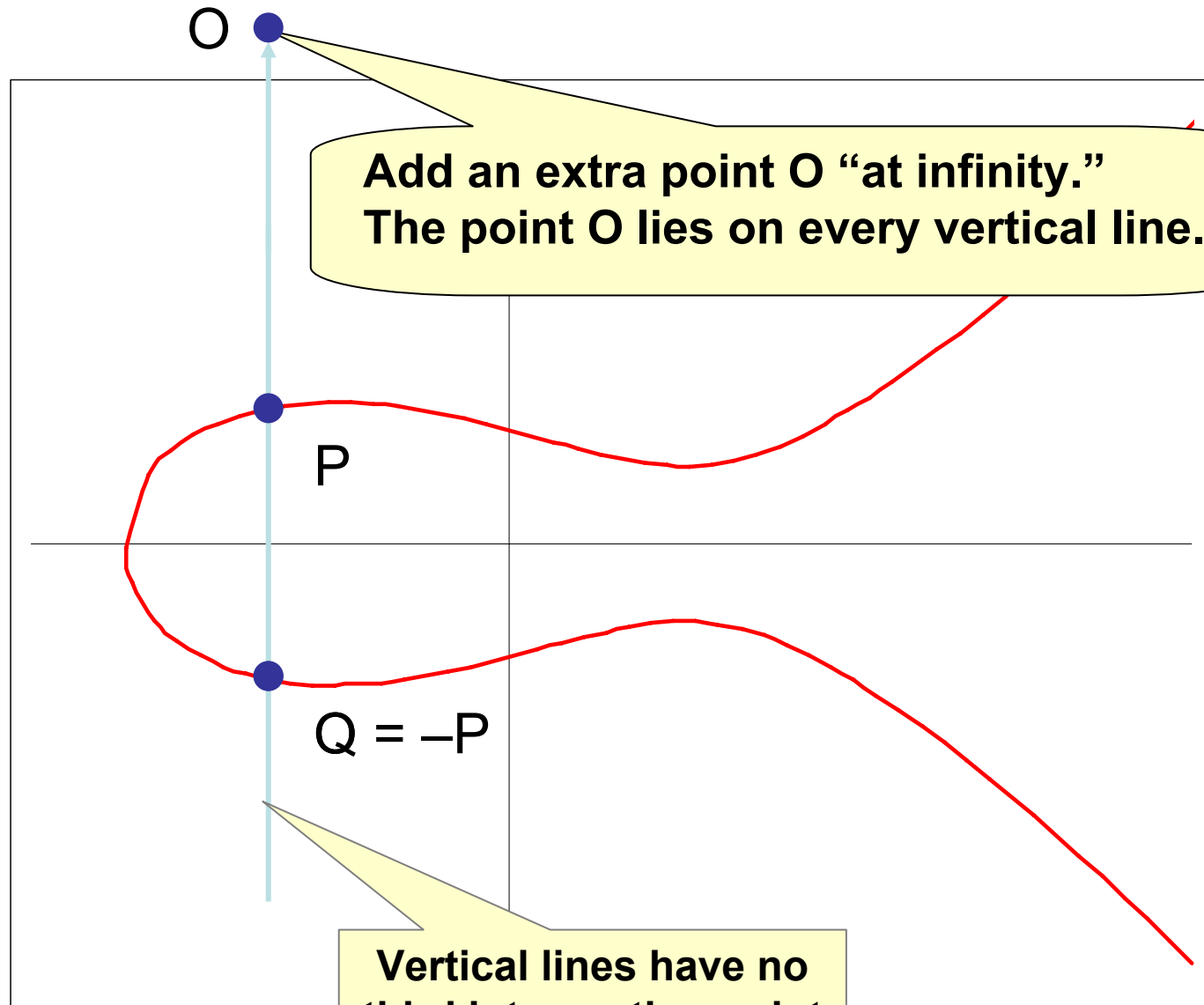
The lack of shame involved in the theft of this slide from Joe Silverman's website should make any graduate student proud.

# Doubling a Point P on E



The lack of shame involved in the theft of this slide from Joe Silverman's website should make any graduate student proud.

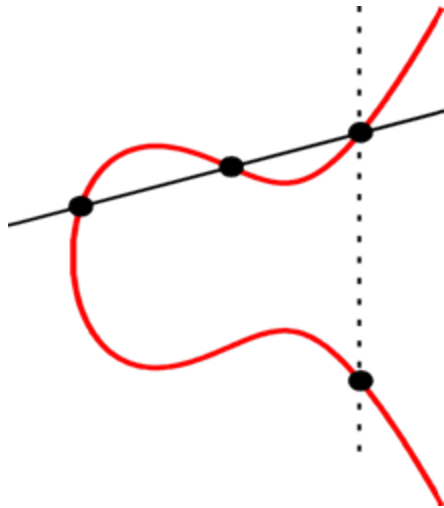
# Vertical Lines and an Extra Point at Infinity



The lack of shame in **third intersection point** from Joe Silverman's website should make any graduate student proud.

# **Part II: Elliptic Divisibility Sequences**

# Elliptic Divisibility Sequences: Seen In Their Natural Habitat



$$P \in E(\mathbb{Q})$$

$$P = \left( \frac{a_P}{d_P^2}, \frac{b_P}{d_P^3} \right)$$

$$P, 2P, 3P, 4P, \dots \in E(\mathbb{Q})$$



$$d_P, d_{2P}, d_{3P}, d_{4P}, \dots \in \mathbb{Z}$$

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

$$P = (0, 0)$$

$$P = \left(\frac{0}{1}, \frac{0}{1}\right)$$

$$d_P = 1$$

$$2P = \left(\frac{3}{1}, \frac{5}{1}\right)$$

$$d_{2P} = 1$$

$$3P = \left(-\frac{11}{9}, \frac{28}{27}\right)$$

$$d_{3P} = -3$$

$$4P = \left(\frac{114}{121}, -\frac{267}{1331}\right)$$

$$d_{4P} = 11$$

$$5P = \left(-\frac{2739}{1444}, -\frac{77033}{54872}\right)$$

$$d_{5P} = 38 = 2 \times 19$$

$$6P = \left(\frac{89566}{62001}, -\frac{31944320}{15438249}\right)$$

$$d_{6P} = 249 = 3 \times 83$$

$$7P = \left(-\frac{2182983}{5555449}, -\frac{20464084173}{13094193293}\right)$$

$$d_{7P} = -2357$$

$$8P = \left(\frac{1169154495}{76860289}, -\frac{41440508823358}{673834153663}\right)$$

$$d_{8P} = 8767 = 11 \times 797$$

# Elliptic Curve Group Law

$$y^2 = x^3 + Ax + B$$

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad P_3 = (x_3, y_3) = P_1 + P_2$$

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = -\lambda x_3 - \nu.$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + A}{2y_1}, & x_1 = x_2 \end{cases} \quad \nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{-x_1^3 + Ax_1 + 2B}{2y_1}, & x_1 = x_2 \end{cases}$$

# So What Happens to Point Multiples?

If  $P = (x, y)$

then  $nP = \left( \frac{\phi_n}{\Psi_n^2}, \frac{\omega_n}{\Psi_n^3} \right)$  where

$$\Psi_1 = 1, \quad \Psi_2 = 2y,$$

$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

$$\Psi_{m+n} \Psi_{m-n} = \Psi_{m+1} \Psi_{m-1} \Psi_n^2 - \Psi_{n+1} \Psi_{n-1} \Psi_m^2$$

$$\phi_n = x \Psi_n^2 - \Psi_{n+1} \Psi_{n-1}$$

$$4y \omega_n = \Psi_{n+2} \Psi_{n-1}^2 - \Psi_{n-2} \Psi_{n+1}^2$$

An ***Elliptic Divisibility Sequence*** is an integer sequence satisfying the following recurrence relation.

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2$$

# Some Example Sequences

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,  
14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35,  
36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46,  
47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57,  
58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68,  
69, 70, 71, 72, 73, 74, 75, 76, 77, ...

# Some Example Sequences

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,  
233, 377, 610, 987, 1597, 2584, 4181,  
6765, 10946, 17711, 28657, 46368,  
75025, 121393, 196418, 317811, 514229,  
832040, 1346269, 2178309, 3524578,  
5702887, 9227465, 14930352, 24157817,  
39088169, ...

# Some Example Sequences

0, 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59,  
129, -314, -65, 1529, -3689, -8209, -  
16264, 83313, 113689, -620297, 2382785,  
7869898, 7001471, -126742987, -  
398035821, 1687054711, -7911171596, -  
47301104551, 43244638645, ...

# Our First Example

0, 1, 1, -3, 11, 38, 249, -2357, 8767,  
496035, -3769372, -299154043, -  
12064147359, 632926474117, -  
65604679199921, -6662962874355342, -  
720710377683595651,  
285131375126739646739,  
5206174703484724719135, -  
36042157766246923788837209,  
14146372186375322613610002376, ...

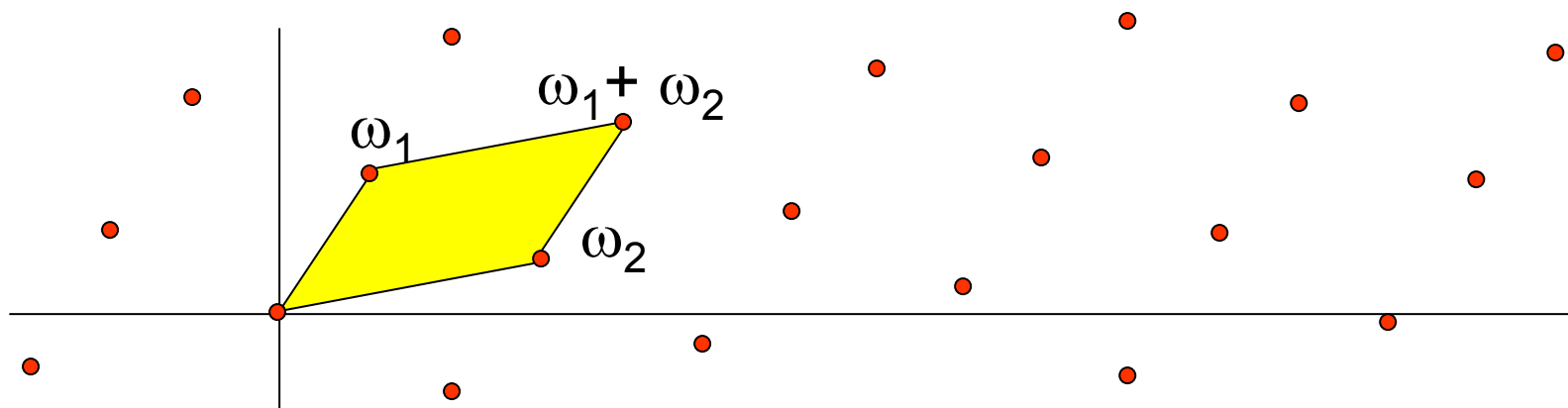
# Some more terms...

0,  
1,  
1,  
-3,  
11,  
38,  
249,  
-2357,  
8767,  
496035,  
-3769372,  
-299154043,  
-12064147359,  
632926474117,  
-65604679199921,  
-6662962874355342,  
-720710377683595651,  
285131375126739646739,  
5206174703484724719135,  
-36042157766246923788837209,  
14146372186375322613610002376,  
13926071420933252466435774939177,  
18907140173988982482283529896228001,  
-23563346097423565704093874703154629107,  
52613843196106605131800510111110767937939,  
191042474643841254375755272420136901439312318,  
201143562868610416717760281868105570520101027137,  
-5095821991254990552236265353900129949461036582268645,  
-16196160423545762519618471188475392072306453021094652577,  
390721759789017211388827166946590849427517620851066278956107,  
-5986280055034962587902117411856626799800260564768380372311618644,  
-108902005168517871203290899980149905032338645609229377887214046958803,  
-4010596455533972232983940617927541889290613203449641429607220125859983231,  
15250620746565227762531462142393791012856442441235840714430103762819736595413,  
-5286491728223134626400431117234262142530209508718504849234889569684083125892420201,  
-835397059891704991632636814121353141297683871830623235928141040342038068512341019315446,  
10861789122218115292139551508417628820932571356531654998704845795890033629344542872385904645,  
13351876087649817486050732736119541016235802111163925747732171131926421411306436158323451057508131,  
2042977307842020707295863142858393936350596442010700266977612272386600979584155605002856821221263113151,  
-666758599738582427580962194986025574476589178060749335314959464037321543378395210027048006648288905711378993,  
333167086588478561672098259752122036440335441580932677237086129099851559108618156882215307126455938552908231344016,  
150866730291138374331025045659005244449458695650548930543174261374298387455590141700233602162964721944201442274446853073,  
113760065777234882865006940654654895718896520042025048306493515052149363166271410666963494813413836495437803419621982027412929,  
-159253169967307321375677555136314569434529937177007635953107117202675658212866813320738037987472039386883798439657624623140677934307,  
44416310167318880256461428190965193979854149844320579714027500283754273952989380044808517851663079825097686172334231751637837837673262107, ...

$$W_n \sim c^{n^2}$$

# **Part III: Elliptic Curves over Complex Numbers**

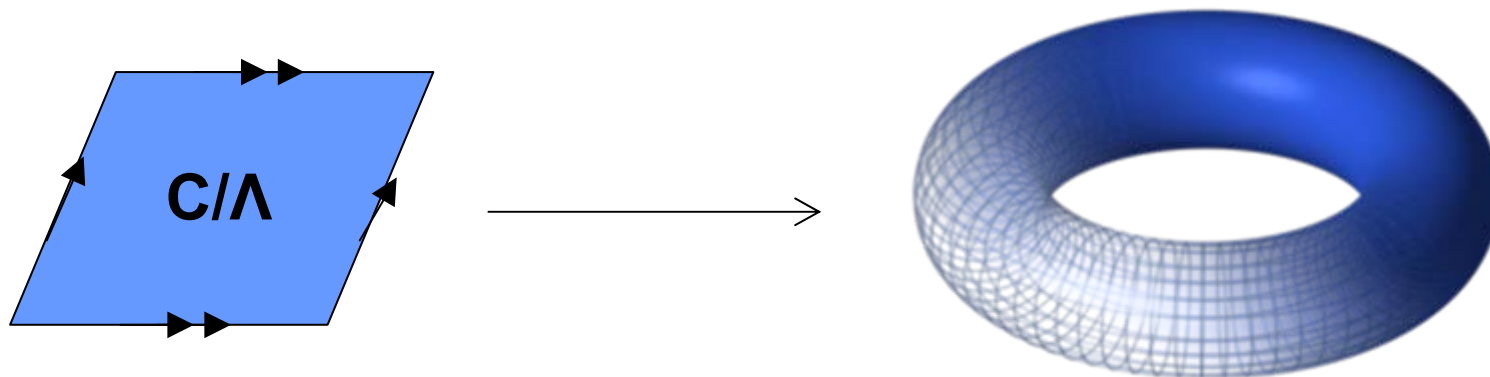
# Take a Lattice $\Lambda$ in the Complex Plane



$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}.$$

The function  $\wp(z)$  (respectively  $\wp'(z)$ ) is periodic with respect to the lattice  $\Lambda$ , and meromorphic with double (respectively triple) poles at each lattice point.

# Elliptic Curves over Complex Numbers



$$\mathbb{C}/\Lambda \longrightarrow E : y^2 = x^3 + Ax + B$$
$$z \longmapsto (\wp(z), -\wp'(z)/2)$$

# Elliptic Functions

Weierstrass sigma function

$$\sigma(z) = z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{(z/\omega) + (z/\omega)^2 / 2}$$

*Not* periodic with respect to  $\Lambda$ .

But elliptic functions can be “built” like rational functions:

$$f = \frac{\sigma(z - a)\sigma(z - b)}{\sigma(z - c)\sigma(z - d)}$$

Zeroes at  $z = a$  and  $z = b$

Poles at  $z = c$  and  $z = d$

# Example Elliptic Functions

$$\wp(z) - \wp(a) = -\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}$$

$$\wp'(z) = -\frac{\sigma(2z)}{\sigma(z)^4}$$

$$\Psi_1 = 1, \quad \Psi_2 = 2y = \frac{\sigma(2z)}{\sigma(z)^4},$$

$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 = \frac{\sigma(3z)}{\sigma(z)^9}$$

...

# **Part IV: Elliptic Divisibility Sequences from Elliptic Functions**

# Elliptic Divisibility Sequences: Two Good Definitions

$$W_n \in \mathbb{Z}, \text{ for all } n \in \mathbb{Z}$$

## Definition A

Define elliptic functions

$$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

Fix elliptic curve  $\mathbb{C}/\Lambda$   
and rational point  $z \in \mathbb{C}/\Lambda$

$$W_n = \Psi_n(z)$$

This is just an elliptic function with zeroes all the  $n$ -torsion points and a pole of order  $n^2$  at the point at infinity.

**Yes, this is the same  $\Psi_n$  as before!**

# Elliptic Divisibility Sequences: Two Good Definitions

$$W_n \in \mathbb{Z}, \text{ for all } n \in \mathbb{Z}$$

## Definition A

Define elliptic functions

$$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

Fix elliptic curve  $\mathbb{C}/\Lambda$   
and rational point  $z \in \mathbb{C}/\Lambda$

$$W_n = \Psi_n(z)$$

## Definition B

Given initial conditions

$$W_0, W_1, W_2, W_3, W_4 \in \mathbb{Z}$$

$$W_0 = 0, W_1 = 1, W_2 | W_4, W_2 W_3 \neq 0$$

and recurrence for all  $m, n \in \mathbb{Z}$

$$W_{m+n} W_{m-n} =$$

$$W_{m+1} W_{m-1} W_n^2 - W_{n+1} W_{n-1} W_m^2$$

## Theorem (M Ward, 1948): A and B are equivalent.

From the initial conditions in Definition B, one can explicitly calculate the curve and point needed for Definition A.

### Definition A

Define elliptic functions

$$\Psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}$$

Fix elliptic curve  $\mathbb{C}/\Lambda$   
and rational point  $z \in \mathbb{C}/\Lambda$

$$W_n = \Psi_n(z)$$

### Definition B

Given initial conditions

$$W_0, W_1, W_2, W_3, W_4 \in \mathbb{Z}$$

$$W_0 = 0, W_1 = 1, W_2 | W_4, W_2 W_3 \neq 0$$

and recurrence for all  $m, n \in \mathbb{Z}$

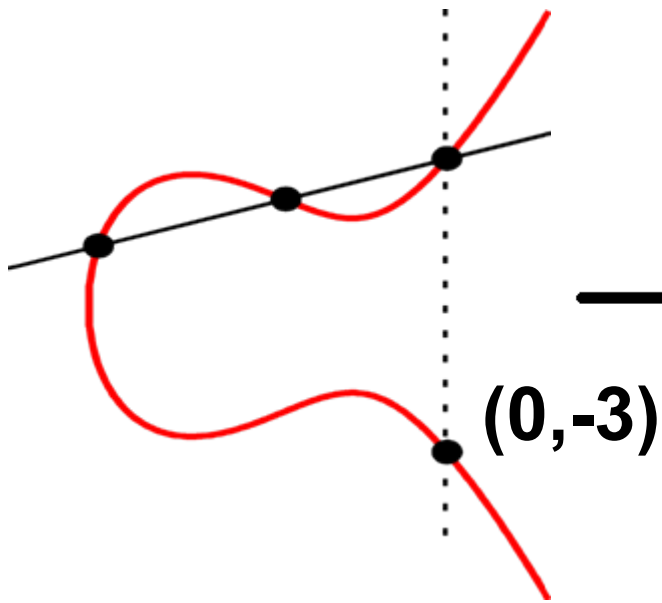
$$W_{m+n} W_{m-n} =$$

$$W_{m+1} W_{m-1} W_n^2 - W_{n+1} W_{n-1} W_m^2$$

# Part V: Reduction Mod $p$

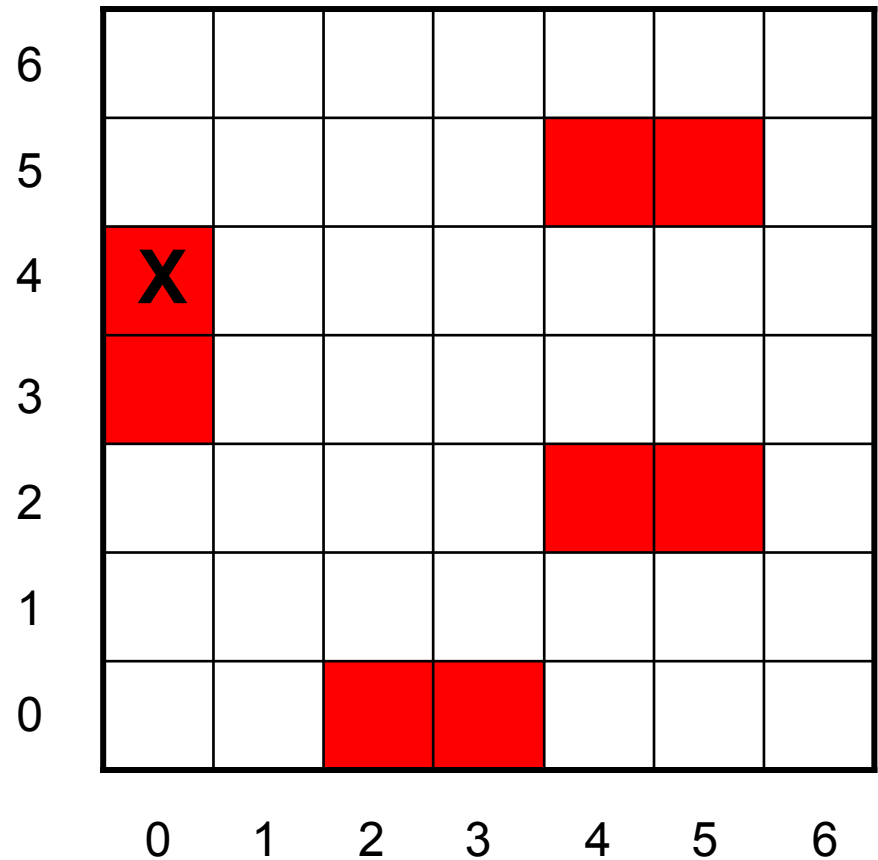
# Reduction of a curve mod $p$

$\mathbb{Q}$  points



$$y^2 = x^3 - 5x + 9$$

$\mathbb{F}_7$  points



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

# Reduction Mod $p$

0, 1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043,  
-12064147359, 632926474117, -65604679199921, -6662962874355342,  
-720710377683595651, 285131375126739646739,  
5206174703484724719135, -36042157766246923788837209,  
14146372186375322613610002376, ...

↓ modulo 11

0, 1, 1, 8, 0, 5, 7, 8, 0, 1, 9, 10, 0, 3, 7, 6, 0, 3, 1, 10, 0, 1, 10, 8,  
0, 5, 4, 8, 0, 1, 2, 10, 0, 3, 4, 6, 0, 3, 10, 10, 0, 1, 1, 8, 0, 5, 7, 8, 0, ...

period is 40

This is the elliptic divisibility  
sequence associated to the curve  
reduced modulo 11

# What do the zeroes mean??

$$\frac{1}{0} = \infty$$

$$nP = 0 \text{ in } E(\mathbb{Q}) \text{ iff } W_n = 0$$

$$n\tilde{P} = \tilde{0} \text{ in } \tilde{E}(\mathbb{F}_p) \text{ iff } W_n \equiv 0 \pmod{p}$$

( Divisibility: If  $n|m$ , then  $W_n|W_m$ . )

# Reduction Mod $p$

0, 1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043,  
-12064147359, 632926474117, -65604679199921, -6662962874355342,  
-720710377683595651, 285131375126739646739,  
5206174703484724719135, -36042157766246923788837209,  
14146372186375322613610002376, ...

↓ modulo 11

0, 1, 1, 8, 0, 5, 7, 8, 0, 1, 9, 10, 0, 3, 7, 6, 0, 3, 1, 10, 0, 1, 10, 8,  
0, 5, 4, 8, 0, 1, 2, 10, 0, 3, 4, 6, 0, 3, 10, 10, 0, 1, 1, 8, 0, 5, 7, 8, 0, ...

The point has order 4, but the sequence has period 40!

# Periodicity of Sequences

If  $W_r \equiv 0 \pmod{p}$ , then there exist  $a$  and  $b$  such that for all  $n$ ,

$$W_{n+kr} \equiv W_n a^{nk} b^{k^2} \pmod{p}$$

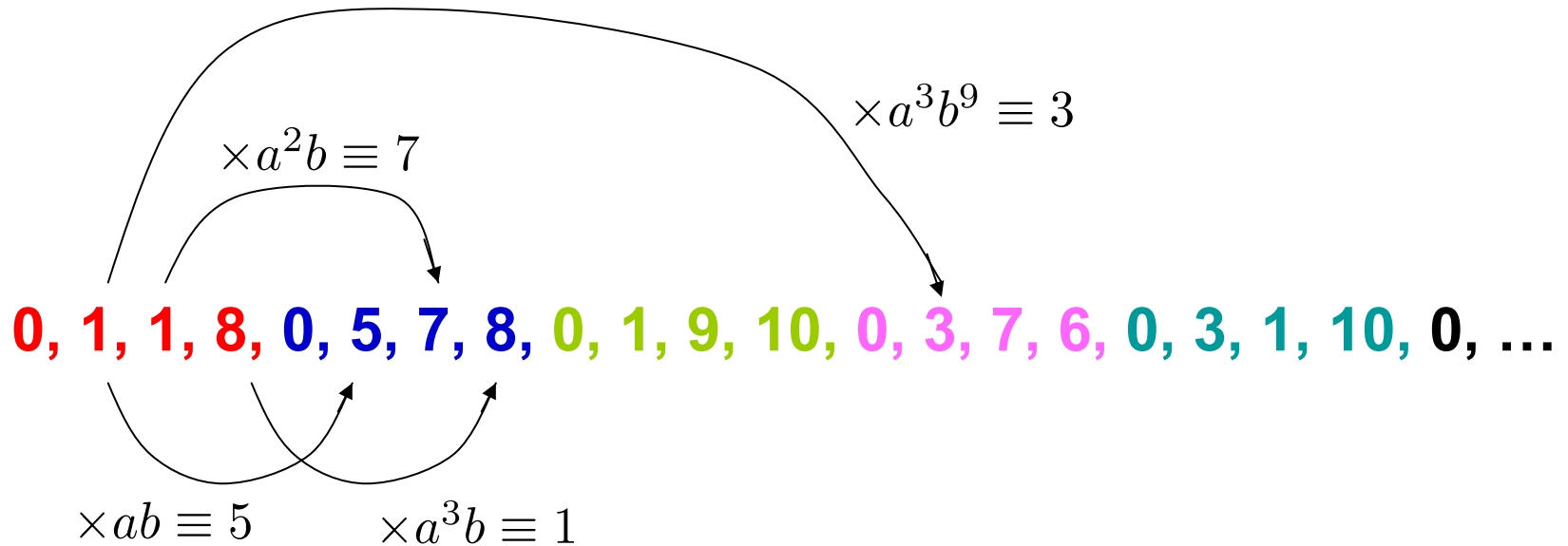
Here we may take

$$a = \frac{W_{r+2}}{W_{r+1}W_2}, \quad b = \frac{W_{r+1}^2 W_2}{W_{r+2}}$$

# Periodicity Example

$$a \equiv 7/5 \equiv 8 \pmod{11}$$

$$b \equiv 5/8 \equiv 2 \pmod{11}$$



# Research (Partial List)

- Applications to Elliptic Curve Discrete Logarithm Problem in cryptography (R. Shipsey)
- Finding integral points (M. Ayad)
- Study of nonlinear recurrence sequences (Fibonacci numbers, Lucas numbers, and integers are special cases of EDS)
- Appearance of primes (G. Everest, T. Ward, ...)
- EDS are a special case of Somos Sequences (A. van der Poorten, J. Propp, M. Somos, C. Swart, ...)
- $p$ -adic & function field cases (J. Silverman)
- Continued fractions & elliptic curve group law (W. Adams, A. van der Poorten, M. Razar)
- Sigma function perspective (A. Hone, ...)
- Hyper-elliptic curves (A. Hone, A. van der Poorten, ...)
- More...

# **Part VI: Elliptic Nets: Jacking up the Dimension**

# The Mordell-Weil Group

The rational points of an elliptic curve  $E$  form a finitely generated abelian group, called the *Mordell-Weil group*.

The elliptic divisibility sequence is associated to the multiples of  $P$ , i.e.

$$\langle P \rangle < E(\mathbb{Q})$$

(the cyclic subgroup generated by  $P$ )

# From Sequences to Nets

It is natural to look for a generalisation that reflects the structure of the entire Mordell-Weil group:

$W_P \in \mathbb{Z}$  indexed by all  $P \in E(\mathbb{Q})$  ??

## In this talk, we work with a rank 2 example

Take  $P, Q \in E(\mathbb{Q})$ . Consider the formal linear combinations of  $P$  and  $Q$ . These can be indexed by  $\mathbb{Z} \times \mathbb{Z}$ :

$$m(P) + n(Q) \rightsquigarrow W_{m,n}$$

***Nearly everything can be done for general rank***

# Elliptic Nets:

Zeros at  $(P, Q)$  such that  $mP + nQ = 0$ .  
Some crazy poles.

$$W_{m,n} \in \mathbb{Z}, \text{ for all } m, n \in \mathbb{Z}$$

## Definition A

Define doubly elliptic functions on  $E \times E$

$$\Psi_{m,n}(z, w) = \frac{\sigma(mz + nw)}{\sigma(z)^{m^2 - mn} \sigma(z + w)^{mn} \sigma(w)^{n^2 - mn}}, \quad m, n \in \mathbb{Z}$$

Fix elliptic curve  $\mathbb{C}/\Lambda$  and rational points  $z, w \in \mathbb{C}/\Lambda$

$$W_{m,n} = \Psi_{m,n}(z, w)$$

# Elliptic Nets: Rank 2 Case

$$W_{m,n} \in \mathbb{Z}, \text{ for all } m, n \in \mathbb{Z}$$

## Definition B

Give initial conditions

$$W_{0,0}, W_{1,0}, W_{0,1}, W_{1,1}, W_{1,2}, W_{1,2}, W_{0,2}, W_{0,2}$$

$$W_{0,0} = 0, W_{1,0} = W_{0,1} = W_{1,1} = 1$$

and recurrence for all  $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in \mathbb{Z} \times \mathbb{Z}$

$$\begin{aligned} W_{\mathbf{p}+\mathbf{q}+\mathbf{s}} W_{\mathbf{p}-\mathbf{q}} W_{\mathbf{r}+\mathbf{s}} W_{\mathbf{r}} \\ + W_{\mathbf{q}+\mathbf{r}+\mathbf{s}} W_{\mathbf{q}-\mathbf{r}} W_{\mathbf{p}+\mathbf{s}} W_{\mathbf{p}} \\ + W_{\mathbf{r}+\mathbf{q}+\mathbf{s}} W_{\mathbf{r}-\mathbf{p}} W_{\mathbf{q}+\mathbf{s}} W_{\mathbf{q}} = 0 \end{aligned}$$

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						

# Equivalence of Definitions

The definitions  $A$  and  $B$  can be generalised to any rank  $n$ . Then we have

**Theorem (S).** *The definitions  $A$  and  $B$  are equivalent. Furthermore, there is a bijection*

$$\begin{array}{ccc} (E, P_1, \dots, P_n) & \longleftrightarrow & (a_1, \dots, a_n) \\ \text{curve} + n \text{ points} & & n + 2 \text{ initial values of net} \end{array}$$

## For any given $n$ , one can compute the explicit bijection

Given initial values  $W_{1,0} = W_{0,1} = W_{1,1} = 1, W_{1,-1} = a,$   
 $W_{2,1} = b, W_{2,-1} = c,$  and  $W_{2,0} = d$  the associated curve is  
 $y^2 = 4x^3 - g_2x - g_3$  where

$$g_2 = \frac{1}{48d^4a^4} (a^8b^4 - 8a^7b^2d^2 + 4a^6b^3c + 4a^6b^3d^2 + 16a^6d^4 - 16a^5bcd^2 + 8a^5bd^4 + 6a^4b^2c^2 + 4a^4b^2cd^2 + 6a^4b^2d^4 - 8a^3c^2d^2 - 8a^3cd^4 + 16a^3d^6 + 4a^2bc^3 - 4a^2bc^2d^2 - 4a^2bcd^4 + 4a^2bd^6 + c^4 - 4c^3d^2 + 6c^2d^4 - 4cd^6 + d^8)$$

$$g_3 = \frac{1}{864d^6a^6} (-a^{12}b^6 + 12a^{11}b^4d^2 - 6a^{10}b^5c - 6a^{10}b^5d^2 - 48a^{10}b^2d^4 + 48a^9b^3cd^2 + 12a^9b^3d^4 + 64a^9d^6 - 15a^8b^4c^2 - 18a^8b^4cd^2 - 15a^8b^4d^4 - 96a^8bcd^4 + 48a^8bd^6 + 72a^7b^2c^2d^2 + 12a^7b^2cd^4 - 36a^7b^2d^6 - 20a^6b^3c^3 - 12a^6b^3c^2d^2 - 12a^6b^3cd^4 - 20a^6b^3d^6 - 48a^6c^2d^4 - 48a^6cd^6 - 120a^6d^8 + 48a^5bc^3d^2 - 12a^5bc^2d^4 + 24a^5bcd^6 - 60a^5bd^8 - 15a^4b^2c^4 + 12a^4b^2c^3d^2 + 6a^4b^2c^2d^4 + 12a^4b^2cd^6 - 15a^4b^2d^8 + 12a^3c^4d^2 - 12a^3c^3d^4 - 36a^3c^2d^6 + 60a^3cd^8 - 24a^3d^{10} - 6a^2bc^5 + 18a^2bc^4d^2 - 12a^2bc^3d^4 - 12a^2bc^2d^6 + 18a^2bcd^8 - 6a^2bd^{10} + -c^6 + 6c^5d^2 - 15c^4d^4 + 20c^3d^6 - 15c^2d^8 + 6cd^{10} - d^{12})$$

# Nets are Integral

**Theorem (S).** *Suppose  $1 \leq n \leq 6$ . Given integral initial terms satisfying a certain finite set of divisibility conditions, the values of a net are all integers.*

(e.g. for  $n = 1$ , the conditions are  $W_2|W_4$ .)

# Reduction Mod $p$

$$1 \leq n \leq 6$$

$\Psi_{\mathbf{v}}$  with  $\mathbf{v} \in \mathbb{Z}^n$

$E$  an elliptic curve over  $\mathbb{Q}$

$p$  prime of good reduction for  $E$

$\delta$  reduction modulo  $p$

**Theorem (S).** *There exists a unique  $f_{\mathbf{v}}$  such that the following diagram commutes and  $\text{div}(f_{\mathbf{v}}) = \delta^*(\text{div}(\Psi_{\mathbf{v}}))$ .*

$$\begin{array}{ccc} E^n(\mathbb{Q}) & \xrightarrow{\Psi_{\mathbf{v}}} & \mathbb{P}^1(\mathbb{Q}) \\ \delta \downarrow & & \downarrow \delta \\ E^n(\mathbb{F}_p) & \xrightarrow{f_{\mathbf{v}}} & \mathbb{P}^1(\mathbb{F}_p) \end{array}$$

# Divisibility Property

**Theorem (S).** *Suppose  $p$  is a prime of good reduction for  $E$ . Then*

$$\{\mathbf{v} \in \mathbb{Z}^n : p \text{ divides } W_{\mathbf{v}}\}$$

*is a sub-lattice of  $\mathbb{Z}^n$ .*

$$n \leq 6$$

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

$P = (0, 0), Q = (1, 0)$

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
↑ Q	0	1	1	-3	11	38	249
	P→						



# Periodicity of Sequences: Restatement

Let  $W$  be an elliptic net and  $K$  a finite field.

If  $W_r = 0$ , there exists an  $\alpha \in \bar{K}$  such that  $\alpha^r \in K$  and  $\alpha^{n^2} W_n$  has period  $r$ .

$$(a = \alpha^{2r} \text{ and } b = \alpha^{r^2})$$

# Periodicity of Nets

**Theorem (S).** *Suppose*

$$W(\mathbf{r}_1) = W(\mathbf{r}_2) = 0.$$

*Let  $d$  be the gcd of the coordinates of the  $\mathbf{r}_i$ . Then there exists an  $\alpha \in \bar{K}$  such that  $\alpha^d \in K$  and*

$$\alpha^{m^2+n^2-mn} W(m, n)$$

*is periodic with respect to the lattice generated by  $\mathbf{r}_1, \mathbf{r}_2$ .*

$$n \leq 6$$

# **Part VII: Elliptic Curve Cryptography**

# Elliptic Curve Cryptography

**For cryptography you need something that is  
*easy to do but difficult to undo.***

Like multiplying vs. factoring.

Or getting pregnant.

*(No one has realised any cryptographic protocols based on this:  
Possible thesis topic anyone?)*

# The (Elliptic Curve) Discrete Log Problem

Let  $A$  be a group and let  $P$  and  $Q$  be known elements of  $A$ .

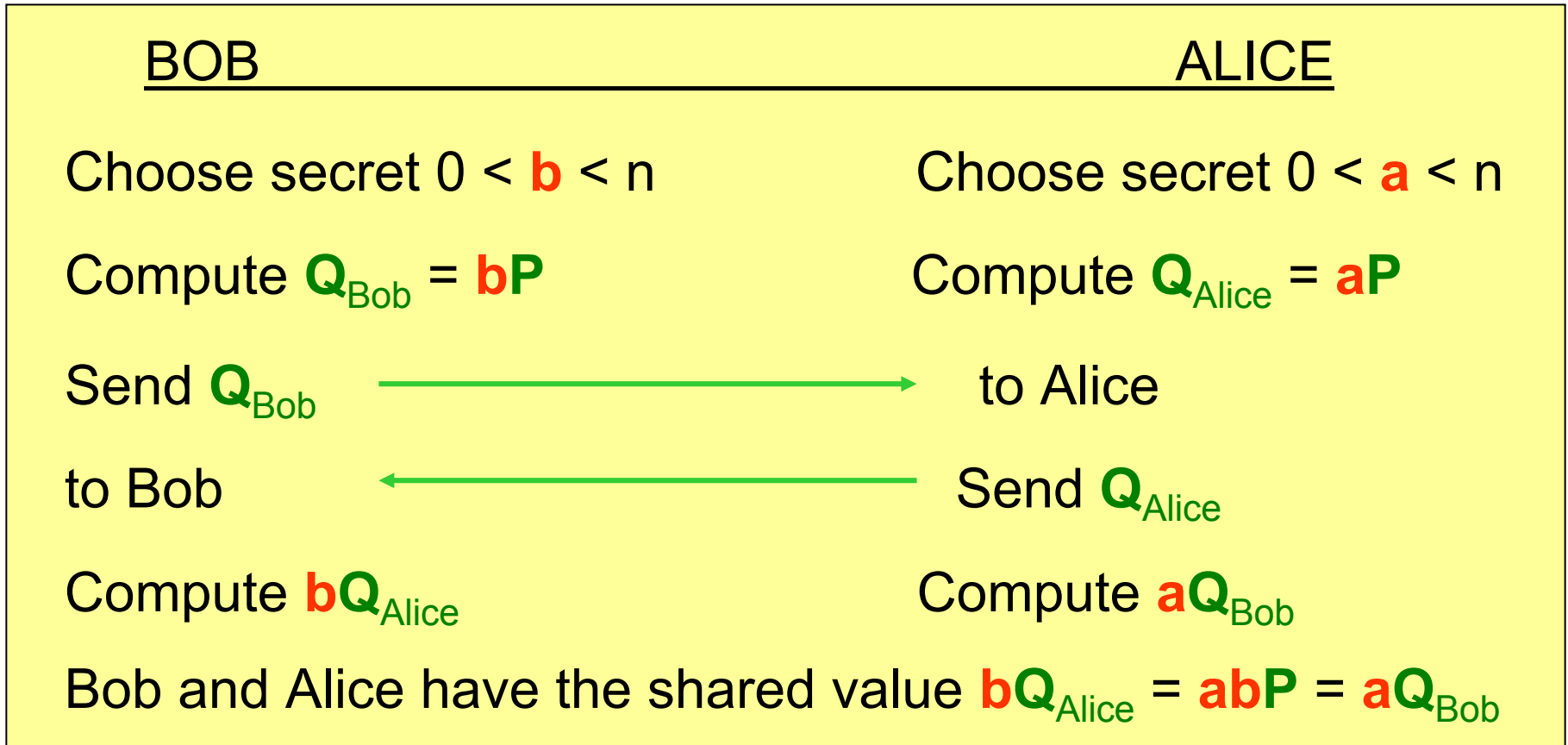
The Discrete Logarithm Problem (DLP) is to find an integer  $m$  satisfying

$$Q = \overbrace{P + P + \dots + P}^{m \text{ summands}} = mP.$$

- Hard but not too hard in  $F_p^*$ .
- Koblitz and Miller (1985) independently suggested using the group  $E(F_p)$  of points modulo  $p$  on an elliptic curve.
- It seems pretty hard there.

# Elliptic Curve Diffie-Hellman Key Exchange

Public Knowledge: A group  $E(\mathbb{F}_p)$  and a point  $P$  of order  $n$ .



Presumably(?) recovering  $abP$  from  $aP$  and  $bP$  requires solving the elliptic curve discrete logarithm problem.

*Yeah, I stole this one too.*

# The Tate Pairing

$$m \in \mathbb{Z}^+$$

$E$  an elliptic curve over field  $K \supset \mu_m$

$$P \in E(K)[m]$$

$$Q \in E(K)/mE(K)$$

$f_P$  such that  $\text{div}(f_P) = m(P) - m(\mathcal{O})$

$D_Q \sim (Q) - (\mathcal{O})$  with disjoint support from  $\text{div}(f_P)$

$$\tau_m : E(K)[m] \times E(K)/mE(K) \rightarrow K^* / (K^*)^m$$

$$\tau_m(P, Q) = f_P(D_Q)$$

This is a **bilinear** nondegenerate pairing.

# Tate Pairing in Cryptography: Tripartite Diffie-Hellman Key Exchange

Public Knowledge: A group  $E(\mathbb{F}_p)$  and a point  $P$  of order  $n$ .

	ALICE	BOB	CHANTAL
Secret	$0 < a < n$	$0 < b < n$	$0 < c < n$
Compute	$Q_{\text{Alice}} = aP$	$Q_{\text{Bob}} = bP$	$Q_{\text{Chantal}} = cP$
Reveal	$Q_{\text{Alice}}$	$Q_{\text{Bob}}$	$Q_{\text{Chantal}}$
Compute	$T_n(Q_{\text{Bob}}, Q_{\text{Chantal}})^a$	$T_n(Q_{\text{Alice}}, Q_{\text{Chantal}})^b$	$T_n(Q_{\text{Alice}}, Q_{\text{Bob}})^c$

*These three values are equal to  $T_n(P, P)^{abc}$*

Security (presumably?) relies on Discrete Log Problem in  $F_p^*$

# **Part VIII: Elliptic Nets and the Tate Pairing**

# Tate Pairing from Elliptic Nets

$m$	$\in \mathbb{Z}^+$
$E$	elliptic curve / $K$
$P$	$\in E(K)[m]$
$Q$	$\in E(K)/mE(K)$
$S$	$\in E(K) \setminus \{\mathcal{O}, -Q\}$

$W$  an elliptic net such that

$$\begin{aligned} W(\mathbf{s}) &\longleftrightarrow S \\ W(\mathbf{p}) &\longleftrightarrow P \\ W(\mathbf{q}) &\longleftrightarrow Q \end{aligned}$$

**Theorem (S).** *The Tate pairing may be calculated by*

$$\tau_m(P, Q) = \frac{W(\mathbf{s} + m\mathbf{p} + \mathbf{q})W(\mathbf{s})}{W(\mathbf{s} + m\mathbf{p})W(\mathbf{s} + \mathbf{q})}$$

# Choosing

This is just the value of  $a$  from the periodicity relation

$$W_{n+kr} \equiv W_n a^{nk} b^{k^2} \pmod{p}$$

If  $W$  is the elliptic net associated to  $E$ ,  $P$ ,  $Q$ , then

$$\tau_m(P, P) = \frac{W(m+2)W(1)}{W(m+1)W(2)}$$

If  $W$  is the elliptic net associated to  $E$ ,  $P$ ,  $Q$ , then

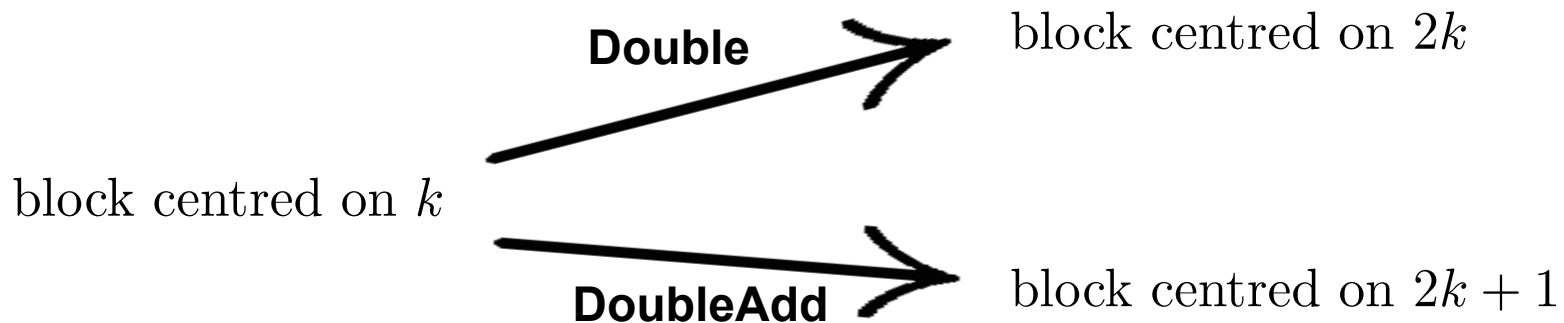
$$\tau_m(P, Q) = \frac{W(m+1, 1)W(1, 0)}{W(m+1, 0)W(1, 1)}$$

# Calculating the Net (Rank 2)

Based on an algorithm by Rachel Shipsey

A block centred on  $k$ :

		$(k-1,1)$	$(k,1)$	$(k+1,1)$			
$(k-3,0)$	$(k-2,0)$	$(k-1,0)$	$(k,0)$	$(k+1,0)$	$(k+2,0)$	$(k+3,0)$	$(k+4,0)$



# Calculating the Tate Pairing

- Find the initial values of the net associated to  $E, P, Q$  (there are simple formulae)
- Use a Double & Add algorithm to calculate the block centred on  $m$
- Use the terms in this block to calculate

$$\tau_m(P, Q) = \frac{W(m+1, 1)W(1, 0)}{W(m+1, 0)W(1, 1)}$$

# Embedding Degree $k$

$$\begin{array}{l} \mathbb{F}_{q^k} \\ \left| \right. \\ \mathbb{F}_q \end{array} \quad \begin{array}{l} m \mid (q^k - 1) \\ \\ P \in E(\mathbb{F}_q)[m] \\ Q \in E(\mathbb{F}_{q^k}) / mE(\mathbb{F}_{q^k}) \end{array}$$

# Efficiency

$S$     squaring in  $\mathbb{F}_q$   
 $M$     multiplication in  $\mathbb{F}_q$   
 $S_k$     squaring in  $\mathbb{F}_{q^k}$   
 $M_k$     multiplication in  $\mathbb{F}_{q^k}$

Algorithm	Double	DoubleAdd
Miller's	$4S + (k + 7)M + S_k + M_k$	$7S + (2k + 19)M + S_k + 2M_k$
Net	$6S + (6k + 26)M + S_k + \frac{3}{2}M_k$	$6S + (6k + 26)M + S_k + 2M_k$

Comparison of Operations for Double and DoubleAdd steps

Embedding degree	2	4	6	8	10	12
Optimised Miller's	18-38	31-58	46-82	64-109	84-140	106-174
Elliptic Net	51-52	76-80	104-112	136-147	171-186	207-228

Approximate  $\mathbb{F}_q$  Multiplications per Step

# Possible Research Directions

- Extend this to Jacobians of higher genus curves?
- Use periodicity relations to find integer points? (M. Ayad does this for sequences)
- Other computational applications: counting points on elliptic curves over finite fields?
- Other cryptographic applications of Tate pairing relationship?

# References

- Morgan Ward. “Memoir on Elliptic Divisibility Sequences”. *American Journal of Mathematics*, 70:13-74, 1948.
- Christine S. Swart. *Elliptic Curves and Related Sequences*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.
- Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*. *Mathematical Surveys and Monographs*, vol 104. American Mathematical Society, 2003.
- Elliptic net algorithm for Tate pairing implemented in the PBC Library, <http://crypto.stanford.edu/pbc/>

**Slides, preprint, scripts at**  
<http://www.math.brown.edu/~stange/>