Elliptic Nets
How To Catch an Elliptic Curve

Katherine Stange

USC Women in Math Seminar
November 7, 2007

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

Part I: Elliptic Curves are Groups

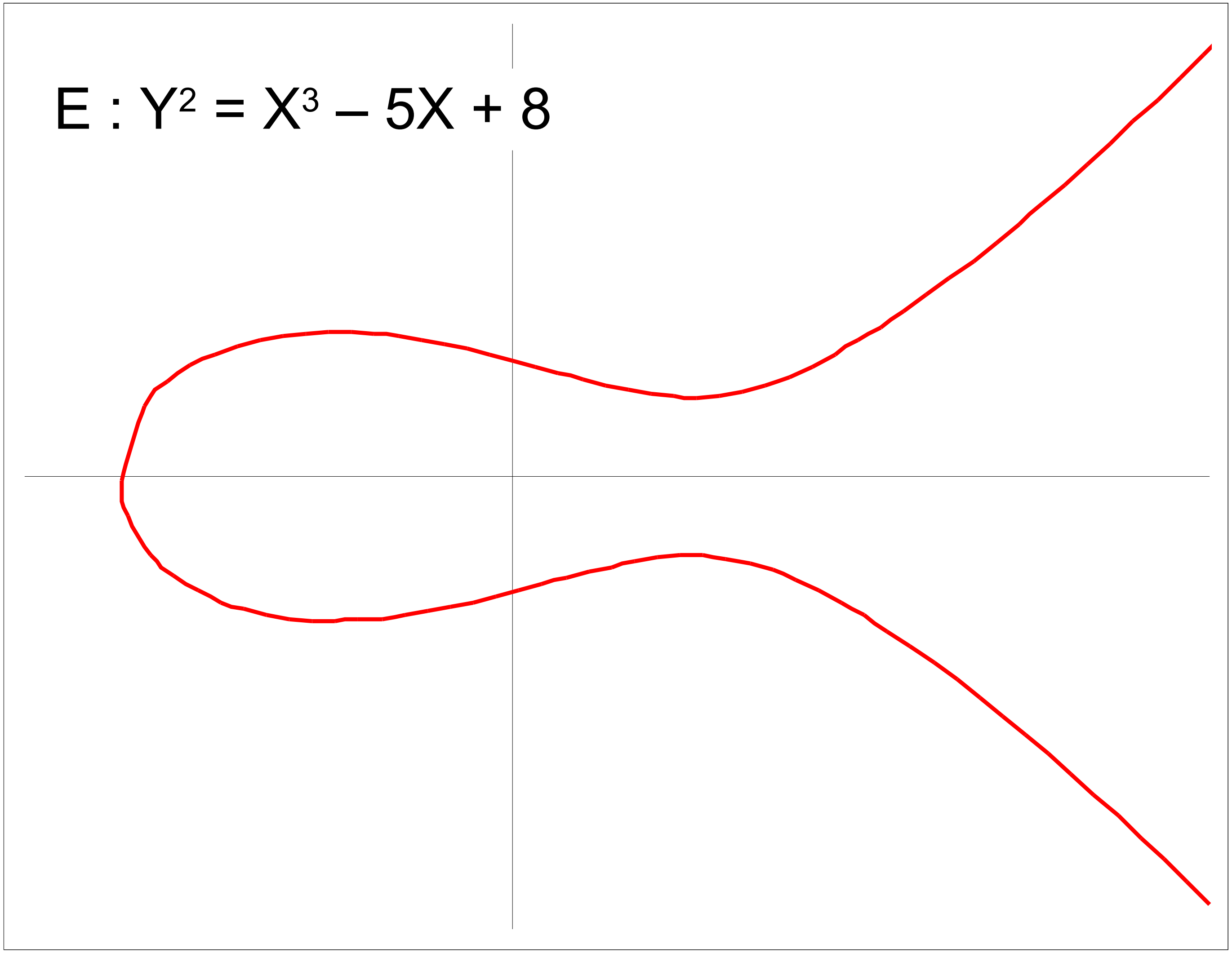
Elliptic Curves

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

Frequently, we may use the simpler equation,

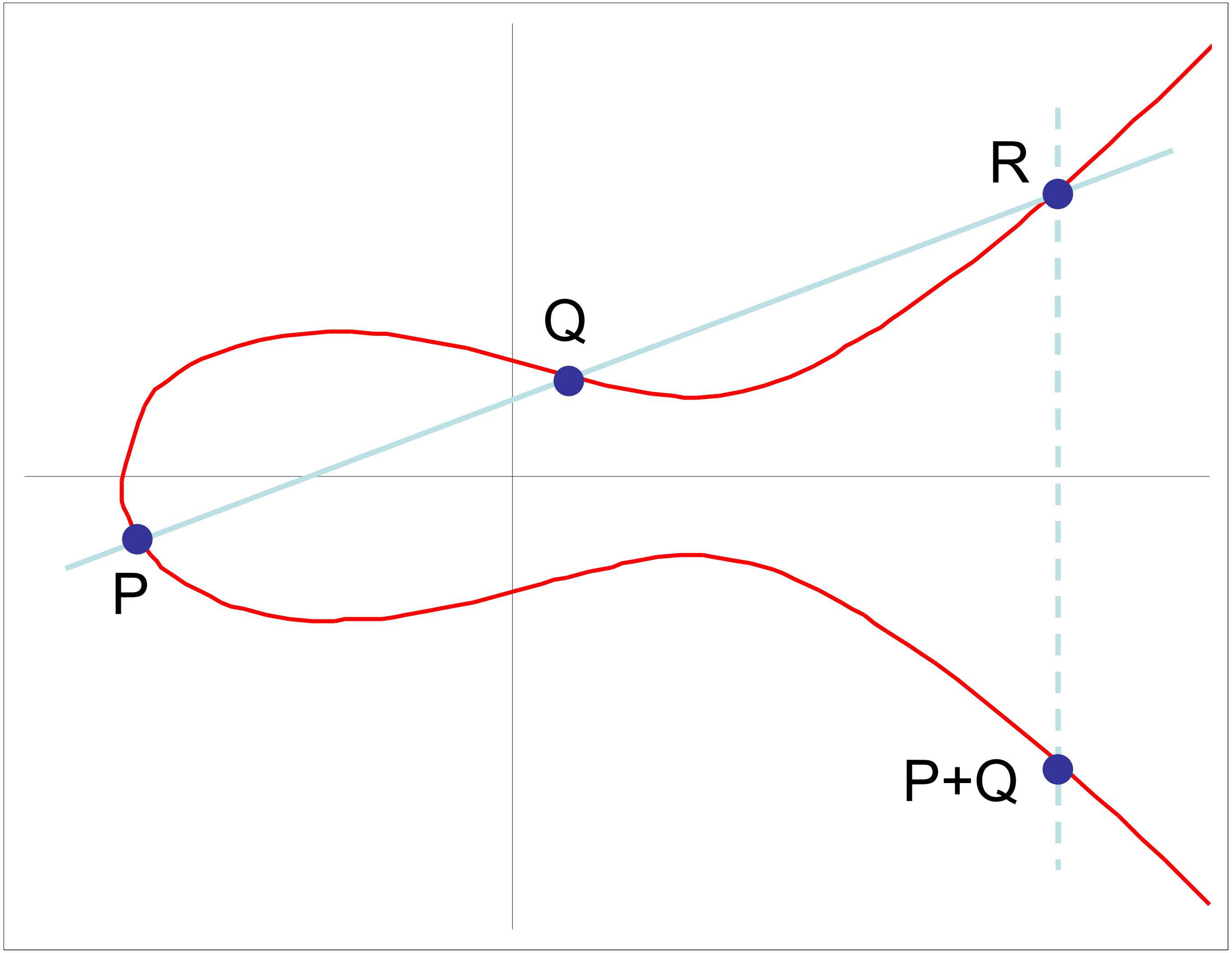
$$y^2 = x^3 + Ax + B$$

A Typical Elliptic Curve E



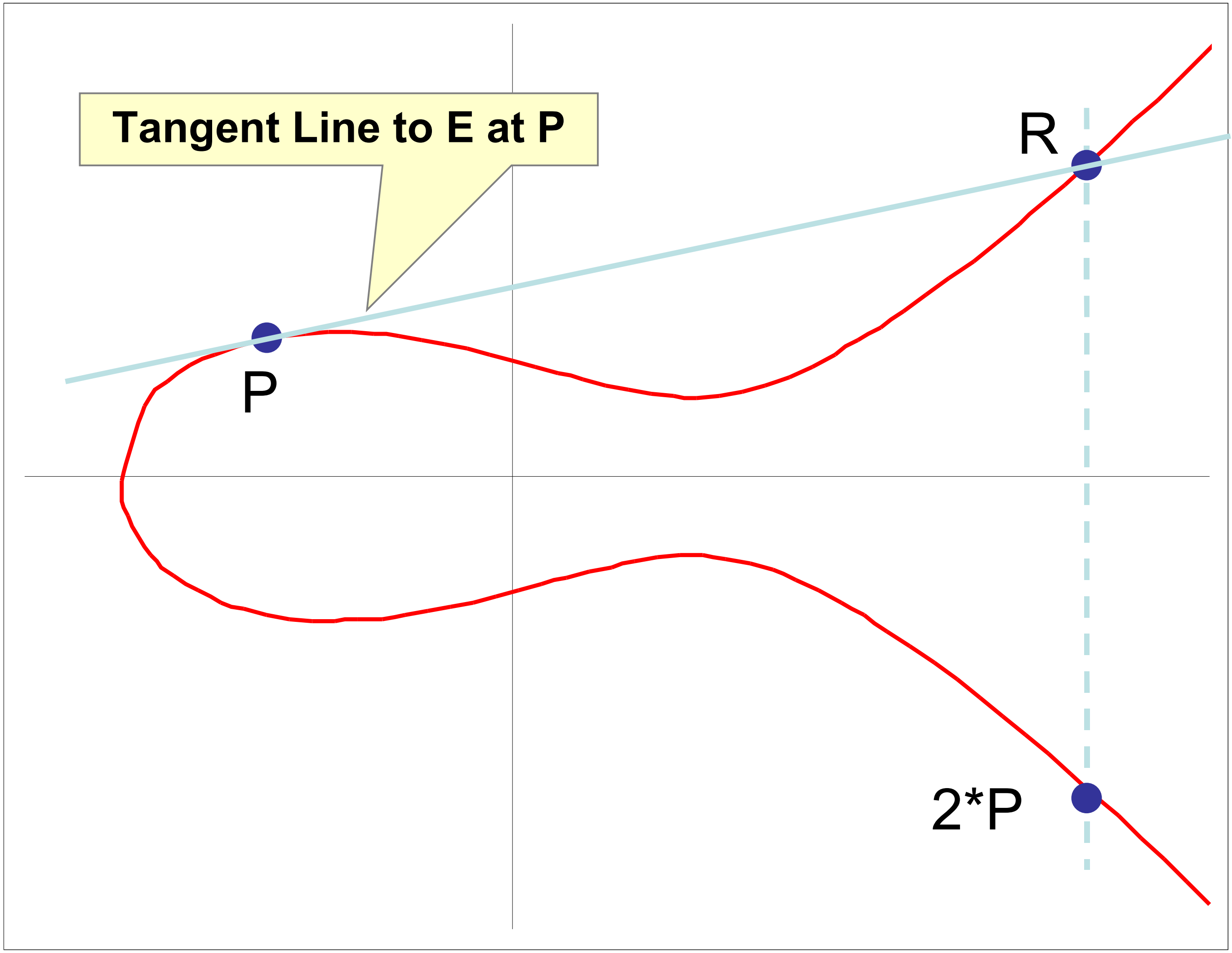
The lack of shame involved in the theft of this slide from Joe Silverman's website should make any graduate student proud.

Adding Points P + Q on E



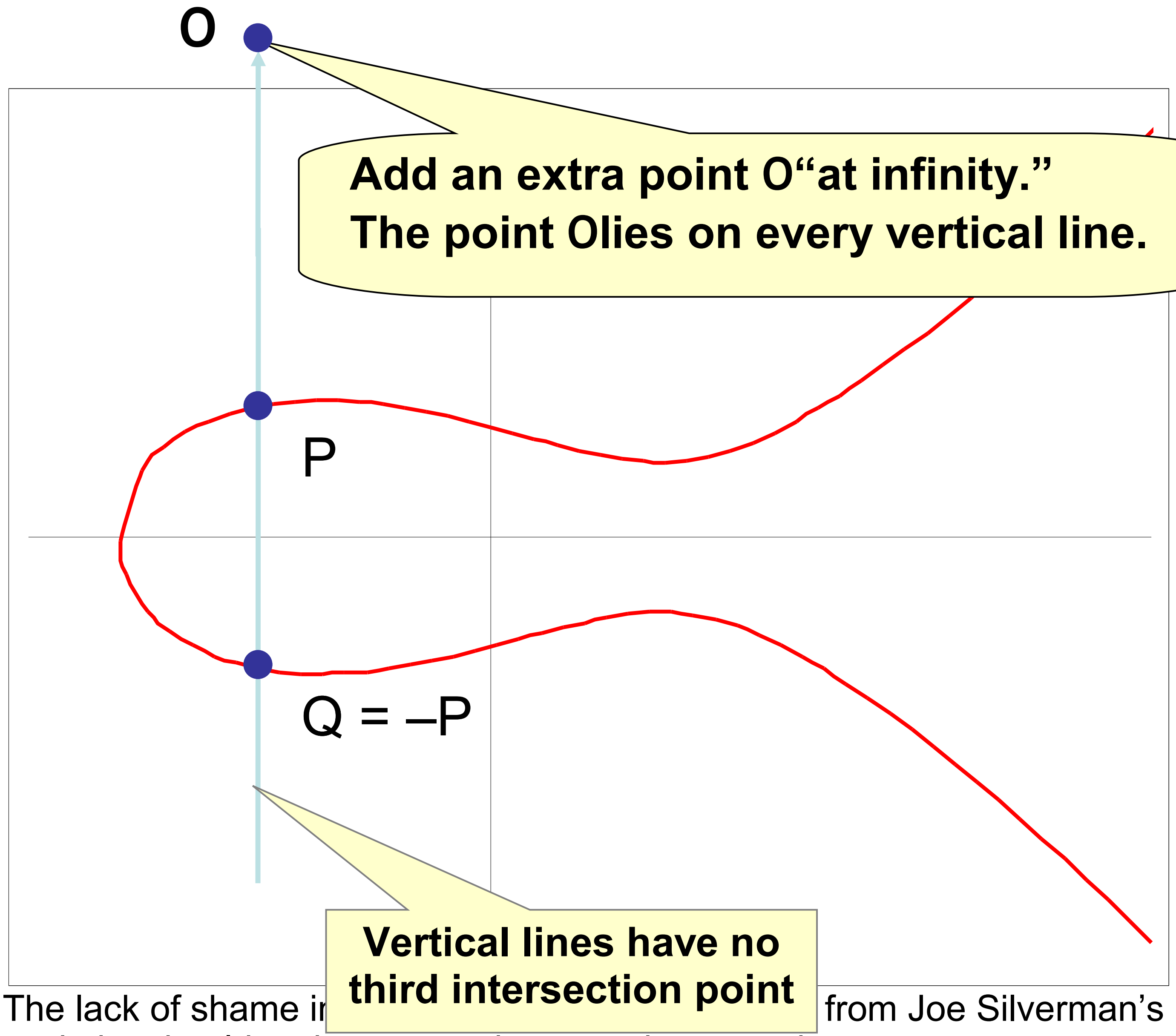
The lack of shame involved in the theft of this slide from Joe Silverman's website should make any graduate student proud.

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 i… from Joe Silverman’s website should make any graduate student proud.

Elliptic Curve Group Law

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

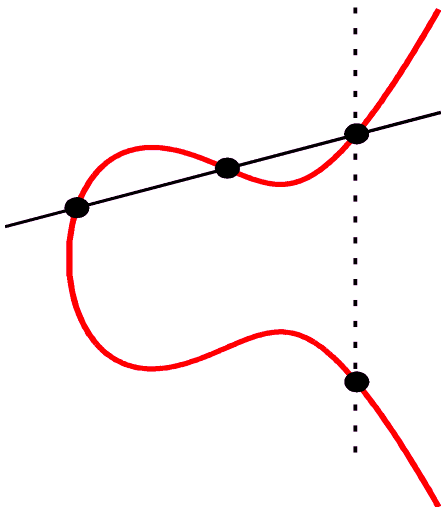
$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2), \qquad P_3 = (x_3, y_3) = P_1 + P_2$$

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = -\lambda x_3 - \nu.$$

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

Part II: Elliptic Divisibility Sequences

Elliptic Divisibility Sequences: Seen In Their Natural Habitat



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

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

$$\begin{array}{cccccc} P, & [2]P, & [3]P, & [4]P, & \ldots & \in E(\mathbb{Q}) \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \\ d_P, & d_{2P}, & d_{3P}, & d_{4P}, & \ldots & \in \mathbb{Z} \end{array}$$

Example: $y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$

$$
\begin{aligned}
P &= (0,0) \\
[2]P &= (3,5) \\
[3]P &= \left(-\frac{11}{3^2}, \frac{28}{3^3}\right) \\
[4]P &= \left(\frac{114}{11^2}, -\frac{267}{11^3}\right) \\
[5]P &= \left(-\frac{2739}{38^2}, -\frac{77033}{38^3}\right) \\
[6]P &= \left(\frac{89566}{249^2}, -\frac{31944320}{249^3}\right) \\
[7]P &= \left(-\frac{2182983}{2357^2}, -\frac{20464084173}{2357^3}\right)
\end{aligned}
$$

$$1, 1, -3, 11, 38, 249, -2357, \ldots$$

Division Polynomials

If $P = (x, y)$

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

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

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

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

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

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

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

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

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

Curves give Sequences

For a fixed elliptic curve E and point $P \in E(\mathbb{Q})$, the sequence

$$\boldsymbol{\Psi_n(P)}$$

forms an elliptic divisibility sequence.

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

1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, 17711, 46368, 121393, 317811, 832040, 2178309, 5702887, 14930352, 39088169, 102334155, 267914296, 701408733, 1836311903, 4807526976, 12586269025, 32951280099, 86267571272, 225851433717, 591286729879, 1548008755920, ...

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, 28513137512673964673 9, 5206174703484724719135, -360421577662469237888372 09, 1414637218637532261361000237 6, …

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,
152506207465652277762531462142393791012856442441235840714430103762819736595413,
-5286491728223134626400431117234262142530209508718504849234889569684083125892420201,
-835397059891704991632636814121353141297683871830623235928141040342038068512341019315446,
10861789122218115292139551508417628820932571356531654998704845795890033629344542872385904645,
13351876087649817486050732736119541016235802111163925747732171131926421411306436158323451057508131,
2042977307842020707295863142858393936350596442010700266977612272386600979584155605002856821221263113151,
-666758599738582427580962194986025574476589178060749335314959464037321543378395210027048006648288905711378993,
333167086588478561672098259752122036440335441580932677237086129099851559108618156882215307126455938552908231344016,
150866730291138374331025045659005244449458695650548930543174261374298387455590141700233602162964721944201442274446853073,
113760065777234882865006940654654895718896520042025048306493515052149363166271410666963494813413836495437803419621982027412929,
-159253169967307321375677555136314569434529937177007635953107117202675658212866813320738037987472039386883798439657624623140677934307,
44416310167318880256461428190965193979854149844320579714027500283754273952989380044808517851663079825097686172334231751637837837673262107, ...

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

Part III: Division Polynomials

Division Polynomials

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

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

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

- The n^{th} division polynomial has as zeroes the n^2 n-torsion points
- Therefore a sequence associated to a point of order n has $W_{nk} = 0$ for all integers k.

Division Polynomials

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

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

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

- These are polynomials in *x*,*y*,*A*,*B*
- Integer coefficients
- So by a change of coordinates $x \longrightarrow u^2x$, $y \longrightarrow u^3y$ (which implies $A \longrightarrow u^4A$, $B \longrightarrow u^6B$), we can obtain an integer sequence.

Curve – Sequence Correspondence

Theorem (Morgan Ward, 1948)

The following sets are in bijection.

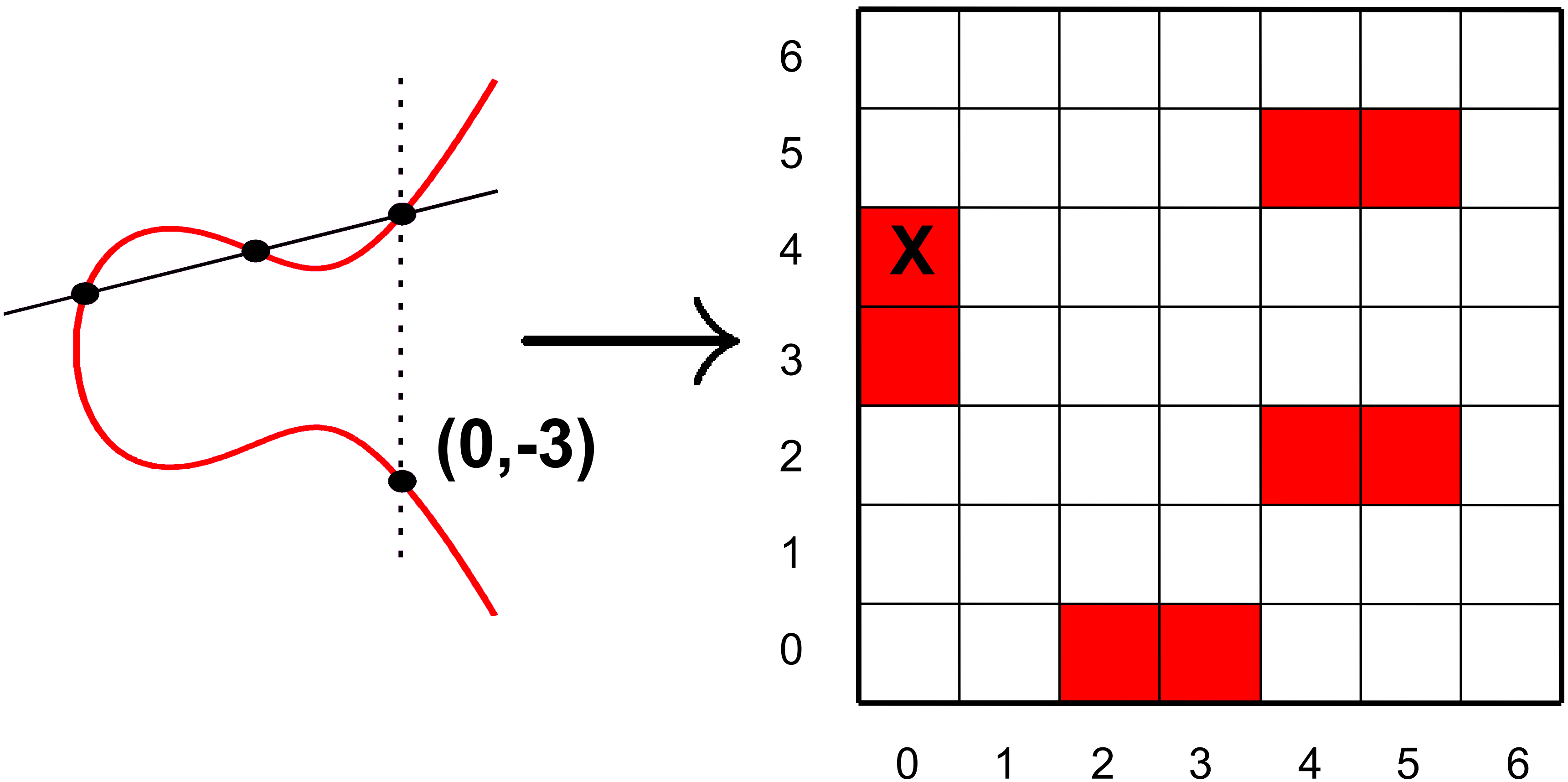
E an elliptic curve + *P* a point on *E* $P, [2]P, [3]P \neq 0$	⟷	W_n an elliptic divisibility sequence $W_1 = 1\ W_2 W_3 \neq 0$

(The bijection is given by explicit formulae.)

Part IV: Reduction Mod p

Reduction of a curve mod *p*

$\mathbb{Q}$ points $\qquad\qquad$ $\mathbb{F}_7$ points



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

Reduction Mod p

0, 1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043, -12064147359, 632926474117, -65604679199921, -6662962874355342, -720710377683595651, 285131375126739646739, 5206174703484724719135, -360421577662469237888837209, 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

Zeroes of the Sequence

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

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

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

(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, 52061747034847724719135, -3604215766246923788837209, 1414637218637532261361002376, …

$$\Big\downarrow \text{ modulo } 11$$

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!

The sequence is *not* a function of the point *[n]P*.

Periodicity of Sequences

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

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

Here we may take

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

Due to Morgan Ward.

Periodicity Example

$a \equiv 7/5 \equiv 8 \mod 11$ $b \equiv 5/8 \equiv 2 \mod 11$

$\times a^3 b^9 \equiv 3$

$\times a^2 b \equiv 7$

0, 1, 1, 8, 0, 5, 7, 8, 0, 1, 9, 10, 0, 3, 7, 6, 0, 3, 1, 10, 0, …

$\times ab \equiv 5$ $\times a^3 b \equiv 1$

$$W_{n+kr} = W_n a^{nk} b^{k^2}$$

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 V: 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

Suppose we take the denominators of linear combinations $[n]P + [m]Q$ of two (or n) points.

Does this array of numbers $W_{n,m}$ satisfy a recurrence relation and have properties similar to those we've seen for elliptic divisibility sequences?

(Question asked by Elkies in 2001)

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; \; P = (0,0), \; Q = (1,0)$$

○ $[3]Q$	○ $[1]P + [3]Q$	○ $[2]P + [3]Q$
○ $[2]Q$	○ $[1]P + [2]Q$	○ $[2]P + [2]Q$
○ $[1]Q$	○ $[1]P + [1]Q$	○ $[2]P + [1]Q$
○ ∞	○ $[1]P$	○ $[2]P$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

$\left(\frac{56}{25}, \frac{371}{125}\right)$	$\left(-\frac{95}{64}, \frac{495}{512}\right)$	$\left(\frac{328}{361}, -\frac{2800}{6859}\right)$
$\left(\frac{6}{1}, -\frac{16}{1}\right)$	$\left(\frac{1}{9}, -\frac{19}{27}\right)$	$\left(\frac{39}{1}, \frac{246}{1}\right)$
$\left(\frac{1}{1}, \frac{0}{1}\right)$	$\left(-\frac{2}{1}, -\frac{1}{1}\right)$	$\left(\frac{5}{4}, -\frac{13}{8}\right)$
∞	$\left(\frac{0}{1}, \frac{0}{1}\right)$	$\left(\frac{3}{1}, \frac{5}{1}\right)$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

- $\left(\frac{56}{5^2}, \frac{371}{5^3}\right)$
- $\left(-\frac{95}{8^2}, \frac{495}{8^3}\right)$
- $\left(\frac{328}{19^2}, -\frac{2800}{19^3}\right)$
- $\left(\frac{6}{1^2}, -\frac{16}{1^3}\right)$
- $\left(\frac{1}{3^2}, -\frac{19}{3^3}\right)$
- $\left(\frac{39}{1^2}, \frac{246}{1^3}\right)$
- $\left(\frac{1}{1^2}, \frac{0}{1^3}\right)$
- $\left(-\frac{2}{1^2}, -\frac{1}{1^3}\right)$
- $\left(\frac{5}{2^2}, -\frac{13}{2^3}\right)$
- ∞
- $\left(\frac{0}{1^2}, \frac{0}{1^3}\right)$
- $\left(\frac{3}{1^2}, \frac{5}{1^3}\right)$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x;\ P = (0,0),\ Q = (1,0)$$

∘ 5	∘ 8	∘ 19
∘ 1	∘ 3	∘ 1
∘ 1	∘ 1	∘ 2
∘ 0	∘ 1	∘ 1

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x;\ P = (0,0),\ Q = (1,0)$$

-5	$+8$	-19
$+1$	$+3$	-1
$+1$	$+1$	$+2$
$+0$	$+1$	$+1$

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
0	1	1	-3	11	38	249

↑ Q

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
0	1	1	-3	11	38	249

Q ↑

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
0	1	1	-3	11	38	249

Q ↑

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
0	1	1	-3	11	38	249

Q ↑

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⟶

Generalising Division Polynomials

$\psi_{n,m}(P,Q)$ should...

- be defined on $E x E$
- be zero exactly when $[n]P + [m]Q = 0$ on the curve
- be the denominator of $[n]P + [m]Q$ up to sign.
- be the usual division polynomials when $(n,m) = (n,0)$ or $(0,m)$

Net Polynomials

$$\Psi_{-1,1} = x_1 - x_2 \ ,$$

$$\Psi_{2,1} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ ,$$

$$\Psi_{2,-1} = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ ,$$

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \ ,$$

$$\begin{aligned}\Psi_{3,1} &= (x_2 - x_1)^{-3}(4x_1^6 - 12x_2x_1^5 + 9x_2^2x_1^4 + 4x_2^3x_1^3 \\ &- 4y_2^2x_1^3 + 8y_1^2x_1^3 - 6x_2^4x_1^2 + 6y_2^2x_2x_1^2 - 18y_1^2x_2x_1^2 \\ &+ 12y_1^2x_2^2x_1 + x_2^6 - 2y_2^2x_2^3 - 2y_1^2x_2^3 + y_2^4 - 6y_1^2y_2^2 \\ &+ 8y_1^3y_2 - 3y_1^4) \ .\end{aligned}$$

Elliptic Nets

Define an elliptic net to be any function

$$W: \mathbf{Z}^n \rightarrow \mathbf{Q}$$

satisfying

$$W_{p+q+s} W_{p-q} W_{r+s} W_{r} + W_{q+r+s} W_{q-r} W_{p+s} W_{p} + W_{r+q+s} W_{r-p} W_{q+s} W_{q} = 0$$

for $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s}$ in $\boldsymbol{Z}^n$.

Curve – Net Correspondence

Theorem (S)

The following sets are in bijection.

E an elliptic curve

+

P, Q points on E

$P, Q, P+Q, P-Q \neq 0$

$\longleftrightarrow$

$W_{n,m}$ an elliptic net

$W_{1,0} = W_{0,1} = W_{1,1} = 1,$
$W_{1,-1} \neq 0$

(The bijection is given by explicit formulae. Works for higher rank as well.)

Part VI: Nets Mod 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
0	1	1	-3	11	38	249

Q ↑

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
0	1	1	-3	11	38	249

Q ↑

P ⟶

Divisibility Property

Consider nets that take integer values. (By a change of coordinates, we can always obtain such a net.)

If *W* is associated to a curve *E*...

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

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

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

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

$P = (0,0),\ Q = (1,0)$ $\mod 5$

	0	4	1	3	1	2	4
	4	4	4	4	1	3	0
	4	3	2	0	3	2	1
	0	3	1	4	4	4	4
	1	3	4	2	4	1	0
	1	1	2	0	2	4	1
Q ↑	0	1	1	2	1	3	4
	P ⟶						

Example of Reduction Mod 5 of an Elliptic Net

1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$\uparrow Q$

$P \longrightarrow$

Periodicity in two dimensions

Theorem (S)

Suppose $\mathbf{r} = (r_1 , r_2)$ such that $[r_1]P + [r_2]Q = 0$.
Then there are $a_{\mathbf{r}}$, $b_{\mathbf{r}}$, $c_{\mathbf{r}}$ such that for all
$\mathbf{s} = (s_1 , s_2)$,

$$\frac{W(\mathbf{r}+\mathbf{s})}{W(\mathbf{s})} = a_{\mathbf{r}}^{s_1} b_{\mathbf{r}}^{s_2} c_{\mathbf{r}}$$

Example of Reduction Mod 5 of an Elliptic Net

1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$\uparrow Q$

$P \rightarrow$

$$\mathbf{r} = (3,1), \qquad a_r = 2, b_r = 2, c_r = 1$$

$$W(4,3) \equiv W(1,2)2^1 2^2 1^1 \equiv 3W(1,2) \mod 5$$

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
↑	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\mathbf{r} = (9,0), \qquad a_r = 4, b_r = 3, c_r = 2$$

$$W(11,3) \equiv W(2,3)4^2 3^3 2^1 \equiv 4W(2,3) \mod 5$$

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

$$Q = \underbrace{P + P + \cdots + P}_{m \text{ summands}} = mP.$$

- Hard but not too hard in $\mathbb{F}_p^*$.
- 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 $\mathbf{E}(\mathbb{F}_p)$ and a point $\mathbf{P}$ of order n.

BOB		ALICE
Choose secret $0 < b < n$		Choose secret $0 < a < n$
Compute $Q_{Bob} = bP$		Compute $Q_{Alice} = aP$
Send Q_{Bob}	→	to Alice
to Bob	←	Send Q_{Alice}
Compute bQ_{Alice}		Compute aQ_{Bob}

Bob and Alice have the shared value $bQ_{Alice} = abP = aQ_{Bob}$

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

Yeah, I stole this one too.

The Tate Pairing

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

$$\tau_m(P, Q) = \frac{f_P(Q+S)}{f_P(S)}$$

- f_P is the function with a pole of order m at 0 and a zero of order m at P
- independent of S

This is a bilinear pairing:

$$\tau_m(P_1 + P_2, Q) = \tau_m(P_1, Q)\tau_m(P_2, Q)$$

$$\tau_m(P, Q_1 + Q_2) = \tau_m(P, Q_1)\tau_m(P, Q_2)$$

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	$Q_{Alice} = aP$	$Q_{Bob} = bP$	$Q_{Chantal} = cP$
Reveal	Q_{Alice}	Q_{Bob}	$Q_{Chantal}$
Compute	$\tau_n(Q_{Bob}, Q_{Chantal})^a$	$\tau_n(Q_{Alice}, Q_{Chantal})^b$	$\tau_n(Q_{Alice}, Q_{Bob})^c$

These three values are equal to $\boldsymbol{\tau_n(P,P)^{abc}}$

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

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

If W is the elliptic net associated to E, P, 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

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

Example of Reduction Mod 5 of an Elliptic Net

	1	4	2	0	2	1	1	4	1	4	4	3	0	3	1	4	4	4	4	1
	0	4	1	3	1	2	4	2	2	0	3	3	1	3	4	2	4	1	0	4
	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2	4	1	1
	4	3	2	0	3	2	1	2	4	3	4	4	0	1	1	2	1	3	4	3
	0	3	1	4	4	4	4	1	3	0	3	4	4	1	4	1	1	2	0	2
	1	3	4	2	4	1	0	4	1	3	1	2	4	2	2	0	3	3	1	3
$\uparrow$	1	1	2	0	2	4	1	1	1	1	4	2	0	2	1	1	4	1	4	4
Q	0	1	1	2	1	3	4	3	2	0	3	2	1	2	4	3	4	4	0	1

$P \rightarrow$

$$\tau_m(P, Q) = \frac{W(m+1,1)W(1,0)}{W(m+1,0)W(1,1)} = \left(\frac{4}{3}\right)\left(\frac{1}{1}\right) = 3$$

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)

block centred on k $\xrightarrow{\textbf{Double}}$ block centred on $2k$

block centred on k $\xrightarrow{\textbf{DoubleAdd}}$ block centred on $2k + 1$

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

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

Calculating the Tate Pairing

- About 100-200% of the time taken by the other known algorithm due to Victor Miller (which has been extensively optimised).
- May be more efficient in certain special cases.

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.

Slides, preprint, scripts at

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