The Arithmetic of Curves

Katherine E. Stange
Stanford University

Boise REU, June 13th, 2011

Remember those rabbits?

$$L_n = L_{n-1} + L_{n-2}$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

More generally, for any p and q we get a Lucas sequence

$$L_n = pL_{n-1} + qL_{n-2}, \quad L_1 = 1, \quad L_2 = p$$

Example ($p = 3$, $q = -1$)

The Evenacci numbers (every second Fibonacci).

$$1, 3, 8, 21, 55, 144, 377, 987, 2584, \ldots$$

The equation $x^2 - px - q = 0$ has two roots, $\alpha, \overline{\alpha}$. If we write

$$L_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}$$

we can check (just by algebra) that

$$L_n = pL_{n-1} + qL_{n-2}, \quad L_1 = 1, \quad L_2 = p$$

Example

Fibonaccis: the roots of $x^2 - x - 1 = 0$ are

$$\alpha, \overline{\alpha} = \frac{1 \pm \sqrt{5}}{2}$$

Evenaccis: the roots of $x^2 - 3x + 1 = 0$ are

$$\alpha, \overline{\alpha} = \frac{3 \pm \sqrt{5}}{2}$$

These numbers live in the number field $\mathbb{Q}(\sqrt{d})$ (e.g. $d = 5$). They look like

$$\alpha = a + b\sqrt{d}$$

They have a norm

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

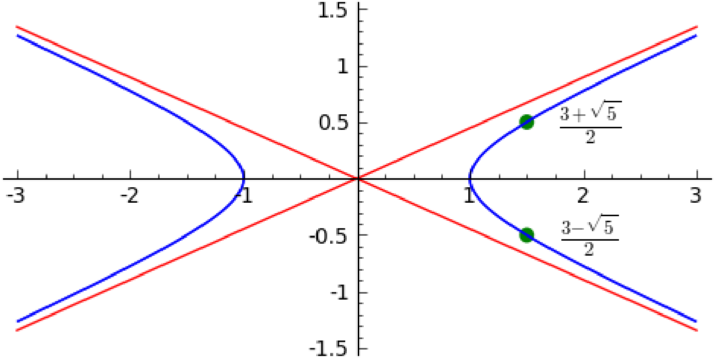
Amazingly (just check the algebra!):

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

The norm is multiplicative. Note that $N(\alpha)$ is the constant coefficient of $x^2 - px - q$, i.e. $N(\alpha) = -q$.

Forget sequences for a minute; let's consider the hyperbola

$$x^2 - 5y^2 = 1$$



The rational points (x, y) on the curve are exactly norm 1 elements

$$x^2 - dy^2 = 1 \quad \text{is} \quad \{(x, y) : N(x + y\sqrt{d}) = 1\}$$

The set

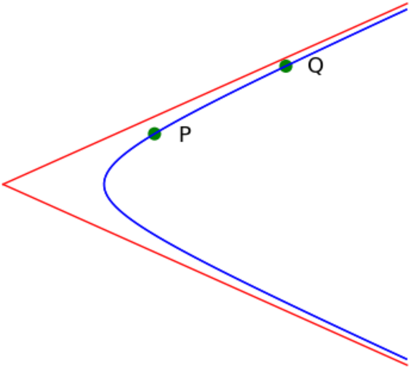
$$\{(x, y) : N(x + y\sqrt{d}) = 1\}$$

is a group, i.e. it has an operation (multiplication) – two points can be combined to get another in this same set.

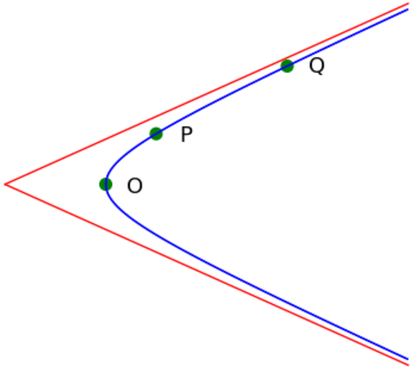
Group axioms

- there's an identity: $1 \times P = P \times 1 = P$ for any P.
- there are inverses: for each P, there's a Q so $P \times Q = 1$.
- it's associative: $(P_1 \times P_2) \times P_3 = P_1 \times (P_2 \times P_3)$.

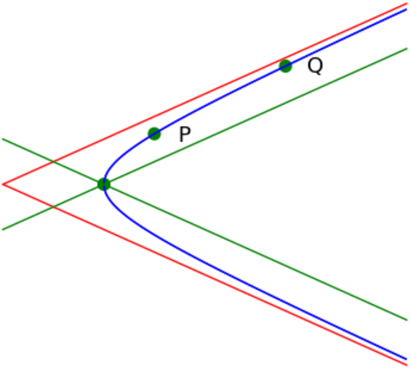
This means $x^2 - dy^2 = 1$ should be a group!



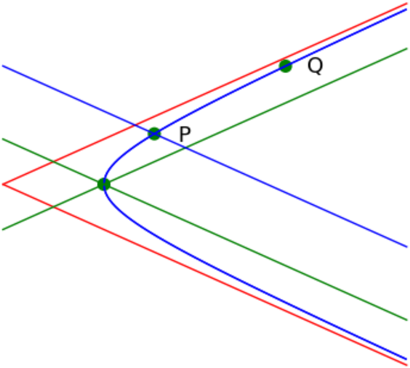
This means $x^2 - dy^2 = 1$ should be a group!



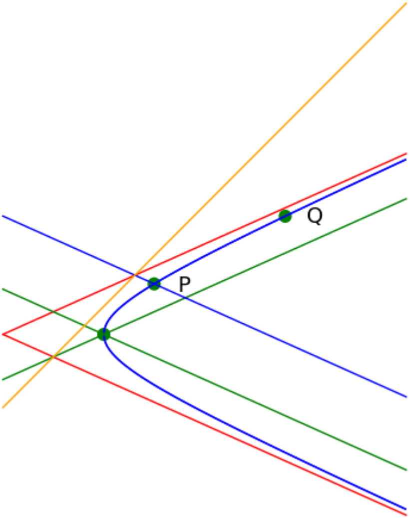
This means $x^2 - dy^2 = 1$ should be a group!



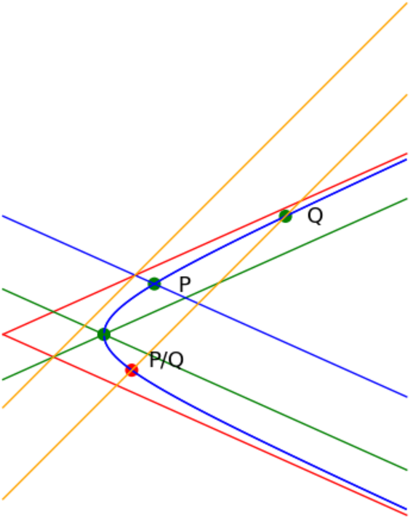
This means $x^2 - dy^2 = 1$ should be a group!



This means $x^2 - dy^2 = 1$ should be a group!



This means $x^2 - dy^2 = 1$ should be a group!



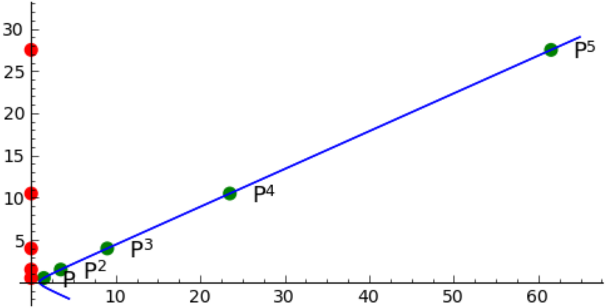
The projection of (x, y) to x-axis:

$$x = \frac{\left((x + y\sqrt{d}) + (x - y\sqrt{d})\right)}{2} = \frac{(\alpha + \overline{\alpha})}{2}$$

The projection of (x, y) to y-axis:

$$y = \frac{\left((x + y\sqrt{d}) - (x - y\sqrt{d})\right)}{2\sqrt{d}} = \frac{(\alpha - \overline{\alpha})}{2\sqrt{d}}$$

$$P, \quad P^2, \quad P^3, \quad P^4, \quad P^5, \quad \ldots$$

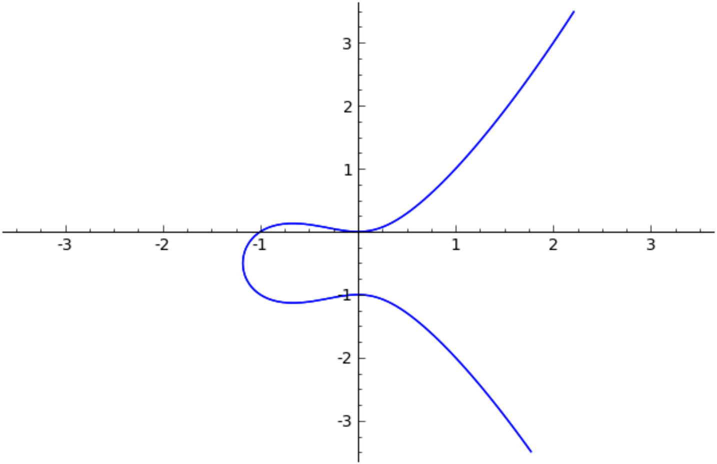


$$P = \left(\frac{3}{2}, \frac{1}{2}\right),$$
$$P^2 = \left(\frac{7}{2}, \frac{3}{2}\right),$$
$$P^3 = \left(\frac{18}{2}, \frac{8}{2}\right),$$
$$P^4 = \left(\frac{47}{2}, \frac{21}{2}\right),$$
$$P^5 = \left(\frac{123}{2}, \frac{55}{2}\right).$$

$$y(\alpha^n) = \frac{(\alpha^n - \overline{\alpha}^n)}{2\sqrt{d}}, \quad L_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} = \frac{y(\alpha^n)}{y(\alpha)}$$

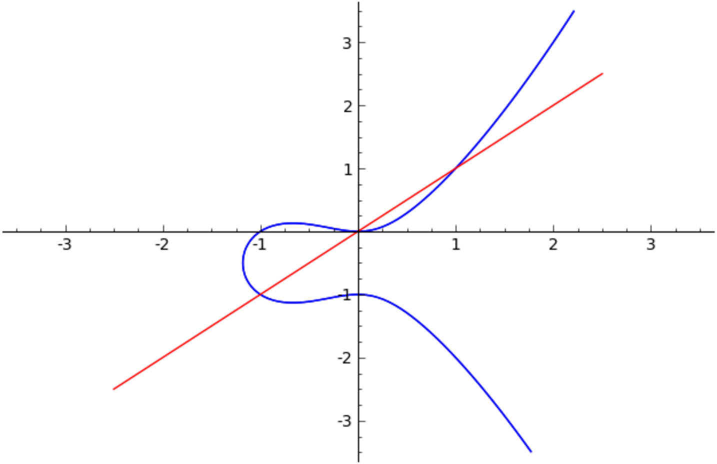
Consider instead a cubic curve

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

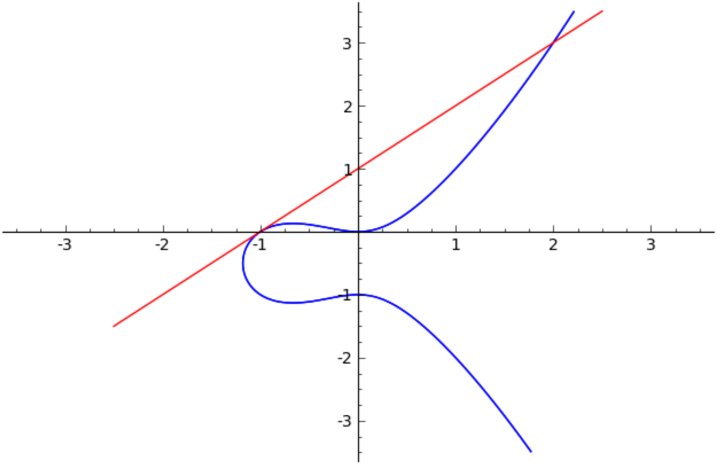


Because it is cubic, if you intersect E with any line $Rx + Sy = T$, you get exactly 3 solutions:

$$\left(\frac{T - Rx}{S}\right)^2 + \left(\frac{T - Rx}{S}\right) = x^3 + x^2$$



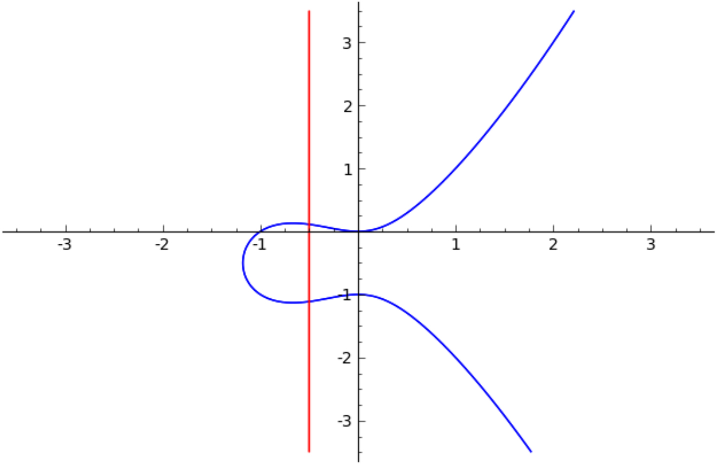
Occasionally, this cubic will have a double root, but that's okay, we just count that one twice.



Well, actually, if $S = 0$ you have to do it this way:

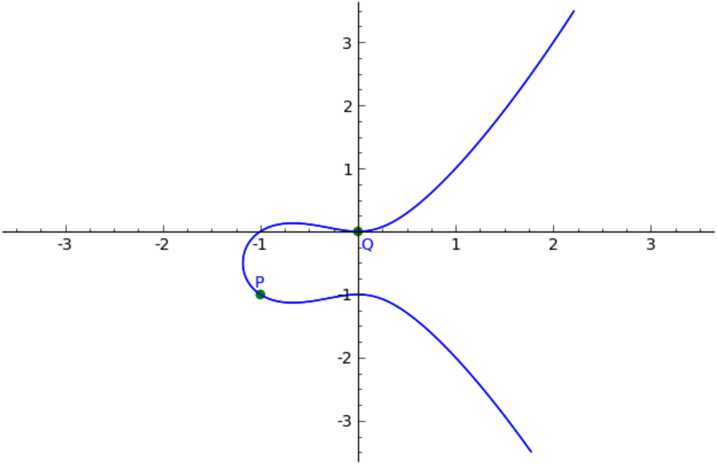
$$y^2 + y = (T/R)^3 + (T/R)^2$$

and it looks like 2 solutions.

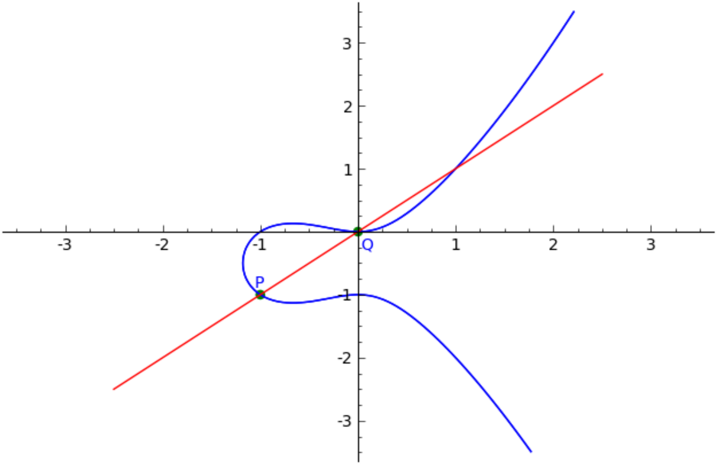


But in this case we imagine an extra "point at infinity", ∞. Any vertical line goes through two points on the curve and ∞.

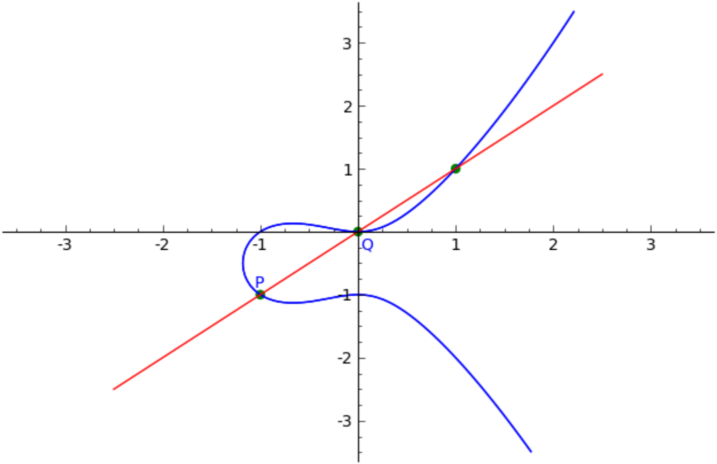
So if we start with two points on the curve...



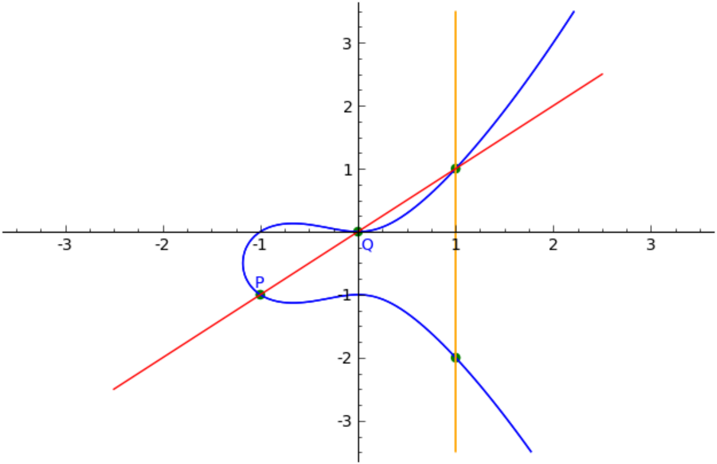
So if we start with two points on the curve, and draw a line through them…



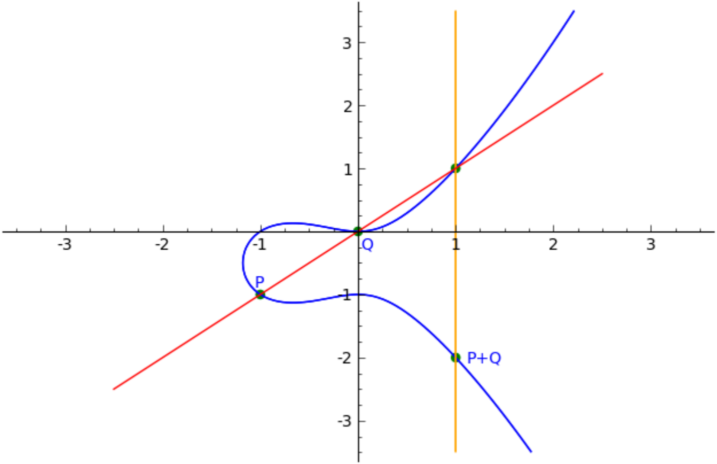
So if we start with two points on the curve, and draw a line through them to get another point...



This is almost a group law. To make it work (all the axioms) we actually have to add a reflection at the end:



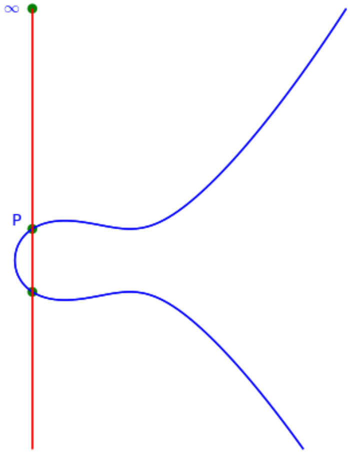
Group Law



And that's how we get $P + Q$.

Identity

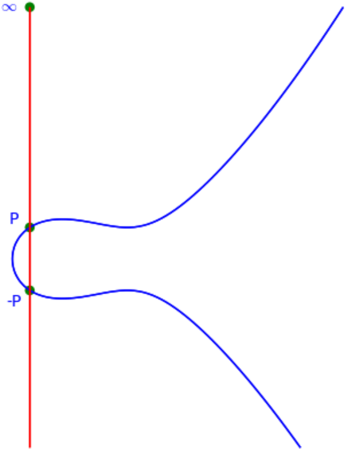
Identity: ∞



A line through P and ∞ is vertical: the other intersection is the reflection through x-axis.

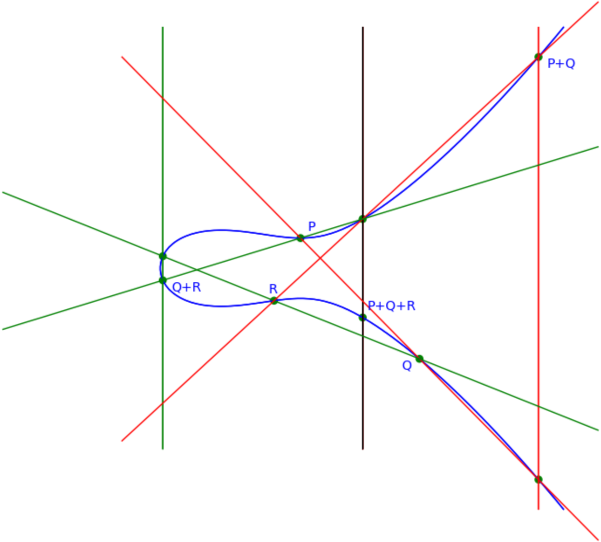
Inverses

Inverses: A vertical line.



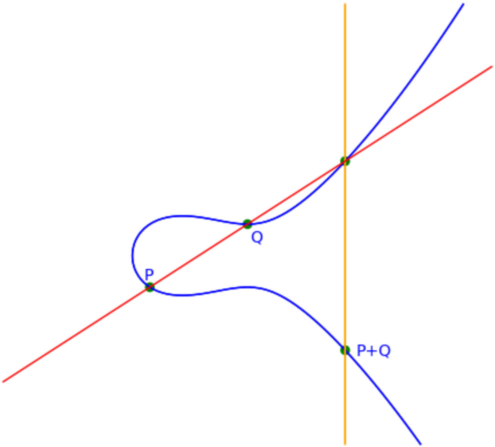
Two points which add to ∞.

Associativity



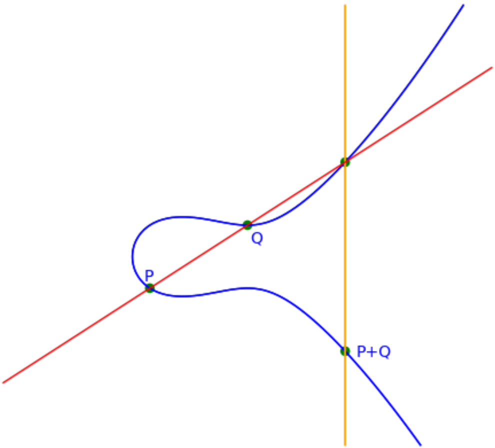
Hard to check, but true!

The points of $y^2 + y = x^3 + x^2$ form a group!



This works for any $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

$E(\mathbb{Q})$ - the Mordell-Weil group of rational points of E



$E(\mathbb{Q})$ - the Mordell-Weil group of rational points of E

Theorem (Mordell, 1922)

$E(\mathbb{Q})$ is finitely generated and abelian, i.e. $P+Q=Q+P$.

An abelian group looks like

$$\mathbb{Z}^r \times \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

r - rank
$\mathbb{Z}^r$ - free part
$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ - torsion part

Theorem (Mazur, 1977)

The torsion part of the Mordell-Weil group is one of:

$$\mathbb{Z}/N\mathbb{Z}, 1 \leq N \leq 10, N = 12 \quad \textit{or} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, 1 \leq N \leq 4.$$

Genus - Number of holes

- topologically a sphere - no holes:
  - e.g. hyperbola
  - infinitely many rational points
- topologically a doughnut - one hole:
  - e.g. elliptic curve
  - finitely many or infinitely many rational points
- topologically many holes:
  - finitely many rational points

Possible Ranks?

Rank $\geq$	Year	Discoverer(s)
3	1945	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer & Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen
28	2008	Elkies

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342$$

$$P1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$$

$$P2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$$

$$P3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$$

$$P4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531]$$

$$P5 = [1534706764467120723885477337, 85429585346017694289021032862781072799531]$$

$$P6 = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]$$

$$P7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931]$$

$$P8 = [1494385729327188957541833817, 88486605527733405986116494514049233411451]$$

$$P9 = [1868438228620887358509065257, 59237403214437708712725140393059358589131]$$

$$P10 = [2008945108825743774866542537, 47690677880125552882151750781541424711531]$$

$$P11 = [2348360540918025169651632937, 17492930006200557857340332476448804363531]$$

$$P12 = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]$$

$$P13 = [2924128607708061213363288937, 28350264431488878501488356474767375899531]$$

$$P14 = [5374993891066061893293934537, 286188908427263386451175031916479893731531]$$

$$P15 = [1709690768233354523334008557, 71898834974686089466159700529215980921631]$$

$$P16 = [2450954011353593144072595187, 4445228173532634357049262550610714736531]$$

$$P17 = [2969254709273559167464674937, 32766893075366270801333682543160469687531]$$

$$P18 = [2711914934941692601332882937, 2068436612778381698650413981506590613531]$$

$$P19 = [20078586077996854528778328937, 277960854113780660465605172562462403009153]$$

$$P20 = [2158082450240734774317810697, 34994373401964026809969662241800901254731]$$

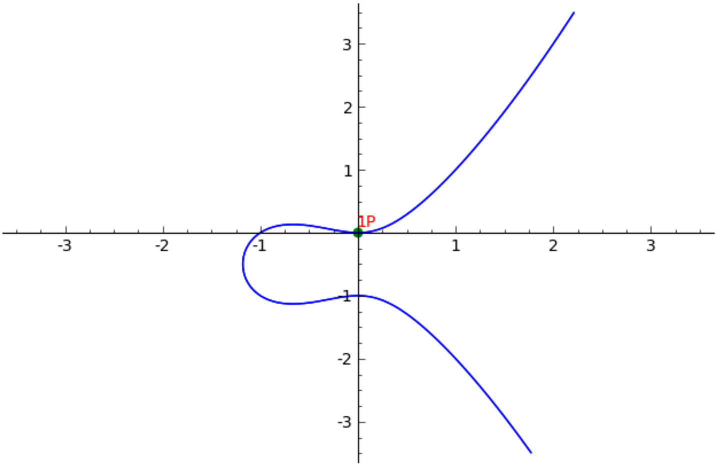
$$P21 = [2004645458247059022403224937, 48049329780704645522439866999888475467531]$$

$$P22 = [2975749450947996264947091337, 33398989826075322320208934410104857869131]$$

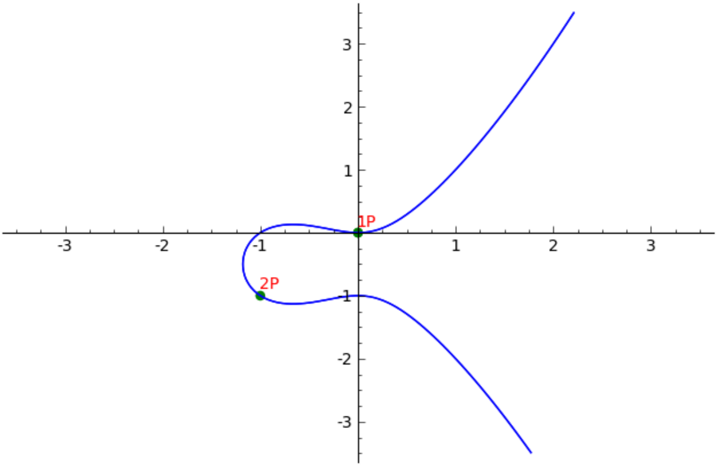
$$P23 = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]$$

$$P24 = [3115831799150630349021945377, 16810438522998060354010947291566015347393]$$

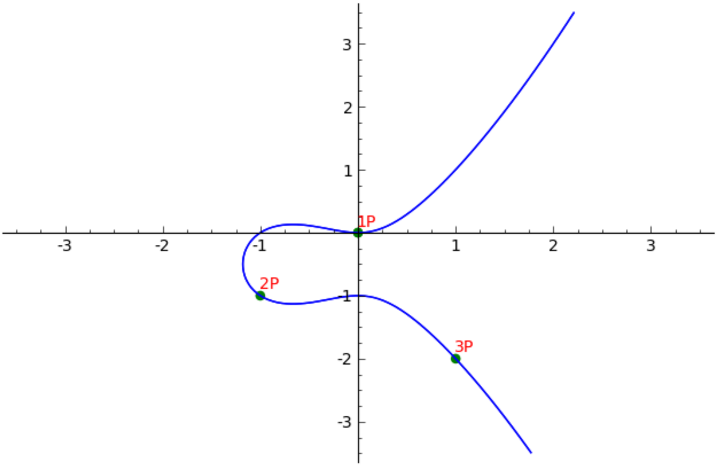
$$y^2 + y = x^3 + x^2, \quad P = (0,0)$$



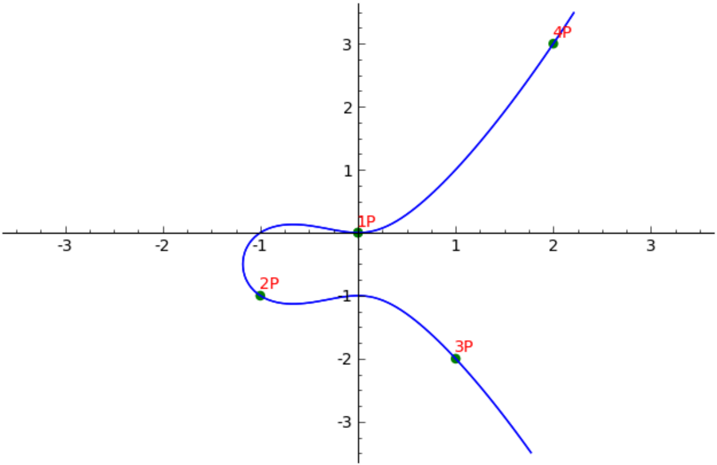
$$y^2 + y = x^3 + x^2, \quad P = (0, 0)$$



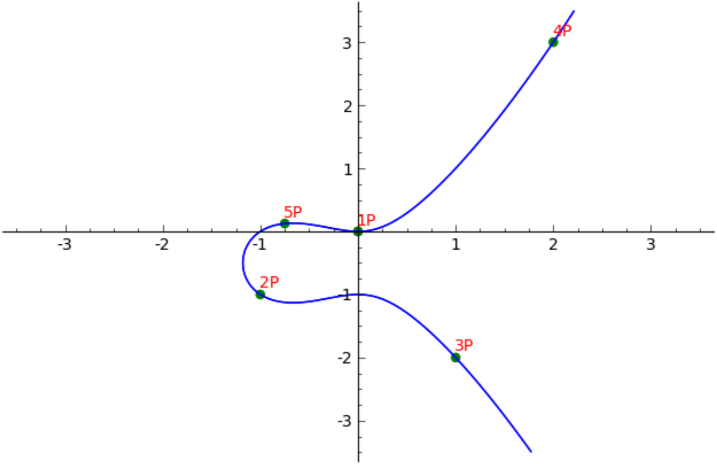
$$y^2 + y = x^3 + x^2, \quad P = (0, 0)$$



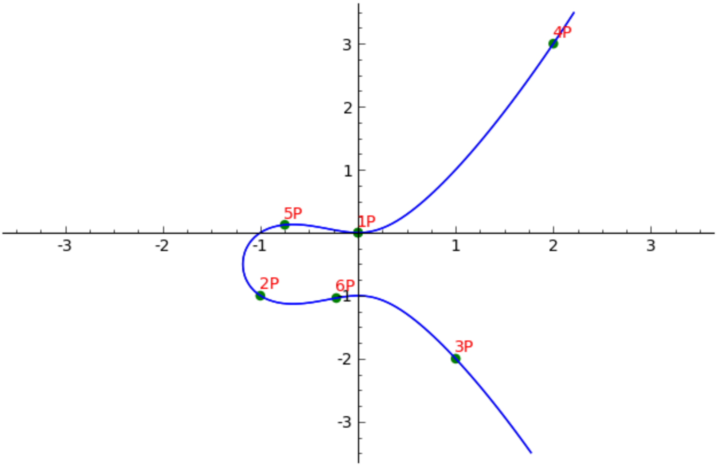
$$y^2 + y = x^3 + x^2, \quad P = (0,0)$$



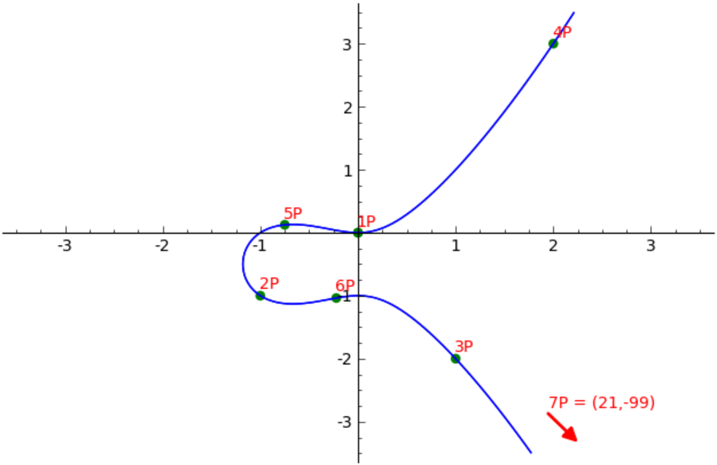
$$y^2 + y = x^3 + x^2, \quad P = (0,0)$$



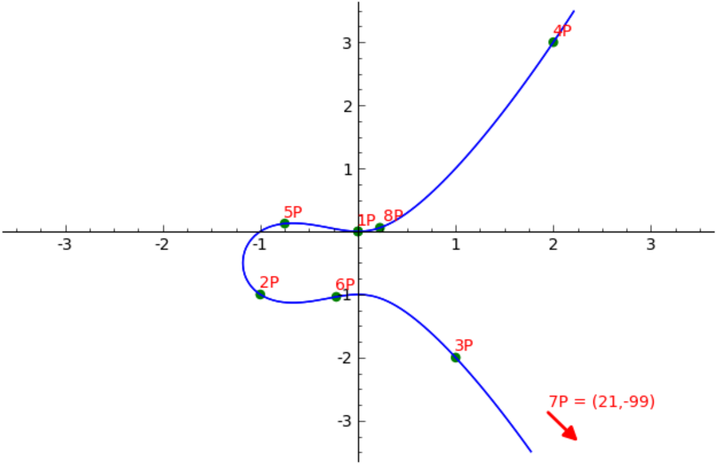
$$y^2 + y = x^3 + x^2, \quad P = (0, 0)$$



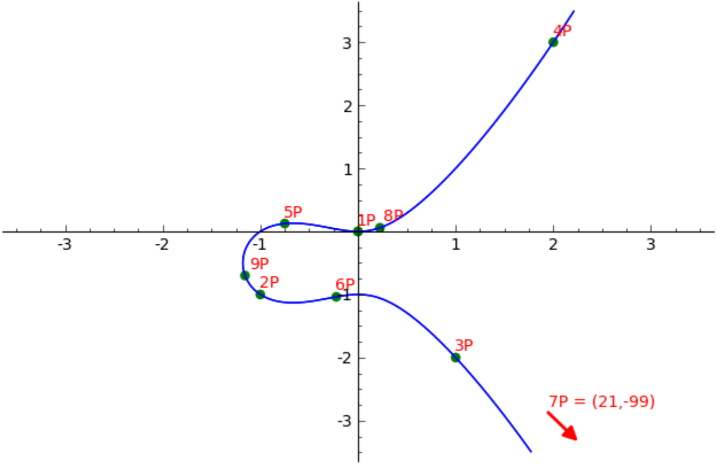
$$y^2 + y = x^3 + x^2, \quad P = (0, 0)$$



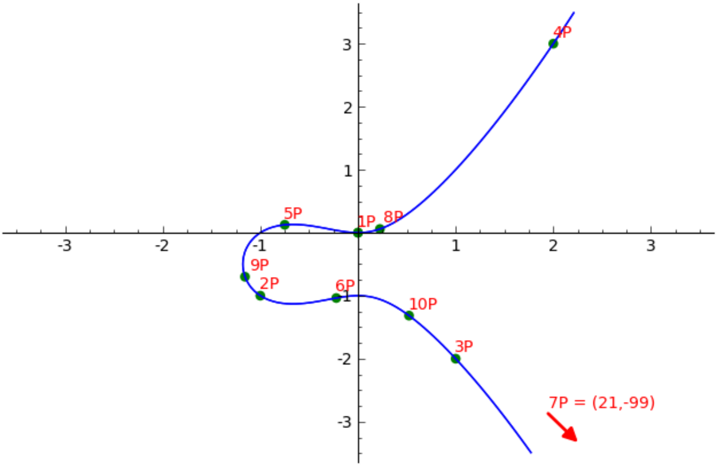
$$y^2 + y = x^3 + x^2, \quad P = (0,0)$$



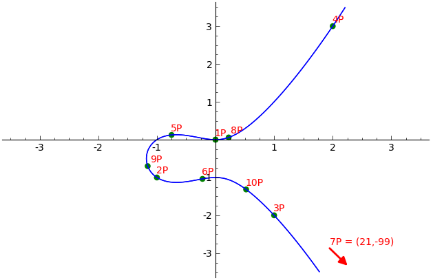
$$y^2 + y = x^3 + x^2, \quad P = (0,0)$$



$$y^2 + y = x^3 + x^2, \quad P = (0, 0)$$



Do we get a sequence from this?

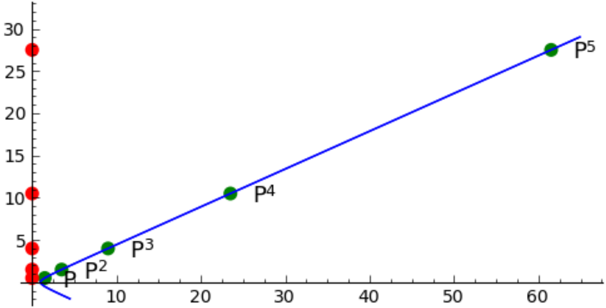


$$
\begin{aligned}
P &= (0, 0) \\
2P &= (-1, -1) \\
3P &= (1, -2) \\
4P &= (2, 3) \\
5P &= (-3/4, 1/8) \\
6p &= (-2/9, -28/27) \\
7P &= (21, -99) \\
8P &= (11/49, 20/343) \\
9P &= (-140/121, -931/1331) \\
10P &= (209/400, -10527/8000)
\end{aligned}
$$

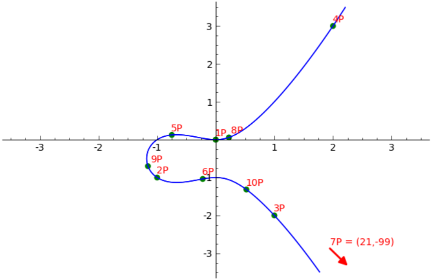
In the hyperbola case, the function

$$y(P)$$

has as zeroes ± 1. It grows as the power of P grows.

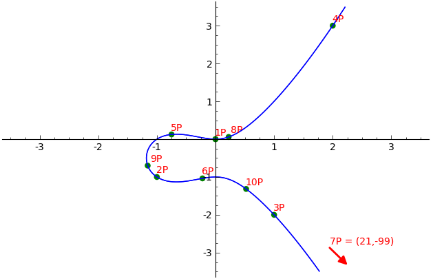


Do we get a sequence from this?



$$
\begin{aligned}
P &= (0, 0) \\
2P &= (-1, -1) \\
3P &= (1, -2) \\
4P &= (2, 3) \\
5P &= (-3/4, 1/8) \\
6p &= (-2/9, -28/27) \\
7P &= (21, -99) \\
8P &= (11/49, 20/343) \\
9P &= (-140/121, -931/1331) \\
10P &= (209/400, -10527/8000)
\end{aligned}
$$

It turns out the right thing to do is to pull out the denominators



$$
\begin{array}{rcll}
P &=& (0,0) & 1\\
2P &=& (-1,-1) & 1\\
3P &=& (1,-2) & 1\\
4P &=& (2,3) & -1\\
5P &=& \left(-\frac{3,}{2^2}, \frac{1}{2^3}\right) & -2\\
6p &=& \left(-\frac{2}{3^2}, -\frac{28}{3^3}\right) & -3\\
7P &=& (21,-99) & -1\\
8P &=& \left(\frac{11}{7^2}, \frac{20}{7^3}\right) & 7\\
9P &=& \left(-\frac{140}{11^2}, -\frac{931}{11^3}\right) & 11\\
10P &=& \left(\frac{209}{20^2}, -\frac{10527}{20^3}\right) & 20
\end{array}
$$

(I'm sweeping the minus signs under the rug here. . .)

$$1, 1, 1, -1, -2, -3, -1, 7, 11, 20, -19, -87, -191, -197, 1018$$

...is an example of ...

Definition

An *elliptic divisibility sequence* is an integer sequence W_n satisfying

$$W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0.$$

Properties:

- can generate it from the first four terms
- satisfies $n \mid m \implies W_n \mid W_m$ (we'll see why!)

$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad P = (x, y)$

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1 a_3, \quad b_6 = a_3^2 + 4a_6, \\
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
W_0 &= 0, \quad W_1 = 1, \quad W_2 = 2y + a_1 y + a_3, \\
W_3 &= 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8, \\
W_4 &= W_2(2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + (b_4 b_8 - b_6^2)) \\
W_{2n+1} &= W_{n+2} W_n^3 - W_{n-1} W_{n+1}^3, \; n \geq 2, \\
W_2 W_{2n} &= W_{n-1}^2 W_n W_{n+1} - W_{n-2} W_n W_{n+1}^2, \; n \geq 3, \\
A_n &= x W_n^2 - W_{n-1} W_{n+1} \\
4y B_n &= W_{n-1}^2 W_{n+2} + W_{n-2} W_{n+1}^2
\end{aligned}
$$

Then

$$nP = \left(\frac{A_n}{W_n^2}, \frac{B_n}{W_n^3} \right),$$

$$W_{n+m} W_{n-m} W_r^2 + W_{m+r} W_{m-r} W_n^2 + W_{r+n} W_{r-n} W_m^2 = 0.$$

$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad P = (x, y)$

$$nP = \left(\frac{A_n}{W_n^2}, \frac{B_n}{W_n^3} \right),$$

$$W_{n+m} W_{n-m} W_r^2 + W_{m+r} W_{m-r} W_n^2 + W_{r+n} W_{r-n} W_m^2 = 0.$$

$$W_n = 0 \iff nP = 0$$

Theorem (Ward, 1948)

Every elliptic divisibility sequence arises this way (as on the previous slide).

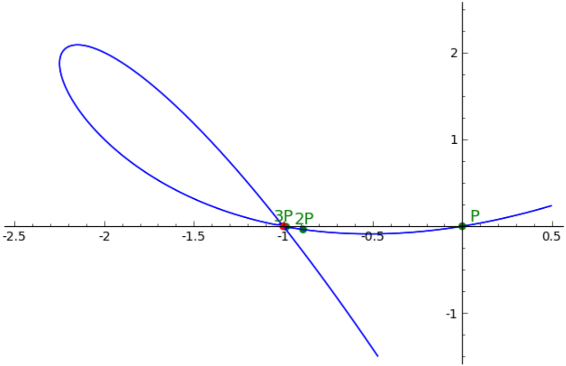
$$1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$$

satisfies

$$W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0.$$

Example

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



$$P = (0,0)\,,$$
$$2P = \left(-\frac{8}{3^2}, -\frac{1}{3^3}\right),$$
$$3P = \left(-\frac{63}{8^2}, -\frac{3}{8^3}\right),$$
$$4P = \left(-\frac{440}{21^2}, -\frac{8}{21^3}\right),$$

$$1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, \ldots$$

This is not really an elliptic curve, because it has a singularity.

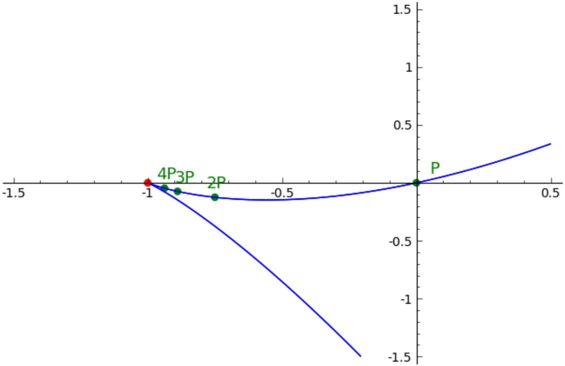
$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$$

satisfies

$$W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0.$$

Example

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



$$P = (0,0)\,,$$
$$2P = \left(-\frac{3}{2^2}, -\frac{1}{2^3}\right),$$
$$3P = \left(-\frac{8}{3^2}, -\frac{2}{3^3}\right),$$
$$4P = \left(-\frac{15}{4^2}, -\frac{3}{4^3}\right),$$

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$$

This is not really an elliptic curve, because it has a singularity.