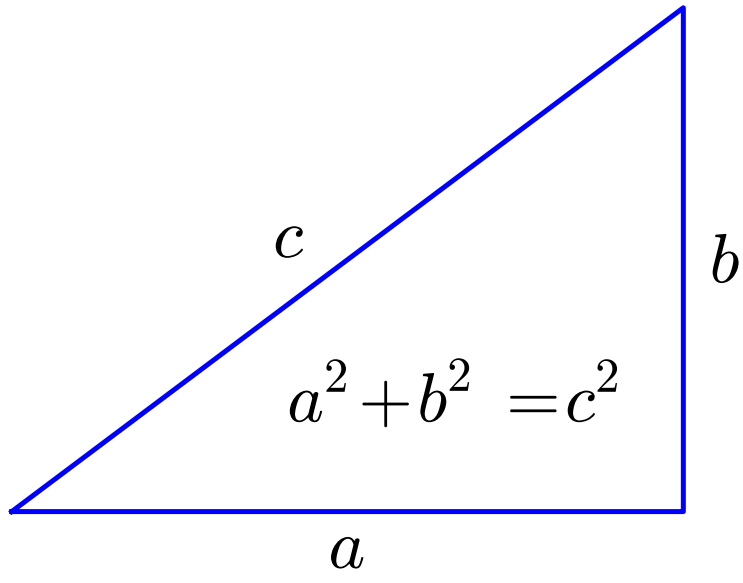
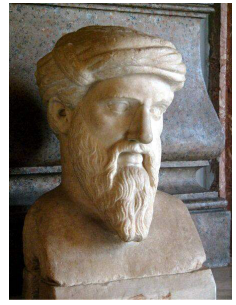
The Birch and Swinnerton-Dyer Conjecture

Benedict Gross and William Stein

January 6, 2012 in Boston, MA

Algebraic equations



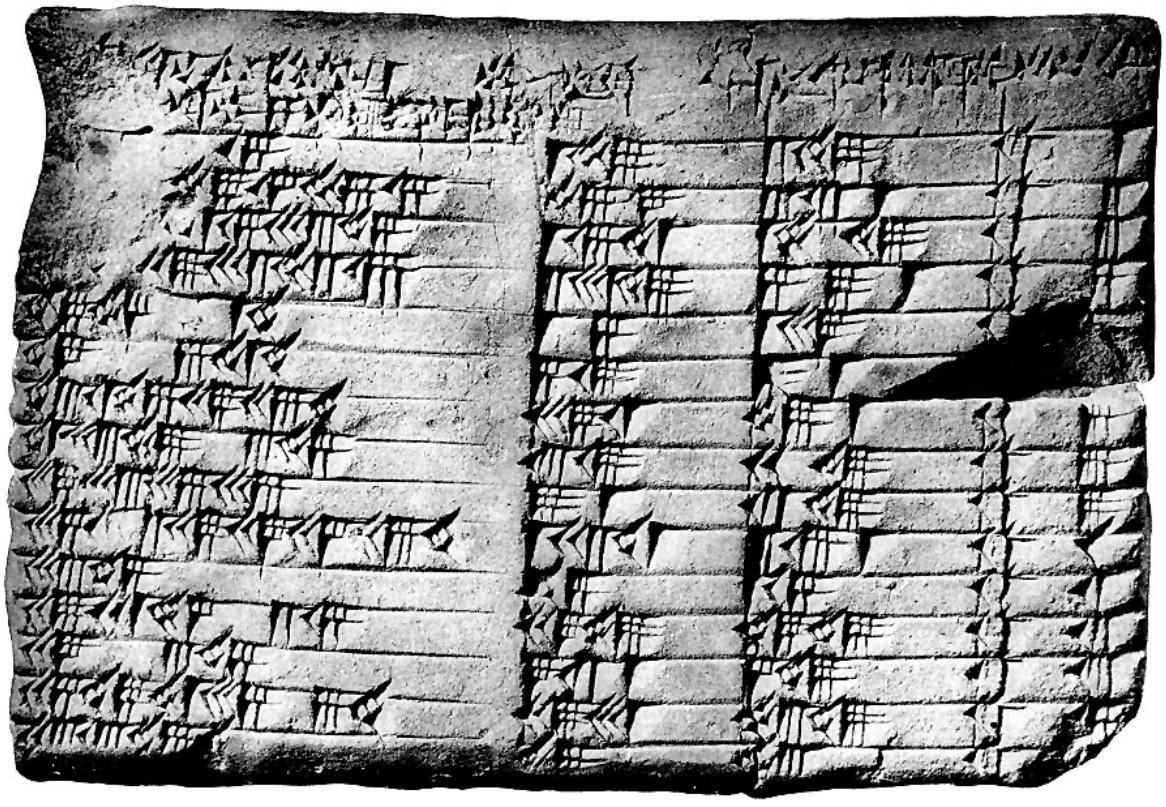


Pythagoras (600 BCE) Baudhāyana (800 BCE)

Pythagorean triples

$a^2 + b^2 = c^2$ has solutions $(3, 4, 5), (5, 12, 13), (7, 24, 25), \ldots$

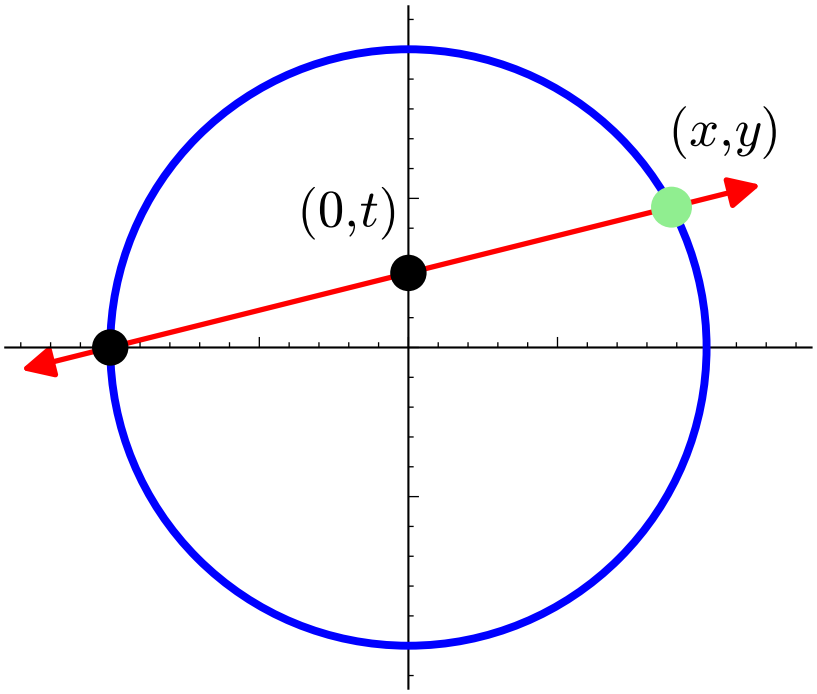
There are more solutions on a Babylonian tablet (1800 BCE):



$(3, 4, 5)$
$(5, 12, 13)$
$(7, 24, 25)$
$(9, 40, 41)$
$(11, 60, 61)$
$(13, 84, 85)$
$(15, 8, 17)$
$(21, 20, 29)$
$(33, 56, 65)$
$(35, 12, 37)$
$(39, 80, 89)$
$(45, 28, 53)$
$(55, 48, 73)$
$(63, 16, 65)$
$(65, 72, 97)$

The general solution of $a^2 + b^2 = c^2$

$x = a/c$ and $y = b/c$ satisfy the equation $x^2 + y^2 = 1$



$$t = \frac{y}{1+x} \qquad x = \frac{1-t^2}{1+t^2} \qquad y = \frac{2t}{1+t^2}$$

Write $t = p/q$. Then

$$x = \frac{q^2 - p^2}{q^2 + p^2} \qquad y = \frac{2qp}{q^2 + p^2}$$

$$a = q^2 - p^2 \qquad b = 2qp \qquad c = q^2 + p^2$$

$$t = 1/2 \longrightarrow (a, b, c) = (3, 4, 5)$$

$$t = 2/3 \longrightarrow (a, b, c) = (5, 12, 13)$$

$$t = 3/4 \longrightarrow (a, b, c) = (7, 24, 25)$$

Cubic equations

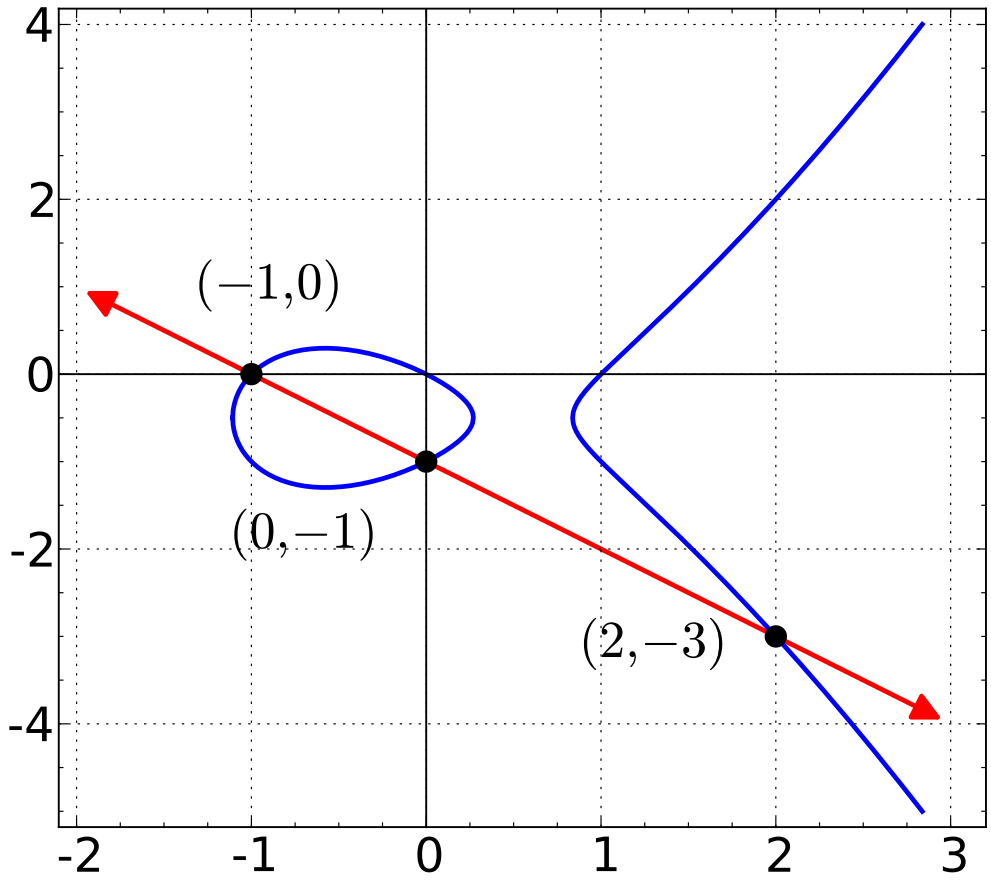
After linear and quadratic equations come cubic equations, like

$$x^3 + y^3 = 1 \qquad\qquad y^2 + y = x^3 - x$$

Here there may be either a finite or an infinite number of rational solutions.

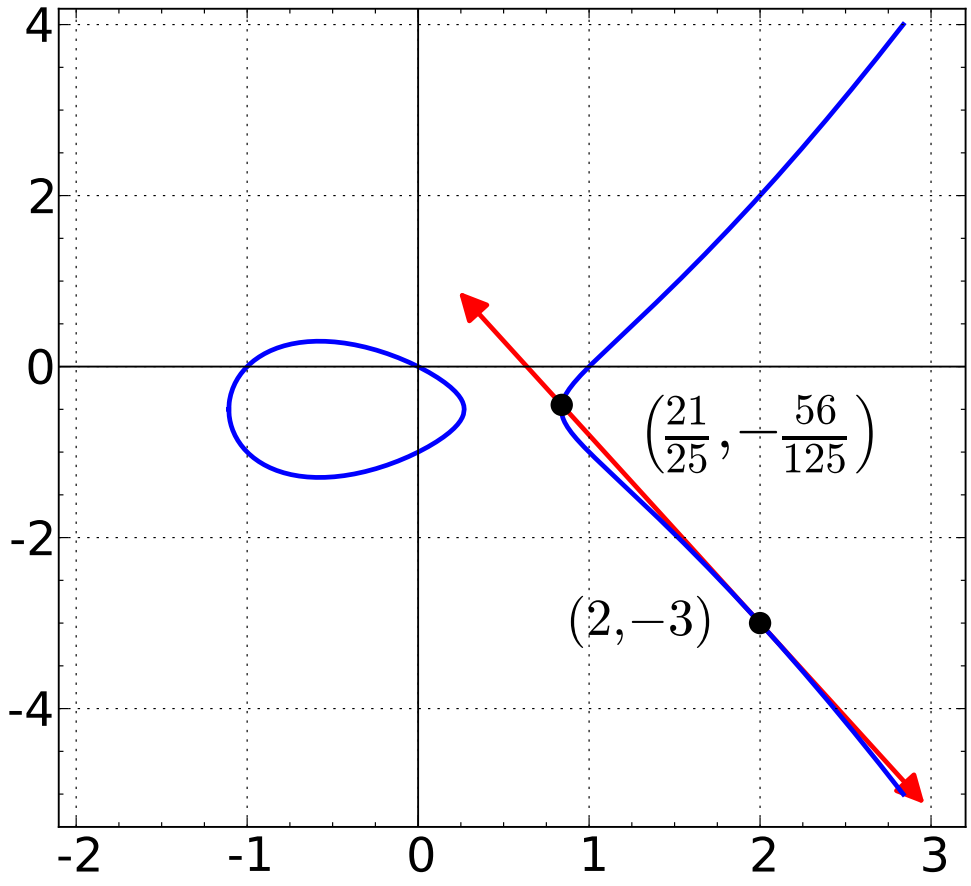
The graph

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



The limit of a secant line is a tangent

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



Large solutions

If the number of solutions is infinite, they quickly become large.

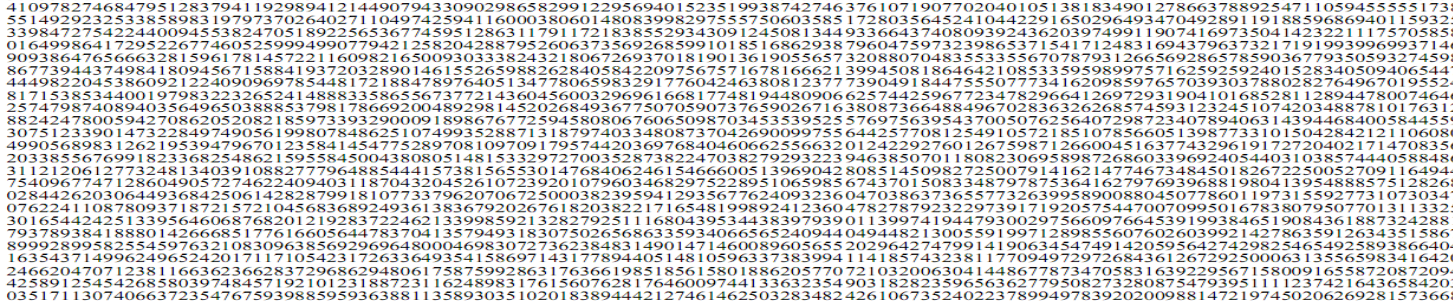
$$y^2 + y = x^3 - x$$

```
(0, 0)
(1, 0)
(-1, -1)
(2, -3)
(1/4, -5/8)
(6, 14)
(-5/9, 8/27)
(21/25, -69/125)
(-20/49, -435/343)
(161/16, -2065/64)
(116/529, -3612/12167)
(1357/841, 28888/24389)
(-3741/3481, -43355/205379)
(18526/16641, -2616119/2146689)
(8385/98596, -28076979/30959144)
(480106/4225, 332513754/274625)
(-239785/2337841, 331948240/3574558889)
(12551561/13608721, -8280062505/50202571769)
(-59997896/67387681, -641260644409/553185473329)
(683916417/264517696, -18784454671297/4302115807744)
(1849037896/6941055969, -318128427505160/578280195945297)
(51678803961/12925188721, 10663732503571536/1469451780501769)
(-270896443865/384768368209, 66316334575107447/23867066449493807 3)
```

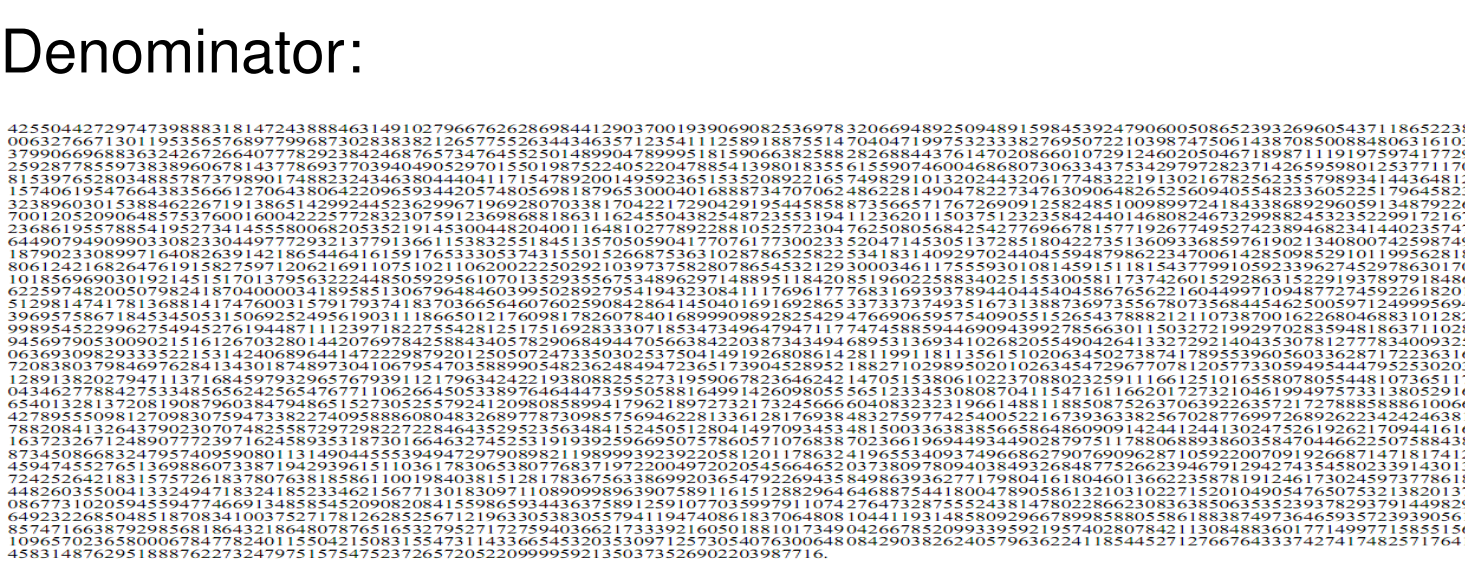
Even the simplest solution can be large (Watkins)

$$y^2 + y = x^3 - 5115523309x - 140826120488927$$

Numerator of x-coordinate of smallest solution (5454 digits):



Denominator:



The rank

The rank of E is essentially the number of independent solutions.

- rank $(E) = 0$ means there are finitely many solutions.
- rank $(E) > 0$ means there are infinitely many solutions.
- The curve $E(a)$ with equation

$$y(y+1) = x(x-1)(x+a)$$

has rank $= 0, 1, 2, 3, 4$ for $a = 0, 1, 2, 4, 16$.

The rank is finite

Can it be arbitrarily large?

The current record is rank(E) $\geq$ 28

$$y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x +$$
$$3448161179503055646703298569039072037485594435931918036126600829629193948732243429$$

P_1 = [-212415009125438107329213746 3, 259854492051899599030515511070780628911531]
P_2 = [233450986603470175688475453 7, 188720041954944691808683165528036279315 31]
P_3 = [-167173605406236906387903866 3, 251709377261144287808506947241319126049131]
P_4 = [213913026013915666649298213 7, 366395091714397292024214596929412975275 31]
P_5 = [153470676446712072388547733 7, 854295853460176942890210328627810727995 31]
P_6 = [-273107948787567703334157506 3, 262521815484332191641284072623902143387531]
P_7 = [277572626684457164970545853 7, 128457554740140602488694876990826403699 31]
P_8 = [149438572932718895754183381 7, 884866055277334059861164945140492334114 51]
P_9 = [186843822862088735850906525 7, 592374032144377087127251403930593585891 31]
P_{10} = [200894510882574377486654253 7, 476906778801255528821517507815414247115 31]
P_{11} = [234836054091802516965163293 7, 174929300062005578573403324764488043635 31]
P_{12} = [-147208400709048117447000866 3, 246643450653503714199947441549759798469131]
P_{13} = [292412860770806121336328893 7, 283502644314888785014883564747673758995 31]
P_{14} = [537499389106606189329393453 7, 286188908427263386451175031916479893731531]
P_{15} = [170969076823335452333400855 7, 718988349746860894661597005292159809216 31]
P_{16} = [245095401135359314407259518 7, 444522817353263435704926255061071473653 1]
P_{17} = [296925470927355916746467493 7, 327668930753662708013336825431604696875 31]
P_{18} = [271191493494169260133288293 7, 206843661277838169865041398150659061353 1]
P_{19} = [200785860779968545287783289 37, 27796085411378066046560517256246240300915 31]
P_{20} = [215808245024073477431781069 7, 349943734019640268099696622418009012547 31]
P_{21} = [200464545824705902240322493 7, 480493297807046455224398669998884754675 31]
P_{22} = [297574945094799626494709133 7, 333989898260753223202089344101048578691 31]
P_{23} = [-210249046768628515014734786 3, 259576391459875789571677393171687203227531]
P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931]
P_{25} = [277393100834186523144377181 7, 126321628346499210024141162737692758134 51]
P_{26} = [215658118814376840936346138 7, 351250929640229088970041505163751780873 31]
P_{27} = [386633049987241250881565913 7, 121197755655944226293036926715025847322531]
P_{28} = [223086828977357602377867873 7, 285587600305974856633870206007686400285 31]

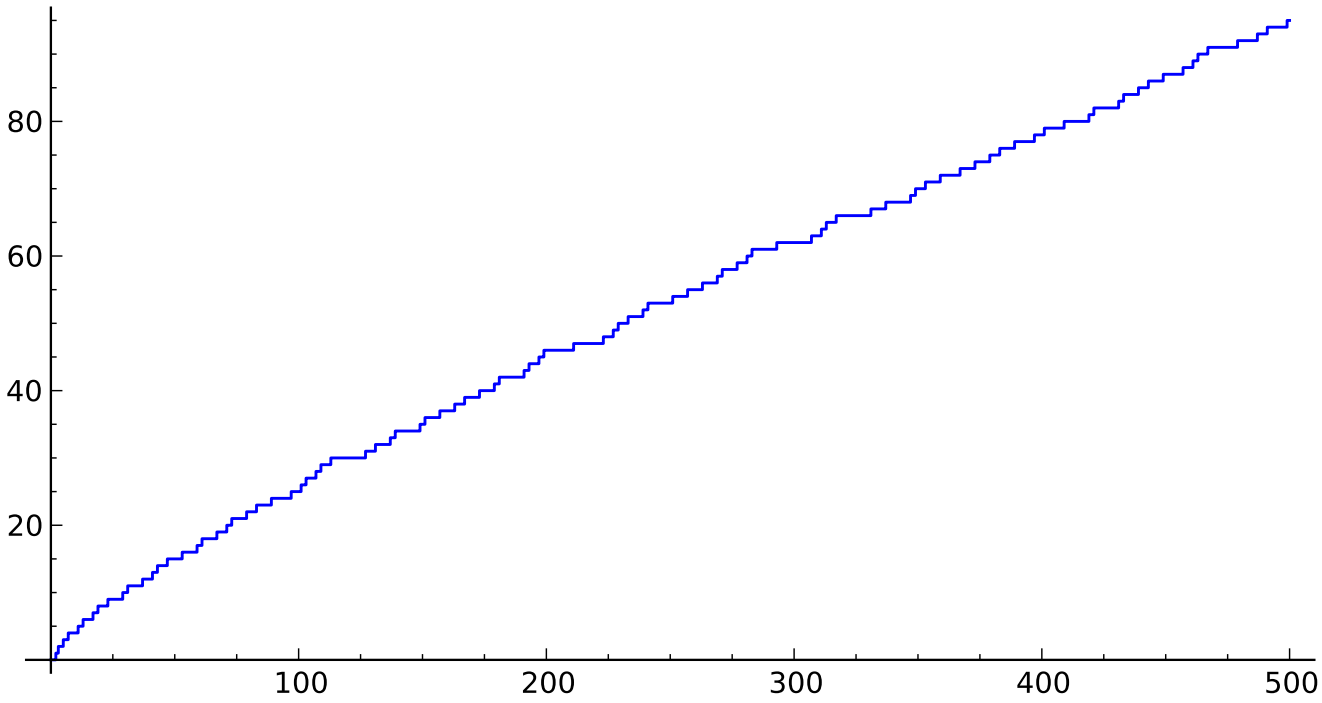
Peter Swinnerton-Dyer and Bryan Birch made a prediction for the rank, based on the average number of solutions at prime numbers p.

Primes

A prime p is a number greater than 1 that is not divisible by any smaller number.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, . . .

There are infinitely many primes. The largest explicit prime known is $2^{43112609} - 1$ with 12,978,189 digits.

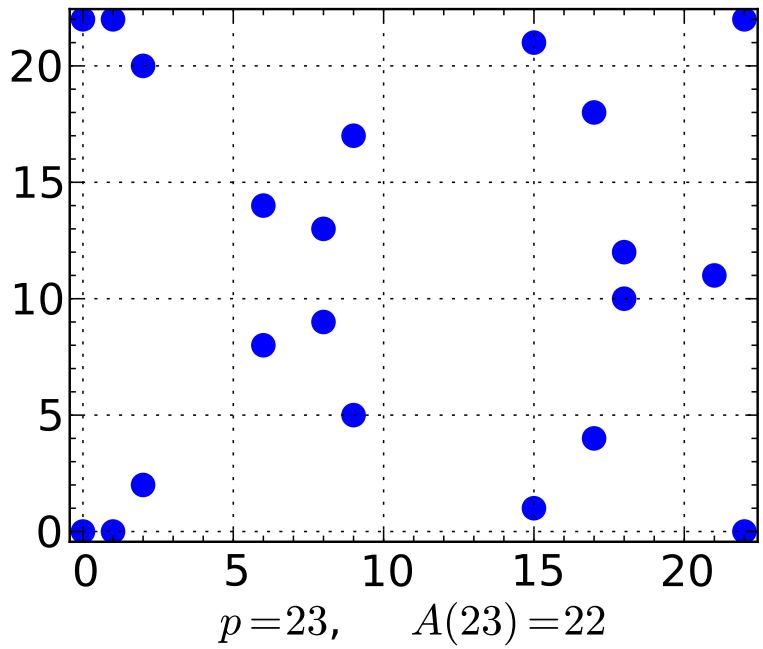


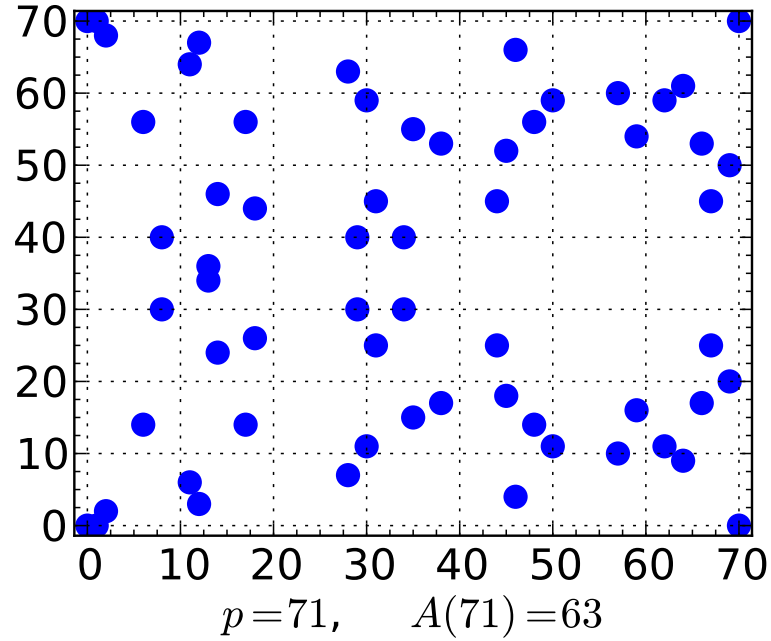
What do we mean by a solution of the cubic equation at the prime number p?

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

$(x, y) \equiv (3, 1)$ is a solution at $p = 11$

There are finitely many solutions $A(p)$ at each prime p.





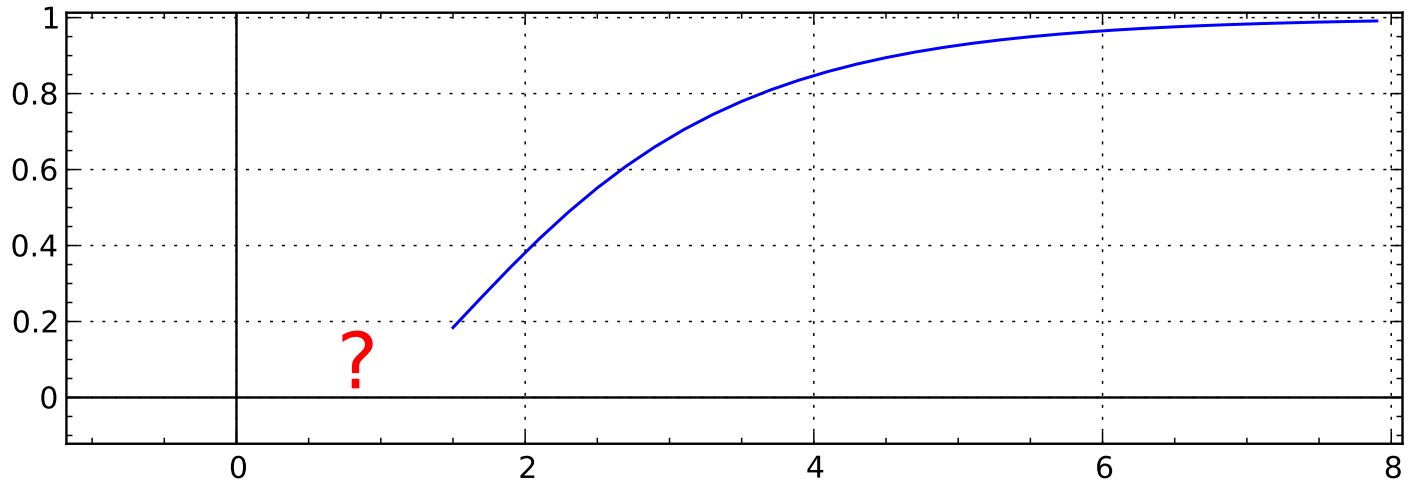
It is common to write

$$\#\{\text{solutions mod } p\} = A(p) = p + 1 - a(p)$$

We define the L-function of E by the infinite product

$$L(E,s) = \prod_{\text{all } p} (1 - a(p)p^{-s} + p^{1-2s})^{-1} = \sum a(n)n^{-s}$$

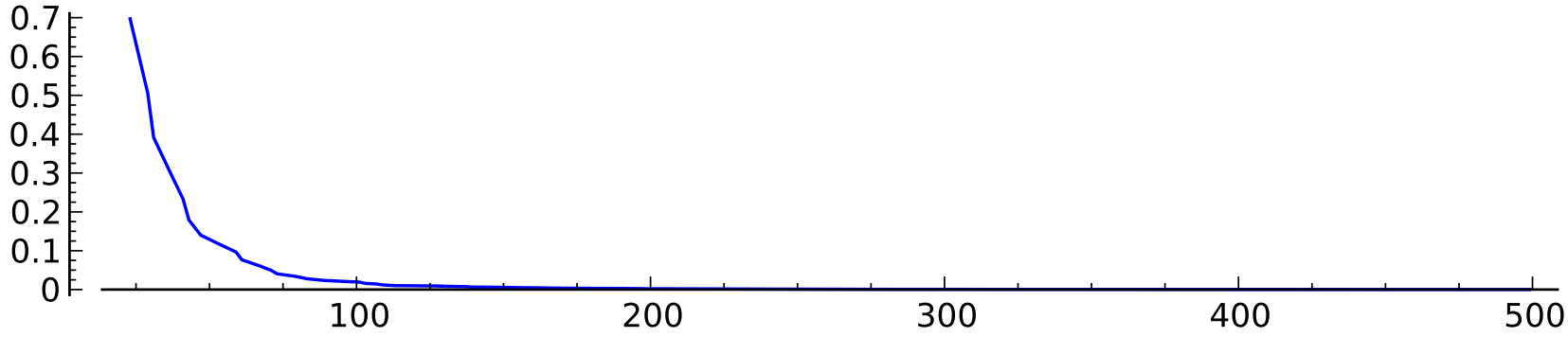
This definition only works in the region $s > 3/2$, where the infinite product converges.



If we formally set $s = 1$ in the product, we get

$$\prod_{\text{all } p}(1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_{\text{all } p} \frac{p}{A(p)}$$

If $A(p)$ is large on average compared with p, this will approach 0. The larger $A(p)$ is on average, the faster it will tend to 0.

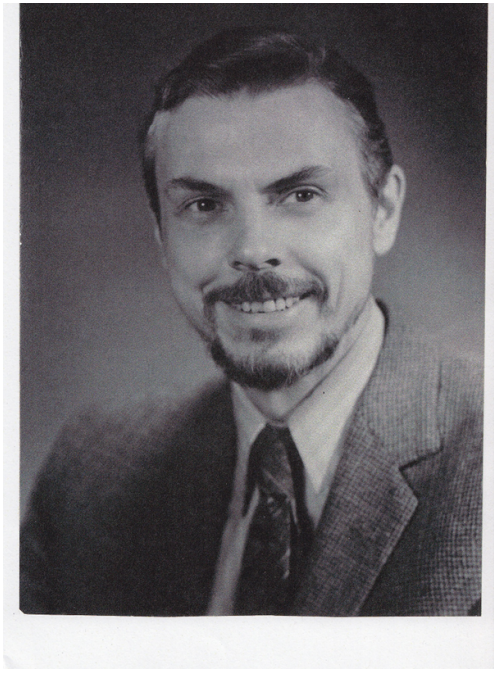


The conjecture of Birch and Swinnerton-Dyer

1. The function $L(E, s)$ has a natural (analytic) continuation to a neighborhood of $s = 1$.
2. The order of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank of E.
3. The leading term in the Taylor expansion of $L(E, s)$ at $s = 1$ is given by certain arithmetic invariants of E.

$$L(E, s) = c(E)(s - 1)^{\text{rank}(E)} + \cdots$$

The most mysterious arithmetic invariant was studied by John Tate and Igor Shafarevich, who conjectured that it is finite. Tate called this invariant $Ш$.



The Birch and Swinnerton-Dyer Conjecture

$$L(E,s) = c(E)(s-1)^{\mathrm{rank}(E)} + \cdots$$

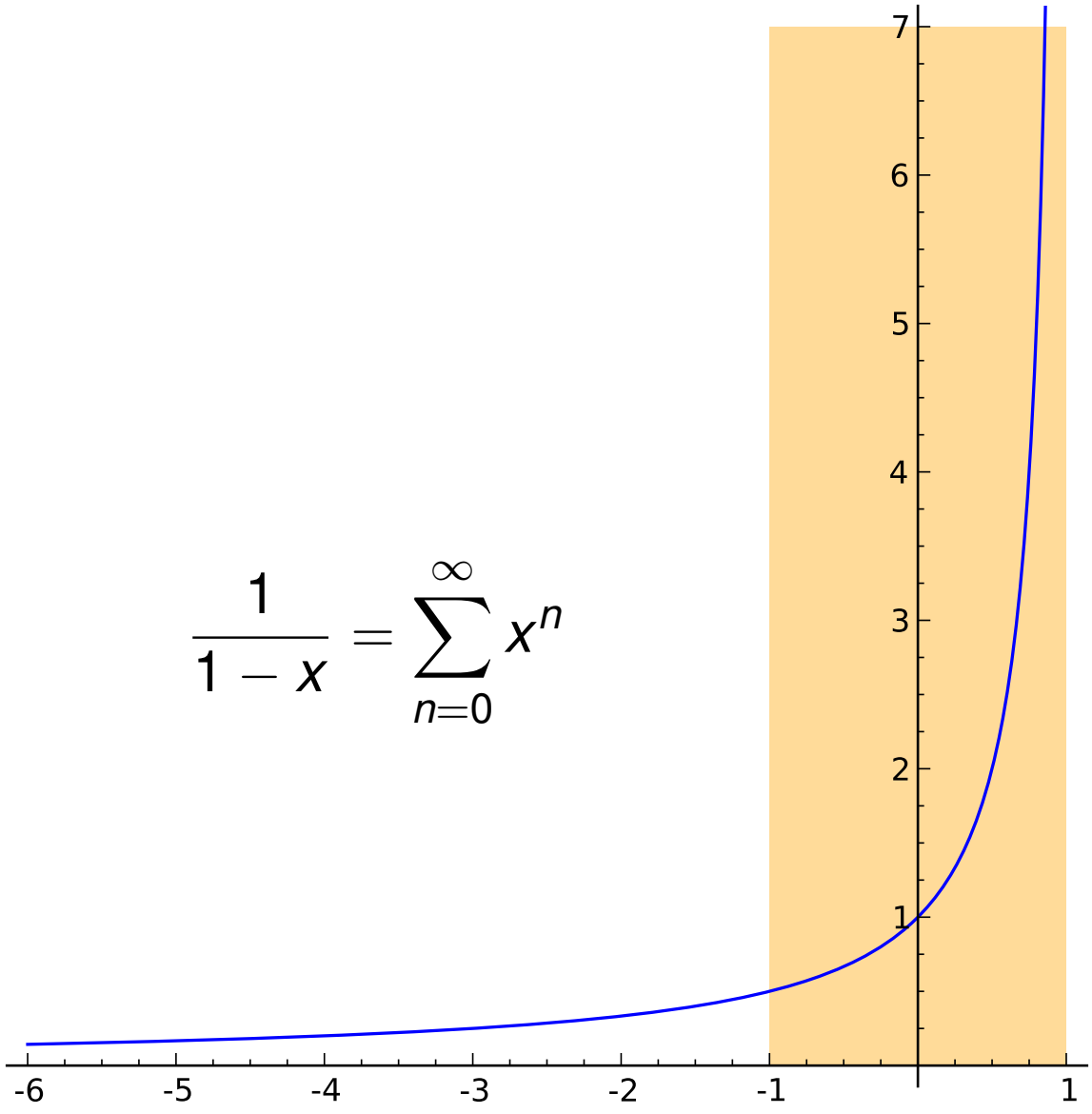
$$c(E) = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#Ш_E \cdot \prod c_p}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}$$

Each quantity on the right measures the size of an abelian group attached to E.

Natural (analytic) continuation

The infinite sum $\sum_{n=0}^{\infty} x^n$ converges when $-1 < x < 1$.

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$$

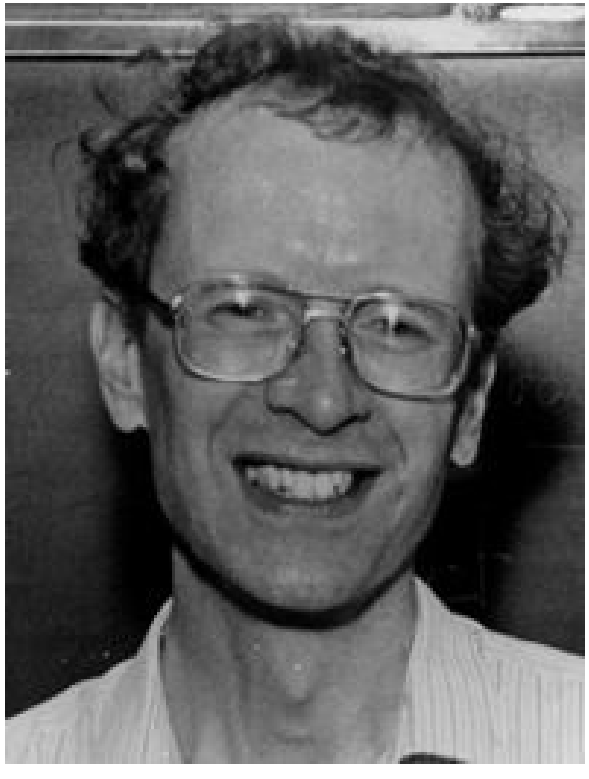


Fermat's Last Theorem

The natural (analytic) continuation of $L(E, s) = \sum a(n)n^{-s}$ was obtained (in most cases) by Andrew Wiles and Richard Taylor (1995). They proved that the function defined by the infinite series

$$F(\tau) = \sum a(n)e^{2\pi in\tau}$$

is a modular form.

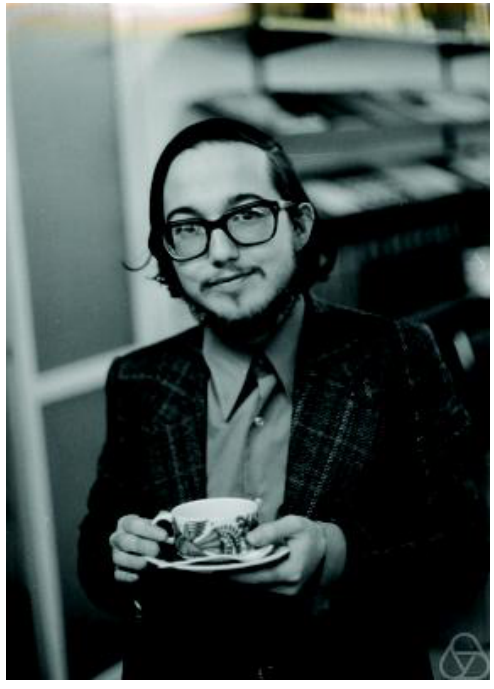


Combining a limit formula of Benedict Gross and Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

If $L(E,1) \neq 0$ the rank is zero, so there are finitely many solutions.

If $L(E,1) = 0$ and $L'(E,1) \neq 0$ the rank is one, so there are infinitely many solutions.

In both cases, we can also show that $Ш$ is finite.



Example: A Rank 1 Curve

```
sage: E = EllipticCurve([0,0,1,-1,0])
sage: L = E.lseries()
sage: Lser = L.taylor_series(); Lser
0.305999773834052*z + 0.186547797268162*z^2 + ...
sage: c = Lser[1]; c
0.305999773834052
sage: Omega_E = E.period_lattice().omega(); Omega_E
5.98691729246392
sage: Reg_E = E.regulator(); Reg_E
0.051111408239968 8
sage: prod_cp = E.tamagawa_product_bsd(); prod_cp
1
sage: T = E.torsion_order()^2; T
1
sage: c / (Omega_E * Reg_E * prod_cp / T^2)
1.00000000000000
```

Example: A Rank 2 Curve

```
sage: E = EllipticCurve([0,1,1,-2,0])
sage: L = E.lseries()
sage: Lser = L.taylor_series(); Lser
-2.69e-23 + (1.52e-23)*z + 0.75931650028*z^2 + ...
sage: E.rank()
2
sage: c = Lser[2]
sage: Omega_E = E.period_lattice().omega()
sage: Reg_E = E.regulator()
sage: prod_cp = E.tamagawa_product_bsd()
sage: T = E.torsion_order()^2
sage: c / (Omega_E * Reg_E * prod_cp / T^2)
1.00000000000000
sage: S = E.sha(); S
Tate-Shafarevich group ...
sage: S.p_primary_bound(5)
0
```

Open Problem: *Prove that* $Ш(E)$ *is finite.*

Example: A Rank 4 Curve

```
sage: E = EllipticCurve([0,15,1,-16,0])
sage: L = E.lseries()
sage: Lser = L.taylor_series(); Lser
4.32e-24 + (-1.96e-23)*z + (2.05e-22)*z^2
         + (-7.97e-22)*z^3 + 10.84*z^4 - ...
sage: E.rank()
4
sage: c = Lser[4]
sage: Omega_E = E.period_lattice().omega()
sage: Reg_E = E.regulator()
sage: prod_cp = E.tamagawa_product_bsd()
sage: T = E.torsion_order()^2
sage: c / (Omega_E * Reg_E * prod_cp / T^2)
0.999999999999999
```

Open Problem: *Prove that* $\mathrm{ord}_{s=1} L(E, s) = 4$.

Thank you