# stein-cubics-2011-11-17

# Solving Cubic Equations

**Benedict Gross (Harvard) and William Stein (Univ of Washington)**

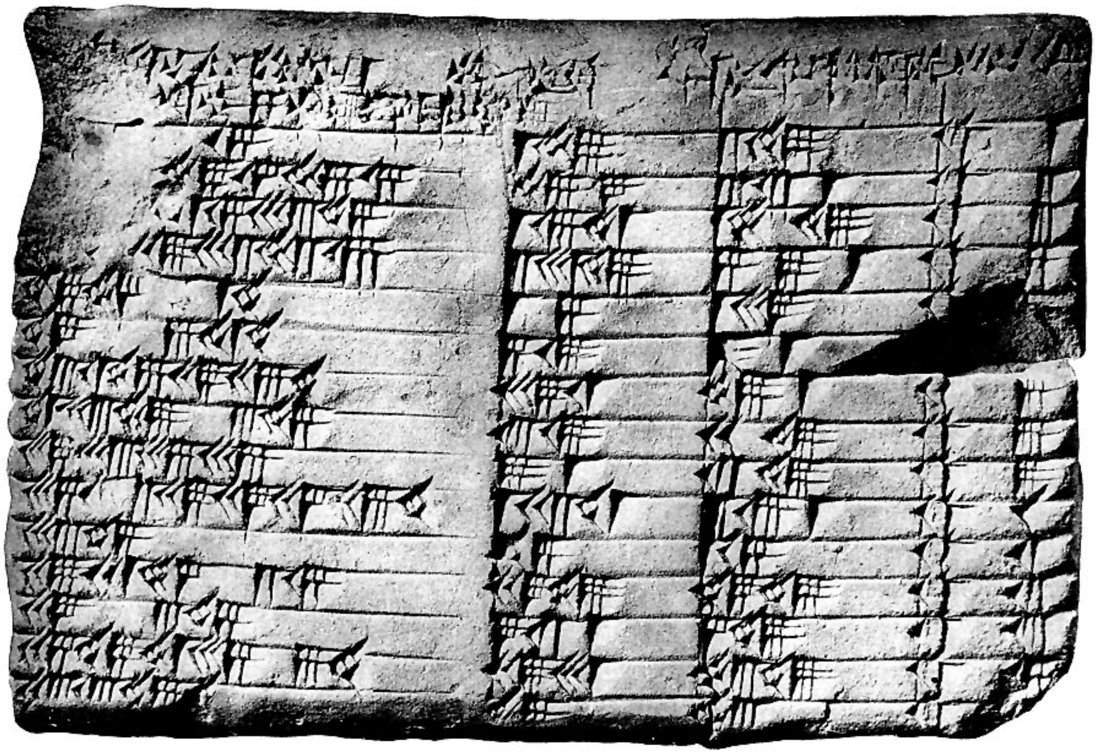
## November 2011

## Algebraic Equations

Mathematicians solve many types of equations:

$x^2 + y^2 = z^2$ has solutions $(3, 4, 5), (5, 12, 13), \ldots$.

There are solutions on a Babylonian tablet from 1800 BCE:



## Finding all of the solutions

$x^2 + y^2 = z^2$ has general solution $x = p^2 - q^2, y = 2pq, z = p^2 + q^2$.

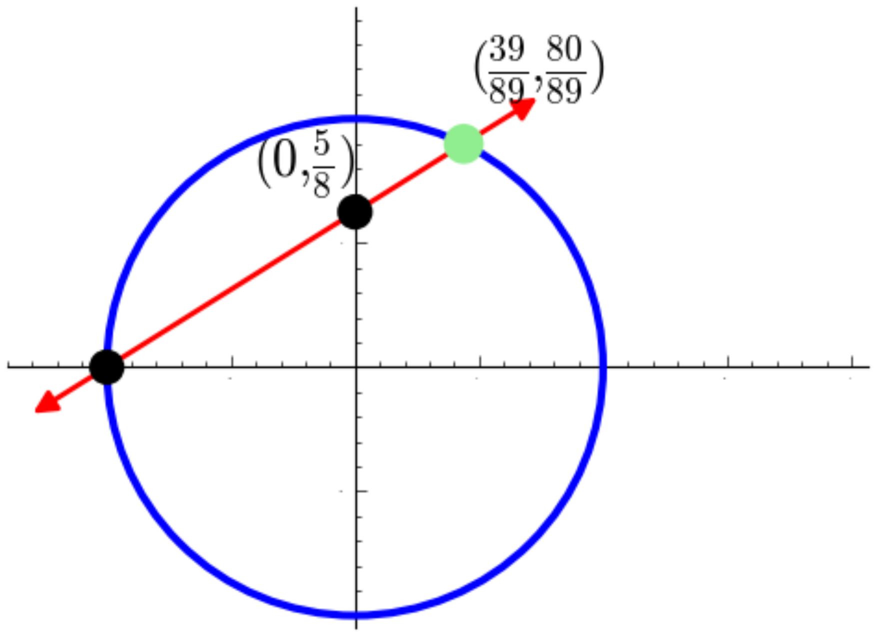
See this by considering the line of slope $t = p/q$ through $(0, -1)$ intersected with the unit circle.

```
%hide
@interact
def _(t=(1/16,1/8,..,1)):
    t0 = t
    x,y,t=var('x,y,t')
    show([x==(1-t^2)/(1+t^2), y==2*t/(1+t^2)])
    t = t0
    (x,y) = ((1-t^2)/(1+t^2), 2*t/(1+t^2))
    a = 1/3
    html('<center>')
    G = circle((0,0), 1, color='blue', thickness=3)
    G += text("$(0,%s)$"%latex(t), (-.2, t+.2), fontsize=20, color='black')
    G += text("$(%s,%s)$"%(latex(x),latex(y)), (x+.3, y+.3), fontsize=20,
color='black')
    G += arrow((-1-a,-t*a), (x+a,y+t*a), head=2, color='red')
    G += point((0,t), pointsize=150, color='black', zorder=100)
```

```
    G += point((-1,0), pointsize=150, color='black', zorder=100)
    G += point((x,y), pointsize=190, color='lightgreen', zorder=100)
    G.show(aspect_ratio=1, ymax=1.4, xmax=2, fontsize=0, figsize=6)
    html('</center>')
```

t 1/16

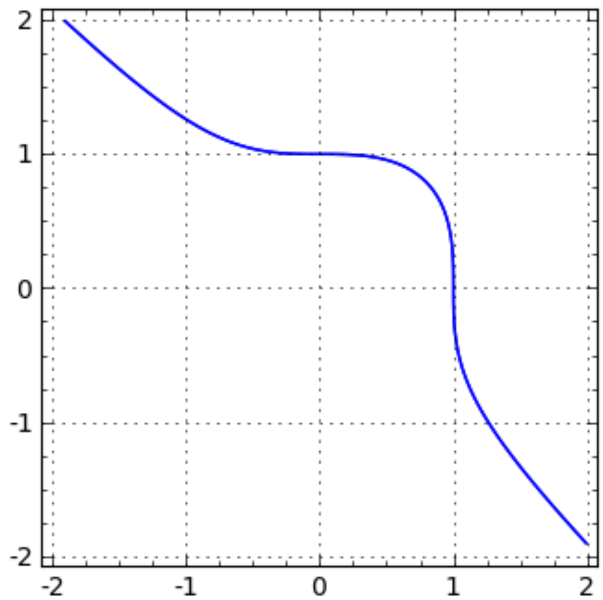
$$\left[x = -\frac{t^2 - 1}{t^2 + 1}, y = \frac{2\,t}{t^2 + 1}\right]$$



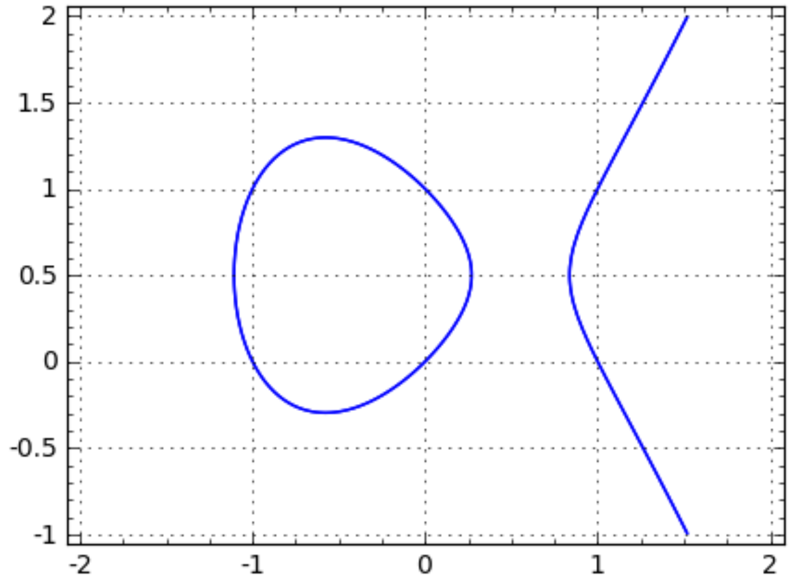
# Cubic Curves

$x^3 + y^3 = 1$

```
var('x,y')
implicit_plot(x^3 + y^3 == 1, (x,-2,2), (y,-2,2), figsize=5, gridlines=True)
```



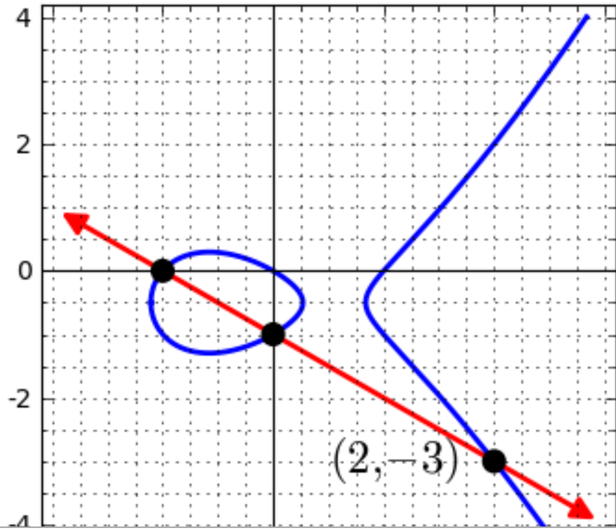
```
implicit_plot(y^2 - y == x^3 - x, (x,-2,2), (y,-1,2), figsize=5, gridlines=True)
```



## New solutions from old ones: The Secant Process

```
%hide
E = EllipticCurve([0,0,1,-1,0])
html('<center><font size=+2>$%s$</font></center>'%latex(E))
G = E.plot(plot_points=600, thickness=2)
G += arrow((-2,1), (3,-4), head=2, color='red', width=2)
G += points([(-1,0), (0,-1), (2,-3)], color='black', pointsize=70,
zorder=50)
G += text("$(2,-3)$", (1.1,-3), fontsize=18, color='black')
G.show(gridlines='minor', frame=True, figsize=[4,4])
```

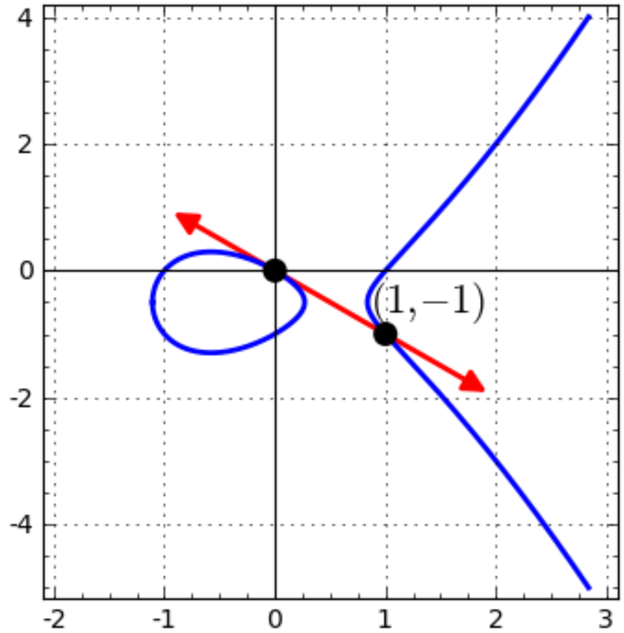
$$y^2 + y = x^3 - x$$




## New solutions from old ones: The Tangent Process

```
%hide
E = EllipticCurve([0,0,1,-1,0])
html('<center><font size=+2>$%s$</font></center>'%latex(E))
G = E.plot(plot_points=600, thickness=2)
G += arrow((-1,1), (2,-2), head=2, color='red', width=2)
G += points([(0,0), (1,-1)], color='black', pointsize=70,
zorder=50)
G += text("$(1,-1)$", (1.4,-.5), fontsize=16, color='black')
G.show(gridlines=True, frame=True, figsize=[4,4], xmin=-2, xmax=3)
```

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




## Large solutions

We can turn this into an abelian group law on the set of solutions. Is it finite or infinite?

If the group is infinite, the solutions become very large.

$P = (0, 0)$ on $y^2 - y = x^3 - x$

Compute $x$-coordinate of $nP$:

```
%hide
@interact
def _(n=(1..65)):
    E = EllipticCurve([0,0,1,-1,0])
    P = E([0,0])
    show((n*P))
```

n 1

$$\left(\frac{1849037896}{6941055969} : -\frac{318128427505160}{578280195945297} : 1\right)$$

## Even the simplest solution can be large

Simplest solution to $y^2 = x^3 + 7823$:

$$x = \frac{2263582143321421502100209233517777}{143560497706190989485475151904721}$$

$$y = \frac{186398152584623305624837551485596770028144776655756}{1720094998106353355821008525938727950159777043481}$$

(Found by Michael Stoll in 2002.)

## The Rank

The **rank** of $E$ is the number of independent solutions of infinite order.

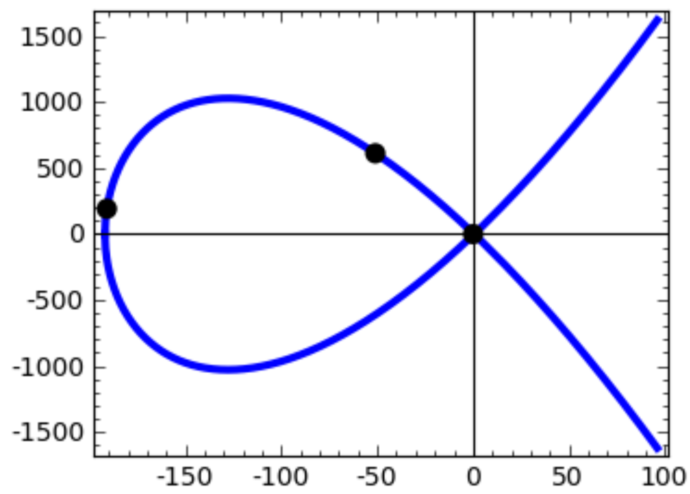
rank($E$) = 0 means there are finitely many solutions.

**Example:** Curve $E(a)$: with equation $y(y+1) = x(x-1)(x+a)$.
Has rank = 0, 1, 2, 3, 4, 5, 6 for a = 0, 1, 2, 4, 16, 79, 298.

```
%hide
@interact
def _(a=(2, (0..300))):
    E = EllipticCurve([0,(a-1),1,-a,0])
    html("<center><font size=+1>$y(y+1)=x(x-1)(x+%s)$,    rank = %s</font>"%
(a,E.rank()))
    v = E.gens()
    v = [(t[0],t[1]) for t in v]
    G = E.plot(thickness=3, plot_points=600)
    xmin = min(G.xmin(), min(t[0] for t in v+[(0,0)]))
    xmax = max(G.xmax(), max(t[0] for t in v+[(-xmin/2,0)]))
    G = E.plot(thickness=3, xmin=xmin, xmax=xmax, plot_points=600)
    G += points([(t[0],t[1]) for t in v], color='black', pointsize=50, zorder=50)
    G.show(figsize=4, frame=True)
    show(v)
    html("</center>")
```

a 2

$y(y+1) = x(x-1)(x+192)$, rank = 3




$[(-191, 191), (-51, 611), (0, -1)]$

## How big can the rank be?

We don't know if the ranks of elliptic curves can be arbitrarily large.

The current record is rank($E$) = 28 for **Noam Elkies**' curve $E$ below, with independent points:

$P_{1}$ = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]
$P_{2}$ = [2334509866034701756884754537, 18872004195494469180868316552803627931531]
$P_{3}$ = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]
$P_{4}$ = [2139130260139156666492982137, 36639509171439729202421459692941297527531]
$P_{5}$ = [1534706764467120723885477337, 85429585346017694289021032862781072799531]
$P_{6}$ = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]
$P_{7}$ = [2775726266844571649705458537, 12845755474014060248869487699082640369931]
$P_{8}$ = [1494385729327188957541833817, 88486605527733405986116494514049233411451]
$P_{9}$ = [1868438228620887358509065257, 59237403214437708712725140393059358589131]
$P_{10}$ = [2008945108825743774866542537, 47690677880125552882151750781541424711531]
$P_{11}$ = [2348360540918025169651632937, 17492930006200557857340332476448804363531]
$P_{12}$ = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]
$P_{13}$ = [2924128607708061213363288937, 28350264431488878501488356474767375899531]
$P_{14}$ = [5374993891066061893293934537, 286188908427263386451175031916479893731531]
$P_{15}$ = [1709690768233354523334008557, 71898834974686089466159700529215980921631]
$P_{16}$ = [2450954011353593144072595187, 4445228173532634357049262550610714736531]
$P_{17}$ = [2969254709273559167464674937, 32766893075366270801333682543160469687531]
$P_{18}$ = [2711914934941692601332882937, 2068436612778381698650413981506590613531]
$P_{19}$ = [20078586077996854528778328937, 2779608541137806604656051725624624030091531]
$P_{20}$ = [2158082450240734774317810697, 34994373401964026809969662241800901254731]
$P_{21}$ = [2004645458247059022403224937, 48049329780704645522439866999888475467531]
$P_{22}$ = [2975749450947996264947091337, 33398989826075322320208934410104857869131]
$P_{23}$ = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]
$P_{24}$ = [311583179915063034902194537, 168104385229980603540109472915660153473931]
$P_{25}$ = [2773931008341865231443771817, 12632162834649921002414116273769275813451]
$P_{26}$ = [2156581188143768409363461387, 35125092964022908897004150516375178087331]
$P_{27}$ = [3866330499872412508815659137, 121197755655944226293036926715025847322531]
$P_{28}$ = [2230868289773576023778678737, 28558760030597485663387020600768640028531]

```
E = EllipticCurve([1,-1,1,
    -20067762415575526585033208209338542750930230312178956502,

34481611795030556467032985690390720374855944359319180361266008296291939448732243429])
```

```
344816117950305564670329856903907203748559443593191803612660082962919394487322434 29])

E
```

```
Elliptic Curve defined by y^2 + x*y + y = x^3 - x^2 -
20067762415575526585033208209338542750930230312178956502*x +
344816117950305564670329856903907203748559443593191803612660082 96291\
939448732243429 over Rational Field
```

# A Prediction

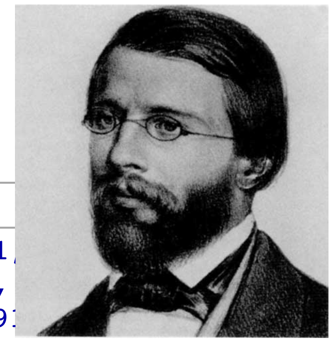
Peter Swinnerton-Dyer and Bryan Birch made a prediction for the rank based on the ***average number of solutions at each prime number*** $p$.

## Prime Numbers

A prime is a number not divisible by any smaller number: 2, 3, 5, 7, 11, ...

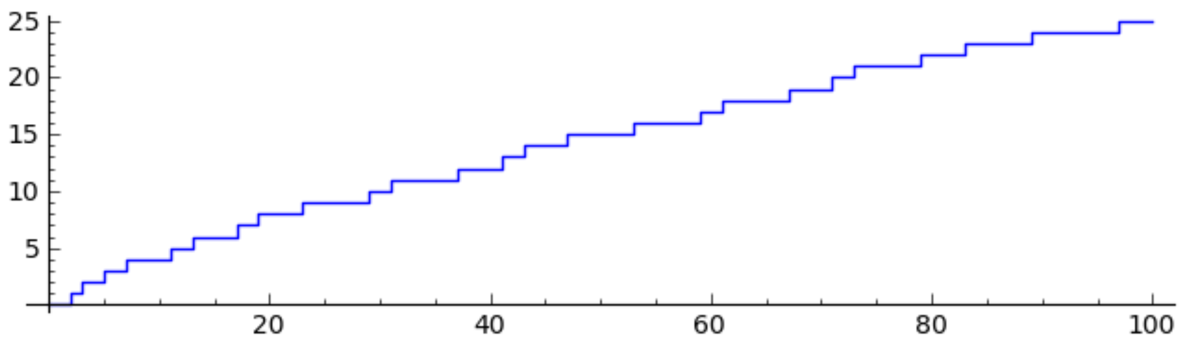
```
prime_range(200)
```

```
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109,
139, 149, 151, 157, 163, 167, 173, 179, 181, 19
```

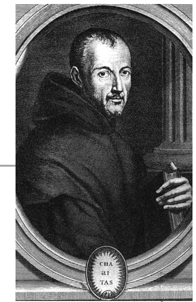


Counting Primes

```
plot(prime_pi, 0,100, figsize=[8,2])
```



# There are infinitely many primes



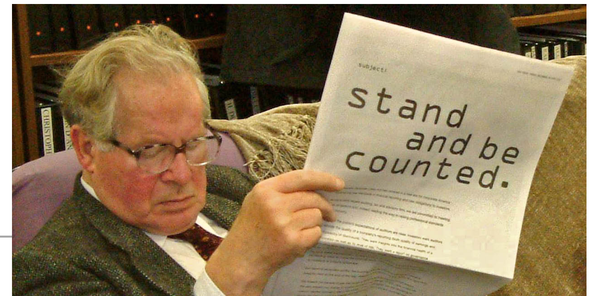
The largest known prime is $p = 2^{43112609} - 1$ with 12,978,189 digits

```
%hide
s_bigp = str(2^43112609 - 1)
@interact
def _(d=(5..10000)):
    print "Showing %.5f percent of the digits"%(100*2.0*d/len(s_bigp))
    print "p = " + s_bigp[:d] + ' ... ' + s_bigp[-d:]
```

d 5

```
Showing 0.01273 percent of the digits
p =
3164702693302559231434537239493375160541061884752646441403041767328 1\
1247493069368692043185121611837856726816539985465097356123432645179 6\
```

## Solutions Modulo $p$




What do we mean by a solution of the cubic equation at the prime number $p$?
Why are there finitely many solutions $A(p)$?

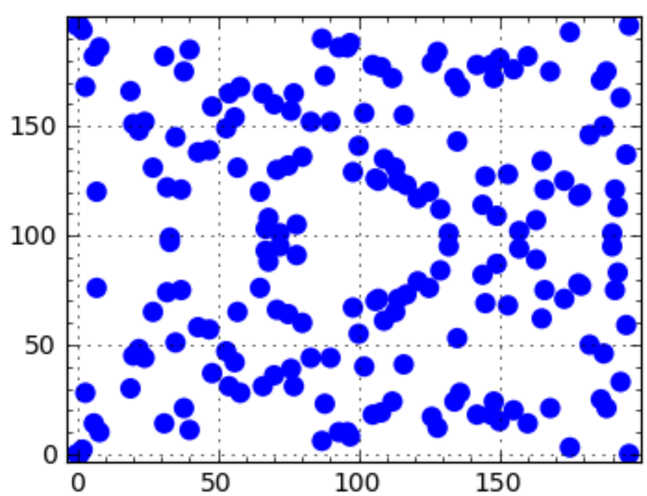
```
%hide
@interact
def _(p=(7,tuple(prime_range(500))), show_coords=False):
    E = EllipticCurve([0,0,1,-1,0])
    html('<center><font size=+1>$%s$ modulo $%s$<br>'%(latex(E),p))
    if E.conductor()%p == 0:
        html('<br><br>Curve has bad reduction...')
    else:
        html('<font color="blue" size=+1>$\\infty$</font><br>')
        G = E.change_ring(GF(p)).plot(pointsize=50)
        G.show(gridlines=True, figsize=4, frame=True, axes=False)
        if show_coords:
            print ', '.join(['(%s,%s)'%(z[0],z[1]) if z[2] else 'infinity'
                   for z in E.change_ring(GF(p)).points()])
    html('<br>$A(%s) = %s$'%(p,p+1-E.ap(p)))
    html('</font></center>')
```

p 7

show_coords

$$y^2 + y = x^3 - x \text{ modulo } 197$$

$\infty$




$A(197) = 195$

$A(197) = 193$

# The $L$-Function

Hasse proved: $p+1-2\sqrt{p} < A(p) < p+1+2\sqrt{p}$

It is common to write: $A(p) = p+1-a(p)$

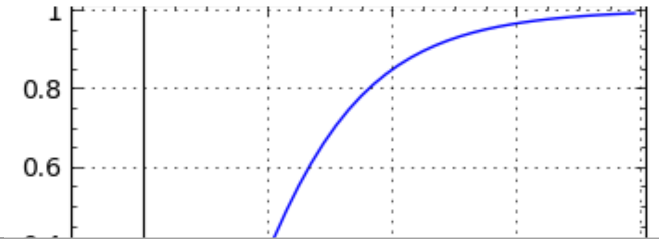
and to define the $L$-function of $E$ by the infinite product

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

This only makes sense as a function when $s > 3/2$, where the product converges.

```
%hide
E = EllipticCurve([0,0,1,-1,0])
L = E.lseries().dokchitser(20)
html('<h3>$L$-series of $%s$</h3>'%(latex(E)))
G = line([(s,L(s).real()) for s in [3/2, 3/2+0.2, .., 8]])
G += text('?', (.6,.1), color='red', fontsize=26)
G.show(xmin=-1, ymin=-.1, figsize=4, frame=True, gridlines=True)
```

### $L$-series of $y^2+y=x^3-x$




## The $L$-function at 1

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

$$\prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p \frac{p}{A(p)}$$

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

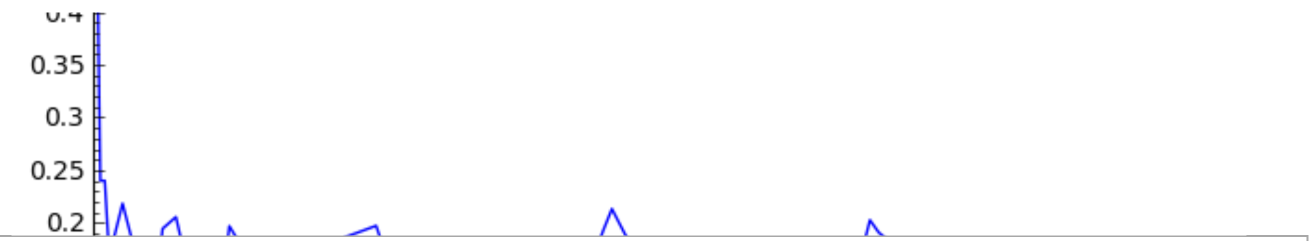
```
%hide
@interact
def _(E = ['y^2 + y = x^3 - x^2', 'y^2 + y = x^3 - x', 'a rank 4 curve', 'elkies
rank>=28 curve', '2011']):
    if E == 'y^2 + y = x^3 - x^2':
        E = EllipticCurve([0,-1,1,0,0])
        r = E.rank()
    elif E == 'y^2 + y = x^3 - x':
        E = EllipticCurve([0,0,1,-1,0])
        r = E.rank()
    elif E == 'a rank 4 curve':
        E = EllipticCurve([1, -1, 0, -79, 289])
        r = 4
    elif E == 'elkies rank>=28 curve':
        E = EllipticCurve([1,-1,1,
    -20067762415575526585033208209338542750930230312178956502,
```

```
34481611795030556467032985690390720374855944359319180361266008296291939448732243429])

        r = ">=28"
    elif E == '2011':
        E = EllipticCurve([0,2011])
        r = "?"

    L_approx = 1
    print '%4s%6s%5s%9s%20s'%('p', 'A(p)', 'p/Ap', '  prod p/Ap', 'Rank = %s'%r)
    v = []
    t = ''
    for p in primes(500):
        if E.discriminant()%p:
            Ap = p+1-E.ap(p)
            L_approx *= float(p/Ap)
            t += '%4s%4s%8.3f%8.3f\n'%(p, Ap, float(p/Ap), L_approx)
            v.append((p, L_approx))
    print t
    line(v).show(figsize=[8,2])
```

E [y^2 + y = x^3 - x^2] [y^2 + y = x^3 - x] [a rank 4 curve] [elkies rank>=28 curve] [2011]

```
   p  A(p) p/Ap  prod p/Ap           Rank = 0
   2   5   0.400   0.400
   3   5   0.600   0.240
   5   5   1.000   0.240
   7  10   0.700   0.168
  13  10   1.300   0.218
  17  20   0.850   0.186
  19  20   0.950   0.176
  23  25   0.920   0.162
  29  30   0.967   0.157
  31  25   1.240   0.194
  37  35   1.057   0.206
  41  50   0.820   0.169
  43  50   0.860   0.145
  47  40   1.175   0.170
  53  60   0.883   0.150
  59  55   1.073   0.161
  61  50   1.220   0.197
  67  75   0.893   0.176
  71  75   0.947   0.167
  73  70   1.043   0.174
  79  90   0.878   0.152
  83  90   0.922   0.141
  89  75   1.187   0.167
  97 105   0.924   0.154
 101 100   1.010   0.156
 103 120   0.858   0.134
 107  90   1.189   0.159
 109 100   1.090   0.173
 113 105   1.076   0.186
 127 120   1.058   0.197
 131 150   0.873   0.172
 137 145   0.945   0.163
 139 130   1.069   0.174
 149 160   0.931   0.162
 151 150   1.007   0.163

 157 165   0.952   0.155
```

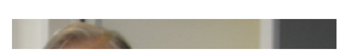
| | | | |
|---|---|---|---|
| 163 | 160 | 1.019 | 0.158 |
| 167 | 180 | 0.928 | 0.147 |
| 173 | 180 | 0.961 | 0.141 |
| 179 | 195 | 0.918 | 0.129 |
| 181 | 175 | 1.034 | 0.134 |
| 191 | 175 | 1.091 | 0.146 |
| 193 | 190 | 1.016 | 0.148 |
| 197 | 200 | 0.985 | 0.146 |
| 199 | 200 | 0.995 | 0.145 |
| 211 | 200 | 1.055 | 0.153 |
| 223 | 205 | 1.088 | 0.167 |
| 227 | 210 | 1.081 | 0.180 |
| 229 | 215 | 1.065 | 0.192 |
| 233 | 210 | 1.110 | 0.213 |
| 239 | 270 | 0.885 | 0.189 |
| 241 | 250 | 0.964 | 0.182 |
| 251 | 275 | 0.913 | 0.166 |
| 257 | 260 | 0.988 | 0.164 |
| 263 | 250 | 1.052 | 0.173 |
| 269 | 260 | 1.035 | 0.179 |
| 271 | 300 | 0.903 | 0.161 |
| 277 | 280 | 0.989 | 0.160 |
| 281 | 300 | 0.937 | 0.150 |
| 283 | 280 | 1.011 | 0.151 |
| 293 | 270 | 1.085 | 0.164 |
| 307 | 300 | 1.023 | 0.168 |
| 311 | 300 | 1.037 | 0.174 |
| 313 | 315 | 0.994 | 0.173 |
| 317 | 305 | 1.039 | 0.180 |
| 331 | 325 | 1.018 | 0.183 |
| 337 | 360 | 0.936 | 0.171 |
| 347 | 320 | 1.084 | 0.186 |
| 349 | 320 | 1.091 | 0.203 |
| 353 | 375 | 0.941 | 0.191 |
| 359 | 380 | 0.945 | 0.180 |
| 367 | 385 | 0.953 | 0.172 |
| 373 | 400 | 0.932 | 0.160 |
| 379 | 385 | 0.984 | 0.158 |
| 383 | 385 | 0.995 | 0.157 |
| 389 | 405 | 0.960 | 0.151 |
| 397 | 400 | 0.992 | 0.150 |
| 401 | 400 | 1.002 | 0.150 |
| 409 | 440 | 0.930 | 0.139 |
| 419 | 400 | 1.047 | 0.146 |
| 421 | 400 | 1.052 | 0.154 |
| 431 | 450 | 0.958 | 0.147 |
| 433 | 445 | 0.973 | 0.143 |
| 439 | 400 | 1.097 | 0.157 |
| 443 | 455 | 0.974 | 0.153 |
| 449 | 415 | 1.082 | 0.166 |
| 457 | 470 | 0.972 | 0.161 |
| 461 | 450 | 1.024 | 0.165 |
| 463 | 475 | 0.975 | 0.161 |
| 467 | 495 | 0.943 | 0.152 |
| 479 | 460 | 1.041 | 0.158 |
| 487 | 465 | 1.047 | 0.165 |
| 491 | 500 | 0.982 | 0.162 |
| 499 | 480 | 1.040 | 0.169 |




## Birch and Swinnerton-Dyer's Precise Conjecture

1. The function $L(E, s)$ has an analytic continuation to a neighborhood of $s = 1$.
2. The order of vanishing at $s = 1$ is equal to the rank of $E$.

## Tate's Refinement



## Tate's Refinement

This conjecture was refined by John Tate, to give the leading term in the Taylor expansion at $s = 1$ in terms of other arithmetic invariants of $E$.

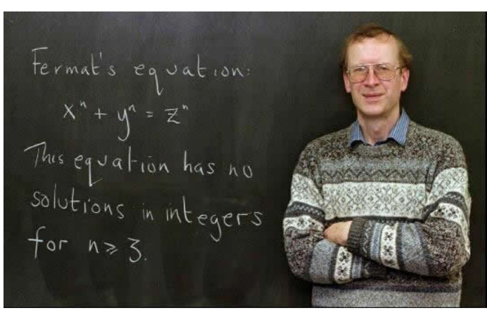
$$L(E, s) \sim c(E) \cdot (s-1)^{\mathrm{rank}(E)} \qquad s \to 1$$

## Analytic Continuation

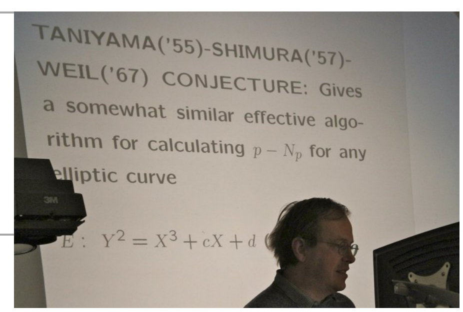
The analytic continuation was proved using the method of Andrew Wiles and Richard Taylor: the function

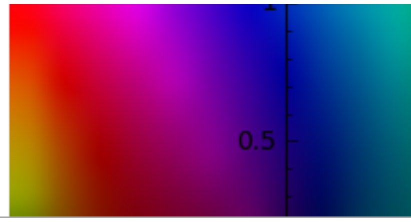
$$F(\tau) = \sum a(n) e^{2\pi i n \tau}$$

is a modular form.




```
%hide
E = EllipticCurve([0,0,1,-1,0])
L = E.lseries().dokchitser(30)
complex_plot(L, (-1,3), (-1,1), plot_points=30)
```






## Work of Gross-Zagier and Kolyvagin when $r=0$ and $r=1$

Combining work of Benedict Gross and Don Zagier with work of Victor Kolyvagin, one can show:

- If $L(E,1)\neq 0$ the rank is zero.
- If $L(E,1)=0$ and $L'(E,1)\neq 0$ the rank is one.



```
E = EllipticCurve([0,2011])
L = E.lseries().dokchitser(10)
L(1)
```

```
^CInterrupting PARI/GP interpreter...

Traceback (click to the left of this block for traceback)
...
__SAGE__
```

## When $r = 2$ and $r = 3$

- Can prove rank conjecture for specific curves one at a time using a computer.
- I don't know of a systematic careful attempt to do this for many curves.

```
E = EllipticCurve([0, 1, 1, -2, 0])
E.rank()
```

```
2
```

```
L = E.lseries(); L(1)
```

```
-1.33174198778018e-19
```

```
L.L1_vanishes()
```

```
True
```

```
L.taylor_series()
```

```
-2.69129566562797e-23 + (1.52514901968783e-23)*z +
0.759316500288427*z^2 - 0.430302337583362*z^3 -
0.193509313829981*z^4 + 0.459971558373642*z^5 + O(z^6)
```

## When $r \geq 4$

## When $r \geq 4$

Conjecture not proved for even a single elliptic curve.

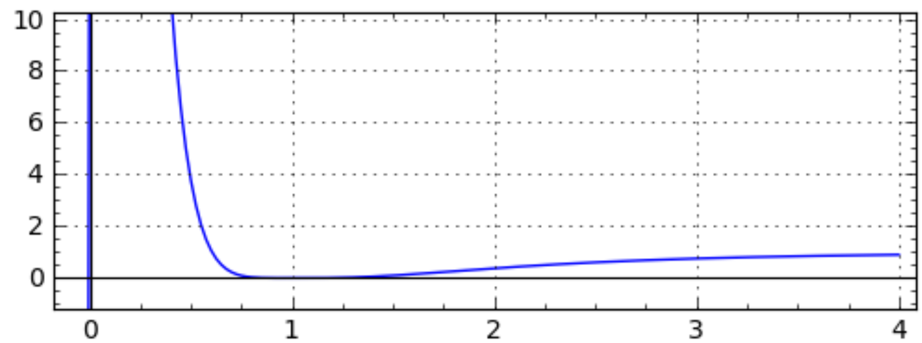
Do ***not*** know conjecture for this rank $4$ curve: $y^2 + xy = x^3 - x^2 - 79x + 289$

Proving the conjecture for this particular curve would be a ***major result***.

```
E = EllipticCurve([1, -1, 0, -79, 289])
L = E.lseries(); L.taylor_series()
```

```
5.54631009473167e-24 + (-2.08951550639391e-23)*z +
(-4.15704192504384e-22)*z^2 + (1.66720224204167e-21)*z^3 +
8.94384739590089*z^4 - 33.6950287693207*z^5 + O(z^6)
```

```
%hide
L = E.lseries().dokchitser(20)
eps = 0.025
G = line([(s,L(s).real()) for s in [-0.1,-0.1+eps, .., 4]])
G.show(figsize=[6,2], frame=True, gridlines=True, ymin=-1, ymax=10)
```




# Questions?

# Questions?

## The Average Rank

Manjul Bhargava has recently made progress on the study of the average rank, for ALL cubic curves with rational coefficients.

Every such curve has an equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers. It is unique if no prime $p$ satisfies $p^4$ divides $A$ and $p^6$ divides $B$.