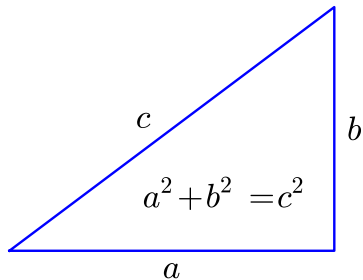


Solving Cubic Equations

Benedict Gross and William Stein

January, 2012

Algebraic equations



Pythagoras (600 BCE)

Baudhāyana (800 BCE)

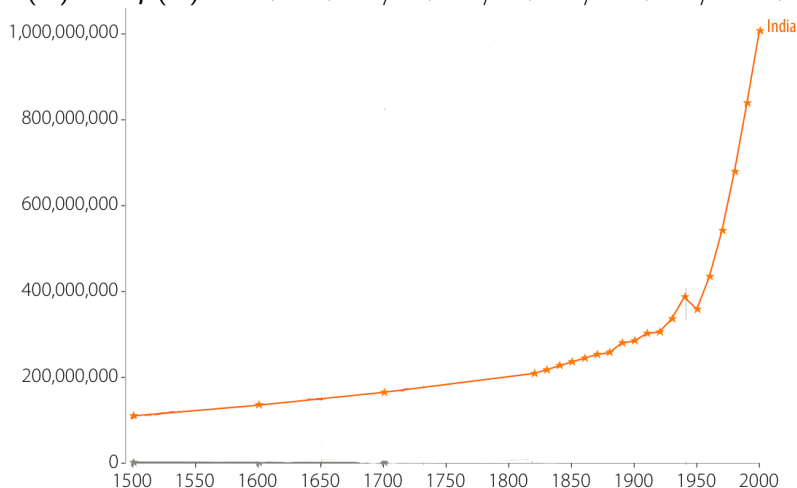
Differential equations

$$F'(T) = F(T)$$

$$dF/dT = F$$

$$F(0) = 1$$

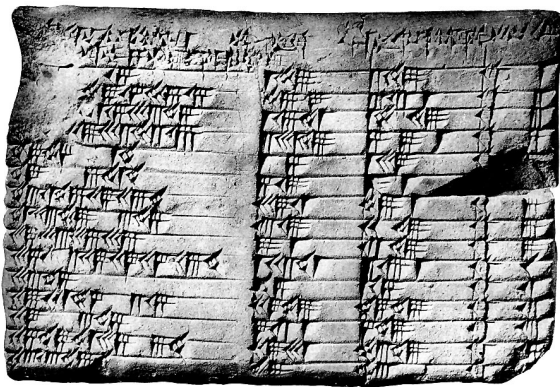
$$F(T) = \exp(T) = 1 + T + T^2/2 + T^3/6 + T^4/24 + T^5/120 + \dots$$



Pythagorean triples

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

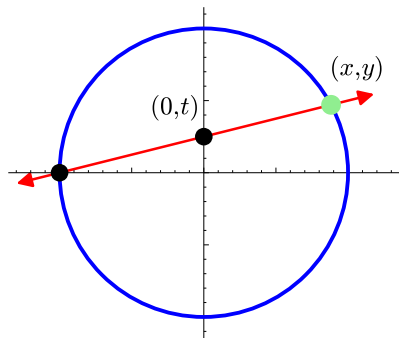
There are more solutions on a Babylonian tablet (1800 BCE):



(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 $x^2 + y^2 = 1$



$$t = \frac{y}{1+x}$$

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

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

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

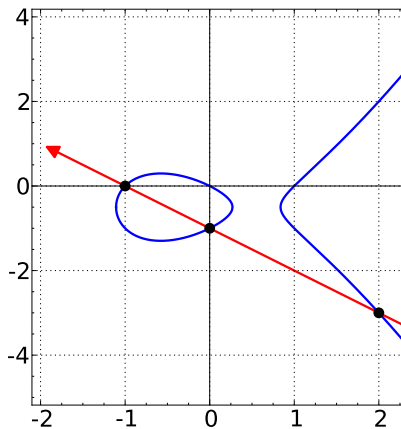
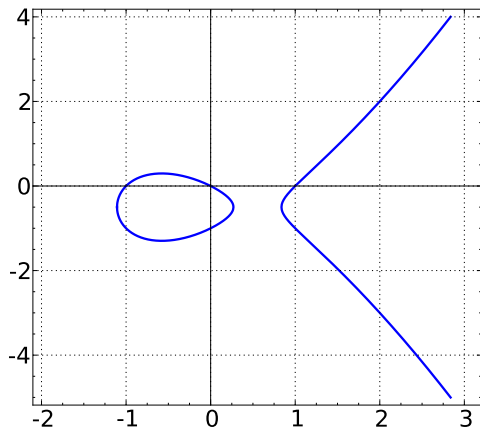
$$x^3 + y^3 = 1 \qquad y^2 + y = x^3 - x$$

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



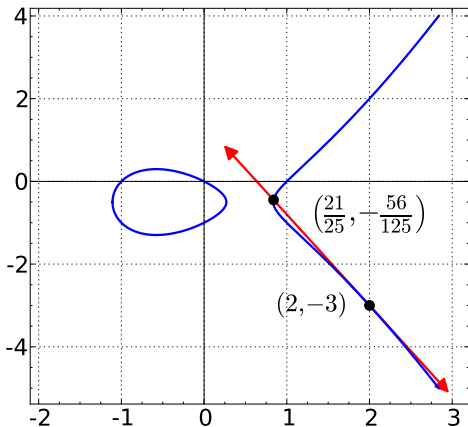
The graph

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



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.

(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, 66316334575107447/238670664494938073)

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

The rank

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

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

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

has $\text{rank} = 0, 1, 2, 3, 4$ for $a = 0, 1, 2, 4, 16$.

The rank is finite



Can it be arbitrarily large?

The current record is $\text{rank}(E) = 28$

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 344816117950305564670329856903907203748559443593191803612660082962919394 48732243429$$

$P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$
 $P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$
 $P_3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$
 $P_4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531]$
 $P_5 = [1534706764467120723885477337, 85429585346017694289021032862781072799531]$
 $P_6 = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]$
 $P_7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931]$
 $P_8 = [1494385729327188957541833817, 88486605527733405986116494514049233411451]$
 $P_9 = [1868438228620887358509065257, 59237403214437708712725140393059358589131]$
 $P_{10} = [2008945108825743774866542537, 47690677880125552882151750781541424711531]$
 $P_{11} = [2348360540918025169651632937, 17492930006200557857340332476448804363531]$
 $P_{12} = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]$
 $P_{13} = [2924128607708061213363288937, 28350264431488878501488356474767375899531]$
 $P_{14} = [5374993891066061893293934537, 286188908427263386451175031916479893731531]$
 $P_{15} = [1709690768233354523334008557, 71898834974686089466159700529215980921631]$
 $P_{16} = [2450954011353593144072595187, 4445228173532634357049262550610714736531]$
 $P_{17} = [296925470927359167464674937, 32766893075366270801333682543160469687531]$
 $P_{18} = [2711914934941692601332882937, 2068436612778381698650413981506590613531]$
 $P_{19} = [20078586077996854528778328937, 2779608541137806604656051725624624030091531]$
 $P_{20} = [2158082450240734774317810697, 34994373401964026809969662241800901254731]$
 $P_{21} = [2004645458247059022403224937, 48049329780704645522439866999888475467531]$
 $P_{22} = [2975749450947996264947091337, 33398989826075322320208934410104857869131]$
 $P_{23} = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]$
 $P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931]$
 $P_{25} = [2773931008341865231443771817, 12632162834649921002414116273769275813451]$
 $P_{26} = [2156581188143768409363461387, 35125092964022908897004150516375178087331]$
 $P_{27} = [3866330499872412508815659137, 121197755655944226293036926715025847322531]$
 $P_{28} = [2230868289773576023778678737, 28558760030597485663387020600768640028531]$



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

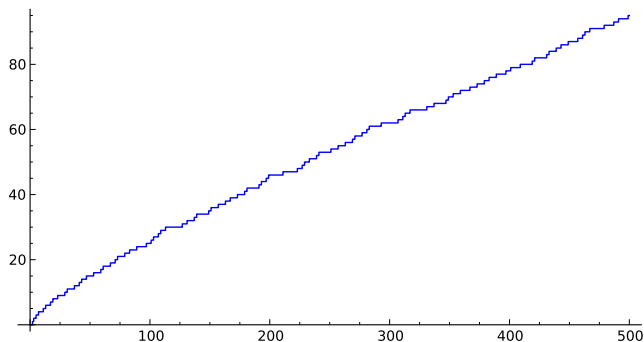


Primes

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.



The Prime Number $2^{9689} - 1 =$

478220278805461202952839298660005909741497172402236500851334510991837895094266297027892768
611270789458682472098152425631930658505267683408748083442943326479742589324762368833102163
320895484735480579994334130982598901374380618710958104314868081377832153049671560156328262
441404039814320762203627219040859079053720347525610556407157926386787524098557335652265610
854212857732105787905232886503535587361567936365588992571157442015383209175242284304691881
142740066213555930351685370397681268638575037622778794958058208183126172570100349820651232
982767723348951095346937568303703837399969677158578890563911552261340549570718452415821920
822376644205901459333065700972215396237685342377048613857808977562130116781129916640736174
660669780818675796691467124607371290420058840892318638773788767529288695379706698096740605
353012285353903696549022478492464900795489867850331465554647550450168618735486696437455261
412064078294962245202778896213860266593314768769632208950427879162465151931232783175655377
937719452467339581928148666857638401959072017941334958297031939388438881049454604034208753
563628321520731816143007176937142623851754052084521466531330118355196259184955893849902
5348780376716477073930634436840084468255937443451690315999349137664638968972614119901530490
654781905622717122494707073971630095377574344130792050186353223446654564569577433188504497
825014866346737213039209989485214519099823287877248665051301081676990289251871925006694721
570653621624869624056925686555429622155221156042777866254593699880107018616260147647429345
983018365127336346273267588306701014035925482914977433929717368076561095959991130918978823
8350131635672661435969218239977196933874395403996623765580528221120713639637085805605116078
177098545257698803233381293927275210194462952749031383555198519709592888523641530178921867
514101454120309619127093436903952209828031766894206132557234964363840305648734929088422378
629288747223121903238528103409182430661894774072726552428489330447486145494207679904173944
716583828167141043583120679050191452732628737033997470720601688256282740427017032260672798
034437932642573009183981307771932245539476396060658821432660315614149074055769805516626304
444758375671151649018119344223685942415184379538933576543212994405485534515585927342456182
514681371472060628778102124092370802149229834963517952727030296297015692768651163505008040
728267425236264469571076976886613730278931360967438271901738550848466337347612084356798306
505955807293511063754424080735066708298723377976887493898358452309563899612061631863439196
711208646438464947096323007272920091258614726799976249670985276950353573392441620265772074
12486835922028289833111408339233024339177979769903114258436193509367544838119440881276338
808420445180491245438388418080094527562666805762895476338464130510775377324708249580453335
571748196502507081973046642282610569751056428979895118219288597635222905389894873761464213
9910911535864505818992696826225754111

Primality testing

Determining that $n > 1$ is a prime can be done quickly.

"PRIMES is in P"

AKS: Manindra Agrawal, Neeraj Kayal, and Nitin Saxena (2002)

If n fails the primality test, it is more difficult to factor it.

123018668453011775513049495838496272077285356959533
479219732245215172640050726365751874520219978646938
995647494277406384592519255732630345373154826850791
702612214291346167042921431160222124047927473779408
0665351419597459856902143413 = RSA-768 =

334780716989568987860441698482126908177047949837137
685689124313889828837938780022876147116525317430877
37814467999489

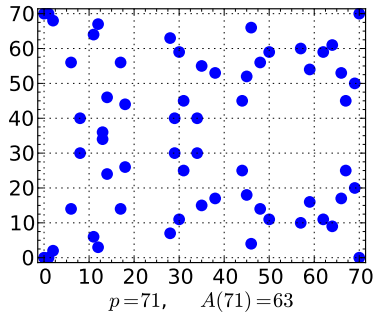
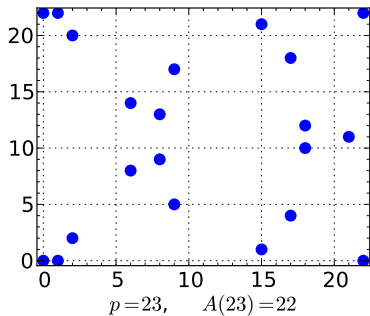
×
367460436667995904282446337996279526322791581643430
876426760322838157396665112792333734171433968102700
92798736308917

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 .



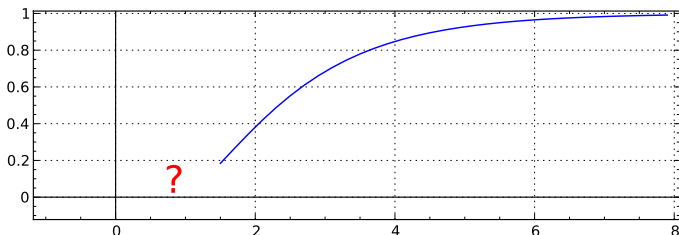
It is common to write

$$A(p) = p + 1 - a(p)$$

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

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

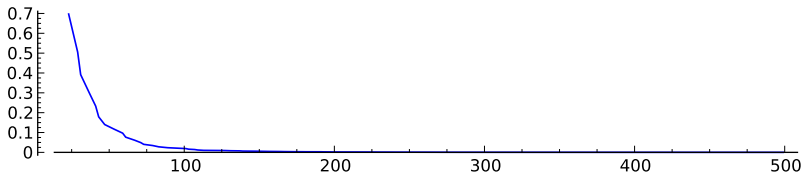
This definition only works in the region $s > 3/2$, where the infinite product converges.



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

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

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.

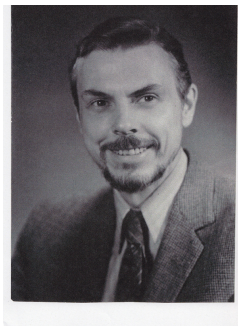


The conjecture of Birch and Swinnerton-Dyer

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 .

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

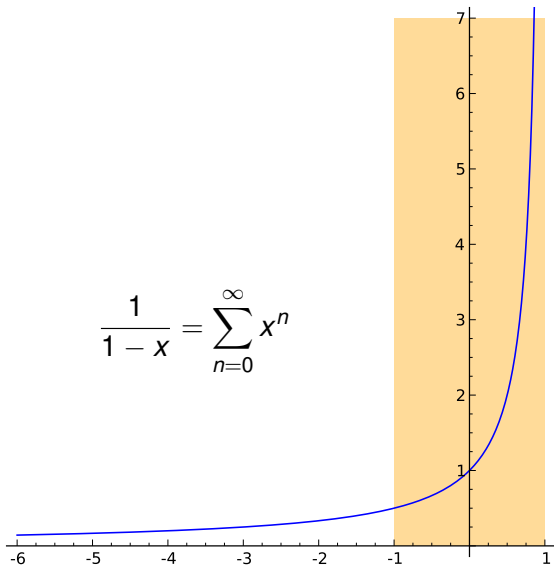
The most mysterious arithmetic invariant was studied by John Tate and Igor Shafarevich, who conjectured that it is finite. Tate called this invariant III.



Natural (analytic) continuation

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

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



The natural (analytic) continuation of $L(E, s) = \sum a(n)n^{-s}$ was obtained 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 I proved with 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 III is finite.



When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general. . .

But the computer has been a great guide.

Here is a summary of the evidence for the simplest rank 2 curve

$$y(y + 1) = x(x - 1)(x + 2)$$

- ▶ the order of vanishing is equal to 2
- ▶ most primes up to 50,000 do not divide the order of III



The average rank

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



Enumerating the curves

- ▶ Every such curve has a unique equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers (not divisible by p^4 and p^6 , for any prime p).
- ▶ Define the height $H(E)$ as the maximum of the positive integers $|A|^3$ and $|B|^2$.
- ▶ For any positive real number X , there are only finitely many curves with $H(E) \leq X$.
- ▶ Call this number $N(X)$. It grows at the same rate as $(X)^{1/2}(X)^{1/3} = X^{5/6}$.

- ▶ Define the average rank by the limit as $X \rightarrow \infty$ of

$$\frac{1}{N(X)} \sum_{H(E) \leq X} \text{rank}(E)$$

- ▶ We suspect that this limit exists, and is equal to $1/2$.
- ▶ In fact, we think that on average half the curves have rank zero and half have rank one.
- ▶ Bhargava and Shankar have shown why there is an upper bound on the limit, and have obtained a specific upper bound which is less than 1.

Thank you

