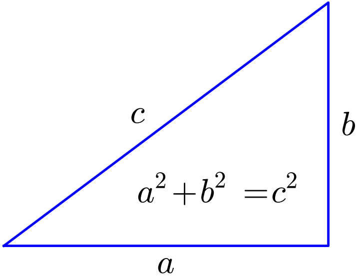
Solving Cubic Equations

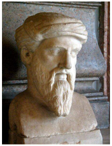
Benedict Gross and William Stein

January, 2012

Algebraic equations



$$a^2 + b^2 = c^2$$

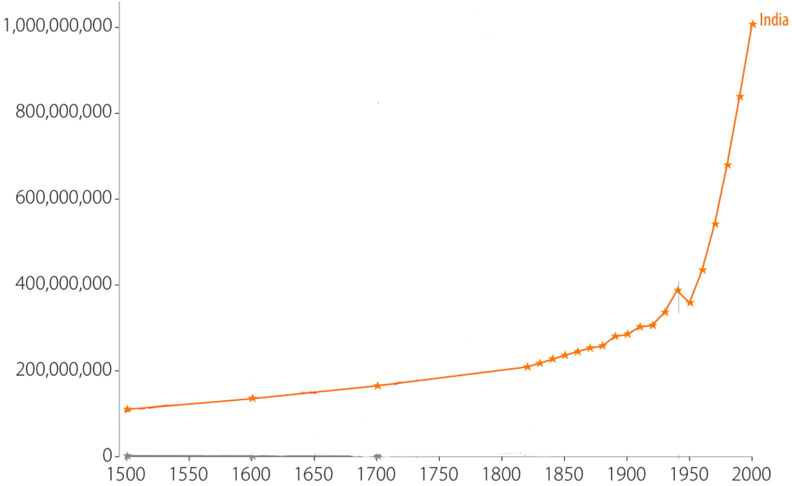


Pythagoras (600 BCE)   Baudhāyana (800 BCE)

Differential equations

$$F'(T) = F(T) \qquad dF/dT = F \qquad F(0) = 1$$

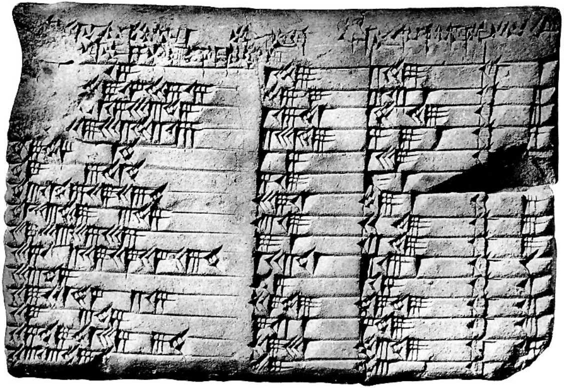
$$F(T) = exp(T) = 1 + T + T^2/2 + T^3/6 + T^4/24 + T^5/120 + \ldots$$



Pythagorean triples

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

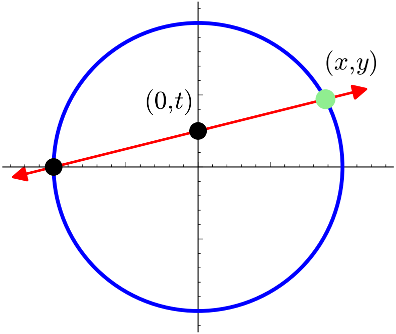
There are more solutions on a Babylonian tablet (1800 BCE):



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

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

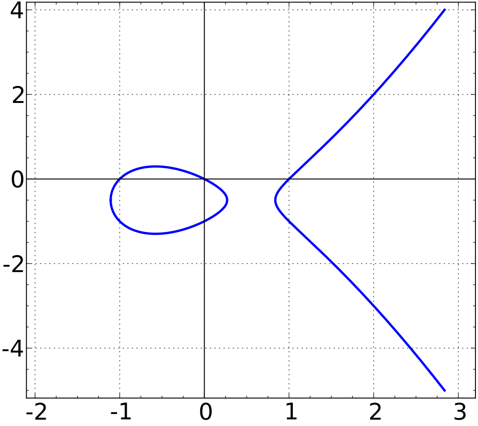
After linear and quadratic equations come cubic equations, like

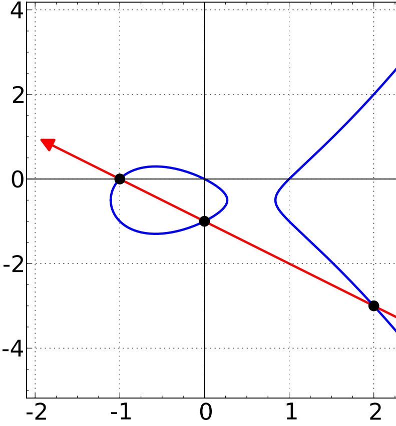
$$x^3 + y^3 = 1 \qquad\qquad y^2 + y = x^3 - x$$

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

The graph

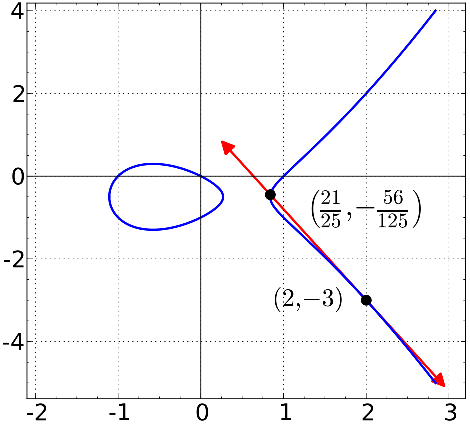
$$y^2 + y = x^3 - x$$





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, 66316334575107447/238670664494938073)
```

Even the simplest solution can be large

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

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

```
36777053718667750661400564234182717008793226949228558472621877006165354634927101580536513437032674306114130646450005288670465199839976647884079191530786174150
72739338026281573250924797082687602171017553858718167805487654785022844156276828471927526818990949626599378706300367603592935770218062374839710749312284163465
07852381696883227650072039964481597215995993299744934117106289850389364006552497835877740257534533113775202882210048356163645919345794812074571029660897173224
37033770105616573500859064029709029870912150626669726646199320182539736999955086814229431275632217741073053282806475960497536924235099356803072693704991160726
41097827468479512837941192989412144907943309029865829912295694015235199387427463761071907702040105138183490127866378892547110594555551738109049119276198990318
55149292325338589831979737026402711049742594116000380601480839982975557506035851728035645241044229165029649347049289119188596869401159325131363345962579503132
33984727542244009455382470518922565367745951286311791172183855293430912450813449336643740809392436203974991190741697350414232211175705858420072502263211616472
01649986417295226774605259994990779421258204288795260637356926859910185168629387960475973239865371541712483169437963732171919939969937146546295368843960579247
90938647656663281596178145722116098216500930333824321806726937018190136190556573208807048355335567078793126656928657859036779350593274598717379730880724034301
86773944374984180945671588419372032890146155265988262840584220975675716781666213994508186464210853359598997571625925924015283405094065447961714768592250085694
44498220453860921224090969785448172188478976405134778065983291776042463808123777390491844755507773416209859765703930378802827649670195524084007307548226764414
81715385344001979832232652414888335865567377214360456003296961668177481944809066257442596772347829664126972931904101685281128944780074646796760942430959617022
25747987408940356496503888537981786692004892981452026849367750705907376590267163808736648849670283632626857459312324510742034887810176312389334765702027559124
88242478005942708620520821859733932900091898676772594580806760650987034535395255769756395437005076256407298723407894063143944684005844559206833619762001218344
30751233901473228497490561998078486251074993528871318797403348087370426900997556442577081254910572185107856605139877331015042842121106080690743578173268489400
49905689831262195394796701235841454775289708109709179574420369768404606625566320124222927601267598712660045163774329619172720402171470835633999876124205952757 9
20338556769918233682548621595584500438080514815332972700352873822470382792932239463850701180823069589872686033969240544031038574440588486055874154005176700326
31121206127732481340391088277796488544415738156553014768406246154666005139690428085145098272500791416214774673484501826722500527091164944262537169595848931680
75409677471286049057274622409403118704320452610723920107960346829752289510659856743701508334879787536416279769396881980413954888575128268715223707826035870523
02844262030644936842506142828799181077337962070672500038239594129356776240932360470386373655773263995890088045077860119731559277310730347065365574614438066227
07622411087809371872157210456836892493613836792026761820382217165481998924123604782787923229739171920575447007099501678380795077013111332598980138572999392081 8
30165442425133956460687682012192837224621339985921328279251116804395344383979390113997419447930029756609766453919938465190843618873242881837330238304638885942
79378938418880142666851776166056447837041357949318307502656863359340665652409440494482130055919971289855607602603992142786359126343515867623548693540215307461
89992899582554597632108309638569296964800046983072736238483149014714600896056552029642747991419063454749142059564274298254654925893866404955146903330024475746
16354371499624965242017117105423172633649354158697143177894405148105963373839941141857432381177094972972684361267292500063135565983416420055444131545100343345
24662047071238116636236628372968629480617587599286317636619851856158018862057707210320063041448677873470583163922956715800916558720872094859132869301288586404
42589125454268580397484571921012318872311624898317615607628176460097441336323549031828235965636277950827328087547939511112374216436584203379248450122647406094
03517113074066372354767593988595936388113589303510201838944421274614625032834824261067352402237899497839202009881472197450206269281573668922975906582209394279
53187053452755989894263352359355056053114113015603211922694308617337435444029085864973053536009094312149332025225287171092144929593300160658102876231441792884
66664888540622702346704213752456372574449563979215782406566937885352945871994541770838871930542220307771671498466518108722622109421676741544945695403509866953
16727762828023246483921500347404889696803754466002975574006558127013908324990321257223041794224979546710070039394431032500967717918210997094334680733501444683
96122825088243240736795841228512083604591663154848919522994493400258965092989359393577217235439331087432419973874470183959253201676376403284079570698454395013
81234605867495003402016724626400855369636521155009147176245904149069225438646928549072337653348704931901764847439772432025275648964681387210234070849306330191
79038041239611544624083258348136637213230084906083526213683231531105290336750385743792050893130528314337942393060136915457253067727886206663888425022179164712
3563828956462530983567929499493346622977494903591722345188975062941907415400740881
```

Denominator:

```
42550442729747398883181472438884631491027966762628698441290370019390690825369783206694892509489159845392479060050865239326960543711865223880415469150998005445
00632766713011953565768977996873028383821265777552634434635712354111258918875514704047199753233382769507221039874750614387085008848063161037557510562940296992 3
37999066968836324267266407778292384246876573476455250148990478999518159066382588282688443761470208660107291246020504671898711119197597417729240821079066147681 88
25928778559738389606781437786937703940490529701550198752240522047885413980183556155907460046868073063343753429797282371426595980125377117083031923094847501187
81539765280348857873798901748823243463804440411715478920014959236515352089221657498291013202443206177483221913021678256235579893414436481218449503035888524081
15740619547664383566612706438064220965934420574805698187965300040168887347070624862281490478227347630906482652560940554823360522517964582349779334663133777009
32389603015388462267191386514299244523629967196928070338170422172904291954458588735666571767269091258248510098997241843386892960591348792269127155872118132361 3
70012052090648575376001600422257728323075912369868818631162455043825487235531941123620115037512323584244014680824673299882453235229917216799756372612183353210
23686195578854195273414555800682053521914530044820400116481027789228810525723047625080568425427769667815771926774952742389468234144023574739674218399717724794
64490794909903308233044977729321377913661153832551845135705059041770761773002335204714530513728518042273513609336859761902134080074259874956489916483283558415
18790233089971640826391421865446416159176533305374315501526687536310287865258225341831409297024404559487986223470061428509852910119956281813557240650373612303
80612421682647619158275971206216911075102110620022250292103973758280786545321293000346117555930108145915118154377991059233962745297863017035414522428825832481
10185696903019214515170137956322244850592956107013529355675348962971488951184208519602258834025155300581173742601529286315229193789791848640470464974617150056
62259748200507982418704000034189585130679648460399502892795419432308411176961777683169393789440445404586765622160449971094877274592261820143359041089932670055
51298147417813688141747600315791793741837036656460760259084286414504016916928653373373749351673138873697355678073568445462500597124999569428768348290694470131
39695758671845345053150692524956190311186650121760981782607840168999098928254294766906595754090551526543788821211073870016226804688310128261364457467501381181
99895452299627549452761944871112397182275542812517516928333071853473496479471177747458859446909439927856630115032721992970283594818637110287101947829555604104 9
94569790530090215161267032801442076978425884340578290684944705663842203873434946895313693410268205549042641332729214043530781277783400932521461065846050516266
06369309829333522153142406896441472229879201250507247335030253750414919268086142811991181135615102063450273874178955396056033628717223631646597545299321971795
72083803798469762841343018748973041067954703588990548236248494723651739045289521882710298950201026345472967707812057733059495444795253020394607206147343184720
12891382027947113716845979329657679391121796342422193808825527319590678236462421470515380610223708802325911166125101655807805544810736511736112015725788207983
04346277884275334856562425654767711062666450533897646444735950588164991426098055565123345308087041154716116620172732104619949757331380529168978624213449372249 3
65401328137208190879603847948651527305255579241209808589941796218972732173245666604083232319661488118850875263706392263572172788858886100669706729508266285662 1
42789555098127098307594733822740958886080483268977873098575694622813361281769384832759774254005221673936338256702877699726892622342424638164907882484814569895
78820841326437902307074825587297298227228464352952356348415245051280414970934534815003363838566586486090914244124413024752619262170944161605020754084937204942
16372326712489077723971624589353187301664632745253191939259669507578605710768387023661969449344902879751178806889386035847044662250758843856626244205371560027
87345086683247957409590801131490445553949472979089821198999392392205812011786324196553409374966862790769096287105922007091926687147181741236537543028535996580
45947455276513698860733871942939615110361783065380776837197220049720205456646520373809780940384932684877526623946791294274354580233914301360048309031821084423
72425264218315757261837807638185861100198403815128178367563386992036547922694358498639362771798041618046013662235878191246173024597377861825966407677879013966
44826035500413324947183241852334621567713018309711089099896390758911615128829646468875441800478905861321031022715201049054765075321382013759982613256651365903
08677310205945594774669134858545209082084155986593443637589125910770359979110742764732875552438147802286623083638506353523937829379144982925749510228726599819
64923226850485187083410037527178126285256712196330538305579411947408618370648081044119314858092966789985880558618838749736465935723939056195292855739824197002
85747166387929856818643218648078765165327952717275940366217333921605018810173490426678520993395921957402807842113084883601771499771585515616148588419257652541
10965702365800067847782401155042150831554731114336654532035309712573054076300648084290382624057963622411854452712766764333742741748257176418629938669049475110 1
4583148762951888762273247975157547523726572052209999592135037352690220398771 6.
```

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) = 28

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629193948 7322434 29$$

$P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$

$P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$

$P_3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$

$P_4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531]$

$P_5 = [1534706764467120723885477337, 85429585346017694289021032862781072799531]$

$P_6 = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]$

$P_7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931]$

$P_8 = [1494385729327188957541833817, 88486605527733405986116494514049233411451]$

$P_9 = [1868438228620887358509065257, 59237403214437708712725140393059358589131]$

$P_{10} = [2008945108825743774866542537, 47690677880125552882151750781541424711531]$

$P_{11} = [2348360540918025169651632937, 17492930006200557857340332476448804363531]$

$P_{12} = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]$

$P_{13} = [2924128607708061213363288937, 28350264431488878501488356474767375899531]$

$P_{14} = [5374993891066061893293934537, 286188908427263386451175031916479893731531]$

$P_{15} = [1709690768233354523334008557, 71898834974686089466159700529215980921631]$

$P_{16} = [2450954011353593144072595187, 4445228173532634357049262550610714736531]$

$P_{17} = [2969254709273559167464674937, 32766893075366270801333682543160469687531]$

$P_{18} = [2711914934941692601332882937, 2068436612778381698650413981506590613531]$

$P_{19} = [20078586077996854528778328937, 279608541137806604656051725624624030091531]$

$P_{20} = [2158082450240734774317810697, 34994373401964026809969662241800901254731]$

$P_{21} = [2004645458247059022403224937, 48049329780704645522439866999888475467531]$

$P_{22} = [2975749450947996264947091337, 33398989826075322320208934410104857869131]$

$P_{23} = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]$

$P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931]$

$P_{25} = [2773931008341865231443771817, 12632162834649921002414116273769275813451]$

$P_{26} = [2156581188143768409363461387, 35125092964022908897004150516375178087331]$

$P_{27} = [3866330499872412508815659137, 121197755655944226293036926715025847322531]$

$P_{28} = [2230868289773576023778678737, 28558760030597485663387020600768640028531]$

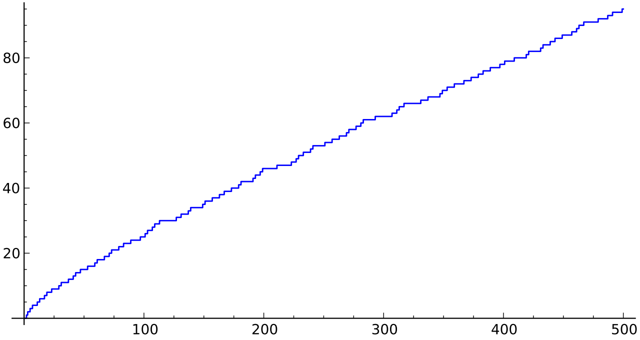
Bryan Birch and Peter Swinnerton-Dyer made a prediction for the rank, based on the average number of solutions at prime numbers *p*.

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
987267723348951095346937568303703837399969677158578890563911552261340549570718452415821920
822376644205901459333065700972215396237685342377048613857808977562130116781129916640736174
660669780818675796691467124607371290420058840892318638773788767529288695379706698096740605
353012285353903696549022478492464900795489867850331465554647550450168618735486696437455261
412064078294962245202778896213860266593314768769632208950427879162465151931232783175655377
937719452467339581928148666857638401959072017941334958297031939388438881049454604034208753
656362833215207318161430072176937142623851754052084521466531330118355196259184955893849902
534878037671647707393063443684008446825593744345169031599934913766463896897261419901530490
654781905622717122494707073971630095377574344130792050186353223446654564569577433188504497
825014866346737213039209989485214519099823287877248665051301081676990289251871925006694721
570653621624869624056925686555429622155221156042777866254593699880107018616260147647429345
983018365127336346273267588306070141035925482914977433929717368076561095959991130918978823
835013163567266143596921823997719693387439540399662367558052821120713639637085805605116078
177098545257698803233381293927275210194462952749031383555198519709592888523641530178921867
514101454120309619127093436903952209828031766894206132557234964363840305648734929088422378
629288747223121903238528103409182430661894774072726552428489330447486145494207679904173944
716583828167141043583120679050191452732628737033997470720601688256282740427017032260672798
034347932642573009183981307771932245539476396060658821432660315614149074055769805516626304
444758375671151649018119344223685942415184379538933576543212994405485534515585927342456182
514681371472060628778102124092370802149229834963517952727030296297015692768651163505008040
728267425236264469571076976886613730278931360967438271901738550848466337347612084356798306
505955807293511063754424080735066708298723377976887493898358452309563899612061631863439196
711208646438464947096323007272920091258614726799976249670985276950353573392441620265772074
124868359220282898331114083392330243391779797699031142584361935093675448381119440881276338
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 $=$

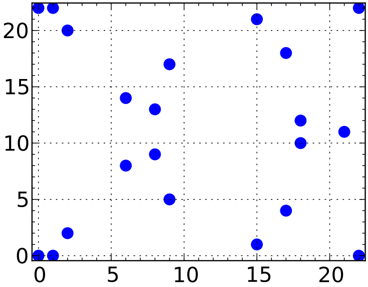
334780716989568987860441698482126908177047949837137
685689124313889828837938780022876147116525317430877
37814467999489
×
367460436667995904282446337996279526322791581643430
876426760322838157396665112792333734171433968102700
92798736308917

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

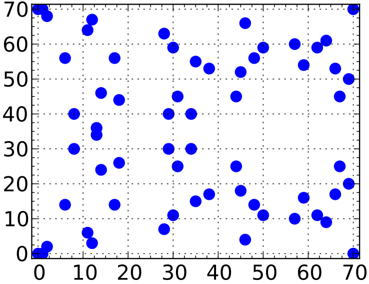
$$y^2 + y = x^3 - x$$

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

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



$p = 23, \quad A(23) = 22$



$p = 71, \quad A(71) = 63$

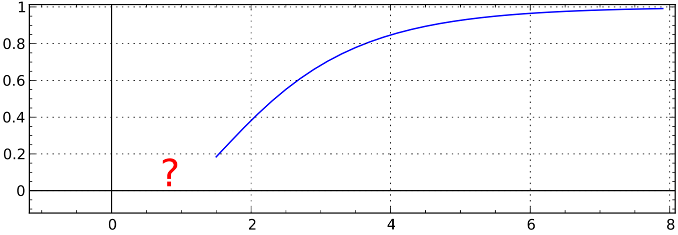
It is common to write

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

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

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

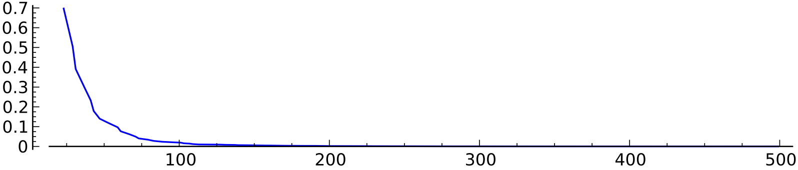
This definition only works in the region $s > 3/2$, where the infinite product converges.



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.

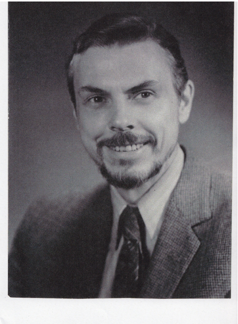


The conjecture of Birch and Swinnerton-Dyer

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.

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

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



The Birch and Swinnerton-Dyer Conjecture

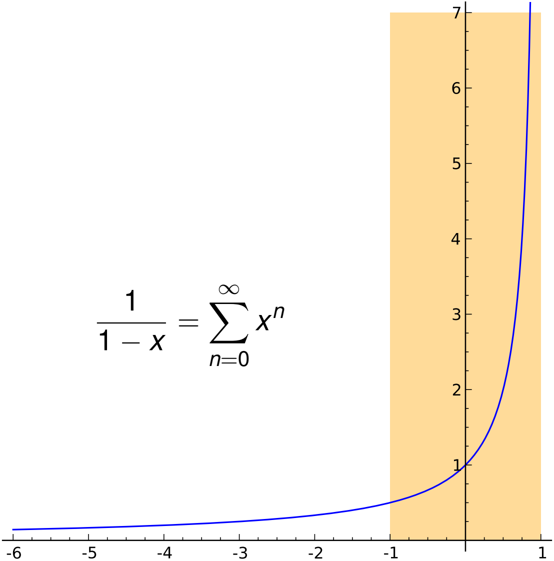
$$L(E,s) = c(E)(s-1)^{\mathrm{rank}(E)} + \cdots$$

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

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 $-1 < x < 1$.



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

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 Ш 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.

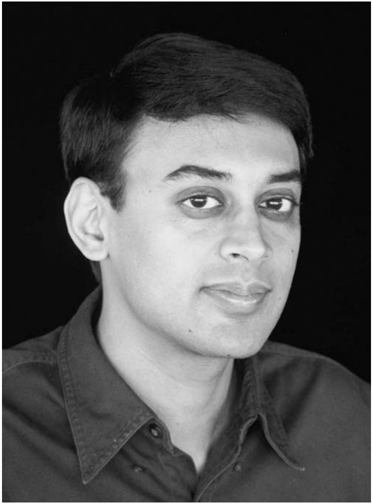
Here is a summary of the evidence for the simplest rank 2 curve

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

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

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 $X \to \infty$ of

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

- 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