RANK OF ELLIPTIC CURVES AND THE BIRCH SWINNERTON-DYER CONJECTURE

J. HSU, S. MILLER

Department of Mathematics
Princeton University

Abstract. We numerically verify the Conjecture of Birch and Swinnerton-Dyer concerning the analytic and geometric rank of an elliptic curve. An algorithm (based on the work of Cremona) is developed in the PARI/GP language for computing the order of vanishing of the L-function for any (non-singular) curve. The analytic rank outputs for several families of curves are compared with readily available data on geometric ranks. Some related results on excess rank are also presented.

1. Introduction

The conjecture of Birch and Swinnerton-Dyer relating the analytic and geometric rank of an elliptic curve is perhaps one of the less debated and widely accepted conjectures in the field. The conjecture is now known to hold for elliptic curves with rank 0 and 1 due to the work of Kolyvagin in 1990. Nevertheless, the general case still remains to be proved (or disproved) after it's first proposal in 1965 [3].

In this project we study the analytic ranks of one-parameter families with forced rank over the rational numbers. In particular, an algorithm is developed to calculate the order of vanishing of the L-function associated to an elliptic curve. The results can then be compared with data of geometric ranks of the same curves in verification of the Birch and Swinnerton-Dyer conjecture.

2. Generalities

A polynomial relation $f(x, y) = 0$ in two variables defines a curve, and the general cubic curve is of the form:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{2.1}$$

If all the coefficients are rational numbers then the cubic is said to be rational. In particular, (non-singular) rational cubic curves can be transformed into a simpler and more manageable form using suitable change of variables and some projective geometry [9]. This is the Weierstrass normal form, generally expressed as $y^2 = x^3 + ax^2 + bx + c$. If the discriminant $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ is non-zero then the curve is an elliptic curve[1]. Instead of completing the square and changing variables fully, we can also write the elliptic curve in the alternate form[2]

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

and many computational programs takes the 5-component vector $[a_1, a_2, a_3, a_4, a_6]$ as the representation of the curve.

We will restrict our investigation to rational elliptic curves, where we can ask for rational solutions to a curve. The set of all such points for an elliptic curve E will be denoted $E(\mathbb{Q})$.

3. Defining the L-function for elliptic curves

We begin by recalling the Riemann zeta function defined by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Using the theorem of unique factorisation and some elementary analysis [7] one can show that an equivalent form for the function is $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ where the product is over all positive primes p. This is the form we will use.

If we restrict an elliptic curve E to a finite field of integers modulo p (prime) $\mathbb{F}_p$, then it is known that $\#\{E(\mathbb{Q}) \mod p\} = p+1-a_p$, where $a_p \leq 2\sqrt{p}$ is a result due to Hasse. With this definition we can defined a local zeta function for the elliptic

[1]The more familiar case is when $a = 0$, $\Delta = -4b^3 - 27c^2$.

[2]See Appendix A

curve reduced modulo p

$$\zeta(E_p, s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})} \tag{3.1}$$

which reduces to $\zeta(E_p, s) = \frac{1}{(1-p^{-s})(1-p^{1-s})}$ if $p \mid \Delta$. The global zeta function is simply defined as the product of local zeta functions over all primes: $\zeta(E, s) = \prod_p \zeta(E_p, s)$. It is easy to see that $\zeta(E, s) = \zeta(s)\zeta(s-1)L(E, s)^{-1}$ if

$$L(E, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1} \tag{3.2}$$

We will take this as the definition for the L-function associated with an elliptic curve. This product converges for $\Re(s) > \frac{3}{2}$ and can be analytically continued [7] to all of $\mathbb{C}$. Thus we can speak of the behaviour of the function at $s = 1$. If the order of vanishing[3] of $L(E, 1)$ is r, then we say the elliptic curve E has analytic rank r and we denote it r_a.

We are now ready to state the conjecture of Birch and Swinnerton-Dyer.

4. The Birch and Swinnerton-Dyer Conjecture

By the theorem of Mordell, it is known that for an elliptic curve E over the rationals $\mathbb{Q}$, the set $E(\mathbb{Q})$ is finitely generated. More explicitly:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbf{T} \tag{4.1}$$

for some non-negative integer r, and $\mathbf{T}$ a finite abelian group. The integer r is called the geometric rank of E, and we shall denote it r_g.

The Birch and Swinnerton-Dyer Conjecture can then be stated simply as: for any elliptic curve E over $\mathbb{Q}$, the analytic and geometric rank equal[4]; that is, $r_a = r_g$. An equivalent way of stating the conjecture is as follows: the Taylor expansion of $L(E, s)$ about $s = 1$ has the form

$$L(E, s) = c(s-1)^r + \text{higher order terms}$$

with $c \neq 0$ and $r(= r_a) = r_g$.

5. Modular forms

The algorithm used for computing the analytic rank of elliptic curves requires the theory of modular functions, we describe some basic properties of these functions before we discuss the algorithm itself.

Consider the upper half complex plane; that is the set of complex numbers z with $\Im(z) > 0$. For a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$; $a, b, c, d \in \mathbb{Z}$ and $\det \gamma = 1$, define its action on a complex number z as $\gamma z = \frac{az+b}{cz+d}$. Note that

$$\Im(\gamma z) = \frac{\Im(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{\Im(adz+bc\overline{z})}{|cz+d|^2} = \frac{\Im(ad-bc)iy}{|cz+d|^2} = \frac{\Im(z)}{|cz+d|^2}$$

[3] That is if $L^{(r)}(E, 1) \neq 0$ but $L^{(k)}(E, 1) = 0 \ \forall k < r$.

[4] A weaker form of the conjecture states that $r_a = r_g \mod 2$, but we shall only consider the general case.

Thus $\Im(z) > 0 \Rightarrow \Im(\gamma z) > 0$.

A function f is said to be modular of weight $2k$ if it satisfies the relation

$$f(\gamma z) = (cz + d)^{-2k} f(z) \tag{5.1}$$

In particular, it is called a modular form if the function is holomorphic everywhere. An important property of modular functions is the existence of a fundamental domain for the group of matrices acting on the half plane. This is the region above the semi-circle $x^2 + y^2 = 1$ bounded on the left by $x = -\frac{1}{2}$ and on the right by $x = \frac{1}{2}$ [8]. Under the action of the two matrices $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ every point on the complex half plane can be transformed into the fundamental domain. It is easily seen that $Tz = z + 1$ and $Sz = -\frac{1}{z}$.

Two properties following immediately from the definitions above are:

$$\begin{aligned} f(z+1) &= f(Tz) = f(z) \\ f(-1/z) &= f(Sz) = z^{2k} f(z) \end{aligned} \tag{5.2}$$

The first relation implies the periodicity of f, and therefore we can express a modular form as a series $f(z) = \sum_{n=0}^{\infty} a_n \exp(2\pi i n z)$ which converges for all z in the upper half complex plane and satisfies the identity as given in the second relation. It is called a cusp form if $a_0 = 0$.

6. Evaluating $L(E, 1)$

Due to the work of Taylor-Wiles and Wiles, it is now known that all elliptic curves are modular. Hence all the properties mentioned in the previous section are valid for elliptic curves. We will derive an explicit expression for $L(E, 1)$ in this section; the method used for higher derivatives is a generalisation of this technique and will be addressed in the following section.

Since an elliptic curve E is modular, we can express it as a series

$$f(iy) = \sum a_n \exp(-2\pi n y) \tag{6.1}$$

which can then be used for the Mellin transform[5] as follows:

$$\begin{aligned} \int_0^\infty f(iy) y^{s-1} dy &= \sum a_n \int_0^\infty \exp(-2\pi n y) y^{s-1} dy \\ &= \sum a_n \int_0^\infty \exp(-t)(2\pi n)^{-s} t^{s-1} dt \\ &= (2\pi)^{-s} \sum a_n n^{-s} \int_0^\infty \exp(-t) t^{s-1} dt \\ &= (2\pi)^{-s} L(E, s) \Gamma(s) \end{aligned} \tag{6.2}$$

where $\Gamma(s) = \int_0^\infty \exp(-y) y^{s-1} dy$ is the usual gamma function defined for all complex numbers. Now modular forms satisfy $f(-\frac{1}{Nz}) = \omega N z^2 f(z)$ with $\omega = \pm 1$ and

[5]Using the substitution $t = 2\pi n y$.

we can evaluate the integral in two parts and apply this equality.

$$\begin{aligned}(2\pi)^{-1}\Gamma(1)L(E,1) &= \int_0^\infty f(iy)dy \\ &= \int_0^{1/\sqrt{N}} f(iy)dy + \int_{1/\sqrt{N}}^\infty f(iy)dy \\ &= \int_{1/\sqrt{N}}^\infty f(iy)dy + \int_0^{1/\sqrt{N}} f(i/Nt)(-1/Nt^2)dt \\ &= \int_{1/\sqrt{N}}^\infty f(iy)dy + \omega\int_{1/\sqrt{N}}^\infty f(it)dt \\ &= (1+\omega)\int_{1/\sqrt{N}}^\infty f(iy)dy \\ &= (1+\omega)\left[\sum \frac{a_n\exp(-2\pi ny)}{-2\pi n}\right]_{1/\sqrt{N}}^\infty\end{aligned} \tag{6.3}$$

So we have the following explicit expression for $L(E,1)$:

$$L(E,1) = (1+\omega)\sum_{n=1}^\infty \frac{a_n\exp(-2\pi n/\sqrt{N})}{n} \tag{6.4}$$

7. Computing derivatives of the L-function

Define the Mellin transform $\int_0^\infty f(iy/\sqrt{N})y^{s-1}dy = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s)$ as a function of f and s, which we denote $\Lambda(f,s)$. For any elliptic curve E, this satisfies the functional equation

$$\Lambda(E,s) = \omega(-1)^k\Lambda(E,k-s) \tag{7.1}$$

for $\omega = \pm 1$. (A specific case of this is $\Lambda(E,s) = \omega\Lambda(E,2-s)$.) If $\omega = -1$ we say the sign of the functional equation is odd, and it is even otherwise. It is known that the parity of the analytic rank of an elliptic curve is the same as that for the functional equation. This is particularly useful as we only need to compute the odd/even derivatives of the L-function in calculating r_a for odd/even sign.

We now generalise the integral transforms for derivatives of the L-function. As before, we split the integral into two parts and re-combine to obtain a single integral over a slightly different interval:

$$\begin{aligned}\Lambda(f,s) &= \int_0^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_0^1 f(iy/\sqrt{N})y^{s-1}dy + \int_1^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_\infty^1 f(iy/\sqrt{N})cy^{1-s}dy + \int_1^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_1^\infty f(iy/\sqrt{N})(y^{s-1} - cy^{1-s})dy\end{aligned} \tag{7.2}$$

Differentiating k times with respect to s gives

$$\Lambda^{(k)}(f,s) = \int_1^\infty f(iy/\sqrt{N})(\log y)^k(y^{s-1} - c(-1)^k y^{1-s})dy \tag{7.3}$$

and at $s = 1$ this simplifies to $\Lambda^{(k)}(f,1) = (1-(-1)^k c)\int_1^\infty f(iy/\sqrt{N})(\log y)^k dy$.

Since the analytic rank r_a is defined as the order of the vanishing of the L-function, it is clear that we need only to consider the case which yields a non-zero value.

$$\Lambda^{(k)}(E,1) = 2\sum_{n=1}^\infty a_n \int_1^\infty \exp(-2\pi ny/\sqrt{N})(\log y)^k dy \tag{7.4}$$

Notice that for $k = 0$ this is equivalent to the expression for $L(E,1)$ we obtained in the previous section since $\Lambda(E,1) = (\sqrt{N}/2\pi)L(E,1)$.

For $k \geq 1$ we can use integration by parts and get

$$\Lambda^{(k)}(f,1) = \frac{\sqrt{N}}{\pi}\sum_{n=1}^\infty \frac{a_n}{n}\int_1^\infty \exp(-2\pi ny/\sqrt{N})(\log y)^{k-1}\frac{dy}{y} \tag{7.5}$$

and obtain the explicit expression for $L^{(r)}(E,1)$ as follows:

$$L^{(r)}(E,1) = 2r!\sum_{n=1}^\infty \frac{a_n}{n} G_r\left(\frac{2\pi n}{\sqrt{N}}\right) \tag{7.6}$$

where $G_r(x) = \frac{1}{(r-1)!}\int_1^\infty \exp(-xy)(\log y)^{r-1}\frac{dy}{y}$.

We can therefore compute the derivatives of the L-functions provided we can compute the functions $G_r(x)$. For the case of $r = 1$ it is simply an exponential integral and we have

$$G_1(x) = \log\frac{1}{x} - \gamma - \sum_{n=1}^\infty \frac{(-x)^n}{n!n} \tag{7.7}$$

where $\gamma = 0.577216$ is the Euler constant. The general case can be obtained by using the relation $G_0(x) = \exp(-x)$ and $G_r'(x) = P_r(\log\frac{1}{x}) + \sum_{n=1}^\infty \frac{(-x)^{n-r}}{n!n^r}$ where P_r is the r-degree polynomial satisfying $P_r'(t) = P_{r-1}(t)$ and $P_0(t) = 0$.

These are precisely the functions we construct in the algorithm, the values for which can be calculated to very high precisions. The sign of the functional equation can be easily obtained, and we can then proceed to calculate the odd/even degrees of the derivatives. The number of terms considered in these summations varies depending on the elliptic curve, and is of order $\sqrt{N}$ where N is the conductor of the curve. The tolerance for determining whether $L(E,1) = 0$ was set at $|0.001|$ which seems to work quite well in practice, as any non-zero values are very large in comparison. The analytic rank is computed as the order at which the sequence of odd/even derivatives does not vanish.

8. Results

The program was first tested with 4 curves of known geometric rank:

$E_1, r_g = 3$: $y^2 + y = x^3 - 7x + 6$
$E_2, r_g = 4$: $y^2 + xy = x^3 - x^2 - 79x + 289$
$E_3, r_g = 5$: $y^2 + y = x^3 - 79x + 342$
$E_4, r_g = 6$: $y^2 + xy = x^3 - 7077x + 235516$

All of them returned the same analytic rank as outputted from the computation.

Two other curves of known geometric rank was also tested much later (due to the time consuming nature of the computations for curves with large conductor):

$E_5, r_g = 7$: $y^2 = x^3 - 12979x + 405826$
$E_6, r_g = 8$: $y^2 = x^3 - 14752493461692x$

Once again, the analytic and geometric ranks agree.

We then proceeded to investigate one-parameter families of elliptic curves; in particular those with forced rank[6] over $\mathbb{Q}(t)$. Three families were tested, as follows:

$E_1(t), r = 2$: $y^2 = x^3 - t^2x + t^4$
$E_2(t), r = 3$: $y^2 = x^3 + 5x^2 - 16t^2x + 64t^2$
$E_3(t), r = 4$: $y^2 = x^3 + 41x^2 + (184 - 16t^2)x + 144$

Among them, those particular curves within each family with analytic rank smaller than the forced rank is selected and ran through another program to search for rational points and determine if they are linearly dependent. Since there are no readily available data on the geometric rank of the curves in these families only the exceptional cases have been used in the verification of the Birch and Swinnerton-Dyer conjecture.

We summarise the distribution of the (analytic) ranks in the following tables.

The first 300 members in $E_1(t)$, $t > 0$

Analytic Rank	Number of Curves
0	0
1	1
2	112
3	156
4	31

The first 100 members in $E_2(t)$, $t > 0$

Analytic Rank	Number of Curves
0	0
1	1
2	4
3	38
4	53
5	4

[6]See Appendix C

The first 50 members in $E_3(t)$, $t > 0$

Analytic Rank	Number of Curves
0	0
1	0
2	3
3	6
4	30
5	10
6	1

A family of rank 0 over $\mathbb{Q}(t)$; $y^2 = x^3 + t$; was also tested, and provided the largest number of raw data. However, a large proportion of the curves in this family have analytic rank 0 or 1, for which the BSD conjecture is already known to be true. Nonetheless, there are quite a number of curves with rank 2 or 3; for which comparison with known data on geometric rank once again confirms the validity of the conjecture.

Rank distribution for $y^2 = x^3 + t$, $t = 1 \ldots 1000$ and $t = -1 \ldots -1000$

Analytic Rank	Number of Curves
0	690
1	965
2	314
3	31

Computations have also been performed for a number of families presented by Fermigier, and all the families tested reaffirm the results published [5]. The families tested are:

Forced Rank	Curve $E(t)$	Values of $t \in \mathbb{Z}$
$r = 0$	$y^2 + y = x^3 + x^2 + x + t$	$-363 \ldots 612$
$r = 0$	$y^2 + xy + 3y = x^3 + tx + 1$	$-150 \ldots 105$
$r = 0$	$y^2 + xy - 2y = x^3 + tx + 1$	$-94 \ldots 183$
$r = 0$	$y^2 + xy + y = x^3 + 2x + t$	$-244 \ldots 576$
$r = 1$	$y^2 + xy + 3y = x^3 + x^2 + tx$	$-131 \ldots 295$
$r = 2$	$y^2 + xy + 7y = x^3 + tx^2 + (-t - 1)x$	$-220 \ldots 368$

9. Technicalities and developments

Since the program is written in the PARI/GP language, it runs slower in comparison to an identical program written in C developed independently in a similar project. Nevertheless, the two programs concur on the analytic rank of all the curves tested; a result which is rather reassuring. The lengthy run-time for curves with high conductor remains problematic for rapid generation of data, and one possible improvement would be to calculate and store all the a_n values in a database in advance and have the program read off values instead of recalculating during each computation.

It is possible, even desirable, to incorporate this program with one which calculates the geometric rank of a given elliptic curve. That way, we can readily verify the Birch and Swinnerton-Dyer conjecture for large number of curves in a family.

Yet another possible use of the program would be in the study of the Gross-Zagier formula relating $L'(E,1)$ to the height of Heegner points on an elliptic curve:

$$\exists \varepsilon \ni L'(E,1) = \varepsilon h(x_E)$$

where $h(x)$ is the canonical height of a point and x_E a Heegner point. Last but not least, as mentioned before, it can be useful for investigations on excess rank for families of curves.

Appendix A. Weierstrass normal form

We outline here the steps in arriving at the Weierstrass normal form of a cubic curve. Begin with a cubic curve C in the projective plane and assume a rational point O_a on C is given. Take $Z = 0$ to be the tangent line to C at O_a. This line intersects C at one other point O_b, and take the $X = 0$ axis to be the tangent to C at O_b. Finally choose $Y = 0$ to be any line except $Z = 0$ going through O_a.

Having chosen the axes in this fashion let $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$. By projective transformation (with linear conditions in the new coordinates) the resulting equation for C will be of the form

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

Multiply through by x and rename xy as y again we obtain

$$y^2 + (ax + b)y = \text{cubic in } x$$

Replace y by $y - \frac{1}{2}(ax + b)$ and completing the square on the left-hand side of the equation finally yields

$$y^2 = \text{cubic in } x$$

(We can always adjust the cubic to be monic by changing variables $x \to \lambda x$, $y \to \lambda^2 y$ where λ is the leading coefficient of the cubic.)

Appendix B. Algorithm in PARI/GP

```
\\ Computing derivatives of L-series

default(primelimit,20000000);

\\ Prime number function
pith(x) = {
  local(l,r,lx);
  if (x <= 2, return (x==2));
  lx = log(x);
  l = floor(x/lx);
  r = floor(l * (1 + 3/(2*lx)));
  while (r-l>1,
    m = (l+r)>>1;
    if (prime(m)<=x, l=m, r=m));
  l;
}

\\ Series expansion
default(seriesprecision,30);
```

```
S=-Euler*s+sum(n=2,30,(-1)^n*zeta(n)/n*s^n); SE=exp(S);
SV=vector(25,i,polcoeff(SE,i-1));

SP(r,t)=local(k);sum(k=0,r,SV[r-k+1]*t^k/factorial(k));

{G(r,x)=
   local(ss,ss0,n,sn);
   if(x>30,return(0));
   ss=SP(r,log(1/x));
   ss0=ss-1;
   n=1;
   sn=-((-1)^r);
   while(abs(ss-ss0)>1e-15,
     ss0=ss;
     ss=ss+sn*x^n/(n^r*factorial(n));
     n=n+1;
     sn=-sn;
   );
  2*ss;
}

\\ Buhler-Gross recursion
getap(r)=if(r<=pn,aplist[r],ellap(F,prime(r)))
getp(r)=if(r<=pn,ellplist[r],prime(r))

{ BGadd(n,i,a,b)=
    local(j,j0,a1);
    if(a==0,j0=i,ES=ES+a*G(Er,X*n)/n;j0=1;);
    j=j0;
    while(j<=i && getp(j)*n<=Ebnd,
        a1=a*getap(j);
        if(j==i && N%getp(j)!=0,
            a1=a1-getp(j)*b);
        BGadd(getp(j)*n,j,a1,a);
        j=j+1;
    )
}

\\ Derivative function for the L-series
{ elllsD(E,r,bnd)=
  local(pmax,loop,N,F);
  F=ellinit(E);
  pmax=sqrt(bnd);
  pn=pith(pmax);
  loop=pith(bnd);
  ellplist=primes(pn);
  aplist=vector(pn,i,ellap(F,ellplist[i]));
  aplist[1]=ellak(F,2);
```

```
  N=ellglobalred(E)[1];
  X=2*Pi/sqrt(N);
  Er=r;
  Ebnd=bnd;
  ES=G(r,X);
  for(i=1,loop,BGadd(getp(i),i,getap(i),1));
  ES;
}

\\ Computing the analytic rank and writing results to a file
{
  ellarank(E)=
  local(sfeq,E1,p,cond,Lbnd,Lr1);
    E=ellchangecurve(E,ellglobalred(E)[2]);
  print("Minimised Curve=",[E[1],E[2],E[3],E[4],E[5]]);
  cond=ellglobalred(E)[1];
  Lbnd=round(2*sqrt(cond));
  print("Summing ",Lbnd," a_n terms");
  sfeq=ellrootno(E);
  if(sfeq==-1,print("Odd"),print("Even"));
  d=(1-sfeq)/2;
  Lr1=0;
  while(abs(Lr1)<0.001,
    Lr1=elllsD(E,d,Lbnd);
    print("L^(",d,")(E,1)=",Lr1);
    d=d+2);
  print("Rank=",d-2);
  print(" ");
```

Appendix C. One parameter families with forced rank

The construction of one-parameter families of curves with forced rank over $\mathbb{Q}(t)$ is quite involved, we outline here only two simple cases of rank 0 and rank 1 family.

C1: Preliminaries

Recall the non-zero elements of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ for p prime forms a cyclic group with generator g such that $\{1, g, g^2, \ldots, g^{p-2}\} = \{1, 2, 3, \ldots, p-1\}$. Define the Legendre symbol $(\frac{x}{p})$ as 0 if $x = 0$, 1 if x is equivalent to a non-zero square modulo p, and -1 if x is not equivalent to a square modulo p. The following properties are immediate:

- $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$
- $(\frac{x+np}{p}) = (\frac{x}{p})$
- $(\frac{x^2}{p}) = (\frac{x^{-1}}{p}) = (\frac{x}{p})$, if $x \neq 0$

Consider now the case of $(\frac{f(x)}{p})$ when $f(x) = ax + b$ is a linear polynomial. We abbreviate $\sum_{x=0}^{p-1}(\frac{x}{p})$ by $\sum_{x(p)}(\frac{x}{p})$. The case when $a = 0$ is easily seen as $\sum_{x(p)}(\frac{b}{p}) = p(\frac{b}{p})$. If $a \neq 0$ we can change variables $t = a^{-1}x$, $u = t + b$ and the sum becomes $\sum_{x(p)}(\frac{ax+b}{p}) = \sum_{t(p)}(\frac{t+b}{p}) = \sum_{u(p)}(\frac{u}{p})$. As u (and hence x also)

progresses through the cyclic group each non-zero square contributes +1 and each non-square contributes -1. There are as many non-zero squares as non-squares, so we obtain the following result:

$$\sum_{x(p)} \left(\frac{ax+b}{p} \right) = \begin{cases} 0, & a = 0 \\ p(\frac{b}{p}), & a \neq 0 \end{cases}$$

Now for the curve $y^2 = x^3 + ax + b$ the Legendre sum $\sum_{x(p)}(1 + (\frac{x^3+ax+b}{p}))$ counts the number of solutions modulo p if we ignore the point at infinity, and so we obtain a Legendre expansion for $a_p = p + 1 - \#\{E(\mathbb{Q}) \mod p\}$ as

$$a_p = -\sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$$

C2: The Silverman-Rosen Theorem

For simplicity, consider a family of elliptic curves F in Weierstrass form $y^2 = x^3+A(T)x+B(T)$, $T \in \mathbb{Z}$. For every choice t of T we get an elliptic curve and denote it by E_t. We can regard F as an elliptic curve over $\mathbb{Q}(t)$. By the Specialisation Theorem of Silverman, all but finitely many E_t will have rank at least r if the family F has rank r over $\mathbb{Q}(t)$. This requires a way of determining the rank of the family of curves over $\mathbb{Q}(t)$. We begin by defining the a_p's for the family as the average of the sum of the a_p's: $A_F(p) = \frac{1}{p}\sum_{t(p)} a_{E_t}(p)$. The Silverman-Rosen Theorem states that for F with $\deg A(T) \leq 3$, $\deg B(T) \leq 5$ we have the equality

$$\lim \frac{1}{X} \sum_{p \leq X} -A_F(p) \log p = rank(F(\mathbb{Q}(t)))$$

Now the prime number theorem states that $\sum_{p \leq X} \log p = X +$ lower order terms and so the rank of the family over $\mathbb{Q}(t)$ is constant if we can show $A_F(p)$ is constant. We will show this for two families.

C3: Example of a rank 0 family

Consider $y^2 = x^3 + t$. Now we calculate the Legendre sum $\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}(\frac{t+x^3}{p}) = \sum_{x=0}\sum_{t=0}^{p-1}(\frac{t+x^3}{p}) + \sum_{x\neq 0}\sum_{t=0}^{p-1}(\frac{t+x^3}{p}) = \sum_{t(p)}(\frac{t}{p}) + \sum_{x\neq 0}\sum_{t=0}^{p-1}(\frac{t+x^3}{p}) = 0 + \sum_{x\neq 0}\sum_{t(p)}(\frac{t+x}{p})$ since $x \to x^3$ is an automorphism, and the sum equals 0 for all t so the rank of the family is $-A_F(p) = 0$.

C4: Example of a rank 1 family

Consider $y^2 + xy + 3y = x^3 + x^2 + tx$ which in Weierstrass normal form is $y^2 = x^3+5x^2+16tx+24x+144$. The Legendre sum $\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}(\frac{x^3+5x^2+16tx+24x+144}{p}) = \sum_{x=0}\sum_{t(p)}(\frac{x^3+5x^2+16tx+24x+144}{p}) + \sum_{x\neq 0}\sum_{t(p)}(\frac{x^3+5x^2+16tx+24x+144}{p}) = (\frac{144}{p})$ and so the rank of the family is $-A_F(p) = \frac{p}{p} = 1$.

References

[1] **Akiyama, Tanigawa**, *Calculation of values of L-functions associated to elliptic curves*, Mathematics of Computation Vol. 68 No. 227 (1999)
[2] **Birch, Swinnerton-Dyer**, *Notes on elliptic curves I*, Journal Reine u. angewandte Math 212 (1963)
[3] **Birch, Swinnerton-Dyer**, *Notes on elliptic curves II*, Journal Reine u. angewandte Math 218 (1965)
[4] **Cremona**, *Algorithms for modular elliptic curves*, Cambridge University Press (1992)
[5] **Fermigier**, *Étude expérimentals du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Experimental Math Vol. 5 (1996)
[6] **Gouvea, Mazur**, *The square-free sieve and the rank of elliptic curves*, Journal of the American Mathematical Society Vol. 4 No. 1 (1991)
[7] **Koblitz**, *Introduction to elliptic curves and modular forms*, Springer-Verlag New York (1984)
[8] **Serre**, *A course in arithmetic*, Springer-Verlag New York (1973)
[9] **Silverman, Tate**, *Rational points on elliptic curves*, Springer-Verlag New York (1992)
[10] **Stephens**, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, Journal fur Mathematik Vol. 231 (1968)