On the rank of elliptic curves

Jorma Jormakka

Contact by: jorma.o.jormakka@gmail.com

Abstract. The paper proves that the Birch and Swinnerton-Dyer conjecture is false.

Key words: Elliptic curves, Euler product, Birch and Swinnerton-Dyer conjecture.

1 Introduction

Let $P = \{p_1, p_2, \ldots | p_j \text{ is a prime}, p_{j+1} > p_j > 1, j \geq 1\}$ be the set of all primes larger than one. In [1] an elliptic curve C over the field of rational numbers Q is a curve defined by the Weierstrass equation

$$y^2 = x^3 + ax + b$$

where $a, b \in Z$ and $x, y \in Q$. The discriminant of the cubic equation is $\Delta = -16(4a^3 - 27b^2) \neq 0$. Let N_{p_j} denote the number of solutions to $y^2 = x^3 + ax + b \bmod p_j$ and let $a_{p_j} = p_j - N_{p_j}$.

The incomplete L-function of the curve C is

$$L(C, s) = \prod_{j \in A_C} (1 - a_{p_j} p_j^{-s} + p_j^{1-2s})^{-1}, \tag{1}$$

where

$$A_C = \{j \in \mathbb{N}, j > 0, p_j \textit{ does not divide } \Delta\}.$$

The Euler product (1) converges absolutely at least if $Re\{s\} > 2$ because $|a_p| \leq 2p$. This upper bound for $< a_p|$ is obvious since x takes p values and y can take

two values for each x. Hasse's statistical bound $|a_p| \leq 2p^{\frac{1}{2}}$ improves the area of absolute convergence to $Re\{s\} > 3/2$ and [1] gives this area. The problem statement [1] tells that $L(C,s)$ has a holomorphic continuation to the whole complex plane, thus it does not have poles.

The Birch and Swinnerton-Dyer conjecture says that the Taylor expansion of $L(C,s)$ at $s = 1$ has the form

$$L(C,s) = c(s-1)^r + \ higher\ order\ terms \tag{2}$$

with $c \neq 0$ and r the rank of C. The rank of an elliptic curve is defined as the rank of the group of solutions in the rational numbers. The number r in the Taylor expansion of $L(C,s)$ is called the algebraic rank of the curve. The conjecture is thus that the rank and the algebraic rank are equal.

Let $p > 2$ be prime, Z_p the cyclic group of integers modulo p, and $Z_p^* = \{1, \ldots, p-1\}$. The set of quadratic residues modulo p is the set

$$QR_p = \{x \in Z_p^* | \exists y \in Z_p^* \text{ such that } y^2 \equiv x \pmod{p}\}$$

and the set of nonresidues modulo p is

$$QNR_p = \{x \in Z_p^* | x \notin QR_p\}.$$

If g is a primitive root of Z_p^*, then

$$Z_p^* = \{g^0, g^1, \ldots, g^{p-2}\}.$$

The set QR_p is the subset where g has even powers:

$$QR_p = \{g^0, g^2, \ldots\}.$$

Thus, $\#QR_p = \#QNR_p$, the sets QR_p and QNR_p have equally many elements. If the integer a divides integer b it is written as $a|b$. For brevity, we write $y \equiv x$ as a shorthand of $y \equiv x \pmod{p}$ when there is no chance of confusion.

There is a recursion formula for deriving rational solutions from a rational base point (x, y)

$$x_{i+1} = S_i^2 - 2x_i \ , y_{i+1} = y_i + S_i(x_{i+1} - x_i) \tag{3}$$

$$S_i = \frac{a + 3x_i^2}{2y_i}$$

This recursion gives a new rational solution in the following way:

$$y_{i+1}^2 = y_i^2 + 2y_iS_i(x_{i+1} - x_i) + S_i^2(x_{i+1} - x_i)^2$$

$$= x_i^3 + ax_i + b + 2y_iS_i(x_{i+1} - x_i) + S_i^2(x_{i+1} - x_i)^2$$

$$= x_{i+1}^3 + ax_{i+1} + b$$

yielding

$$x_{i+1}^2 + x_{i+1}x_i + x_i^2 + a = 2y_iS_i + (x_{i+1} + 2x_i)(x_{i+1} - x_i)$$

which gives

$$3x_i^2 + a = 2y_iS_i.$$

The recursion may end or it may generate an infinite number of rational solutions. An example where the recursion ends is the following:

We define the curve C_1 by a Weiestrass form with $a = 33$ and $b = -26$. As the base point we take $x_0 = 3$ and $y_0 = 10$. The recursion (3) shows that $x_1 = x_0$, $y_1 = y_0$. It follows that recursion generates only one solution $(3, 10)$. The curve C_1 is a special case of

$$x_0 = 3s^2 \qquad y_0 = 9s^2 \pm s \tag{4}$$

$$a = 27s^4 \pm 6s^2 \qquad b = s^2 - 27s^6$$

with $s = 1$. For every nonzero integer value s the solution (4) gives $x_1 = x_0$, $y_1 = y_0$. These solutions are found by setting $x_1 = x_0$ in (3).

The rank of an elliptic curve is the number of independent base points from which the recursion derives an infinite number of rational solutions. For C_1 the recursion gives only finitely many points, but for that special elliptic curve there may be other base points that give infinitely many different points. An example of an elliptic curve having infinitely many rational solutions is $y^2 = x^3 - 5^2x$. This is known since 5 is a congruent number. If d is a noncongruent number, such as r^2 for any integer r there are only three solutions: $(0,0)$ and $(\pm d, 0)$.

The recursion formula (3) has a corresponding operation in integers modulo p in the form

$$x_{i+1} \equiv S_i^2 - 2x_i \pmod{p} \tag{5}$$

$$S_i \equiv (s + 3x_i^2)(2t_i)^{-1} \pmod{p}$$

$$t_i \equiv x^3 + ax + b \pmod{p}.$$

If (x_i, y_1) is a solution in Z_p^* then the recursion formula in Z_p gives another solution (x_{i+1}, y_{i+1}), $x_{i+1}, y_{i+1} \in Z_p^*$, where

$$y_{i+1}^2 \equiv t_{i+1} \pmod{p}.$$

The operation also takes a pair (x_i, t_i) where $t_i \in QNR_p$ into a pair (x_{i+1}, t_{i+1}) where $t_{i+1} \in QNR_p$. Iterating the operation gives classes of pairs (x_i, y_i). If there is a solution in Q, then all of the iterated solutions map to the same set of (x_i, y_i) in Z_p.

The claim that the Birch and Swinnerton-Dyer conjecture should hold seems to be based on the idea that an infinite number of solutions in rationals for an elliptic curve C would give more solutions in the modular case. This is a very

strange idea because there are very many solutions for a modular equation e.g. in knapsack problems and it is very difficult to find integer solutions to knapsack problems. The modular problem and the integer problem are quite different issues. The same should be the case with the modular problem and the rational problem in elliptic curves. The natural expectation is that these problems are very different and one does not give information of the other.

Two elliptic curves over rationals are known to have very high rank (one exactly or rank 20 and the other of rank at least 28). They are of the form

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

where $b \in \mathbb{N}$. Writing this curve in the Weierstrass form gives

$$y_1^3 = x_1^3 + (-\frac{49}{48})x_1 + (-\frac{2149}{576} - b)$$

$$y_1 = y + \frac{1}{2}(x+1) \qquad x_1 = x - \frac{5}{12}$$

and in the form where coefficients are integers is

$$y_2^3 = 9x_1^3 - 147x_1 - 2149 - 576b$$

$$y_2 = 24y + 12x + 12 \qquad x_2 = 4x - \frac{5}{3}$$

As a and b in the Weierstrass form are not integers in these elliptic curves, they are not elliptic curves considered in [1] and in this paper.

2 Calculation of a_{p_j} for $y^2 = x^3 - d^2x$

Lemma 1. *Let $p > 2$ be prime and a an integer. Assume $-1 \in QNR_p$ and $a \not\equiv 0 \pmod{p}$. The number N_p of solutions to the modular equation*

$$y^2 \equiv x^3 + ax \pmod{p} \tag{6}$$

is $N_p = p$.

Proof. Let

$$A = \{x \in Z_p^* | t_1 \in QR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

$$B = \{x \in Z_p^* | t_1 \in QNR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

and $m_1 = \#A$, $m_2 = \#B$. We can write

$$A_1 = \{x = 1, \ldots, \frac{p-1}{2} | t_1 \in QR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

$$A_2 = \{x = \frac{p+1}{2}, \ldots, p-1 | t_1 \in QR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

$$B_1 = \{x = 1, \ldots, \frac{p-1}{2} | t_1 \in QNR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

$$B_2 = \{x = \frac{p+1}{2}, \ldots, p-1 | t_1 \in QNR_p, t_1 \equiv x(x^2 + a) \pmod{p}\},$$

and $m_{1,i} = \#A_i$, $m_{2,i} = \#B_i$, $i = 1, 2$. The sets A_1 and A_2 are disjoint and $A = A_1 \cup A_2$. Similarly, the sets B_1 and B_2 are disjoint and $B = B_1 \cup B_2$. Calculating

$$A_2 = \{-x = -\frac{p+1}{2}, \ldots, -p-1 | t_1 \in QR_p, t_1 \equiv x(x^2 + a) \pmod{p}\}$$

$$= \{-x = p - \frac{p+1}{2}, \ldots, p - p + 1 | t_1' \in QR_p$$

$$t_1' = p - t_1 \equiv (-x)((-x)^2 + a) \pmod{p}\}$$

$$= \{-x = 1, \ldots, \frac{p-1}{2} | t_1' \in QR_p, t_1' \equiv (-x)((-x)^2 + a) \pmod{p}\}.$$

If it were true that $-1 \in QR_p$, then there would exists ϵ such that $-1 \equiv \epsilon^2$. Then for any y holds $-y^2 \equiv (\epsilon y)^2 \in QR_p$. But as we require that $-1 \in QNR_p$ it is not possible that $-y^2 \equiv h^2$ for any h because if it is $-1 \equiv (y^{-1}h)^2 \in QR_p$. Thus,

$-y^2 \in QNR_p$ for every y. Therefore

$$A_2 = \{x' = 1, \ldots, \frac{p-1}{2} | t'_1 \in QNR_p, t'_1 \equiv x'(x'^2 + a) \pmod{p}\} = B_1.$$

Similarly, $A_1 = B_2$. It follows that

$$m_1 = m_{1,1} + m_{1,2} = m_{1,1} + m_{2,1},$$

$$m_2 = m_{2,1} + m_{2,2} = m_{2,1} + m_{1,1}.$$

Thus, $m_1 = m_2$. Let $a \in QR_p$. Then there are two values $x \in Z_p^*$ that yield $t_1 \equiv 0 \pmod{p}$. Therefore

$$m_1 + m_2 = p - 3 \ \Rightarrow m_1 = \frac{p-3}{2}.$$

Every $x \in A$ yields two solutions $y, p - y$ to (6). Every x giving $t_1 \equiv 0 \pmod{p}$ yields one solution $y = 0$ to (6). The number of solutions is

$$N_p = 2\frac{p-3}{2} + 3 = p.$$

If $a \in QNR_p$ then $m_1 + m_2 = p - 1$ and

$$N_p = 2\frac{p-1}{2} + 1 = p.$$

The lemma is proved. □

Let us give an example of Lemma 1. Let $d = 1$ and $p = 11$. Then $QR_{11} = \{1, 3, 4, 5, 9\}$. When x ranges from 0 to 10 the values of $x(x^2 - 1)$ give the sequence $0, 0, 6, 2, 5, 10, 1, 6, 9, 5, 0$. Removing zeros from this sequnce as they are neither in QR_p nor in QNR_p we notice that $-6 \equiv 5$. Because $-1 \in QNR_p$ we have $6 \in QNR_p$ and $-5 \in QR_p$. Likewise $-2 \equiv 9$, so $2 \in QNR_p$ and $9 \in QR_p$; $-10 \equiv 1$. The same is with $-1 \equiv 10 \in QNR_p$ and $1 \in QR_p$. We get $2(p-3)/2 = 8$

solutions: $(4,4)$, $(4,7)$, $(6,1)$, $(6,10)$, $(7,3)$, $(7,8)$, $(9,4)$, $(9,7)$, that is, for each x there are two y values. Additionally we have the zeros. They give three solutions $(1,0)$ and $(10,0)$ from $x^2-1\equiv 0$ and $(0,0)$ is a solution. Together there are $11=p$ solutions.

Lemma 2. *Let $p>2$ be prime. The number of solutions y^2 to the equation*

$$y^2 - c \equiv x^2 \pmod{p} \tag{7}$$

satisfying $y^2, x^2 \in Z_p^*$ is

$\frac{p-5}{4}$ if $-1 \in QR_p$ and $c \in QR_p$,

$\frac{p-3}{4}$ if $-1 \in QNR_p$,

$\frac{p-1}{4}$ if $-1 \in QR_p$ and $c \in QNR_p$.

Proof. Let us assume that (7) holds. Thus there exists $z \in Z_p^*$ such that the modular equation

$$y^2 - x^2 = (y-x)(y+x) \equiv c$$

can be written as

$$y - x \equiv z \ , \ y + x \equiv z^{-1}c.$$

Then

$$y \equiv 2^{-1}x^{-1}(z^2+c) \ , \ x \equiv 2^{-1}z^{-1}(z^2-c).$$

Let $\pm\epsilon$ denote the two roots of $z^2 \equiv -1$ if $-1 \in QR_p$. If $-1 \in QNR_p$ there are no such roots.

If $c \in QNR_p$ and $-1 \in QR_p$ there are no solutions to the equations

$$z^2 \equiv c \qquad , \qquad (\epsilon z)^2 \equiv -c. \tag{8}$$

In this case we let z range over the $p-1$ numbers in Z_p^* in the equation for y. If two values z_1 and z_2 give the same y, then

$$z_1^{-1}(z_1^2 + c) \equiv z_2^{-1}(z_2^2 + c)$$

i.e.,

$$z_1 + cz_1^{-1} \equiv z_2 + cz_2^{-1},$$

$$z_1 - z_2 \equiv c(z_2^{-1} - z_1^{-1}).$$

Multiplying by $z_1 z_2$

$$z_1 z_2(z_1 - z_2) \equiv z_1 z_2 c(z_2^{-1} - z_1^{-1}) \equiv c(z_1 - z_2)$$

and $z_1 z_2 \equiv c$, i.e, $z_2 \equiv cz_1^{-1}$. When z ranges over all values in Z_p^* the number y gets all values it can get and exactly two values z map to the same y. The number of different y is therefore $\frac{p-1}{2}$.

If some value of z gives y, another value of z gives $-y$. As $\pm y$ yield the same y^2 the number of different y^2 is half of the numbers of y, that is, $\frac{p-1}{4}$.

If $c \in QR_p$ and $-1 \in QR_p$ then there are two solutions z to both of the equations in (8). These four values of z are all different. Removing them gives $p-5$ values for the range of z. The number of different values y^2 is $\frac{p-5}{4}$.

If $c \in QR_p$ and $-1 \in QNR_p$ there are two solutions for $z^2 \equiv c$ but no solutions to $z^2 \equiv -c$. The number of different y^2 is $\frac{p-3}{4}$.

If $c \in QNR_p$ and $-1 \in QNR_p$ there are no solutions for $z^2 \equiv c$ but two solutions to $z^2 \equiv -c$. The number of different y^2 is $\frac{p-3}{4}$. □

Lemma 3. *Let $p > 2$ be prime and a an integer. Let $-1 \in QR_p$, $a \not\equiv 0 \pmod{p}$ and g a primitive root of Z_p^*. The number N_p of solutions to the modular equation*

$$y^2 \equiv x^3 + ax \pmod{p} \tag{9}$$

is

$N_p = 8n_1 + 7$ if $-a \equiv g^{2i}$ and i is even,

$N_p = 2p - 8n_1 - 7$ if $-a \equiv g^{2i}$ and i is odd,

$N_p = 8n_g + 3$ if $-a \equiv g^{2i+1}$ and i is even,

$N_p = 2p - 8n_g - 3$ if $-a \equiv g^{2i+1}$ and i is odd.

Here n_c is the number of solutions $y^4 \in Z_p^*$ yielding $y^4 - c \in QR_p$, $c = 1$ or $c = g$.

Proof. Let

$$B = \{x' \in Z_p^* | t' \in QR_p, t' \equiv x'^3 + ax' \pmod{p}\}. \tag{10}$$

If $-a \equiv g^{2i}$ we insert $t \equiv g^{-3i}t'$ and $x \equiv g^{-1}x'$. Then $t' \equiv x'^3 + ax'$ changes to $g^{3i} \equiv g^{3i}x^3 - g^{2i}g^i x$, i.e., to $t \equiv x^3 - x$. We reduced $-a$ to $c = 1$.

If $-a \equiv g^{2i+1}$ we insert the same t and x as above. Then $t' \equiv x'^3 + ax'$ changes to $g^{3i} \equiv g^{3i}x^3 - g^{2i+1}g^i x$, i.e., to $t \equiv x^3 - gx$. We reduced $-a$ to $c = g$.

We write both of these cases as $t \equiv x^3 - cx$ where $c = 1$ if $-a = g^{2i}$ and $c = g$ if $-a = g^{2i+1}$.

Let

$$A = \{x \in Z_p^* | t_1 \in QR_p, t_1 \equiv x^3 - cx \pmod{p}\} \tag{11}$$

$$A' = \{x \in Z_p^* | t_1 \in QNR_p, t_1 \equiv x^3 - cx \pmod{p}\}.$$

If i is even then g^i is in QR_p and in the substitution $t = g^{3i}t'$ holds: if $t \in QR_p$ then $t' \in QR_p$. If i is odd, then $t \in QR_p$ implies that $t' \in QNR_p$. Thus, for even i $B = A$ while for odd i $B = A'$.

Let us write the sets A and A' differently

$$A = \{g^k | g^k(g^{2k} - c) \in QR_p, k = 0, \ldots, p-2\} \tag{12}$$

$$A' = \{g^k | g^k(g^{2k} - c) \in QNR_p, k = 0, \ldots, p-2\}$$

and let us divide them into subsets of even and odd indices of k

$$A_1 = \{g^{2k} | g^{2k}(g^{4k} - c) \in QR_p, k = 0, \ldots, \frac{p-3}{2}\}$$

$$A_2 = \{g^{2k} | g^{2k+1}(g^{2(2k+c)} - c) \in QR_p, k = 0, \ldots, \frac{p-3}{2}\}$$

$$A_1' = \{g^{2k+1} | g^{2k}(g^{4k} - c) \in QNR_p, k = 0, \ldots, \frac{p-3}{2}\}$$

$$A_2' = \{g^{2k+1} | g^{2k+1}(g^{2(2k+c)} - c) \in QNR_p, k = 0, \ldots, \frac{p-3}{2}\}.$$

Then $A = A_1 \cup A_2$, $\#A = \#A_1 + \#A_2$ and $A' = A_1' \cup A_2'$, $\#A' = \#A_1' + \#A_2'$.

We also define sets that do not have the $x = g^k$ term in $t = x(x^2 - c)$.

$$C = \{g^{2k} | g^{2k} - c \in QR_p, k = 0, \ldots, \frac{p-3}{2}\} \tag{13}$$

$$C' = \{g^{2k} | g^{2k} - c \in QNR_p, k = 0, \ldots, \frac{p-3}{2}\}$$

and divide these sets into subsets where a set with a running index $2k$ is divided into two sets with running indices $4k$ and $4k + 2$:

$$C_1 = \{g^{4k} | g^{4k} - c \in QR_p, g^{4k} \leq \frac{p-1}{2}, k = 0, \ldots, \frac{p-3}{2}\} \tag{14}$$

$$C_2 = \{g^{4k+2} | g^{4k+2} - c \in QR_p, g^{4k+2} \leq \frac{p-1}{2}, k = 0, \ldots, \frac{p-3}{2}\},$$

$$C_1' = \{g^{4k} | g^{4k} - c \in QNR_p, g^{4k} \leq \frac{p-1}{2}, k = 0, \ldots, \frac{p-3}{2}\},$$

$$C_2' = \{g^{4k+2} | g^{4k+2} - c \in QNR_p, g^{4k+2} \leq \frac{p-1}{2}, k = 0, \ldots, \frac{p-3}{2}\}.$$

The rule $g^{4k} \leq \frac{p-1}{2}$ and $g^{4k+2} \leq \frac{p-1}{2}$ removes half of the values of the running index. Then $C = C_1 \cup C_2$, $\#C = \#C_1 + \#C_2$ and $C' = C_1' \cup C_2'$, $\#C' = \#C_1' + \#C_2'$.

The idea is to map the solutions of $t \equiv g^k(g^{2k} - c)$ bijectively to solutions of $t' \equiv g^{2k} - c$. Clearly, if $g^k \in QNR_p$ multiplying with it changes $t' \in QR_p$ to $t \in QNR_p$ and if $g^k \in QR_p$ multiplying by it does not change the set. This is

why we divided the sets to A_i, A'_i, $i = 1, 2$. In $i = 2$ sets $g^k \in QNR_p$, so if an element of C'_2 is multiplied by g^k we get an element of A_2. Likewise, C_2 and A'_2 correspond to each other.

The following relations hold

$$\begin{aligned}
\#A &= \#2C_1 + \#2C'_2 \\
\#A' &= \#2C'_1 + \#2C_2 \\
\#C_2 &= \#C - \#C_1 \\
\#C'_2 &= \#C' - \#C'_1.
\end{aligned}$$

Solving $\#A$ yields

$$\begin{aligned}
\#A &= 2\#C_1 + 2\#C'_2 \\
&= 2\#C_1 + 2\#C' - 2\#C'_1.
\end{aligned}$$

The value a is used in the proof of this lemma in two places only. One is in (10): if $-a \equiv g^{2i}$ or $-a \equiv g^{2i+1}$ and the index i is even, then $B = A$. If i is odd, then $B = A'$. The other place is in Lemma 2 where the numbers of solutions in the different cases depend on if whether $-a \equiv g^{2i}$ or $-a \equiv g^{2i+1}$, i.e., if $c = 1$ or $c = g$.

Case 1: $-a = g^{2i}$, i even. Then $c = 1$ and the relation

$$\#C' = \tfrac{p-3}{2} - \#C.$$

holds. In this relation we have counted the values of k in $C \cup C'$ and excluded the one value of k that gives $g^{2k} - 1 \equiv 0 \pmod{p}$ because $0 \notin QR_p \cup QNR_p$. Thus, the number of valid indices k is one less than the number $\frac{p-1}{2}$ of indices $k = 0, \ldots, \frac{p-3}{2}$ in (13). The correct value of valid indices $\frac{p-3}{2}$.

Counting indices k in $C_1 \cup C'_1$ in (14) gives

$$\#C'_1 = \tfrac{p-5}{4} - \#C_1.$$

In this relation we have excluded the solution to $g^{2k} - c \equiv 0 \pmod{p}$. In C_1 and C'_1 the counted element is not the number of indices k. It is the number of values g^{4k}. This number must be reduced by one. The result follows as $\frac{p-1}{4} - 1 = \frac{p-5}{4}$.

Calculating $\#A$ gives

$$\#A = 2\#C_1 + p - 3 - 2\#C - \tfrac{p-5}{2} + 2\#C_1$$

$$= 4\#C_1 - 2\#C + \tfrac{p-1}{2}.$$

Writing $\#C_1 = n_1$ and inserting from Lemma 2 the case $-1 \in QR_p$ and $c \in QR_p$ where $\#C = \frac{p-5}{4}$ yields

$$\#\text{A} = 4n_1 - \tfrac{p-5}{2} + \tfrac{p-1}{2} = 4n_1 + 2.$$

In Case 1 holds $N_p = 2\#A + 3$ because if there is a solution $y^2 \equiv x(x^2-1)$, then it is satisfied by two y values, $\pm y$, and there are three solutions where $y \equiv 0$, namely $x \equiv 0$, $x^2 \equiv \pm 1$. Thus $N_p = 8n_1 + 7$.

Case 2: $-a = g^{2i}$, i odd. Then $B = A'$. Thus

$$\#A' = 2\#C_1' + 2\#C_2$$
$$= \tfrac{p-5}{2} - 2\#C_1 + 2\#C - 2\#C_1$$
$$= \tfrac{p-5}{2} - 4n_1 + \tfrac{p-5}{2} = p - 4n_1 - 5$$

In Case 2 $N_p = 2\#A' + 3$, thus $N_p = 2p - 8n_1 - 7$.

Case 3: $-a = g^{2i+1}$, i even. The differences to Case 1 are

$$N_p = 2\#A + 1$$
$$\#C' = \tfrac{p-1}{2} - \#C$$
$$\#C_1' = \tfrac{p-3}{4} - \#C_1$$
$$\#C = \tfrac{p-3}{4}$$

because $c = g$ and $g^{2k} - g \equiv 0$ is not possible.

We denote $\#C_1 = n_g$ and insert from Lemma 2 the case $-1 \in QR_p$ and $c \in QNR_p$ where $\#C = \frac{p-1}{4}$. Making these changes to the calculation of Case 1 gives $N_p = 8n_g + 3$.

Case 4: $-a = g^{2i+1}$, i odd. Analogically with Cases 2 and 3 we get $N_p = 2p - 8n_g - 3$.

The definition of C_1 is a bit complicated as the running index k loops over twice as many indices than are needed and the set has a test to discard half of the values values k because in this way C is clearly the union of C_1 and C_2. It is good to notice that the set C_1 has as many members as the set

$$\{y^4 | y^4 - c \in QR_p\}$$

where $c = 1$ for Cases 1 and 2 and $c = g$ for Cases 3 and 4.

The proof of the lemma is completed. □

Let us look at an example of Lemma 2. Let $a = -d^2$ for $d = 1$ in (9) and $p = 13$. As g we choose 2, which is a primitive root for Z_{13}^*. Then $1 \equiv 2^0$, $2 \equiv 2^1$, $3 \equiv 2^4$, $4 \equiv 2^2$, $5 \equiv 2^9$, $6 \equiv 2^5$, $7 \equiv 2^{11}$, $8 \equiv 2^3$, $9 \equiv 2^8$, $10 \equiv 2^{10}$, $11 \equiv 2^7$ and $12 \equiv 2^6$. The sets are

$$A = \{2^3, 2^9\} \qquad A' = \{2^1, 2^2, 2^4, 2^5, 2^7, 2^8, 2^{10}, 2^{11}\}$$

$$A_1 = \emptyset \qquad A_2 = \{2^3, 2^9\}$$

$$A_1' = \{2^2, 2^4, 2^8, 2^{10}\} \qquad A_2' = \{2^1, 2^5, 2^7, 2^{11}\}$$

$$C = \{2^1, 2^5\} \qquad C' = \{2^2, 2^3, 2^4, 2^9\}$$

$$C_1 = \emptyset \qquad C_2 = \{2^1, 2^5\}$$

$$C_1' = \{2^2, 2^4\} \qquad C_2' = \{2^9\}$$

There is a direct correspondence between C_1 and the first half of A_1, as there is between C_1' and the second half of A_1'. This is because if $g^{2k}(g^{4k} - 1) \in QR_p$ then $g^{4k} - 1 \in QR_p$ and if $g^{4k} - 1 \in QR_p$ then $\pm g^{2k}(g^{4k} - 1) \in QR_p$ since $-1 \in QR_p$. There is also a direct correspondence between C_2' and the first half of A_2, as there is between C_2 and A_2'. This is because if $g^{2k+1}(g^{2(2k+1)} - 1) \in QR_p$ then $g^{2(2k+1)} - 1 \in QNR_p$ as $g \in QNR_p$, and if $g^{2(2k+1)} - 1 \in QNR_p$ then $\pm g^{2k+1}(g^{2(2k+1)} - 1) \in QR_p$ since $-1 \in QR_p$. This gives the relations between the sizes of the sets.

The case of Lemma 1 covers half of all p because of Lemma 4.

Lemma 4. *The following statements hold:*

(i) $-1 \in QR_p$ if and only if $4|(p-1)$

(ii) The number of $p < N$ such that $4|(p-1)$ approaches half when N grows to infinity.

Proof. Let g be a primitive root of Z_p^*. If $4|(p-1)$, then $a \equiv g^{\frac{p-1}{4}}$ is in Z_p^* and $a^2 \equiv -1$. If $-1 \in QR_p$, then $-1 \equiv g^{2i}$ for some i, $0 \leq i \leq p-2$. Since $-1 \not\equiv 1$ holds $2i \not\equiv 0 \pmod{(p-1)}$. Thus $2i \neq 0$ and $2i \neq p-1$. As $(-1)^2 \equiv 1 \equiv g^{p-1} \equiv g^{4i}$ holds $4i = k(p-1)$ for some k where k has the possible values $1, 2, 3$. If $k = 2$, then $-1 \equiv g^{2i} \equiv g^{p-1} \equiv 1$, which is impossible. Thus, $k \in \{1, 3\}$. Then $gcd(4, k) = 1$ and therefore $4|(p-1)$. This proves the claim (i).

Claim (ii) is shown true by considering the Sieve of Eratosthenes. In this algorithm primes are found by reserving a memory vector for all numbers and marking the place of 1 as full and all other places empty at the beginning. On each step the first unmarked place is taken as the next prime p. The place of p is marked and all multiples of p are marked. In this algorithm the first step takes $p = 2$ and marks all multiples of 2. The unmarked numbers are all odd. The next prime is $p = 3$, the first unmarked number. All multiples of 3 are marked. The numbers that are marked for p, i.e., multiples of p, are are all odd and equally distributed modulo 4. Consequently, the numbers that remain unmarked are all odd and equally distributed modulo 4. This continues in each step, thus the numbers that remain unmarked are all odd and equally distributed between 1 (mod 4) and 3 (mod 4).

In each step the first unmarked number is the next prime p. It is selected as the smallest number in a set of unmarked numbers that are always odd and distributed equally between two sets 1 (mod 4) and 3 (mod 4). The next prime p has half a chance in belonging to either set. The number $p-1$ is always even and if $p \equiv 1$ modulo 4, then $4|(p-1)$. This is so in half of the cases when N approaches infinity. □

3 The Birch and Swinnerton-Dyer conjecture

The original reason why Birch and Swinnerton-Dyer formulated their conjecture was that the function

$$\log \prod_{j=1}^{n} \frac{N_{p_j}}{p_j}$$

was growing approximatively linearly for some values of d for elliptic curves of the type $y^2 = x(x^2 - d^2)$, while for some other values of d the function did not tend to infinity when n grows.

The function they studied in [2] can be written as

$$\log \prod_{j=1}^{n} \frac{N_{p_j}}{p_j} = -\log \prod_{j=1}^{n} (1 - a_{p_j} p_j^{-1})^{-1}$$

$$= \sum_{j=1}^{n} \log(1 - a_{p_j} p_j^{-1}) = -\sum_{j=1}^{n} a_{p_j} p_j^{-1} + \sum_{j=1}^{n} a_{p_j}^2 p_j^{-2} + \cdots$$

As a_{p_j} is on the range of $p_j^{\frac{1}{2}}$ by the Hasse bound, the higher terms converge. The first two terms may diverge at $s = 1$.

The function studied can be completed into a complex function that is evaluated at $s = 1$:

$$\prod_{j=1}^{\infty} (1 - a_{p_j} p_j^{-1})^{-1} \to \prod_{j=1}^{\infty} (1 - a_{p_j} p_j^{-s})^{-1}.$$

Let the sum to be over the set A

$$L_2(C, s) = \prod_{j \in A} (1 - a_{p_j} p_j^{-s})^{-1}.$$

The difference with this function and $L(C, s)$ in (1) is that the term p_j^{1-2s} in (1) is missing.

We will derive a small result. Let $f(s)$ be holomorphic in the whole complex plane with the exception of isolated poles and let $f(s)$ have an Euler product

expression

$$f(s) = \prod_{j \in A} (1 - f(s)_j)^{-1}$$

which converges absolutely when $Re\{s\}$ is sufficiently large. When the product converges absolutely we have

$$f'(s)f(s)^{-1} = \frac{d}{ds} \ln f(s) = -\sum_{j \in A} \frac{d}{ds} \ln(1 - f_j(s))$$

$$= \sum_{j \in A} f_j'(s)(1 - f_j(s))^{-1} = \sum_{k=0}^{\infty} \sum_{j \in A} f_j'(s) f_j(s)^k.$$

Let us define

$$g_2(s) = \sum_{k=2}^{\infty} \sum_{j \in A} f_j'(s) f_j(s)^k$$

$$g_1(s) = \sum_{j \in A} f_j'(s) f_j(s)$$

$$h(s) = \sum_{j \in A} f_j'(s).$$

In the area where $g_2(s)$ converges absolutely holds

$$f'(s)f(s)^{-1} - g_2(s) = h(s) + g_1(s).$$

If the function $f(s)$ has a zero or a pole at s_0, then the function $h(s) + g_1(s)$ has a simple pole at s_0. The residue of a pole of $h(s) + g_1(s)$ is always an integer and all poles of $h(s) + g_1(s)$ are simple poles.

For $L_2(C, s)$ the function $f_j(s) = a_{p_j} p^{-s}$ and $h(s)$ has the expression

$$h(s) = h_1(s) = \sum_{j \in A} f_j'(s) = -\sum_{j \in A} a_{p_j} \ln(p_j) p_j^{-s}.$$

The sum diverges at $s = 1$ and $h(s)$ may have a simple pole at $s = 1$. The function $g_1(s)$ is

$$g_1(s) = -\sum_{j \in A} \ln(p_j) a_{p_j}^2 p_j^{-2s}.$$

The part of the sum expression of $g_1(s)$ diverging at $s = 1$ is

$$g_{1,1}(s) = g_1(s).$$

The sum diverges at $s = 1$ and $g_{1,1}(s)$ may have a simple pole at $s = 1$.

For $L(C, s)$ the function $f_j(s) = a_{p_j} p^{-s} - p^{1-2s}$ and $h(s)$ has the expression

$$h(s) = \sum_{j \in A} f_j'(s) = -\sum_{j \in A} (a_{p_j} \ln(p_j) p_j^{-s} - 2 \ln(p_j) p_j^{1-2s}) = h_1(s) + h_2(s).$$

The sum diverges at $s = 1$ and $h(s)$ may have a simple pole at $s = 1$. The function $g_1(s)$ is

$$g_1(s) = -\sum_{j \in A} \ln(p_j) a_{p_j}^2 p_j^{-2s} + \sum_{j \in A} \ln(p_j) a_{p_j} \left(3p_j^{1-3s} - 2p_j^{2-4s}\right).$$

The part of the sum expression of $g_1(s)$ diverging at $s = 1$ is

$$g_{1,1}(s) = \sum_{j \in A} \ln(p_j) a_{p_j}^2 p_j^{-2s}.$$

The sum diverges and $g_{1,1}(s)$ may have a simple pole at $s = 1$.

Thus, the (possibly) divergent part $g_{1,1}(s)$ of $g_1(s)$ is the same for $L_2(C, s)$ and for $L(C, s)$, but the function $h(s)$ for $L_2(C, s)$ lacks the second part $h_2(s)$ in $h(s)$ for $L(C, s)$. This missing function has a first order pole and residue one at $s = 1$ as the following lemma shows.

Lemma 4. *Close to $s = 1$ holds*

$$h_2(s) = 2 \sum_{j \in A} \ln(p_j) p_j^{1-2s} = \frac{1}{s-1} + \text{finite terms}.$$

Proof. The Riemann zeta function $\zeta(s)$ has a simple pole of residue 1 at $s = 1$. Thus, close to $s = 1$ zeta is

$$\zeta(s) = \prod_{p_j} (1 - p_j^{-s})^{-1} = \frac{1}{s-1} + \text{finite terms.}$$

Derivating gives $h(s)$ for the zeta function:

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{(s-1)^2} \cdot \frac{s-1}{1} + \text{finite terms} = h(s) + g(s).$$

Calculating from the infinite product we get

$$\frac{d}{ds} \ln(\zeta(s)) = h(s) + g(s)$$

where

$$h(s) = -\sum_j \ln(p_j) p_j^{-s}$$

$$g(s) = -\sum_j \ln(p_j) p_j^{-2s} + \cdots$$

and $g(s)$ converges when $Re\{s\} > \frac{1}{2}$. Thus, the divergent part is

$$\sum_j \ln(p_j) p_j^{-s} = \frac{1}{s-1} + \text{finite terms}$$

close to $s = 1$. Changing $-s = 1 - 2z$ yields

$$2 \sum_j \ln(p_j) p_j^{1-2z} = 2 \frac{1}{2z-2} + \text{finite terms}$$

that is

$$2 \sum_j \ln(p_j) p_j^{1-2s} = \frac{1}{s-1} + \text{finite terms.}$$

Since A excludes only those values of p_j that divide Δ, the sum over A gives the same result. □

The Theorem on page 4 in [1] states that it is proven that if the elliptic curve C has rank zero then the L-function $L(C,s)$ has the algebraic rank zero. There is a conflict: Theorem 1 proves that Theorem on page 4 in [1] is in contradiction with the initial experiments of Birch and Swinnerton-Dyer, assuming they have been correctly described in the literature:

Theorem 1. *Assuming that $L_2(C,s)$ satisfies the Birch and Swinnerton-Dyer conjecture for rank zero, then $L(C,s)$ cannot satisfy the conjecture for rank zero.*

Proof. Birch and Swinnerton-Dyer studied elliptic curves of the form $y^2 = x(x^2 - d^2)$ with several values of d including values $d = 1$ and $d = 5$. These curves have rank zero if $d = k^2$ for some integer k. Assuming that Birch and Swinnerton-Dyer concluded that the function they studied, $L_2(C,s)$, has a finite nonzero value at $s = 1$ for $d = 1$, then it follows that $h(s) + g_{1,1}(s)$ must be finite at $s = 1$ for $d = 1$. For $L_2(C,s)$ holds $h(s) = h_1(s)$, thus $h_1(s) + g_{1,1}(s)$ must be finite for $d = 1$.

Consequently, if $L_2(C,s)$ fills the conjecture for rank zero, then the function $L(C,s)$ cannot have a finite nonzero value at $s = 1$ for elliptic curves with $a = -d^2 = -1$ and $b = 0$. The function $h_2(s)$ has a pole at $s = 1$ and is of the form

$$h_2(s) = \frac{1}{s-1} + \text{finite terms.}$$

Therefore

$$h_1(s) + h_2(s) + g_{1,1}(s) = \frac{1}{s-1} + \text{finite terms.}$$

Because of this pole, the function $L(C,s)$ has a zero at $s = 1$. Thus, for an elliptic curve of rank zero the L-function $L(C,s)$ has a zero at $s = 1$ and has the algebraic rank one. □

Errors happen, but if Theorem on page 4 in [1] (and the literature results that it is based on) is correct, then Birch and Swinnerton-Dyer were a bit mixed up:

they thought that a pole of $L_2(C,s)$ at $s=1$ for $d=1$ is a nonzero value of $L_2(C,s)$ and that a nonzero value of $L_2(C,s)$ at $s=1$ for $d=5$ is a zero.

Though it seems that the problem as stated in [1] is solved in negative without any use of Lemmas 1-4 simply because it contradicts what Birch and Swinnerton-Dyer found in [2], these lemmas were given for the purpose of solving the problem statement in [1]. Thus, we will assume that the problem statement [1] is correct in its claims and show that it leads to a contradiction without referring to the results of Birch and Swinnerton-Dyer in [2].

The problem statement [1] says that $L(C,s)$ is analytic in the whole plane implying that it does not have a pole at $s=1$ for any d. Theorem on page 4 in [1] says that for rank one and zero the Birch and Swinnerton-Dyer conjecture is true.

The function $h_2(s)$ has a pole with residue 1 at $s=1$.

Let us consider the values $a=-d^2$ with $d=1$, $d=5$ and $d=19$ for the simple elliptic curves that Birch and Swinnerton-Dyer studied: thus $a=-d^2$ and $b=0$. The numbers 1 and 19 are noncongruent numbers and give an elliptic curve with zero rank, while $d=5$ is a congruent number and gives an elliptic curve with rank one.

The value $d_1=1$ is a square number and picks up only the first case with $i=0$ in Lemma 3. Thus, $a_p=N_p-p=8n_1+7-p$. The other two values of d give a choice of the two first cases in Lemma 3: if $d\in QR_p$, then $a_{p_j,d}=a_{p_j,1}$, while if $d\in QNR_p$, then $a_{p_j,d}=-a_{p_j,1}$.

The divergent part $g_{1,1}(s)$ of $g_1(s)$ has a square of a_{p_j} and therefore it is the same function for all three values of d. Let the residue of the (possible) pole of $g_{1,1}(s)$ at $s=1$ be r. That is, if there is no pole, then $r=0$.

The function $h_1(s)$ is different for different values of d. Let us write $h_{1,d}(s)$ for the function $h_1(s)$ for the value d. We will denote the value of the residue of the (possible) pole of $h_{1,d}(s)$ at $s=1$ by $-r_d$. If there is no pole, then $r_d=0$.

Assuming that the conjecture holds for ranks zero and one, the (possible) poles of $h(s) = h_{1,1}(s)+h_2(s)$ and $g_{1,1}(s)$ must cancel at $s = 1$. We have $-r_1+1+r = 0$. For $d = 5$ the function $h_{1,5}(s)+h_2(s)+g_{1,1}(s)$ has a simple pole with residue one. Thus $-r_5 + 1 + r = 1$. These two equations give

$$r_5 = r_1 - 1 < r_1. \tag{15}$$

The value $d = 19$ is a noncongruent number. Since Theorem on page 4 in [1] says that the conjecture holds, the value $d = 19$ must give zero algebraic rank. Thus,

$$r_{19} = r_1. \tag{16}$$

Theorem 2. *If statistical arguments of the distribution of prime numbers are not allowed in the proof, then the problem statement in [1] is not well-defined and cannot be answered. If statistical arguments of the distribution of prime numbers are allowed in the proof, then the Birch and Swinnerton-Dyer conjecture for $L(C, s)$ fails in rank one.*

Proof. The Hesse bound is a statistical bound and requires treating prime numbers in a statistical manner. If statistical arguments are not allowed, then the problem statement should not use the Hesse bound. As it does make an argument with the Hesse bound, the problem statement is not well formulated and a poorly formulated problem statement cannot be answered.

No statistical arguments are needed in Lemmas 1-3 and Lemma 4 claim (i). In Lemma 4 claim (ii) there is a statistical argument using the Sieve of Eratosthenes. Prime numbers can be deterministically generated by the Sieve of Eratosthenes. Because of the construction of this sieve we can make some statistical observations, such as the claim (ii) in Lemma 4.

The number of solutions for $y^2 - 1 \in QR_p$ is $(p - 5)/4$ for the case $-1 \in QR_p$ according to Lemma 2. Exactly half of the numbers y are in QR_p and half are in

QNR_p. We will now make a statistical argument: for a randomly chosen prime p (about) half of the solutions $y^2 - 1 \in QR_p$ have $y \in QR_p$ and if p_j ranges over all values, the probability that $y \in QR_p$ is exactly 0.5. Thus, the expectation value for n_1 is $(p-5)/8$ where the expectation value means that the number p is randomly chosen. It follows that the expectation value of a_{p_j} for $d = 1$ is $E[a_{p_j}] = p_j - 5 + 7 - p_j = 2$. Because the mean of a_{p_j} is 2, the function $h_{1,1}(s)$ for diverges at $s = 1$. It has a simple pole with residue $-r_1$ for some $r_1 > 0$.

We will make another statistical assumption: the prime d, where $d = 5$ or $d = 19$, does not have any special relationship with a randomly chosen large prime p_j. Therefore the expectation value of a_{p_j} is 2 if the randomly chosen prime p_j is chosen from the set satisfying $d \in QR_p$. Likewise, the expectation value of a_{p_j} is 2 if the randomly chosen prime p_j is chosen from the set satisfying $d \in QNR_p$.

We need another statistical assumption: because the prime d, where $d = 5$ or $d = 19$, does not have any special relationship with a randomly chosen large prime p_j, the probability that $d \in QR_p$ for a randomly chosen p_j is 0.5.

If these statistical assumptions are accepted in a proof, then we can make the following observations. Let $a_{p_j,d}$ denote the number a_{p_j} for the value d.

By Lemma 1, if $-1 \in QNR_p$, then $a_p = N_p - p = 0$ for every d.

By the claim (ii) in Lemma 4 holds $-1 \in QNR_p$ for half of the randomly chosen primes p_j. It follows that $a_{p_j,d}$ is zero for every d for half of the randomly chosen primes p_j.

For the other half of the randomly chosen primes p_j holds $-1 \in QR_{p_j}$. Of these values half have $d \in QR_{p_j}$ for $d \neq 1$ and then $a_{p_j,d} = a_{p_j,1}$. The rest (i.e., half) have $d \in QNR_p$ and thus $a_{p_j,d} = -a_{p_j,1}$. Let $d \in \{1, 5, 19\}$ and

$$A_{1,d} = \{j \in A | d \in QR_{p_j}, -1 \in QR_{p_j}\}$$

$$A_{2,d} = \{j \in A | d \in QNR_{p_j}, -1 \in QR_{p_j}\}.$$

The statistical assumptions mean that for $d \in \{5, 19\}$ we have

$$\sum_{j \in A_{1,d}} a_{p_j,d} p^{-s} = \sum_{j \in A_{1,1}} a_{p_j,1} p^{-s} \tag{17}$$

$$\sum_{j \in A_{2,d}} a_{p_j,d} p^{-s} = - \sum_{j \in A_{2,1}} a_{p_j,1} p^{-s}$$

$$\sum_{j \in A_{1,d}} a_{p_j,d} p^{-s} = - \sum_{j \in A_{2,d}} a_{p_j,d} p^{-s}.$$

Therefore for $d = 5$ we get

$$h_{1,5}(s) = \sum_{j \in A_{1,5}} a_{p_j,5} p^{-s} + \sum_{j \in A_{2,5}} a_{p_j,5} p^{-s} = 0$$

and $r_5 = 0$. Thus, by (15) follows $r_1 = 1$ and thus $r = 0$.

But by the same argument, for $d = 19$ holds

$$h_{1,19}(s) = \sum_{j \in A_{1,19}} a_{p_j,19} p^{-s} + \sum_{j \in A_{2,19}} a_{p_j,19} p^{-s} = 0$$

and $r_{19} = 0$. This is in contradiction with (16).

Thus, if statistical arguments are allowed, the Birch and Swinnerton-Dyer conjecture fails for rank one for $L(C, s)$. □

It is not any better for $L_2(C, s)$:

Corollary 1. *If statistical arguments of the distribution of prime numbers in Theorem 2 are allowed, then the Birch and Swinnerton-Dyer conjecture for $L_2(C, s)$ fails in rank one.*

Proof. If statistical assumptions of Theorem 2 are allowed, then (17) holds. We get the same contradiction for $L_2(C, s)$ as for $L(C, s)$. The only difference is that $r = 1$. □

References

1. A. Wiles, The Birch and Swinnerton-Dyer Conjecture. *available on-line at* www.claymath.org.
2. B. Birch and P. Swinnerton-Dyer, Notes on Elliptic Curves (II). *J. Reine Math.* 165 (218): 79-108, 1965.