All polynomials and rational functions in this essay are assumed to have coefficients in \( \mathbb{Q} \). Fix an integer \( n \geq 1 \). An \textbf{affine variety} is a simultaneous irreducible system of polynomial equations in \( n \) variables. The \textbf{\( \mathbb{Q} \)-points}, \textbf{\( \mathbb{R} \)-points} and \textbf{\( \mathbb{C} \)-points} of the affine variety are all solutions of the polynomial system in \( \mathbb{Q}^n \), \( \mathbb{R}^n \) and \( \mathbb{C}^n \), respectively.

\textbf{Rational projective} \( n \)-space \( \overline{\mathbb{Q}}^n \) is the set of lines through the origin in \( \mathbb{Q}^{n+1} \). For example, the projective plane \( \mathbb{Q}^2 \) is a quotient of the unit sphere in \( \mathbb{Q}^3 \) modulo the relation \((X,Y,Z) \sim (−X,−Y,−Z)\). We define \( \overline{\mathbb{R}}^n \) and \( \overline{\mathbb{C}}^n \) similarly. A \textbf{projective variety} is a simultaneous irreducible system of homogeneous polynomial equations in \( n+1 \) variables. The \( \mathbb{Q} \)-points, \( \mathbb{R} \)-points and \( \mathbb{C} \)-points of the projective variety are all solutions of the polynomial system in \( \overline{\mathbb{Q}}^n \), \( \overline{\mathbb{R}}^n \) and \( \overline{\mathbb{C}}^n \), respectively; these are \((n+1)\)-tuples, not \( n \)-tuples as before.

A \textbf{curve} is a projective variety corresponding to one homogeneous polynomial equation \( p(X,Y,Z) = 0 \). In particular, \( n+1 = 3 \); that is, \( n = 2 \). Such a curve is \textbf{smooth} or \textbf{non-singular} if there is no \( \mathbb{C} \)-point at which the partial derivatives \( p_X \), \( p_Y \), \( p_Z \) all vanish. For example, the conic

\[ ax^2 + bxy + cy^2 + dx + ey + f = 0 \]

is expressed in homogeneous coordinates as

\[ aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0; \]

irreducibility implies smoothness in this case. Triples \((X,Y,Z)\) satisfying this equation with \( Z = 0 \) are called \textbf{points at infinity}.

Let \( F \) denote a smooth projective curve and \( F(\mathbb{C}) \) denote the \( \mathbb{C} \)-points of \( F \). The \textbf{genus} \( g \) of \( F \) is defined topologically as the number of handles in the Riemann surface \( F(\mathbb{C}) \), and algebraically as \((m − 1)(m − 2)/2\), where \( m \) is the degree of the polynomial \( p \). Lines and conics have genus 0 while smooth cubics have genus 1.

Any two smooth projective curves of genus 0 with a rational point must be \textbf{isomorphic} or \textbf{birationally equivalent} [1]. This means that the bijection between the curves, as well as its inverse, can be given locally by rational functions. For

---

[1] Copyright © 2005 by Steven R. Finch. All rights reserved.
Elliptic Curves over \( \mathbb{Q} \)

example, the circle \( x^2 + y^2 = 1 \) is isomorphic to the hyperbola \( x^2 - y^2 = 1 \) via the change of coordinates \( (x, y) \mapsto (1/x, y/x) \). It is isomorphic to the line \( y = 0 \) via the function \( (x, y) \mapsto y/(x + 1) \). The circle, moreover, is a commutative group under addition-of-angles, with identity element \( (x, y) = (1, 0) \). Its group of rational points is the direct sum of \( \mathbb{Z}_4 \), the cyclic group of order 4, and countably many copies of \( \mathbb{Z} \) [2, 3, 4, 5, 6].

In contrast, there are (up to isomorphism) infinitely many smooth projective curves of genus 1 with a rational point. These are called elliptic curves (not to be confused with ellipses). Each such isomorphism class possesses a unique Weierstrass minimal model [7]

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_j \in \mathbb{Z}, \quad a_1, a_3 \in \{0, 1\}, \quad a_2 \in \{0, \pm 1\},
\]

for which \( |\Delta| \) is minimized, where

\[
\Delta = -(a_1^2 + 4a_2)^2 (a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_3^2)
-8(a_1a_3 + 2a_4)^3 - 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + 4a_2)(a_1a_3 + 2a_4)(a_3^2 + 4a_6)
\]

is the discriminant of the cubic. For example, the Fermat cubic \( x^3 + y^3 = 1 \) is isomorphic to the elliptic curve \( y^2 = x^3 - 3x \) via the change of coordinates \( (x, y) \mapsto ((36-y)/(6x), (36+y)/(6x)) \). Its minimal model is \( y^2 + y = x^3 - 7 \), however, obtained via the additional transformation \( (x, y) \mapsto (4x, 8y+4) \). We will soon present a table of isomorphism classes, ordered according to increasing conductor \( N \), along with several other associated constants.

An elliptic curve \( E \) is also a commutative group, with addition given by the familiar chord-and-tangent law, and with identity element the unique point at infinity \( (X, Y, Z) = (0, 1, 0) \). It is a prototypal example of what is known as an abelian variety. Let \( E(\mathbb{Q}) \) denote the group of rational points of \( E \). By Mordell’s theorem,

\[
E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus E_{\text{tors}}(\mathbb{Q})
\]

where the rank \( r \) is a nonnegative integer and the torsion subgroup \( E_{\text{tors}}(\mathbb{Q}) \) is finite. Define \( t \) to be the order of \( E_{\text{tors}}(\mathbb{Q}) \), for convenience’s sake. The overlap of geometry (\( E \) is a smooth curve) and algebra (\( E \) is an abelian variety) makes this subject rich and interesting.

0.1. Naive Height. If \( x \in \mathbb{Q} \), write \( x = a/b \), where \( a \) and \( b \) are coprime integers. Define \( H(x) = \max\{|a|, |b|\} \). The set of \( x \in \mathbb{Q} \) for which \( H(x) \leq k \) is clearly finite and \([1, 8, 9, 10, 11]\)

\[
\lim_{k \to \infty} \frac{1}{k^2} \sum_{H(x) \leq k} 1 = \frac{12}{\pi^2} = \frac{2}{\zeta(2)}
\]
Alternatively, if \( x \in \overline{\mathbb{Q}} \), then \( x \) is represented by \((a, b)\) in homogeneous coordinates and the same asymptotic result applies. The projective line is identical to the affine line in this regard.

Given a rational point \((x, y)\) on the circle \( x^2 + y^2 = 1 \), define \( H(x, y) \) to be simply \( H(x) \). The set of such rational points for which \( H(x, y) \leq k \) is again finite and \([12]\)

\[
\lim_{k \to \infty} \frac{1}{k} \sum_{\substack{H(x) \leq k, \\
x^2 + y^2 = 1}} 1 = \frac{4}{\pi}.
\]

Observe that it makes no sense to sum over all points \((x, y)\) in \( \mathbb{Q}^2 \) of bounded height. However, on the projective plane \( \overline{\mathbb{Q}}^2 \), choose an integer triple \((a, b, c)\) representing a given rational point \((x, y)\), where \(\gcd(a, b, c) = 1\). Defining \( H(x, y) = \max\{|a|, |b|, |c|\} \), we obtain \([1, 9, 10, 11]\)

\[
\lim_{k \to \infty} \frac{1}{k^3} \sum_{H(x, y) \leq k} 1 = \frac{4}{\zeta(3)}
\]

where \(\zeta(3)\) is Apéry’s constant \([13]\). For example, \( c > 0 \) may be taken to be the least common denominator of \(x\) and \(y\), and thus \( a = cx \) and \( b = cy \).

Given a rational point \((x, y, z)\) on the sphere \( x^2 + y^2 + z^2 = 1 \), define \( H(x, y, z) \) to be the least common denominator of \(x, y\) and \(z\). In this case, it is known that \([14]\)

\[
\lim_{k \to \infty} \frac{1}{k^2} \sum_{\substack{H(x, y, z) \leq k, \\
x^2 + y^2 + z^2 = 1}} 1 = \frac{3}{2G}
\]

where \(G\) is Catalan’s constant \([15]\). An open frontier of asymptotic results like these, for higher-dimensional varieties and assorted height functions, awaits discovery.

Let us return to the affine plane. Consider an elliptic curve \( E \) and define the **naive height** \( H(x, y) = H(x) \) for any rational point \((x, y)\) on \( E \) (ignoring the vertical component, just as we did for the circle). The set of rational points for which \( H(x, y) \leq k \) can be proved to be finite and \([1, 16, 17, 18, 19, 20]\)

\[
\Theta = \lim_{k \to \infty} \frac{1}{\ln(k)^{r/2}} \sum_{\substack{H(x) \leq k, \\
(x, y) \in E}} 1 = \frac{\pi^{r/2}}{\Gamma\left(1 + \frac{r}{2}\right)} \frac{t}{\sqrt{R}}
\]

where the integers \( r \geq 0 \) and \( t \geq 1 \) were defined previously and the real number \( R > 0 \) is the **regulator** of \( E \). We will demonstrate how to compute \( R \) shortly \([0, 2]\).
0.2. **Canonical Height.** Let \( h(x, y) = \ln(H(x, y)) \), the logarithm of the naive height on \( E \). We also need the duplication formula, that is, the algorithm by which to calculate \( 2 \cdot (x, y) = (x, y) + (x, y) \):

\[
2 \cdot (x, y) = (\nu, -(\lambda + a_1)\nu - \mu - a_3)
\]

where

\[
\lambda = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}, \quad \mu = \frac{-x^3 + a_4x + 2a_6 - a_3y}{2y + a_1x + a_3}
\]

and \( \nu = \lambda^2 + a_1\lambda - a_2 - 2x \). In fact, \( y = \lambda x + \mu \) is the line \( L \) tangent to \( E \) at \((x, y)\) and \( \nu \) is the horizontal component of the other point of \( L \cap E \). Clearly \( 2^n \cdot P = 2 \cdot [2^{n-1} \cdot P] \) for all positive integers \( n \), for any rational point \( P \) on \( E \). Define the **canonical height** or **Néron-Tate height** of \( P \) to be \([7, 21, 22, 23, 24]\)

\[
\hat{h}(P) = \frac{1}{2} \lim_{n \to \infty} \frac{h(2^n \cdot P)}{2^n}.
\]

For example, given the elliptic curve \( y^2 + y = x^3 - x \) and the point \( P = (0, 0) \), we have

\[
2 \cdot P = (1, 0), \quad 4 \cdot P = (2, -3), \quad 8 \cdot P = \left( \frac{21}{25}, -\frac{69}{125} \right), \quad 16 \cdot P = \left( \frac{180106}{3225}, \frac{332513754}{274625} \right)
\]

and \( \hat{h}(P) = 0.0255557041... \). It can be shown that \( \hat{h} \) is a nonnegative definite quadratic form on \( E(\mathbb{Q}) \) that differs from \( h/2 \) by at most a constant. In particular, the **height pairing**

\[
\langle , \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}
\]

\[
\langle P_i, P_j \rangle = \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)
\]

is a symmetric bilinear form. The \( r \times r \) determinant

\[
R = \det (\langle P_i, P_j \rangle)_{1 \leq i \leq r, 1 \leq j \leq r}
\]

is independent of the choice of basis \( \{P_1, P_2, \ldots, P_r\} \) for \( E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q}) \), and this defines the regulator. Continuing our example, we have \( r = 1 \) and \( R = 2\hat{h}(P) = 0.0511114082... \). Since \( t = 1 \), it follows that the asymptotic growth constant \( \Theta = 8.8464916552... \).

Different variations on \( \hat{h} \) and \( \langle , \rangle \) abound, all involving factors of 2. Our conventions are consistent with the software package PARI/GP [25, 26, 27], which is freely available.

Numerical algorithms exist for computing \( \hat{h} \) to arbitrary precision [28, 29, 30, 31, 32, 33]. Here is a curious approach, based on what is called an **elliptic divisibility sequence** [34, 35, 36]:

\[
s_{2n+1} = s_{n+2}s_n^3 - s_{n-1}s_{n+1}^3, \quad s_{2n} = s_n \left( s_{n+2}s_{n-1}^2 - s_{n-2}s_{n+1}^2 \right)
\]
with initial terms $s_0 = 0$, $s_1 = 1$, $s_2 = 1$, $s_3 = -1$, $s_4 = 1$. It can be proved that $s_n | s_m$ whenever $n | m$, that

$$s_{m-n}s_{m+n} = s_{m+1}s_{m-1}s_n^2 - s_{n+1}s_{n-1}s_m^2$$

for all $m \geq n \geq 0$, and that $\lim_{n \to \infty} n^{-2} \ln |s_n| = 0.0255557041$. This is the same value $\hat{h}(P)$ obtained in our example.

Another example is the elliptic curve $y^2 + y = x^3 + x^2$; we compute $\hat{h}(P) = 0.0314082535$ for the point $P = (0,0)$. These two cases constitute the two “simplest” rank-one elliptic curves. Table 1 summarizes these, as well as the “simplest” rank-two and rank-three elliptic curves [37, 38]. “Simplicity” means smallest possible conductor $N$; we will define this quantity later [0.5].

<table>
<thead>
<tr>
<th>$N$</th>
<th>elliptic curve</th>
<th>$r$</th>
<th>$t$</th>
<th>$P_1$</th>
<th>$R$</th>
<th>$\Theta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>$y^2 + y = x^3 - x$</td>
<td>1</td>
<td>1</td>
<td>$(0, 0)$</td>
<td>0.0511114082...</td>
<td>8.8464916552...</td>
</tr>
<tr>
<td>43</td>
<td>$y^2 + y = x^3 + x^2$</td>
<td>1</td>
<td>1</td>
<td>$(0, 0)$</td>
<td>0.0628165070...</td>
<td>7.9798201588...</td>
</tr>
<tr>
<td>389</td>
<td>$y^2 + y = x^3 + x^2 - 2x$</td>
<td>2</td>
<td>1</td>
<td>$(0, 0), (1, 0)$</td>
<td>0.1524601779...</td>
<td>8.0458449949...</td>
</tr>
<tr>
<td>5077</td>
<td>$y^2 + y = x^3 - 7x + 6$</td>
<td>3</td>
<td>1</td>
<td>$(0, 2), (1, 0), (2, 0)$</td>
<td>0.4171435587...</td>
<td>6.4855354622...</td>
</tr>
</tbody>
</table>

0.3. Real Period. The complex torus $E(\mathbb{C})$ is isomorphic (as a Riemann surface) to $\mathbb{C}/\Lambda$, where $\Lambda$ is a certain lattice $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ such that $\omega_1 > 0$ and $\text{Im}(\omega_2) > 0$. Clearly the minimal model for $E$ can be rewritten as

$$(2y + a_1x + a_3)^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + (a_3^2 + 4a_6);$$

let us denote the right-hand side of this equation by $f(x)$. Define the zeroes of $f(x)$ to be $e_1$, $e_2$, $e_3$ with the understanding that $e_1 < e_2 < e_3$ if $\Delta > 0$ and $e_1 \in \mathbb{R}$ uniquely if $\Delta < 0$. These two cases correspond to $E(\mathbb{R})$ being disconnected or connected, respectively ($\Delta \neq 0$ since otherwise $E$ would be singular). Also define the arithmetic-geometric mean $M(u, v)$ of two numbers $u$, $v$ to be the common limit as $n \to \infty$ of the sequences $\{u_n\}, \{v_n\}$, where

$$u_n = \frac{u_{n-1} + v_{n-1}}{2}, \quad v_n = \sqrt{u_{n-1}v_{n-1}}, \quad u_0 = u, \quad v_0 = v.$$

It follows that, if $\Delta > 0$,

$$\omega_1 = \int_{e_1}^{e_2} \frac{2 \, dx}{\sqrt{f(x)}} = \int_{e_3}^{\infty} \frac{2 \, dx}{\sqrt{f(x)}} = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})}.$$
$\omega_2 = \int_{-\infty}^{e_1} \frac{2 \, dx}{\sqrt{f(x)}} = \int_{e_2}^{e_3} \frac{2 \, dx}{\sqrt{f(x)}} = \frac{\pi i}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})}$

and, if $\Delta < 0$,

$\omega_1 = \int_{e_1}^{\infty} \frac{2 \, dx}{\sqrt{f(x)}} = \frac{2\pi}{M(2\sqrt{\eta}, \sqrt{2\eta + \xi})}$,  \hspace{1cm} \omega_2 = -\frac{1}{2} \omega_1 + \frac{\pi i}{m(2\sqrt{\eta}, \sqrt{2\eta - \xi})}$

where [18, 39]

$\xi = 3e_3 + \frac{1}{4}(a_1^2 + 4a_2), \hspace{1cm} \eta = \sqrt{3e_3^2 + \frac{1}{2}(a_1^2 + 4a_2)e_3 + \frac{1}{8}(a_1a_3 + 2a_4)}.$

A path integral expression for $\omega_2$ in the latter case also exists; the AGM sequences converge quadratically and are vastly preferred over numerical integration.

The real period $\Omega$ is $2\omega_1$ when $\Delta > 0$ and $\omega_1$ when $\Delta < 0$, and the real volume $V$ is $\omega_1 \Im(\omega_2)$. Observe that $\omega_1$ is the smallest positive real number contained in $\Lambda$ and $V$ is the area of the associated fundamental parallelogram. A related quantity is the Faltings height $\omega$, defined to be the reciprocal of $V$.

Table 2 contains $\Omega$ and $V$ for the elliptic curves given in Table 1, preceded by several rank-zero elliptic curves not mentioned earlier. In fact, there are three isomorphism classes of elliptic curves with conductor $N = 11$, six classes with $N = 14$ and eight classes with $N = 15$. No examples with $N < 11$ exist [40]. We use the notation of Cremona [37] to refer to certain elliptic curves. For instance, 11A1 refers to the first curve in Table 2, while 11A2 refers to

$y^2 + y = x^3 - x^2 - 7820x - 263580$

with $\Delta = -11$, $\Omega_{11A2} = (1/5)\Omega_{11A1}$ and $V_{11A2} = (1/5)V_{11A1}$, and 11A3 refers to

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

with $\Delta = -11$, $\Omega_{11A3} = 5\Omega_{11A1}$ and $V_{11A3} = 5V_{11A1}$. More generally, elliptic curves possessing the same conductor $< 26$ have the same real period and real volume, up to rational multiples.

<table>
<thead>
<tr>
<th>$N$</th>
<th>elliptic curve</th>
<th>$\Delta$</th>
<th>$\Omega$</th>
<th>$V$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>$y^2 + y = x^3 - x^2 - 10x - 20$</td>
<td>$-161051$</td>
<td>$1.2692093042\ldots$</td>
<td>$1.8515436234\ldots$</td>
</tr>
<tr>
<td>14</td>
<td>$y^2 + xy + y = x^3 + 4x - 6$</td>
<td>$-21952$</td>
<td>$1.9813419560\ldots$</td>
<td>$2.6262514055\ldots$</td>
</tr>
<tr>
<td>15</td>
<td>$y^2 + xy + y = x^3 + x^2 - 10x - 10$</td>
<td>$50625$</td>
<td>$2.8012060846\ldots$</td>
<td>$2.2357017126\ldots$</td>
</tr>
<tr>
<td>37</td>
<td>$y^2 + y = x^3 - x$</td>
<td>$37$</td>
<td>$5.9869172924\ldots$</td>
<td>$7.3381327407\ldots$</td>
</tr>
<tr>
<td>43</td>
<td>$y^2 + y = x^3 + x^2$</td>
<td>$-43$</td>
<td>$5.4686895299\ldots$</td>
<td>$7.4548214176\ldots$</td>
</tr>
<tr>
<td>389</td>
<td>$y^2 + y = x^3 + x^2 - 2x$</td>
<td>$389$</td>
<td>$4.9804251217\ldots$</td>
<td>$4.9100459911\ldots$</td>
</tr>
<tr>
<td>5077</td>
<td>$y^2 + y = x^3 - 7x + 6$</td>
<td>$5077$</td>
<td>$4.1516879830\ldots$</td>
<td>$3.0733872268\ldots$</td>
</tr>
</tbody>
</table>
Elliptic Curves over \( \mathbb{Q} \)

Familiar numbers among the real periods include the lemniscate constants [41, 42, 43, 44]

\[
\Omega_{32A1} = \frac{1}{2\sqrt{2\pi}} \Gamma \left( \frac{1}{4} \right)^2 = 2.6220575542... = \frac{1}{2}(5.2441151085...),
\]

\[
\Omega_{432A1} = \frac{1}{4\pi} \Gamma \left( \frac{1}{3} \right)^3 = 1.5299540370... = \frac{1}{2}(3.0599080741...)
\]

corresponding to the elliptic curves \( y^2 = x^3 + 4x \) and \( y^2 = x^3 - 16 \), respectively. Note that \( y^2 = x^3 - x \) and \( y^2 = x^3 + x \) are related to the former:

\[
\Omega_{32A2} = 2\Omega_{32A1}, \quad \Omega_{64A4} = \sqrt{2}\Omega_{32A1}
\]

while \( y^2 = x^3 - 1 \) and \( y^2 = x^3 + 1 \) are related to the latter:

\[
\Omega_{144A1} = \frac{4}{\sqrt{16}} \Omega_{432A1}, \quad \Omega_{36A1} = \frac{4\sqrt{3}}{\sqrt{16}} \Omega_{432A1}.
\]

Such exact expressions in terms of gamma function values seem to be rare. General formulas for \( \omega_1 \) and \( \omega_2 \) in terms of hypergeometric function values are found in [45]. It would be good to better understand \( \omega_1 = 2.9934586462... \) and \( \omega_2 = (2.4513893819...)i \) for the special curve 37A1, in particular [18, 46].

0.4. Isogenies. Let \( E \) and \( E' \) be two elliptic curves and denote the point at infinity by \( \mathcal{O} \). Any isomorphism \( E \rightarrow E' \) that maps \( \mathcal{O} \) to itself induces an isomorphism \( E(\mathbb{Q}) \rightarrow E'(\mathbb{Q}) \) of groups. It is natural to attempt to classify all elliptic curves up to isomorphism; recall, for example, the three isomorphism classes 11A1, 11A2, 11A3 with conductor 11. A weaker notion is as follows. Any homomorphism \( E(\mathbb{Q}) \rightarrow E'(\mathbb{Q}) \) that is not identically \( \mathcal{O} \) is called an isogeny. It can be proved, in fact, that any isogeny is necessarily surjective. For example, an isogeny from 11A3 to 11A1 is given by [18, 47]

\[
(x, y) \mapsto \left( x + \frac{1}{x^2} + \frac{2}{x-1} + \frac{1}{(x-1)^2}, y - (2y+1) \left( \frac{1}{x^3} + \frac{1}{(x-1)^3} + \frac{1}{(x-1)^2} \right) \right),
\]

which clearly fails to be injective. We remarked earlier that every isomorphism class is represented uniquely by a minimal model; an algorithm for computing such representative curves is due to Tate [48, 49]. Isogeny classes encompass one or more isomorphism classes. The curves 11A1, 11A2, 11A3 all fall in one isogeny class, which is written simply as 11A. It can be proved that isogenic curves \( E \) and \( E' \) possess the same conductor \( N \) and the same L-series (see [0,5]). The first \( N \) for which two isogeny classes exist is 26; these are denoted 26A and 26B. The first \( N \) for which three isogeny classes exist is 57; these are denoted 57A, 57B and 57C [37, 50, 51, 52].
0.5. L-Series. For any prime \( p \), let \( \mathbb{Z}_p \) denote the field of integers modulo \( p \). Starting with the minimal model for an elliptic curve \( E \) over \( \mathbb{Q} \), define \( E_p \) to be its reduction over \( \mathbb{Z}_p \):

\[
y^2 + a_1 xy + a_3 y \equiv x^3 + a_2 x^2 + a_4 x + a_6 \mod p.
\]

Let \( N_p \) denote the number of points \( (x, y) \in \mathbb{Z}_p^2 \) on \( E_p \), plus one, and let \( [53] \)

\[
b_p = \begin{cases} 
    p + 1 - N_p & \text{if } p \nmid \Delta, \\
    \pm 1 & \text{if } p \mid \Delta \text{ and } p \nmid (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4), \\
    0 & \text{if } p \mid \Delta \text{ and } p \mid (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4),
\end{cases}
\]

The three cases correspond to when \( E_p \) is non-singular, has a node, or has a cusp, respectively. The last two cases, of course, correspond to when \( E \) has bad reduction at \( p \). It remains for us to specify the sign of \( b_p \) in the nodal case. Does there exist a quadruple \( (x_0, y_0, \alpha, \beta) \in \mathbb{Z}_p^4 \) for which \( (x_0, y_0) \) is a singular point on \( E_p \),

\[
y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 
\equiv [(y - y_0) - \alpha(x - x_0)][(y - y_0) - \beta(x - x_0)] - (x - x_0)^3 \mod p
\]

and \( \alpha \neq \beta \)? If yes, the reduction is said to be split at \( p \) and \( b_p = 1 \). If no, the reduction is non-split and \( b_p = -1 \). Finally, the Hasse-Weil L-series of \( E \) is defined to be

\[
L_E(z) = \sum_{n=1}^{\infty} b_n n^{-z}, \quad \Re(z) > \frac{3}{2}
\]

where \( b_1 = 1 \), \( b_{p^k} = b_{p^{k-1}}b_p - p b_{p^{k-2}} \) for \( k \geq 2 \) and \( b_m b_n = b_{mn} \) for coprime integers \( m, n \). This can also be written as an infinite product:

\[
L_E(z) = \prod_{p \mid \Delta} \frac{1}{1 - b_p p^{-z}}, \prod_{p \nmid \Delta} \frac{1}{1 - b_p p^{-z} + p^{1-2z}}, \quad \Re(z) > \frac{3}{2}.
\]

The combined efforts of Wiles [54], Taylor & Wiles [55] and others [56, 57, 58, 59] yield that \( L_E(z) \) can be analytically continued over the whole complex plane.

For example, the elliptic curve 11A3 has bad reduction only at \( p = 11 \). It has split multiplicative reduction since \( 11 \nmid 16 \) and since \( (x_0, y_0, \alpha, \beta) = (-3, 5, 1, -1) \) satisfies the required equation; hence \( b_{11} = 1 \). As another example, \( E = 37A1 \) has bad reduction only at \( p = 37 \). It has non-split multiplicative reduction since \( 37 \nmid 48 \).
and since \((x_0, y_0) = (5, 18)\) is the only singular point of \(E_{37}\) but no slopes \((\alpha, \beta) \in \mathbb{Z}_{37}^2\) work with this; hence \(b_{37} = -1\). All other coefficients \(b_p\) are obtained easily. For the isogeny class \(11A\), there is a miraculous \(q\)-expansion result [53, 59, 60]:

\[
\sum_{n=1}^{\infty} b_n q^n = q \prod_{k=1}^{\infty} (1 - q^k)^2 (1 - q^{11k})^2
\]

(a weight 2 cusp form of level 11) and similarly for 14A and 15A. Corresponding generating functions for \(37A\) are much more complicated [46, 61].

Let us return to the entire function \(L_E(z)\) and define the modification

\[
\hat{L}_E(z) = \left( \frac{\sqrt{N}}{2\pi} \right)^z \Gamma(z)L_E(z),
\]

where \(N\) is the conductor of \(E\). Then the following functional equation

\[
\hat{L}_E(z) = \varepsilon \cdot \hat{L}_E(2 - z)
\]

is satisfied everywhere, where \(\varepsilon = \pm 1\) is the root number of \(E\). This equation serves to characterize \(N\) uniquely (the actual computation of \(N\) turns out to be difficult). The conductor \(N\) divides \(\Delta\) and is divisible only by primes where \(E\) has bad reduction. It is conjectured that \(\varepsilon = (-1)^r\), where \(r\) is the rank of \(E\).

Consider the value of \(L_E\) and its derivatives at \(z = 1\). Let \(m\) denote the smallest integer for which \(L_E^{(m)}(1) \neq 0\). The famous Birch/Swinnerton-Dyer conjecture predicts that \(m = r\) and that

\[
\frac{L_E^{(r)}(1)}{r!} \frac{t^2}{\Omega R} \in \mathbb{Z}^+,
\]

where \(t\) is the torsion order of \(E\), \(\Omega\) is the real period and \(R\) is the regulator (we take \(R = 1\) in the event \(r = 0\)). More can be said if we introduce one additional quantity into the denominator – the Tamagawa number \(c\) – which cannot be defined here for reasons of space. The new ratio is then conjectured to be an integer square always (see Table 3). It is known exactly when \(r = 0\) and approximately when \(r > 0\) [37]. The first case for which the ratio equals 4 is the elliptic curve 66B3; the first case for which it equals 9 is 182B3. Associated with each elliptic curve \(E\) is the Tate-Shafarevich group \(III(E)\) whose order is at issue. No effective procedure for computing \(|III(E)|\) is known, short of assuming the truth of the BSD conjecture and numerically calculating \(m, L_E^{(m)}(1), t, \Omega, R\) and \(c\). Gross & Zagier [62] and Kolyvagin [63, 64] proved that if \(m = 0\), then \(r = 0\); if \(m = 1\), then \(r = 1\); and that there exists an \(E\) with \(m = r = 3\). (The curves 389A1 and 5077A1 provably satisfy \(m = r = 2\) and \(m \geq r = 3\), respectively.) We do not yet know an \(E\) with \(m = r = 4\), or even an \(E\) with \(r \geq 4\) and \(L_E^{(r)}(1) = 0\) [19, 29, 37, 38, 65, 66, 67, 68].
Table 3. BSD Ratio, for Nine Selected Isomorphism Classes of Elliptic Curves

<table>
<thead>
<tr>
<th>elliptic curve</th>
<th>r</th>
<th>t</th>
<th>$L_E^{(r)}(1)/r!$</th>
<th>c</th>
<th>$L_E^{(r)}(1)/r!(t^2/(c\Omega R))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11A1</td>
<td>0</td>
<td>5</td>
<td>0.2538418608...</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>14A1</td>
<td>0</td>
<td>6</td>
<td>0.3302236593...</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>15A1</td>
<td>0</td>
<td>8</td>
<td>0.3501507605...</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>11A1</td>
<td>1</td>
<td>1</td>
<td>0.305997738...</td>
<td>1</td>
<td>1.0</td>
</tr>
<tr>
<td>43A1</td>
<td>1</td>
<td>1</td>
<td>0.3435239746...</td>
<td>1</td>
<td>1.0</td>
</tr>
<tr>
<td>66B3</td>
<td>0</td>
<td>2</td>
<td>1.1021925301... (= $\Omega$)</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>182B3</td>
<td>0</td>
<td>1</td>
<td>1.9204065875... (= 9$\Omega$)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>389A1</td>
<td>2</td>
<td>1</td>
<td>0.7593165002...</td>
<td>1</td>
<td>1.0</td>
</tr>
<tr>
<td>5077A1</td>
<td>3</td>
<td>1</td>
<td>1.7318499001...</td>
<td>1</td>
<td>1.0</td>
</tr>
</tbody>
</table>

0.6. Areas of Rational Right Triangles. A square-free positive integer $d$ is a congruent number if the set

$$
\{(u,v) \in \mathbb{Q}^2 : \frac{1}{2}uv = d \text{ and } u^2 + v^2 = w^2 \text{ for some } w \in \mathbb{Q}\}
$$

is nonempty [69, 70]. We wish to effectively distinguish congruent $d$ from non-congruent $d$. Let $E_d$ denote the elliptic curve $y^2 = x^3 - d^2x$; recall the special case $E_1 = 32A2$ from [0.3]. It is known that $d$ is congruent if and only if $E_d$ has nonzero rank. By the (weak) BSD conjecture, the latter condition is equivalent to $L_{E_d}(1) = 0$. Another miraculous $q$-expansion result holds for $E_1$:

$$
\sum_{n=1}^{\infty} b_n q^n = q \prod_{k=1}^{\infty} (1 - q^{4k})^2 (1 - q^{8k})^2
$$

and this carries over to $E_d$ via the quadratic twist

$$
L_{E_d}(z) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) b_n n^{-z}
$$

of $L_{E_1}(z)$ by the Dirichlet character $(d/n)$. For instance, $(1/n) = 1$ always,

$$(2/n)|_{n=1,2} = \{1,0\},$$

$$(3/n)|_{n=1,2,3} = \{1,-1,0\}$$

and other examples appear in [71].
Define \((i, j) = (1, d)\) if \(d\) is odd and \((i, j) = (2, d/2)\) if \(d\) is even. In both cases, \(j\) is an odd square-free integer and \(ij = d\). Define coefficients \(c_{i,j}\) via the \(q\)-expansions

\[
\sum_{n=1}^{\infty} c_{1,n} q^n = q \prod_{k=1}^{\infty} \left( 1 - q^{8k} \right) \left( 1 - q^{16k} \right) \cdot \sum_{m=-\infty}^{\infty} q^{2m^2} = \sum_{(u,v,w) \in \mathbb{Z}^3, \ v \equiv 1 \mod 2} \left( q^{2u^2+v^2+32w^2} - \frac{1}{2} q^{2u^2+v^2+8w^2} \right),
\]

\[
\sum_{n=1}^{\infty} c_{2,n} q^n = q \prod_{k=1}^{\infty} \left( 1 - q^{8k} \right) \left( 1 - q^{16k} \right) \cdot \sum_{m=-\infty}^{\infty} q^{4m^2} = \sum_{(u,v,w) \in \mathbb{Z}^3, \ v \equiv 1 \mod 2} \left( q^{4u^2+v^2+32w^2} - \frac{1}{2} q^{4u^2+v^2+8w^2} \right).
\]

Tunnell [72, 73, 74] proved the following remarkable formula:

\[
L_{E_d}(1) = \frac{1}{8\sqrt{2\pi}} \Gamma \left( \frac{1}{4} \right)^2 \cdot c_{i,j}^2 \sqrt{\frac{i}{j}} = \frac{1}{4} (2.6220575542...) \cdot c_{i,j}^2 \sqrt{\frac{i}{j}},
\]

which provides the required identification algorithm (flawed only in that it rests on the validity of an unproved conjecture). On the one hand, since \(c_{1,1} = 1\), \(c_{2,1} = 1\) and \(c_{1,3} = 2\), we have \(L_{E_1}(1) = 0.6555143885...\),

\[
L_{E_2}(1) = \sqrt{2} L_{E_1}(1) = 0.9270373386..., \quad L_{E_3}(1) = \frac{1}{\sqrt{3}} L_{E_1}(1) = 1.5138456348...\]

On the other hand, since \(c_{1,5} = c_{2,3} = c_{1,7} = 0\), we deduce that \(L_{E_5}(1) = L_{E_6}(1) = L_{E_7}(1) = 0\). By the BSD conjecture, it can be concluded that 5, 6, 7 are congruent numbers and 1, 2, 3 are not. (These particular facts, however, are obtained via elementary means as well. We are merely illustrating the method.)

Observe that the change of variables \((x, y) \mapsto (x/d, (1/\sqrt{d})(y/d))\) maps \(E_1\) to \(E_d\).

It is not an isomorphism over \(\mathbb{Q}\) because of the presence of the irrationality \(\sqrt{d}\); it is, rather, an isomorphism over \(\mathbb{Q}(\sqrt{d})\). Other relevant papers on congruent numbers include [75, 76, 77, 78, 79, 80, 81]. A consequence of the BSD conjecture is that any square-free positive integer \(\equiv 5, 6, 7 \mod 8\) is a congruent number. Further, random matrix theory predicts that [82]

\[
\# \{ n \leq N : n \equiv 1, 2, 3 \mod 8 \text{ is a congruent number} \} \sim C N^{3/4} \ln(N)^{11/8}
\]
as \(N \to \infty\), for some positive constant \(C\).
Let us turn attention away from the curve $32A2$ and instead briefly to $E_1 = 11A3$. The L-series for $E_1$ was specified in [0.5]; the L-series for the quadratic twist $E_{-3}$ corresponds to the curve $99D1$ given by $y^2 + y = x^3 - 3x - 5$. It is known that, for fundamental discriminants $\delta$ satisfying $0 > \delta \equiv 2, 6, 7, 8, 10 \mod 11$, we have [83, 84, 85]

$$L_{E_\delta}(1) = \gamma \cdot c_\delta^2 \frac{1}{\sqrt{-\delta}}$$

where

$$\sum_{n=1}^{\infty} c_n q^n = \frac{1}{2} \sum_{(u,v,w) \in \mathbb{Z}^3, u \equiv v \mod 2} q^{u^2 + 11v^2 + 11w^2} - \frac{1}{2} \sum_{(u,v,w) \in \mathbb{Z}^3, u \equiv v \mod 3, v \equiv w \mod 2} q^{(u^2 + 11v^2 + 33w^2)/3}$$

and $\gamma = \sqrt{3 \Omega_{99D1}} = 2.9176332338\ldots$. An expression for the real period of $99D1$ in terms of gamma function values seems not to be available. This formula for $L_{E_\delta}(1)$ is only the tip of a more general theory due to Shimura [86], Waldspurger [87] and Kohnen & Zagier [88]. See also [89, 90, 91, 92, 93, 94].

The curve $E_1 = 144A1$ (mentioned in [0.3]) has quadratic twist $E_d$ given by $y^2 = x^3 - d^3$. We have, for example [95],

$$L_{E_d}(1) = \frac{1}{2\sqrt{16\pi}} \Gamma \left(\frac{1}{3}\right)^3 \cdot \frac{c_d^2}{\sqrt{d}} = \frac{2}{\sqrt{16}}(1.5299540370\ldots) \cdot \frac{c_d^2}{\sqrt{d}}$$

where $0 < d \equiv 1 \mod 24$ is square-free and

$$\sum_{n=1}^{\infty} c_n q^n = q \prod_{k=1}^{\infty} (1 - q^{12k})^2 \sum_{m=-\infty}^{\infty} q^{m^2}.$$ 

The Fermat cubic $F_1 = 27A1$ (mentioned near the beginning) has quadratic twist $F_d$ given by $y^2 = x^3 - 432d^3$. Similar complicated formulas for $L_{F_d}(1)$ hold, depending again on the sign and modulus of $d$ [96]. We will revisit $F_1$ shortly.

Here is an exercise that is vaguely similar to the congruent number problem [97]. Define

$$g(n) = \# \{(u, v) \in \mathbb{Z}^2 : uv = n \text{ and } u + v = w^2 \text{ for some } w \in \mathbb{Z}\}.$$ 

It turns out, for square-free $d > 0$, that $g(d)$ is a lower bound for $2^{r+2}$, where $r$ is the rank of the elliptic curve $y^2 = x^3 + dx$. No one knows whether $\lim_{d \to \infty} g(d) = \infty$, which would imply that there exist elliptic curves of arbitrarily large rank. We do
know, however, that \( \limsup_{n \to \infty} g(n) = \infty \) and more precisely that [98]

\[
\lim_{N \to \infty} N^{-3/4} \sum_{n=1}^{N} g(n) = 2 \int_{0}^{1} \sqrt{x + \frac{1}{x}} \, dx - \frac{4}{3} = \frac{4}{3} \left( \sqrt{2} - 1 \right) + \frac{1}{3\sqrt{\pi}} \Gamma \left( \frac{1}{4} \right)^2 = 3.0243843195...
\]

0.7. Sums of Two Rational Cubes. Let \( d \) be a cube-free positive integer and \( F_d \) denote the elliptic curve \( y^2 = x^3 - 432d^2 \); recall the special case \( F_1 = 27A1 \) from earlier. Note that the factor here is \( d^2 \) rather than \( d^3 \) as before. It is known that \( 2 < d = u^3 + v^3 \) for \((u, v) \in \mathbb{Q}^2\) if and only if \( F_d \) has nonzero rank. (Reason: the group \( F_d(\mathbb{Q}) \) is torsion-free, hence \( F_d(\mathbb{Q}) \) contains infinitely many points if and only if \( F_d(\mathbb{Q}) \) contains at least one point [99, 100, 101].) By the (weak) BSD conjecture, the latter condition is equivalent to \( L_{F_d}(1) = 0 \). Yet another miraculous \( q \)-expansion result holds for \( F_1 \):

\[
\sum_{n=1}^{\infty} b_n q^n = q \prod_{k=1}^{\infty} \left( 1 - q^{3k} \right)^2 \left( 1 - q^{9k} \right)^2
\]

but formulas for \( L_{F_d}(z) \) via the cubic twist \( F_d \) of \( F_1 \) are considerably more complicated. We defer these until later [102]. No theorem analogous to Tunnell’s is yet known. On the one hand, we have

\[
L_{F_1}(1) = \frac{\sqrt{3}}{18\pi} \frac{1}{3} = 0.5888795834..., \\
L_{F_2}(1) = \frac{3}{3\sqrt{\pi}} L_{F_1}(1) = 0.7010910526..., \\
L_{F_3}(1) = \frac{3^2}{3\sqrt{\pi}} L_{F_1}(1) = 1.129126745..., \\
L_{F_4}(1) = \frac{3^2}{3\sqrt{\pi}} L_{F_1}(1) = 1.129126745..., \\
L_{F_5}(1) = \frac{3^3}{3\sqrt{\pi}} L_{F_1}(1) = 1.0331366085....
\]

On the other hand, \( L_{F_6}(1) = L_{F_7}(1) = L_{F_9}(1) = 0 \). By the BSD conjecture, it can be concluded that 6, 7, 9 are sums of two rational cubes and 3, 4, 5 are not. (Again, these facts are elementary – just for illustration – as are \( 1 = 0^3 + 1^3 \) and \( 2 = 1^3 + 1^3 \).)

Observe that the change of variables \((x, y) \mapsto \left( \sqrt[3]{dx}, \sqrt[3]{dy} \right)\) maps \( F_1 \) to \( F_d \) and is an isomorphism over \( \mathbb{Q}(\sqrt[3]{d}) \). The L-series arising in this case differ from the L-series of \( x^3 + y^3 = 1 \) twisted by cubic Dirichlet characters [103]; hence confusion is possible when surveying the literature. More on \( x^3 + y^3 = d \) is found in [104, 105, 106, 107, 108]. A consequence of the BSD conjecture is that any square-free positive integer \( \equiv 4, 6, 7, 8 \mod 9 \) is a sum of two rational cubes. Further, random matrix theory predicts that [109]

\[
\# \{n \leq N : n \equiv 1, 2, 3, 5 \mod 9 \text{ is square-free and is a sum of two rational cubes} \} \sim C N^{5/6} \ln(N) \sqrt{3/2}^{-1/8}
\]
as \( N \to \infty \), for some positive constant \( C \). It would be more natural to express these asymptotics for cube-free integers, but apparently the result becomes less tractable.

**0.8. Lang’s Conjecture.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Recall that the canonical height \( \hat{h} : E(\mathbb{Q}) \to \mathbb{R} \) satisfies \( \hat{h}(P) = 0 \) if and only if \( P \) is a torsion point. We wonder whether \([110, 111, 112]\)

\[
\inf_{E} \inf_{P \in E(\mathbb{Q})} \text{nontorsion} \hat{h}(P) > 0.
\]

The infimum is certainly small: taking \( E \) to be the minimal model \( y^2 + xy + y = x^3 + x^2 - 125615x + 61201397 \) and \( P \) to be the point \((7107, -602054)\), we obtain \( \hat{h}(P) < 0.0045 \).

Let \( \Delta \) denote the discriminant of \( E \) and let \( E_D \) denote the set of all minimal models \( E \) satisfying \( |\Delta| \geq D \). Lang [113] predicted that the aforementioned infimum is positive and further conjectured that

\[
\inf_{D > 0} \inf_{E \in E_D} \inf_{P \in E(\mathbb{Q})} \text{nontorsion} \frac{\hat{h}(P)}{\ln |\Delta|} > 0.
\]

Again, the infimum is small: for our earlier example, \( \Delta = -149401860048000000 \) and thus \( \hat{h}(P)/\ln |\Delta| < 1.07 \times 10^{-4} \). Elkies [114] found a different example with ratio less than \( 0.85 \times 10^{-4} \). Hindry & Silverman [115], however, demonstrated that Lang’s conjecture would follow from a proof of the important Masser-Oesterlé \( ABC \) conjecture [116, 117, 118]. Another interesting constant is the value of

\[
\lim_{D \to \infty} \inf_{E \in E_D} \inf_{P \in E(\mathbb{Q})} \frac{\hat{h}(P)}{\ln |\Delta|},
\]

which may or may not exceed the preceding. Progress in resolving these issues is reported in \([30, 31, 35, 110, 115, 119, 120, 121]\).

We conclude with a final glimpse at the height \( \hat{h}(P) = 0.0255557041... \) of the point \( P = (0,0) \) on the elliptic curve \( E = 37A1 \). Consider the lattice \( \omega_1 \mathbb{Z} \oplus \omega_2 \mathbb{Z} \), where \( \omega_1, \omega_2 \) are given at the end of \([0.3]\). Over all nonzero lattice points \( \omega \), define the **Weierstrass sigma function**

\[
\sigma(z) = z \prod_{\omega \neq 0} \left( 1 - \frac{z}{\omega} \right) \exp \left( \frac{z}{\omega} + \frac{z^2}{2\omega^2} \right)
\]

as well as constants

\[
\kappa = \int_{1}^{\infty} \frac{dx}{\sqrt{4x^3 - 4x + 1}} = 1.1342732156..., \quad \sigma(\kappa) = 1.1055557990....
\]
Elliptic Curves over $\mathbb{Q}$

It would be good someday to prove that $\hat{h}(P)$ is transcendental; one formula for achieving this might be [36, 122, 123, 124]

$$\hat{h}(P) = \frac{\kappa^2}{4\omega_1} \frac{\sigma'(\omega_1/2)}{\sigma(\omega_1/2)} - \frac{1}{4} \ln (\sigma(\kappa)).$$

Another helpful formula (a decomposition of $\hat{h}(P)$ into a sum of local heights over all primes $p$) appears in [31, 125]. No algebraic height $\hat{h}(P)$, for any curve $E$ and nontorsion point $P$, has ever been found. But a transcendentality proof for even a single case escapes all known efforts.

0.9. Addendum. We merely mention certain averages [126] without details; $p$ and $\ell$ denote primes throughout. Concerning the value distribution of L-series coefficients $b_p$, we have a constant [127, 128, 129]

$$\prod_{\ell} \left(1 - \frac{1}{(\ell - 1)^2(\ell + 1)}\right) = 0.6151326573....$$

Concerning the growth of primes $p$ such that $N_p$ is prime, we have [130, 131, 132]

$$\prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right) = 0.5051661682....$$

Concerning the growth of primes $p$ such that the group $E_p$ (together with a point at infinity) is cyclic, we have [133, 134]

$$\prod_{\ell} \left(1 - \frac{1}{\ell(\ell - 1)^2(\ell + 1)}\right) = 0.8137519061....$$

The constant $2C_{\text{twin}}/\pi^2 = 0.1337767531...$ appears in [135, 136]; recent progress on Lang’s conjecture is reported in [137].

References


[27] T. Dokchitser, ComputeL – Computing special values of L-functions, downloadable PARI scripts from http://maths.dur.ac.uk/~dma0td/computel/.


Elliptic Curves over $\mathbb{Q}$


Elliptic Curves over $\mathbb{Q}$


Elliptic Curves over $\mathbb{Q}$


Elliptic Curves over $\mathbb{Q}$


[111] W. A. Stein, Elliptic curves, the ABC conjecture, and points of small canonical height (Notes from a seminar talk by M. Baker), http://modular.ucsd.edu/mcs/archive/Fall2001/notes/12-10-01/.


