The Structure of Rational Points on Elliptic Curves

Universidad de Sevilla

December 15th, 2006

Two classical results.

Theorem[Mordell]

The group of rational points on an elliptic curve is finitely generated.

Two classical results.

Theorem[Mordell]

The group of rational points on an elliptic curve is finitely generated.

Theorem[Siegel 1929]

The set of integral points on an elliptic curve is finite.

Generalizations

Theorem[Mahler 1934]

Given any elliptic curve E in Weierstrass form, for $P \in E(\mathbb{Q})$, let

$$x(P) = A_P/B_P^2$$

as usual. Fix any finite set S of primes then only finitely many points $P \in E(\mathbb{Q})$ have B_P divisible only by the primes in the set S.

Generalizations

Theorem[Mahler 1934]

Given any elliptic curve E in Weierstrass form, for $P \in E(\mathbb{Q})$, let

$$x(P) = A_P/B_P^2$$

as usual. Fix any finite set S of primes then only finitely many points $P \in E(\mathbb{Q})$ have B_P divisible only by the primes in the set S.

Rationals whose denominators are formed by primes from a set S are called S-*integral*. Thus Mahler's Theorem says there are only finitely many S-integral points on an elliptic curve.

Theorem[Silverman 1986]

Given any infinite set of rational points on an elliptic curve in Weierstrass form. Let

$$x(P) = A_P/B_P^2$$

as usual. Then

$$\frac{\log |A_P|}{2 \log B_P} \to 1,$$

as $\widehat{h}(P) \to \infty$.

2. PRIMALITY

1. Elliptic Curves in Homogeneous Form

Suppose E denotes an elliptic curve defined by an equation

$$E_D : X^3 + Y^3 = D,$$

for some non-zero, cube-free $D \in \mathbb{Q}$. For a rational point on $P \in E(\mathbb{Q})$, write

$$X(P) = \frac{A_P}{B_P}$$

with $A_P, B_P (> 0) \in \mathbb{Z}$, in lowest terms.

Theorem[GE+Miller+Stephens Proc. AMS 2004]
Suppose E denotes an elliptic curve defined by an equation

$$E_D : X^3 + Y^3 = D,$$

for some non-zero, cube-free $D \in \mathbb{Q}$. There are only finitely many points $P \in E(\mathbb{Q})$ for which the integer B_P is a prime (power).

Theorem[GE+Miller+Stephens Proc. AMS 2004]
Suppose E denotes an elliptic curve defined by an equation

$$E_D : X^3 + Y^3 = D,$$

for some non-zero, cube-free $D \in \mathbb{Q}$. There are only finitely many points $P \in E(\mathbb{Q})$ for which the integer B_P is a prime (power).

Note This is not uniform but it is a statement about all rational points - not just the multiples of a single rational point.

Example The taxi-cab equation

$$E_{1729} : X^3 + Y^3 = 1729,$$

has two distinct integral solutions. These give rise to points $P = [1, 12]$ and $Q = [9, 10]$ on the elliptic curve. The only rational points which seem to yield prime power denominators are $2Q$ and $P + Q$ (and their inverses).

Proof

The proof follows easily using the bi-rational transformation we used before as well as Silverman's generalization of Siegel's Theorem. We showed that if

$$P' = \left(\frac{A'_P}{B'^2_P}, \frac{C'_P}{B'^3_P}\right) \in E'_D,$$

with $\gcd(A'_P, B'_P) = 1$, then

$$X(nP) = \frac{36DB'^3_P + C'_P}{6A'_P B'_P}.$$

Proof

The proof follows easily using the bi-rational transformation we used before as well as Silverman's generalization of Siegel's Theorem. We showed that if

$$P' = \left(\frac{A'_P}{B'^2_P}, \frac{C'_P}{B'^3_P}\right) \in E'_D,$$

with $\gcd(A'_P, B'_P) = 1$, then

$$X(nP) = \frac{36DB'^3_P + C'_P}{6A'_P B'_P}.$$

Any cancellation between numerator and denominator divides $6D$ hence it is bounded. By Silverman's Theorem,

$$|A'_P| \text{ and } B'_P \to \infty \text{ as } \widehat{h}(P') \to \infty.$$

Proof

The proof follows easily using the bi-rational transformation we used before as well as Silverman's generalization of Siegel's Theorem. We showed that if

$$P' = \left(\frac{A'_P}{B'^2_P}, \frac{C'_P}{B'^3_P}\right) \in E'_D,$$

with $\gcd(A'_P, B'_P) = 1$, then

$$X(nP) = \frac{36DB'^3_P + C'_P}{6A'_P B'_P}.$$

Any cancellation between numerator and denominator divides $6D$ hence it is bounded. By Silverman's Theorem,

$$|A'_P| \text{ and } B'_P \to \infty \text{ as } \widehat{h}(P') \to \infty.$$

Hence the denominator of $x(P)$ is divisible by two distinct primes with only finitely many exceptions.

2. Elliptic Curves in Weierstrass Form

Let E denote an elliptic curve in Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6,$$

where $a_1, \ldots, a_6 \in \mathbb{Z}$ and $\Delta_E \neq 0$.

Let $P \in E(\mathbb{Q})$ denote a rational point on E. Write

$$x(P) = \frac{A_P}{B_P^2}$$

with $A_P, B_P (> 0) \in \mathbb{Z}$, in lowest terms.

Isogenies

An *isogeny* is a homomorphism between two elliptic curves which is given by rational functions. The *degree* of the isogeny is the degree of the rational functions.

Isogenies

An *isogeny* is a homomorphism between two elliptic curves which is given by rational functions. The *degree* of the isogeny is the degree of the rational functions.

ExampleThe multiplication by m map on an elliptic curve which sends P to mP is an isogeny of degree m^2.

Factorizing Multiplication

More importantly, the $\times m$ map factorizes as a composite of two degree-m isogenies:

$$\phi : E \to E' \text{ and } \phi^* : E' \to E.$$

So the picture is

$$E \to E' \to E \text{ with } \phi^* \phi(P) = mP.$$

Factorizing Multiplication

More importantly, the $\times m$ map factorizes as a composite of two degree-m isogenies:

$$\phi : E \to E' \text{ and } \phi^* : E' \to E.$$

So the picture is

$$E \to E' \to E \text{ with } \phi^* \phi(P) = mP.$$

The map ϕ^* is called the *dual* of ϕ.

The Richelot Isogeny

Suppose E denotes an elliptic curve in the form

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Q}$. The point $[0, 0]$ is a 2-torsion point.

The Richelot Isogeny

Suppose E denotes an elliptic curve in the form

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Q}$. The point $[0, 0]$ is a 2-torsion point.

Consider also the curve E' defined the equation

$$Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

The Richelot Isogeny

Suppose E denotes an elliptic curve in the form

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Q}$. The point $[0, 0]$ is a 2-torsion point.

Consider also the curve E' defined the equation

$$Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

The map

$$\phi(x, y) = (X, Y) \text{ with } X = \frac{y^2}{x^2}$$

is a 2-isogeny between E and E'. A rational point lies in the image of such an isogeny if and only if it is a rational square.

Example 1

Let $a = 0$ and $b = -25$ then the image is the curve

$$Y^2 = X^3 + 100X.$$

The point $[-4, 6]$ maps to $\left[\frac{9}{4}, \frac{41}{8}\right]$.

Example 1

Let $a = 0$ and $b = -25$ then the image is the curve

$$Y^2 = X^3 + 100X.$$

The point $[-4, 6]$ maps to $\left[\frac{9}{4}, \frac{41}{8}\right]$.

Note that the x-coordinate of the image is a square.

For an elliptic curve

$$y^2 = x^3 - T^2 x,$$

the rational point P lies is the image of rational point under a 2-isogeny if and only if $x(P)$ or $x(P) \pm T$ is a rational square.

For an elliptic curve

$$y^2 = x^3 - T^2x,$$

the rational point P lies is the image of rational point under a 2-isogeny if and only if $x(P)$ or $x(P) \pm T$ is a rational square.

Example 2

When $T = 5$ (yesterday) and $P = [-4, 6]$.

Theorem[GE+Stephens+Miller+King]

Suppose $B = (B_n)$ is an EDS coming from an elliptic curve E and $P \in E(\mathbb{Q})$. If P is the image of an algebraic point P' under a non-trivial isogeny and

$$[\mathbb{Q}(P') : \mathbb{Q}] < \deg(\sigma),$$

with $\mathbb{Q}(P')/\mathbb{Q}$ Galois, then only finitely many terms B_n are prime (powers).

Theorem[GE+Stephens+Miller+King]

Suppose $B = (B_n)$ is an EDS coming from an elliptic curve E and $P \in E(\mathbb{Q})$. If P is the image of an algebraic point P' under a non-trivial isogeny and

$$[\mathbb{Q}(P') : \mathbb{Q}] < \deg(\sigma),$$

with $\mathbb{Q}(P')/\mathbb{Q}$ Galois, then only finitely many terms B_n are prime (powers).

For example the theorem applies if P' is a rational point. There are many examples.

Example 1 $E : y^2 = x^3 - 25x, P = [-4, 6]$
There is a non-trivial isogeny mapping a rational point onto P.

Example 1 $E : y^2 = x^3 - 25x, P = [-4, 6]$ There is a non-trivial isogeny mapping a rational point onto P.

n	Factors of B_n
1	1
2	2^2.3
3	37.61
4	2^3.3.7^2.31.41
5	5.13.17.761.10601
6	2^2.3^2.11.37.61.71.587.4799
7	197.421.215153.3498052153
8	2^4.3.7^2.31.41.113279.3344161.4728001
9	37.61.26209.14764833973.1147163247400141

Note

When a point satisfies the condition of the theorem it is said to be *magnified* from P' (because the height increases).

Note

When a point satisfies the condition of the theorem it is said to be *magnified* from P' (because the height increases).

By generalizing this to number fields, there are examples of chains of points, with each point magnified from the previous one. When this happens stronger statements can be proved about the divisibility of the terms in the EDS.

Example

Consider the elliptic curve

$$E : y^2 = x^3 - x^2 - 4x - 2.$$

The point $P = [3, 2]$ lies on E.

Example

Consider the elliptic curve

$$E : y^2 = x^3 - x^2 - 4x - 2.$$

The point $P = [3, 2]$ lies on E.

Let

$$a^2 - 4a - 4 = 0$$

then either point Q with $x(Q) = a$ satisfies $2Q = P$.

Example

Consider the elliptic curve

$$E : y^2 = x^3 - x^2 - 4x - 2.$$

The point $P = [3, 2]$ lies on E.

Let

$$a^2 - 4a - 4 = 0$$

then either point Q with $x(Q) = a$ satisfies $2Q = P$.

Thus P is magnified from Q because the isogeny has degree 4 whereas the extension is quadratic (hence Galois).

Example continued

Now let $b^4 - 16b^3 - 24b^2 - 16b - 8 = 0$ then either point R with $x(R) = b$ satisfies $2R = Q$ hence Q is itself magnified from R.

Example continued

Now let $b^4 - 16b^3 - 24b^2 - 16b - 8 = 0$ then either point R with $x(R) = b$ satisfies $2R = Q$ hence Q is itself magnified from R.

Results of GE+King (2005) show the equation

$$B_n = p^e q^f$$

with p and q distinct primes has only finitely many solutions. In other words, only finitely many terms in the EDS are divisible by at most two distinct prime factors.

Comment

If the elliptic Lehmer problem has an affirmative answer then there are algebraic points which cannot be magnified.

Comment

If the elliptic Lehmer problem has an affirmative answer then there are algebraic points which cannot be magnified.

Reason: Every time a point is magnified, the quantity

$$\frac{\widehat{h}(P)}{[\mathbb{Q}(P):\mathbb{Q}]}$$

goes down by a factor at least 2. The ELP asks if this quantity is uniformly bounded below by a positive constant.

Stronger Conjecture

Given an elliptic curve in Weierstrass form and a non-torsion rational point, let $B = (B_n)$ denote the corresponding EDS. Given any t, there is N_0 such that for all $n > N_0$, B_n has more than t distinct prime factors.

Comments - positive

1. If the stronger conjecture is true, an EDS is the anti-thesis of a sequence such as Mersenne.

Comments - positive

1. If the stronger conjecture is true, an EDS is the anti-thesis of a sequence such as Mersenne.

2. It might even be true that for all large n, B_n has more than t distinct primitive prime factors.

Comments - positive

1. If the stronger conjecture is true, an EDS is the anti-thesis of a sequence such as Mersenne.

2. It might even be true that for all large n, B_n has more than t distinct primitive prime factors.

3. If the curve is in minimal form, perhaps it will be true that N_0 depends on t only.

Comments - negative

1. Although the theorem above resolves the primality conjecture in some cases, the hypothesis is quite strong, and can hold even in higher rank. Thus it a theorem about the structure of rational points in the image of an isogeny.

Comments - negative

1. Although the theorem above resolves the primality conjecture in some cases, the hypothesis is quite strong, and can hold even in higher rank. Thus it a theorem about the structure of rational points in the image of an isogeny.

2. When the rank is greater than 1, and there is no such isogeny, we expect there will indeed be infinitely many prime square denominators.

Comments - negative

1. Although the theorem above resolves the primality conjecture in some cases, the hypothesis is quite strong, and can hold even in higher rank. Thus it a theorem about the structure of rational points in the image of an isogeny.

2. When the rank is greater than 1, and there is no such isogeny, we expect there will indeed be infinitely many prime square denominators.

3. We have not yet found method of proof that is sensitive to our set of rational points being the multiples of a single point.

The theorem that follows generalizes the one stated which was stated earlier for EDSs. It is a theorem about rational points lying inside the image of an isogeny.

Definition We say a subset $G \subset E(\mathbb{Q})$ is *magnified* if it lies in the image of a set G' of algebraic points under a non-trivial isogeny and

$$[\mathbb{Q}(G') : \mathbb{Q}] < \deg(\sigma),$$

with $\mathbb{Q}(G')/\mathbb{Q}$ Galois.

Theorem[GE+Reynolds+Stevens]

Suppose $\sigma : E' \to E$ denotes a non-trivial isogeny defined over $\mathbb{Q}$. Let G denote a magnified subset of $E(\mathbb{Q})$ lying in Im(σ). Writing

$$x(P) = A_P/B_P^2$$

for $P \in G$:

Theorem[GE+Reynolds+Stevens]

Suppose $\sigma : E' \to E$ denotes a non-trivial isogeny defined over $\mathbb{Q}$. Let G denote a magnified subset of $E(\mathbb{Q})$ lying in $\mathrm{Im}(\sigma)$. Writing

$$x(P) = A_P/B_P^2$$

for $P \in G$:

(i) Only finitely many B_P are primes.

Theorem[GE+Reynolds+Stevens]

Suppose $\sigma : E' \to E$ denotes a non-trivial isogeny defined over $\mathbb{Q}$. Let G denote a magnified subset of $E(\mathbb{Q})$ lying in Im(σ). Writing

$$x(P) = A_P/B_P^2$$

for $P \in G$:

(i) Only finitely many B_P are primes.

(ii) The number of prime terms is bounded above in the form

$$c^{\omega(\Delta_E)(r_G+1)}$$

where c depends on deg(σ), r_G denotes the rank of G and $\omega(n)$ denotes the number of distinct prime factors of n.

Theorem[GE+Reynolds+Stevens]

Suppose $\sigma : E' \to E$ denotes a non-trivial isogeny defined over $\mathbb{Q}$. Let G denote a magnified subset of $E(\mathbb{Q})$ lying in $\mathrm{Im}(\sigma)$. Writing

$$x(P) = A_P/B_P^2$$

for $P \in G$:

(i) Only finitely many B_P are primes.

(ii) The number of prime terms is bounded above in the form

$$c^{\omega(\Delta_E)(r_G+1)}$$

where c depends on $\deg(\sigma)$, r_G denotes the rank of G and $\omega(n)$ denotes the number of distinct prime factors of n.

(iii) The exceptions are effectively computable.

Proof Easy case: G' consists of rational points. (a) Finiteness: Write

$$T' \in \text{ker}(\sigma) \text{ and } \sigma(P') = P.$$

Then T' is a torsion point of order dividing deg(σ). Now $P' + T'$ and P' both map to P under σ. However the gcd of the denominators divides the degree of σ.

(i) Let S consist of the primes dividing deg(σ) as well as the bad reduction primes.

(i) Let S consist of the primes dividing deg(σ) as well as the bad reduction primes.

Provided each of P' and $P' + T'$ is not an S-integral point their denominators must include distinct primes. Hence the denominator of P is divisible by at least two distinct primes.

(i) Let S consist of the primes dividing deg(σ) as well as the bad reduction primes.

Provided each of P' and $P' + T'$ is not an S-integral point their denominators must include distinct primes. Hence the denominator of P is divisible by at least two distinct primes.

There are only finitely many S-integral points by Mahler's Theorem.

(ii) The explicit bound follows from a Theorem of Silverman and Gross, which gives an explicit bound for the number of S-integral points on an elliptic curve.

Proof

(iii) Effectiveness: follows using elliptic transcendence theory, some local height analysis as well as the functoriality of the height under isogeny.

Proof

(iii) Effectiveness: follows using elliptic transcendence theory, some local height analysis as well as the functoriality of the height under isogeny.

If $\sigma(P') = P$ then

$$\widehat{h}(P) = \mathrm{deg}(\sigma)\widehat{h}(P').$$

The rational points on G are finitely generated. Writing

$$x(n_1P_1 + \cdots + n_rP_r) = \frac{A_{\underline{n}}}{B_{\underline{n}}^2}.$$

Proof

(iii) Effectiveness: follows using elliptic transcendence theory, some local height analysis as well as the functoriality of the height under isogeny.

If $\sigma(P') = P$ then

$$\widehat{h}(P) = \mathrm{deg}(\sigma)\widehat{h}(P').$$

The rational points on G are finitely generated. Writing

$$x(n_1P_1 + \cdots + n_rP_r) = \frac{A_{\underline{n}}}{B_{\underline{n}}^2}.$$

Also, using the same kind of argument as before,

$$\widehat{h}(n_1P_1 + \cdots + n_rP_r) = Q(\underline{n}) \sim \log B_{\underline{n}}^2,$$

for some positive-definite quadratic form.

Note Use of elliptic transcendence means effectiveness is moral rather than practical. However in some cases, very tight bounds can be found.

Example (Jonathan Reynolds)
For every integer $T > 1$ consider the elliptic curve

$$y^2 = (x + 1)(x - T^2)(x - T^4)$$

together with the EDS generated by the point

$$P = (0, T^3).$$

For all $T > 1$ and all $n > 2$ the denominator of $x(nP)$ is divisible by at least two distinct primes.

Notes on Example

1. This is a parametrised family of curves with a 2-isogeny.

Notes on Example

1. This is a parametrised family of curves with a 2-isogeny.

2. When T is a power of 2, so is B_2.

3. Perfect Powers

Theorem[GE+Reynolds+Stevens]

Let E denote an elliptic curve in Weierstrass form. For any fixed power $f > 1$, there are only finitely many P as above for which B_P is an f-power.

Remarks

1. This theorem is a generalization of Siegel's Theorem that an elliptic curve has only finitely integral points (take $B_P = 1 = 1^f$).

Remarks

1. This theorem is a generalization of Siegel's Theorem that an elliptic curve has only finitely integral points (take $B_P = 1 = 1^f$).

2. Our proof actually shows that for a fixed S, only finitely many points P have B_P equal to an S-integer times an f-power.

Remarks

1. This theorem is a generalization of Siegel's Theorem that an elliptic curve has only finitely integral points (take $B_P = 1 = 1^f$).

2. Our proof actually shows that for a fixed S, only finitely many points P have B_P equal to an S-integer times an f-power.

3. Assuming the ABC-conjecture for number fields, for all sufficiently large f there are no rational points P with B_P equal to an f-power.

Example The elliptic curve

$$E : y^2 = x^3 - 2$$

has $E(\mathbb{Q}) \simeq \mathbb{Z}$ with generator $P = [3, \pm 5]$. Perhaps these two points yield the only perfect power values ($B_P = 1$).

The Toolkit

(I) Faltings' Theorem is invoked at a critical stage.

The Toolkit

(I) Faltings' Theorem is invoked at a critical stage.

(II) The proof is based upon one of the proofs of the theorem about S-integral points, the one which reduces the problem to solving a finite set of S-unit equations.

The genus

Suppose $F(X, Y, Z) = 0$ defines a projective curve of degree $d > 1$. If the curve is non-singular, the *genus* of the curve is defined to be

$$\frac{(d-1)(d-2)}{2}.$$

The genus

Suppose $F(X,Y,Z) = 0$ defines a projective curve of degree $d > 1$. If the curve is non-singular, the *genus* of the curve is defined to be

$$\frac{(d-1)(d-2)}{2}.$$

For example, an elliptic curve is a non-singular cubic curve of genus

$$\frac{(3-1)(3-2)}{2} = 1.$$

(I) Faltings' Theorem

A deep theorem of Faltings says that if C is a curve, defined over a number field K, and the genus of the curve is greater than 1, then the curve will contain only finitely many K-rational points.

(I) Faltings' Theorem

A deep theorem of Faltings says that if C is a curve, defined over a number field K, and the genus of the curve is greater than 1, then the curve will contain only finitely many K-rational points.

Example As soon as $d > 2$, the equation

$$ax^d + by^d = c,$$

with $a, b, c \in K, abc \neq 0$, has only finitely many solutions $x, y \in K$.

Remark Using results of Farhi it is possible, in principle, to give an explicit upper bound for the number of rational points P with B_P equal to an f-power.

Remark Using results of Farhi it is possible, in principle, to give an explicit upper bound for the number of rational points P with B_P equal to an f-power.

This bound will depend upon E and f as well as the maximal K-rank of a finite number of Abelian varieties.

Remark Using results of Farhi it is possible, in principle, to give an explicit upper bound for the number of rational points P with B_P equal to an f-power.

This bound will depend upon E and f as well as the maximal K-rank of a finite number of Abelian varieties.

The dependence upon E arises as the maximal naïve height of the identity elements on these varietes; hence it manifests as the height of a very complicated rational number which is a rational function in the coordinates of the curve.

(II) Valuations and S-units

Let K be a field extension of $\mathbb{Q}$ of finite degree.

(II) Valuations and S-units

Let K be a field extension of $\mathbb{Q}$ of finite degree.

The absolute values on K, written M_K, consist of the usual archimedean absolute values together with the non-archimedean, $\wp$-adic absolute values, one for each prime ideal $\wp$ of K.

(II) Valuations and S-units

Let K be a field extension of $\mathbb{Q}$ of finite degree.

The absolute values on K, written M_K, consist of the usual archimedean absolute values together with the non-archimedean, $\wp$-adic absolute values, one for each prime ideal $\wp$ of K.

Write K_v for the completion of K with respect to v.

Notation

It is often more convenient to work with the *valuation* rather than the absolute value. Thus, if $|.|_v$ is an absolute value, the valuation is

$$v(.) = -\log |.|_v.$$

Notation

It is often more convenient to work with the *valuation* rather than the absolute value. Thus, if $|.|_v$ is an absolute value, the valuation is

$$v(.) = -\log |.|_v.$$

Example If $K = \mathbb{Q}$ and p denotes a prime then v corresponds to a p-adic absolute value $|.|_p$, and for $x \in \mathbb{Q}_p$,

$$v(x) \geq 0 \text{ if and only if } x \in \mathbb{Z}_p.$$

Let $S \subset M_K$ denote a finite set of valuations containing the archimedean valuations. The ring O_S of S-integers is given by

$O_S = \{x \in K : \nu(x) \geq 0$ for all $\nu \in M_K, \nu \notin S\}$

and the unit group O_S^* of O_S is given by

$O_S^* = \{x \in K : \nu(x) = 0$ for all $\nu \in M_K, \nu \notin S\}$.

Thus the S-integers O_S are all the elements of the field which are $\wp$-integral for all prime ideals outside of S.

Thus the S-integers O_S are all the elements of the field which are $\wp$-integral for all prime ideals outside of S.

The S-units are the invertible elements of O_S; all the field elements with numerator and denominator consisting of primes in S.

Examples

1. Let $K = \mathbb{Q}$ and take $S = \{|.|\}$. The ring of S-integers is $\mathbb{Z}$. The group of S-units is $\{\pm 1\}$.

Examples

1. Let $K = \mathbb{Q}$ and take $S = \{|.|\}$. The ring of S-integers is $\mathbb{Z}$. The group of S-units is $\{\pm 1\}$.

2. Let $K = \mathbb{Q}$ and take $S = \{|.|, |.|_2\}$. The ring of S-integers is

$$\mathbb{Z}_S = \left\{ \frac{a}{2^r} : a \in \mathbb{Z}, r \in \mathbb{N} \right\}.$$

The group of S-units is

$$\mathbb{Z}_S^* = \{\pm 2^r : r \in \mathbb{Z}\}.$$

Two Classical Theorems about S-units.

Theorem[Dirichlet's Theorem for S-units.] The group of S-units is finitely generated.

Two Classical Theorems about S-units.

Theorem[Dirichlet's Theorem for S-units.] The group of S-units is finitely generated.

Theorem[Siegel] For any $a, b \in K^*$, the equation

$$au + bv = 1$$

has only finitely many solutions u, v in S-units.

Here again is the theorem we will prove.

Theorem

Let E denote an elliptic curve in Weierstrass form. For any fixed power $f > 1$, there are only finitely many P as above for which B_P is an f-power.

Proof of the Theorem

Completing the square in the Weierstrass equation, it is sufficient to consider an equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where $x^3+a_2x^2+a_4x+a_6 \in \mathbb{Q}[x]$ has distinct zeros $\alpha_1, \alpha_2, \alpha_3$ in some finite extension K of $\mathbb{Q}$.

Proof of the Theorem

Completing the square in the Weierstrass equation, it is sufficient to consider an equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

where $x^3 + a_2x^2 + a_4x + a_6 \in \mathbb{Q}[x]$ has distinct zeros $\alpha_1, \alpha_2, \alpha_3$ in some finite extension K of $\mathbb{Q}$.

Of course we might have introduced powers of 2 into the denominators in (1); we will see that this does not matter.

Let $P = (x/q^2, y/q^3)$ be a solution to (1) with $x, y \in \mathbb{Q} \cap O_S$, $q = m^f$ and $\gcd(xy, q) = 1$. We will show that, for fixed $f > 1$, there are finitely many choices for P.

Let $P = (x/q^2, y/q^3)$ be a solution to (1) with $x, y \in \mathbb{Q} \cap O_S$, $q = m^f$ and $\gcd(xy, q) = 1$. We will show that, for fixed $f > 1$, there are finitely many choices for P.

By factorising the cubic and multipling through by q^6, from (1) we obtain

$$y^2 = (x - q^2\alpha_1)(x - q^2\alpha_2)(x - q^2\alpha_3). \qquad (2)$$

Let S be a sufficiently large (finite) subset of M_K so that O_S is a PID and $2, \alpha_i - \alpha_j \in O_S^*$ for all $i \neq j$.

Let S be a sufficiently large (finite) subset of M_K so that O_S is a PID and $2, \alpha_i - \alpha_j \in O_S^*$ for all $i \neq j$.

Now let L/K be the extension of K obtained by adjoining to K the square root of every element of O_S^*.

Let S be a sufficiently large (finite) subset of M_K so that O_S is a PID and $2, \alpha_i - \alpha_j \in O_S^*$ for all $i \neq j$.

Now let L/K be the extension of K obtained by adjoining to K the square root of every element of O_S^*.

Note that L/K is a finite extension, since $O_S^*/(O_S^*)^2$ is finite from Dirichlet's S-unit theorem.

Let S be a sufficiently large (finite) subset of M_K so that O_S is a PID and $2, \alpha_i - \alpha_j \in O_S^*$ for all $i \neq j$.

Now let L/K be the extension of K obtained by adjoining to K the square root of every element of O_S^*.

Note that L/K is a finite extension, since $O_S^*/(O_S^*)^2$ is finite from Dirichlet's S-unit theorem.

Further let $T \subset M_L$ be a finite set containing the absolute values of L lying over elements of S and such that O_T is a PID where, by abuse of notation, O_T denotes the ring of T-integers in L.

Let $\wp$ be a prime ideal of O_S dividing $x - q^2\alpha_i$; then $\wp$ cannot divide q, since $(x, q) = 1$.

Let $\wp$ be a prime ideal of O_S dividing $x-q^2\alpha_i$; then $\wp$ cannot divide q, since $(x,q)=1$.

Hence $\wp$ can divide at most one term $x-q^2\alpha_i$, since if it divides both $x-\alpha_i q^2$ and $x-\alpha_j q^2$ then it divides also $(\alpha_i-\alpha_j)q^2$.

Let $\wp$ be a prime ideal of O_S dividing $x-q^2\alpha_i$; then $\wp$ cannot divide q, since $(x,q)=1$.

Hence $\wp$ can divide at most one term $x-q^2\alpha_i$, since if it divides both $x-\alpha_i q^2$ and $x-\alpha_j q^2$ then it divides also $(\alpha_i-\alpha_j)q^2$.

From (2) it follows that there are elements $z_i \in O_S$ and units $b_i \in O_S^*$ so that

$$x-\alpha_i q^2 = b_i z_i^2.$$

We have $b_i = \beta_i^2$, for some $\beta_i \in O_T$ so

$$x - \alpha_i q^2 = (\beta_i z_i)^2. \tag{3}$$

We have $b_i = \beta_i^2$, for some $\beta_i \in O_T$ so

$$x - \alpha_i q^2 = (\beta_i z_i)^2. \tag{3}$$

Taking the difference of any two of these equations yields

$$(\alpha_j - \alpha_i)q^2 = (\beta_i z_i - \beta_j z_j)(\beta_i z_i + \beta_j z_j).$$

We have $b_i = \beta_i^2$, for some $\beta_i \in O_T$ so

$$x - \alpha_i q^2 = (\beta_i z_i)^2. \qquad (3)$$

Taking the difference of any two of these equations yields

$$(\alpha_j - \alpha_i)q^2 = (\beta_i z_i - \beta_j z_j)(\beta_i z_i + \beta_j z_j).$$

Note that $\alpha_j - \alpha_i \in O_T^*$ while each of the two factors on the right is in O_T. It follows that each of these factors is made from primes $\pi | m$ in O_T.

We have $b_i = \beta_i^2$, for some $\beta_i \in O_T$ so

$$x - \alpha_i q^2 = (\beta_i z_i)^2. \tag{3}$$

Taking the difference of any two of these equations yields

$$(\alpha_j - \alpha_i)q^2 = (\beta_i z_i - \beta_j z_j)(\beta_i z_i + \beta_j z_j).$$

Note that $\alpha_j - \alpha_i \in O_T^*$ while each of the two factors on the right is in O_T. It follows that each of these factors is made from primes $\pi | m$ in O_T.

Further we may assume these factors are coprime, since if $\pi | m$ divides $2\beta_i z_i$ then from (3) π divides x.

Siegel's identity is the following:

$$\frac{\beta_1 z_1 \pm \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \mp \frac{\beta_2 z_2 \pm \beta_3 z_3}{\beta_1 z_1 - \beta_3 z_3} = 1.$$

Siegel's identity is the following:

$$\frac{\beta_1 z_1 \pm \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \mp \frac{\beta_2 z_2 \pm \beta_3 z_3}{\beta_1 z_1 - \beta_3 z_3} = 1.$$

This gives

$$a_m^{2f} u + b_m^{2f} v = c_m^{2f} \tag{4}$$

for T-units u and v where $a_m, b_m, c_m \in O_T$ divide m and are pairwise coprime.

Note that the group $O_T^*/(O_T^*)^{2f}$ is finite so we fix once and for all a set of coset representatives.

Note that the group $O_T^*/(O_T^*)^{2f}$ is finite so we fix once and for all a set of coset representatives.

Then (4) gives us a solution of an equation:

$$ux^{2f} + vy^{2f} = 1, \qquad x, y \in L,$$

with $2f \geq 4$, where u and v belong to this finite set of representatives, which depends only upon T and f.

Note that the group $O_T^*/(O_T^*)^{2f}$ is finite so we fix once and for all a set of coset representatives.

Then (4) gives us a solution of an equation:

$$ux^{2f} + vy^{2f} = 1, \qquad x, y \in L,$$

with $2f \geq 4$, where u and v belong to this finite set of representatives, which depends only upon T and f.

Each such curve has genus

$$(2f-1)(f-1) \geq 3.$$

Note that the group $O_T^*/(O_T^*)^{2f}$ is finite so we fix once and for all a set of coset representatives.

Then (4) gives us a solution of an equation:

$$ux^{2f} + vy^{2f} = 1, \qquad x, y \in L,$$

with $2f \geq 4$, where u and v belong to this finite set of representatives, which depends only upon T and f.

Each such curve has genus

$$(2f-1)(f-1) \geq 3.$$

Faltings' Theorem guarantees there are only finitely many solutions.

Hence, since f is fixed, there are finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Hence, since f is fixed, there are finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Multiplying these two numbers, there are finitely many choices for

$$\frac{(\alpha_1 - \alpha_2) q^2}{(\beta_1 z_1 - \beta_3 z_3)^2},$$

Hence, since f is fixed, there are finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Multiplying these two numbers, there are finitely many choices for

$$\frac{(\alpha_1 - \alpha_2) q^2}{(\beta_1 z_1 - \beta_3 z_3)^2},$$

hence finitely many for

$$\frac{q}{\beta_1 z_1 - \beta_3 z_3}.$$

Hence, since f is fixed, there are finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Multiplying these two numbers, there are finitely many choices for

$$\frac{(\alpha_1 - \alpha_2) q^2}{(\beta_1 z_1 - \beta_3 z_3)^2},$$

hence finitely many for

$$\frac{q}{\beta_1 z_1 - \beta_3 z_3}.$$

But

$$\frac{\beta_1 z_1}{q} = \frac{1}{2}\left[\frac{\beta_1 z_1 - \beta_3 z_3}{q} + \frac{(\alpha_3 - \alpha_1) q}{\beta_1 z_1 - \beta_3 z_3}\right]$$

Hence, since f is fixed, there are finitely many choices for

$$\frac{\beta_1 z_1 + \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3} \text{ and } \frac{\beta_1 z_1 - \beta_2 z_2}{\beta_1 z_1 - \beta_3 z_3}.$$

Multiplying these two numbers, there are finitely many choices for

$$\frac{(\alpha_1 - \alpha_2) q^2}{(\beta_1 z_1 - \beta_3 z_3)^2},$$

hence finitely many for

$$\frac{q}{\beta_1 z_1 - \beta_3 z_3}.$$

But

$$\frac{\beta_1 z_1}{q} = \frac{1}{2}\left[\frac{\beta_1 z_1 - \beta_3 z_3}{q} + \frac{(\alpha_3 - \alpha_1) q}{\beta_1 z_1 - \beta_3 z_3}\right]$$

so from (3) there are finitely many choices for $x(P)$. For each choice of $x(P)$ there are at most two choices for $y(P)$.