

A Generalisation of Siegel's Theorem

Jonathan Reynolds

School of Mathematics
University of East Anglia
Norwich

November 2006

Let K be a number field and R its ring of integers. Let M_K consist of the standard absolute values on K . Let S denote a fixed finite subset of M_K containing the archimedean absolute values. The ring R_S of S -integers is given by

$$R_S = \{x \in K : |x| \leq 1 \text{ for all } |\cdot| \in M_K, |\cdot| \notin S\}.$$

Let K be a number field and R its ring of integers. Let M_K consist of the standard absolute values on K . Let S denote a fixed finite subset of M_K containing the archimedean absolute values. The ring R_S of S -integers is given by

$$R_S = \{x \in K : |x| \leq 1 \text{ for all } |\cdot| \in M_K, |\cdot| \notin S\}.$$

Assume that S contains the finitely many non-archimedean absolute values which make R_S a principal ideal domain.

Example of an S -integer ring

Let

$$S = \{3, 7, \infty\}.$$

Then

$$\{3^n 7^m a : n, m, a \in \mathbb{Z}\}$$

is the ring of S -integers

Example of an S -integer ring

Let

$$S = \{3, 7, \infty\}.$$

Then

$$\{3^n 7^m a : n, m, a \in \mathbb{Z}\}$$

is the ring of S -integers and

$$\{\pm 3^n 7^m : n, m \in \mathbb{Z}\}$$

is the group of S -units.

Example of an S-integer ring

Let $K = \mathbb{Q}(\sqrt{2})$ and

$$S = \{1 \pm 2\sqrt{2}, \infty_{\pm}\}$$

where ∞_{\pm} correspond to the archimedean absolute values on K given by

$$|a + b\sqrt{2}|_{\infty_{\pm}} = |a \pm b\sqrt{2}|_{\infty}.$$

Example of an S -integer ring

Let $K = \mathbb{Q}(\sqrt{2})$ and

$$S = \{1 \pm 2\sqrt{2}, \infty_{\pm}\}$$

where ∞_{\pm} correspond to the archimedean absolute values on K given by

$$|a + b\sqrt{2}|_{\infty_{\pm}} = |a \pm b\sqrt{2}|_{\infty}.$$

Then

$$\frac{3}{7} = \frac{-3}{(1 + 2\sqrt{2})(1 - 2\sqrt{2})}$$

is an S -integer of K because 7 is an S -unit.

Let E denote an elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + ax^2 + bx + c \quad (1)$$

with S -integral coefficients $a, b, c \in R_S$.

Let E denote an elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + ax^2 + bx + c \quad (1)$$

with S -integral coefficients $a, b, c \in R_S$. For an element $P \in E(K)$, using the shape of the equation (1) we can write

$$P = \left(\frac{A_P}{B_P^2}, \frac{C_P}{B_P^3} \right) \quad (2)$$

where A_P, B_P, C_P are coprime in R_S .

- ▶ A consequence of Siegel's Theorem (first proven in 1929) is that there are finitely many $P \in E(K)$ such that $B_P = 1$. Siegel gave two proofs: one uses distance functions and heights, another uses an S -unit equation.

- ▶ A consequence of Siegel's Theorem (first proven in 1929) is that there are finitely many $P \in E(K)$ such that $B_P = 1$. Siegel gave two proofs: one uses distance functions and heights, another uses an S -unit equation.
- ▶ It is enough to prove that $u + v = 1$ has finitely many solutions in S -units u, v . This can be done using Roth's theorem (1955).

Roth's Theorem for \mathbb{Q}

Let $\alpha \in \overline{\mathbb{Q}}$. Given any $\epsilon > 0$, there are finitely many $p/q \in \mathbb{Q}$ satisfying the inequality

$$\left| \frac{p}{q} - \alpha \right| < \frac{1}{q^{2+\epsilon}}$$

Roth's Theorem (1955)

Let $\alpha \in \overline{K}$ and $\nu \in M_{K(\alpha)}$. Then for any constant C , there exist only finitely many $x \in K$ satisfying the inequality

$$|x - \alpha|_\nu < C \left(\prod_{\nu \in M_K} \max\{|x|_\nu, 1\} \right)^{-(2+\epsilon)}$$

Roth's Theorem (1955)

Let $\alpha \in \overline{K}$ and $\nu \in M_{K(\alpha)}$. Then for any constant C , there exist only finitely many $x \in K$ satisfying the inequality

$$|x - \alpha|_\nu < C \left(\prod_{\nu \in M_K} \max\{|x|_\nu, 1\} \right)^{-(2+\epsilon)}$$

There were several earlier versions of this statement. In 1921, Siegel proved the statement with $2 + \epsilon$ replaced by

$$\sqrt{2[K(\alpha) : K]} + \epsilon.$$

- ▶ Roth's theorem is ineffective. Baker, Coates, Lang, Zagier and others have found effective methods in certain cases.

Example where all S -integer points are known

$$E : y^2 = x^3 - 172x + 505$$

Pethő, Zimmer, Gebel and Herrmann have proven that there are exactly:

- ▶ 58 integer points on E
- ▶ 144 S -integer points on E where $S = \{3, 5, 7, \infty\}$.

Amongst the largest are

$$(1402464, 1660877429) \text{ and } \left(\frac{33524044}{3^2}, \frac{194104052639}{3^3} \right).$$

Fix an integer $f > 1$. In the proof of Siegel's Theorem, by replacing Roth's Theorem by Faltings' Theorem (1983), we will see that there are finitely many $P \in E(K)$ with B_P equal to an S -integer raised to the power f .

Faltings' Theorem (1983)

- ▶ Given a curve C , there exists an integer (invariant under birational transformation) called the genus of C .
- ▶ Faltings' Theorem says that if C/K has genus greater than 1, then there are finitely many K -rational points on C .

The genus of certain curves

An elliptic curve has genus 1 (by definition).

For a positive integer m and any non-zero $\alpha, \beta \in \mathbb{C}$, the curve

$$\alpha X^m + \beta Y^m = 1$$

has genus

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

- ▶ The proof is ineffective - there is no procedure for finding all points $P \in E(K)$ with B_P equal to an S -integer raised to the power $f(> 1)$.
- ▶ Currently, there is no elliptic curve with positive rank where all such points are known.

Motivation behind Siegel's proof

Long before the work of Siegel, all integral solutions to

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

and

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

were known.

Motivation behind Siegel's proof

Assume $x, y \in \mathbb{Z}$. The equation

$$y^2 = x^3 + x = x(x^2 + 1)$$

forces x and $x^2 + 1$ to be squares in \mathbb{Z} . It follows that $x = y = 0$.
The equation

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

is dealt with by factorising in $\mathbb{Z}[\sqrt{-2}]$.

Motivation behind Siegel's proof

In general, the idea is similar.

- ▶ Assume $x, y \in R_S$.
- ▶ Factorise the equation as

$$y^2 = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

- ▶ “Force the factors $x - \alpha_i$ to be squares.”
- ▶ Deduce that there are finitely many choices for x .

Adapting Siegel's proof

By substituting P into the given Weierstrass equation, we deduce

$$C_P^2 = (A_P - \alpha_1 B_P^2)(A_P - \alpha_2 B_P^2)(A_P - \alpha_3 B_P^2)$$

where $\alpha_1, \alpha_2, \alpha_3$ are the zeros of $x^3 + ax^2 + bx + c$.

Adapting Siegel's proof

Let $K' = K(\alpha_1, \alpha_2, \alpha_3)$. Let T be a fixed finite set of $M_{K'}$ containing:

1. the valuations which extend the valuations in S ;
2. for all $i \neq j$, the valuations which divide $(\alpha_i - \alpha_j)$;
3. the finitely many valuations required to make the ring of T -integers of K' a unique factorisation domain.

Adapting Siegel's proof

Let \mathcal{R}_T denote the ring of T -integers of K' . If a prime $\pi \in \mathcal{R}_T$ dividing C_P divides $(A_P - \alpha_i B_P^2)$ and $(A_P - \alpha_j B_P^2)$ then it divides

$$(\alpha_i - \alpha_j)B_P^2.$$

So the factors $(A_P - \alpha_i B_P^2)$ are coprime in \mathcal{R}_T .

Dirichlet's S -unit Theorem

Fix a positive integer m . The set of cosets $R_S^*/(R_S^*)^m$ is finite.

Dirichlet's S -unit Theorem

Fix a positive integer m . The set of cosets $R_S^*/(R_S^*)^m$ is finite.

So fix coset representatives u_1, \dots, u_t where $t = |\mathcal{R}_T^*/(\mathcal{R}_T^*)^2|$. Put

$$L = K'(\sqrt{u_1}, \dots, \sqrt{u_t}).$$

Forcing $A_P - \alpha_i B_P^2$ to be square

Let U be a fixed finite set of M_L containing:

1. the valuations which extend the valuations in T ;
2. the valuations which divide 2;
3. the finitely many valuations required to make the ring of U -integers of L a unique factorisation domain.

Forcing $A_P - \alpha_i B_P^2$ to be square

Let \mathfrak{R}_U be the ring of U -integers of L , then

$$A_P - \alpha_i B_P^2 = z_i^2$$

where $z_i \in \mathfrak{R}_U$.

Adapting Siegel's proof

Subtracting any two different factors gives

$$\begin{aligned}(\alpha_j - \alpha_i)B_P^2 &= z_i^2 - z_j^2 \\ &= (z_i - z_j)(z_i + z_j).\end{aligned}$$

Hence $z_i \pm z_j$ are made from primes dividing B_P and are coprime.

Getting back to P

Suppose a condition on P forced there to be finitely many choices for

$$\frac{z_1 \pm z_2}{z_1 - z_3}.$$

Getting back to P

Multiplying these two numbers, there would be finitely many choices for

$$\frac{(z_1 + z_2)(z_1 - z_2)}{(z_1 - z_3)^2} = \frac{(\alpha_1 - \alpha_2)B_P^2}{(z_1 - z_3)^2},$$

hence finitely many for

$$\frac{B_P}{z_1 - z_3}.$$

Getting back to P

Multiplying these two numbers, there would be finitely many choices for

$$\frac{(z_1 + z_2)(z_1 - z_2)}{(z_1 - z_3)^2} = \frac{(\alpha_1 - \alpha_2)B_P^2}{(z_1 - z_3)^2},$$

hence finitely many for

$$\frac{B_P}{z_1 - z_3}.$$

But

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

and

$$x(P) = \frac{A_P}{B_P^2} = \alpha_1 + \frac{z_1^2}{B_P^2}.$$

Siegel's identity

Siegel's identity:

$$\frac{z_1 \pm z_2}{z_1 - z_3} \mp \frac{z_2 \pm z_3}{z_1 - z_3} = 1$$

restricts the values that

$$\frac{z_1 \pm z_2}{z_1 - z_3}$$

can take.

$$B_p = 1$$

If $B_p = 1$, then Siegel's identity becomes

$$u + v = 1, \quad u, v \in \mathfrak{R}_U^*$$

Using Dirichlet's theorem,

$$\alpha X^m + \beta Y^m = 1, \quad X, Y \in \mathfrak{R}_U^*$$

where there are finitely many choices for α, β .

$$B_p = 1$$

Roth's Theorem can be used to show that, for

$$m > 2[L : \mathbb{Q}||U|,$$

there are finitely many choices for X , so finitely many for

$$\alpha X^m = \frac{z_1 \pm z_2}{z_1 - z_3}.$$

$$B_P = 1$$

Roth's Theorem can be used to show that, for

$$m > 2[L : \mathbb{Q}||U|,$$

there are finitely many choices for X , so finitely many for

$$\alpha X^m = \frac{z_1 \pm z_2}{z_1 - z_3}.$$

Theorem (Siegel)

There are finitely many $P \in E(K)$ with $B_P = 1$.

$$B_p = r^f, f > 1$$

Fix an integer $f > 1$. If B_p is an S -integer raised to the power f , then Siegel's identity becomes

$$\alpha x^{2f} + \beta y^{2f} = 1, \quad x, y \in L$$

where there are finitely many choices for α, β .

$$B_P = r^f, f > 1$$

These curves have genus > 1 . So by Faltings' Theorem, there are finitely many choices for x , hence finitely many for

$$\alpha x^{2f} = \frac{z_1 \pm z_2}{z_1 - z_3}.$$

$$B_P = r^f, f > 1$$

These curves have genus > 1 . So by Faltings' Theorem, there are finitely many choices for x , hence finitely many for

$$\alpha x^{2f} = \frac{z_1 \pm z_2}{z_1 - z_3}.$$

Theorem

Fix an integer $f > 1$. There are finitely many $P \in E(K)$ with B_P equal to an S -integer raised to the power f .

$$B_P = r^f, f > 1$$

Assuming the *ABC*-conjecture for number fields, for all sufficiently large f there are no points $P \in E(K)$ with B_P equal to an S -integer raised to the power f .

ABC-Conjecture for \mathbb{Q}

Let A, B, C be non-zero pairwise coprime integers satisfying $A + B + C = 0$. Define

$$N = \prod_{p|ABC} p.$$

Then for every $\epsilon > 0$, there exists $\kappa(\epsilon) > 0$ such that

$$\max\{|A|, |B|, |C|\} < \kappa N^{1+\epsilon}.$$

ABC-Conjecture for number fields

Let $\alpha, \beta, \gamma \in K$ satisfy $\alpha + \beta + \gamma = 0$. Define the conductor:

$$N(\alpha, \beta, \gamma) = \prod_{\mathfrak{p} \in I} |\mathfrak{p}|_{\mathfrak{p}}^{-1}$$

where I denotes the set of prime ideals \mathfrak{p} such that $|\alpha|_{\mathfrak{p}}, |\beta|_{\mathfrak{p}}, |\gamma|_{\mathfrak{p}}$ are not all equal. Then for every $\epsilon > 0$, there exists $\kappa(\epsilon, K) > 0$ such that

$$\prod_{\nu \in M_K} \max\{|\alpha|_{\nu}, |\beta|_{\nu}, |\gamma|_{\nu}\} \leq \kappa N(\alpha, \beta, \gamma)^{1+\epsilon}.$$

ABC-Conjecture \implies Fermat's Last Theorem

Suppose $x, y, z \in \mathbb{Z}$ are such that $\gcd(x, y, z) = 1$ and $x^n + y^n = z^n$. By ABC,

$$\max\{|x^n|, |y^n|, |z^n|\} < \kappa |xyz|^{1+\frac{\epsilon}{3}}$$

So $|xyz|^n < \kappa^3 |xyz|^{3+\epsilon}$.

ABC-Conjecture \implies Fermat's Last Theorem

Suppose $x, y, z \in \mathbb{Z}$ are such that $\gcd(x, y, z) = 1$ and $x^n + y^n = z^n$. By ABC,

$$\max\{|x^n|, |y^n|, |z^n|\} < \kappa |xyz|^{1+\frac{\epsilon}{3}}$$

So $|xyz|^n < \kappa^3 |xyz|^{3+\epsilon}$. Hence if $|xyz| > 1$, then n is bounded.

A good contender?

Maybe if

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

has a rational point $P \in E(\mathbb{Q})$ with B_P a perfect power in \mathbb{Z} then

$$P = [3, \pm 5]$$

n	B_{nP}
2	$2 \cdot 5$
3	$3^2 \cdot 19$
5	$29 \cdot 211 \cdot 2069$
7	$7^2 \cdot 769 \cdot 1049 \cdot 1487809$

Prime values of B_P

If $B_P = \pi$ is a prime in R_S then Siegel's identity gives

$$\alpha\rho_1^2 + \beta\rho_2^2 = \rho_3^2$$

where $\rho_1, \rho_2, \rho_3 \in \mathfrak{K}_U$ divide π and are pairwise coprime.

Are there finitely many choices for $\frac{\rho_1}{\rho_3}$?

Prime values of B_P

- ▶ For some “well behaved” curves the method does bound $|B_P|$ explicitly.
- ▶ Height estimates can then be used to bound the number of points.

Example

Let

$$E : y^2 = x^3 - 25x.$$

This curve has rank 1 with non-torsion generator $(-4, 6)$.

There are no points $P \in E(\mathbb{Q})$ with B_P prime.