1 Introduction

1.1 Pythagorean Triples

We begin with a problem that most high school students have seen the solution to: what triples of integers represent the sides of a right triangle?

The Pythagorean equation for a triangle with sides $x, y, z$ says that the sum of the squares of the two legs must equal to the square of the hypotenuse. By Pythagoras’s theorem, the problem of finding right triangles with integer sides becomes the problem of finding integral points on the projective curve $x^2 + y^2 = z^2$.

Since the solutions to Pythagoras’s equation are homogenous we can make the substitutions $X = x/z$ and $Y = y/z$ to obtain the new equation $X^2 + Y^2 = 1$. Solutions to $x^2 + y^2 = z^2$ in integers correspond to rational solutions of $X^2 + Y^2 = 1$. However, $X^2 + Y^2 = 1$ is a familiar geometric object: it defines the unit circle in $\mathbb{R}^2$.

By projecting from the point $(0, 1)$ we can parametrize the unit circle. A line of slope $-t$ starting at $(0, 1)$ intersects the circle at one other point, $(2t, t^2 - 1)$. Then, $X$ and $Y$ are rational if and only if $t$ is rational, so letting $t = m/n$ for integers $m, n$ relatively prime, we get the solution

$$(X, Y) = \left( \frac{2mn}{n^2 + m^2}, \frac{m^2 - n^2}{n^2 + m^2} \right)$$

or $(x, y, z) = (2mn, m^2 - n^2, m^2 + n^2)$ up to some scaling factor $\lambda \in \mathbb{Z}$.

In finding solutions to Pythagoras’s equation we relied on the fact that we could parametrize the circle using lines through a single point: however, this is only possible for a genus zero curve. Any genus zero curve is isomorphic to a conic, and if it has a rational point on it, then it is isomorphic to $\mathbb{P}^1$. Thus, the rational points of $\mathbb{P}^1$ give us the
rational points of the curve, and we can find infinitely many rational points. However, for higher genus curves, this is a much harder problem.

In addition to finding actual integer triples, we may want to ask how many coprime integer triples with absolute value at most \( N > 0 \) we can find: in this case, we are asking that \(|x|, |y|, |z| < N\), and the equation \( m^2 + n^2 < N^{1/2} \) shows that we are looking for integer points inside a circle of radius \( N^{1/4} \). There are about \( N^{1/2} \) such points, though we must multiply by a constant to rule out non-coprime solutions. Throughout the rest of this paper we will explore these problems of finding integral points on curves and bounding their absolute value in the setting of higher genus curves. To get there, we will need to develop new techniques, a more general notion of absolute value, a notion of the height of a rational number, and a theory of Diophantine approximation, measuring how close we can come to approximating an algebraic number using a rational number of bounded height.

1.2 Fermat’s Last Theorem

The problem of finding integer points on higher genus curves also has a long and famous history. Fermat generalized Pythagoras’s problem of finding integer solutions to \( x^2 + y^2 = z^2 \), asking whether the equation \( x^n + y^n = z^n \) has integer solutions. For \( n = 3 \), the genus of the projective curve \( x^3 + y^3 = z^3 \) is given by \( (n-1)(n-2)/2 \), so solving Fermat’s equation reduces to finding integer points on the elliptic curve \( x^3 + y^3 = z^3 \).

Elliptic curves have a group law, and, given a rational point \( P \) on the curve \( X^3 + Y^3 = 1 \), we can find another rational point by taking the tangent to \( P \) and seeing where it hits the curve \( X^3 + Y^3 = 1 \). Bezout’s theorem implies that a line meets a degree 3 curve at exactly three points, so when two of these points are rational, as in the case of a tangent at a rational point, or a chord connecting two rational points, then the third is guaranteed to be rational too. While it is beyond the scope of this paper, it bears noting that Mordell proved that to find all rational points on an elliptic curve, one only needs to start with a finite set of rational points, and from there, using tangents at rational points and lines connecting the rational points, one can obtain all other rational points. In group-theoretic language, Mordell proved that the group of rational points on an elliptic curve is finitely generated. Looking at the rank of this group of rational points, we can actually figure out how many rational points have absolute value at most \( N \): it is given by \( C(\log N)^r/2 \) where \( r \) is the rank, and \( C \) is a positive constant depending on the curve. In the case of the Fermat curve of degree three, \( r = 0 \) so there are only finitely many rational solutions to \( x^3 + y^3 = z^3 \), which are known to be \((1, 0, 1), (0, 1, 1)\) and \((-1, 1, 0)\).

2 The ABC Conjecture

Masser and Oesterlé generalized the Fermat equation and other Diophantine equations to the problem of finding \( A, B, C \) are coprime integers such that \( A + B = C \). For reasons that
will become clear as we continue to study these types of equations, they conjectured the following condition on the prime factors of $A, B, C$, called the ABC Conjecture.

**Conjecture 1** (Masser-Oesterlé). *Given $\varepsilon > 0$, there exists $K_\varepsilon > 0$ such that*

$$\text{rad}(ABC) > K_\varepsilon C^{1-\varepsilon}$$

*for any coprime integers $A, B, C$ such that $A + B = C$.*

*More symmetrically, we can restate this as, given $\varepsilon > 0$, there exists $K_\varepsilon > 0$ such that*

$$\text{rad}(ABC) > K_\varepsilon \max\{|A|, |B|, |C|\}^{1-\varepsilon}$$

*for all coprime integers $A, B, C$ such that $\pm A \pm B \pm C = 0$.*

**Definition.** If $n \in \mathbb{N}$ is a natural number, we define

$$\text{rad}(N) := \prod_{p|n, p \text{ prime}} p$$

to be the product of primes dividing $n$ without multiplicity (i.e. the smallest square-free number dividing $n$.)

As one example of the power of the ABC conjecture, we can show that the ABC conjecture implies an asymptotic version of Fermat’s Last Theorem: one way to see this is by defining the power,

$$\theta(A, B, C) := \frac{\log(C^n)}{\log(\text{rad}(ABC))}$$

noting that $C = \text{rad}(ABC)^{\theta(A, B, C)}$. Then the ABC conjecture is equivalent to the statement that

$$\limsup_{(A, B, C) \to (A, B, C)} \theta(A, B, C) \leq 1$$

where $(A, B, C)$ runs over all coprime triples $A + B = C$. Then setting $(x^n, y^n, z^n) = (A, B, C)$ we can see that

$$\theta(x^n, y^n, z^n) = \frac{\log(z^n)}{\log(\text{rad}(x^n y^n z^n))} \geq \frac{n \log(z)}{\log(\text{rad}(a) \text{ rad}(b) \text{ rad}(c))} > \frac{n \log(c)}{\log(c^3)} = \frac{n}{3}.$$ 

Thus ABC implies that there can be only finitely many $A^n + B^n = C^n$ for which Fermat’s equation can hold when $n > 3$, since $1 \geq \theta(A, B, C) > \frac{2}{3}$ for all but finitely many $A, B, C$. 

2.1 Mason-Stothers Theorem

As evidence for the ABC Conjecture, it is possible to prove it when \(a, b, c \in K[t]\) are nonconstant polynomials. We will let \(K\) be an algebraically closed field of characteristic 0 and provide two proofs: one elementary proof using derivatives and linear algebra, and another proof which uses the Riemann-Hurwitz theorem and exploits the geometry of the situation.

The following elementary proof is due to Noah Snyder. We define \(\Delta(t)\) to be the determinant of the two by two matrix

\[
\begin{bmatrix}
a(t) & b(t) \\
a'(t) & b'(t)
\end{bmatrix}
\]

which can also be written

\[
\Delta(t) = a(t)c'(t) - a'(t)c(t) = c(t)b'(t) - c'(t)b(t)
\]

by adding one column to another, and using the fact that \(a'(t) + b'(t) = c'(t)\). Furthermore, \(\Delta(t) \neq 0\), because \(b(t)\) is not a scalar multiple of \(a(t)\).

Notice that \(\gcd(a, a')\) divides \(a(t)c'(t) - a'(t)c(t) = \Delta(t)\) and symmetrically, so do \(\gcd(b, b')\) and \(\gcd(c, c')\). Since \(a, b,\) and \(c\) are coprime, we must have that the product \(\gcd(a, a') \gcd(b, b') \gcd(c, c')|\Delta(t)\) and thus that

\[
\deg(\gcd(a, a')) + \deg(\gcd(b, b')) + \deg(\gcd(c, c')) \leq \deg(\Delta(t)).
\]

Then we can compute \(\deg(\gcd(a, a'))\) using the fact that a polynomial and its derivative share a common factor if and only if the polynomial has a repeated root.

If \(a(t) = (t - r_1)^{e_1} \cdots (t - r_i)^{e_i}\) then \(\gcd(a(t), a'(t)) = (t - r_1)^{e_1 - 1} \cdots (t - r_i)^{e_i - 1}\) so the degree of \(\gcd(a, a')\) is simply \((e_1 + \cdots + e_i - i) = \deg(a) - i\) the degree of \(a\) minus the number of distinct roots of \(a\), which we will denote \(N(a)\).

Thus, substituting this into the above equation in degrees, we see that

\[
\deg(a) + \deg(b) + \deg(c) - N(a) - N(b) - N(c) \leq \deg(a) + \deg(b) - 1
\]

or, rearranging

\[
\deg(c) \leq N(a) + N(b) + N(c) - 1.
\]

Since \(a, b, c\) are relatively prime polynomials \(N(abc) = N(a) + N(b) + N(c)\) so we can rewrite this in a familiar form

\[
\deg(c) \leq N(abc) - 1.
\]

Using symmetry in the definition of \(\Delta\), we can replace \(c\) by \(a\) or \(b\), and obtain the desired result:
max(deg(a), deg(b), deg(c)) ≤ deg(rad(abc)) − 1.

However, there is a more sophisticated proof of the Mason Stothers theorem using Riemann-Hurwitz which we also present here.

Suppose $a, b, c$ as above are in $K[t]$ with $a + b = c$. Then consider the rational function

$$
\pi(t) := \frac{a(t)}{c(t)} : \mathbb{P}^1 \to \mathbb{P}^1.
$$

Riemann-Hurwitz implies, since $\mathbb{P}^1$ has genus 0, that

$$
2 \deg(\pi) = 2 + \sum_{z \in \mathbb{P}^1} (\deg(\pi) - \#\pi^{-1}(z)).
$$

Then $\deg(\pi) = \max(\deg(a), \deg(b))$, since in general $\pi^{-1}(z)$ has $\max(\deg(a), \deg(b))$ solutions, by solving $a(t) - zb(t) = 0$. Thus we can get an upper bound on degree by considering the ramification indices of $\pi$ over the subset $\{0, 1, \infty\}$: in these cases it is easy to compute that $\#\pi^{-1}(0) = N(a)$, $\#\pi^{-1}(1) = N(b)$, and $\#\pi^{-1}(\infty) = N(c)$, excluding $\infty$, which is in at most one of these. Thus we have that

$$
\max(\deg(a), \deg(b)) \leq N(abc) − 1
$$

and since $a + b = c$ so $\deg(c) \leq \max(\deg(a), \deg(b))$, this is equivalent to the desired result.

### 2.2 Integral Points on Curves

Unsurprisingly, there are a number of other results about finding integral points on higher genus curves which relate to the ABC Conjecture. Many of these results prove the finiteness of integral solutions to Diophantine equations, but fall short of proving an ABC-like result which would bound the size of the result. When there are bounds on the size of the solution, they are often quite large. In many of these cases, a proof of the ABC conjecture would prove a stronger result.

In this section we take a tour of classical results of integral points on curves related to Diophantine approximation. Faltings’ theorem, perhaps the most monumental result in Diophantine finiteness from the 20th century, tells us that for a projective curve $X$ with genus greater than 1 the rational points of $X$ are finite. Then, by scaling, $X(\mathbb{Q}) = X(\mathbb{Z})$ so this gives a bound on the integral points, too. However, in this section we are interested in integral points on affine curves, which is a different situation. For example, an affine elliptic curve of rank one has infinitely many rational points but only finitely many integral points. It is important to keep in mind this difference between affine and projective models throughout.

Before we can get to the actual statements, we develop some rudimentary number theory tools. When possible, we work over a number field $K$, instead of $\mathbb{Q}$. We thus will define the set of places $M_K$ on $K$, the completion with respect to a non-Archimedean place $v ∈ M_K$, and the $v$-integers.
Definition. Let $K$ be a field. Then an absolute value or place on $K$ is a function $|·|_v : K \rightarrow \mathbb{R}$ such that

(i) For all $x \in K$, $|x|_v \geq 0$ and $|x|_v = 0$ if and only if $x = 0$.

(ii) $|xy|_v = |x|_v |y|_v$ for all $x, y \in K$.

(iii) $|x + y|_v \leq |x|_v + |y|_v$ for all $x, y \in K$.

If in addition to (iii) it satisfies $|x + y|_v \leq \max(|x|_v, |y|_v)$ we say that it is non-archimedean. Otherwise, it is archimedean or infinite. The trivial absolute value is the absolute value for which $|x|_v = 1$ for all $x \neq 0$ in $K$.

For example, in addition to the usual absolute value on $\mathbb{Q}$, we have $|·|_p$ the $p$-adic absolute values for each $p \in \mathbb{Q}$ such that if $a \in \mathbb{Q}$ can be written as $p^e(s/t)$ with $s, t$ relatively prime and not divisible by $p$, then $|a|_p = 1/p^e$. We can define a metric on $K$ by letting $d_v(x, y) = |x - y|_v$. Then we consider two absolute values equivalent if they generate the same topology. Further we can define the completion of $K$ with respect to this metric, $K_v$. If $K = \mathbb{Q}$ and $v = |·|_p$ is a $p$-adic absolute value, then $K_v = \mathbb{Q}_p$ is the $p$-adics.

Theorem 1 (Ostrowski). Every archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value, and every nontrivial non-archimedean absolute value on $\mathbb{Q}$ is equivalent to the $p$-adic absolute value for some $p$.

In fact, if $K$ is an arbitrary number field then any absolute value on $K$ is equivalent to the $p$-adic absolute value for a prime $p$ in $O_K$ or equivalent to an absolute value coming from a real or complex embedding of $K$. This motivates the study of places as an analogue to primes.

Proposition 1. We let $M_K$ be a set of equivalence class representatives of absolute values on $K$. Then we can pick representatives such that, for all $x \in K^*$, one has the product formula

$$\prod_{v \in M_K} |x|_v = 1.$$
For example, if $K = \mathbb{Q}$ and $S = \{\cdot|_{\infty}, \cdot|_p\}$ then the ring $A_S$ is the $p$-adic integers $\mathbb{Z}_p$.

**Definition.** If $x \in \mathbb{P}^n(K)$, $x = (x_0, \ldots, x_n)$ we set the height function $H_K(x)$ to be

$$H_K(x_0, \ldots, x_n) = \prod_{v \in \mathcal{M}_K} \max_{0 \leq i \leq n} |x_i|_v.$$ 

For example, if $K = \mathbb{Q}$ the height function $H_\mathbb{Q}(x)$ is simply $\max_i |x_i|$ where $|\cdot|$ is the usual absolute value.

Before we turn to the major results on the finiteness of integral points on curves, we must spend some time talking about Diophantine approximation. The key idea is that if $(x, y)$ is an integral solution to $x^3 - 2y^3 = k$ for $k \in \mathbb{Z}$ then $x/y$ is a rational approximation of $\sqrt[3]{2}$. Since we will show that we can only approximate irrational numbers by rational numbers to a certain precision, this will give us a bound on the number of integral points on $x^3 - 2y^3 = k$.

The simplest approximation theorem was proved by Dirichlet around 1840:

**Proposition 2** (Dirichlet). Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then there are infinitely many $p/q \in \mathbb{Q}$ such that

$$\left| \frac{p}{q} - \alpha \right| \leq \frac{1}{q^2}.$$

**Proof.** The proof of Dirichlet’s theorem is a simple pigeonhole argument: let $N > 0$ be a large integer. If we pick coset representatives in the interval $[0, 1)$ for $\mathbb{R}/\mathbb{Z}$ and consider $c\alpha$ in $\mathbb{R}/\mathbb{Z}$, for $c = 0, 1, \ldots, N$, then by the irrationality of $\alpha$, we get $N + 1$ distinct cosets in $\mathbb{R}/\mathbb{Z}$. However, by the pigeonhole principle at least two of these are within $1/N$ of each other, say $c_1 \alpha$ and $c_2 \alpha$. Then

$$\left| \frac{\lfloor c_2\alpha \rfloor - \lfloor c_1\alpha \rfloor}{c_2 - c_1} - \alpha \right| \leq \frac{1}{|c_2 - c_1|N} \leq \frac{1}{(c_2 - c_1)^2},$$

giving us the desired approximation. \qed

Conversely, around 1850 Liouville proved the following approximation result.

**Proposition 3** (Liouville). Let $\alpha$ be an algebraic integer of degree $d \geq 2$ over $\mathbb{Q}$. Then there is a constant $C > 0$, depending only on $\alpha$, such that for all rational number $p/q$

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}.$$

The proof of this is also quite simple and uses the mean value theorem, but as it is beside the main point of this paper we refer the reader to Silverman [5]. Liouville’s result motivates the following definition.
Definition. Let $K$ be a number field. Let $\tau(d) : \mathbb{N} \to \mathbb{R}_{>0}$. Then $\tau$ is an approximation exponent for $K$ if for any $\alpha$ algebraic over $K$ such that $[K(\alpha) : K] = d$, and for any $v \in M_K$ an absolute value on $K$ (extended to $K(\alpha)$ in some way), then for any $C$ there are only finitely many $x \in K$ such that

$$|x - \alpha|_v < CH_K(x)^{-\tau(d)}.$$ 

Then note that Liouville implies that $\tau(d) = d + \varepsilon$ is an approximation exponent for $\mathbb{Q}$ for any $\varepsilon > 0$. In 1955 Roth improved Liouville’s result (which had, actually, been improved by Thue and Siegel earlier in the early 1900s) to the following.

**Theorem 2** (Roth’s Theorem). For every $\varepsilon > 0$, and every number field $K$, $\tau(d) = 2 + \varepsilon$ is an approximation estimate.

We will not prove Roth’s theorem, because it is quite long, but it is worth noting that the ABC conjecture implies a stronger version of Roth’s theorem, see Lang [3]. Given these approximation theorems, we proceed to the problem of finding integral points on curves.

**Example.** From Silverman [5]. The curve $x^3 - 2y^3 = k$ has only finitely many integral points. Assume that $y \neq 0$, then, factoring we have that

$$\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta \sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta^2 \sqrt[3]{2}\right) = \frac{k}{y^3}$$

where $\zeta$ is a primitive third root of unity. Then the second and third factors are bounded away from zero, so there exists a constant $C$ not depending on $x, y$ such that

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{C}{|y|^{3}}.$$ 

Applying Roth’s theorem we deduce there are only finitely many possibilities for $x, y$.

The main goal of our next section is to apply Roth’s theorem to prove Siegel’s theorem, thus deducing several corollaries about integral points on curves, including the $S$-unit theorem, a similar result to the ABC Conjecture.

### 3 Siegel’s Theorem and its Consequences

We start with a statement of Siegel’s theorem.

**Theorem 3** (Siegel). Let $K$ be a number field and $S$ be a finite set of places of $K$ containing the archimedian places. For any affine curve $X$ of genus greater than 1, or of genus zero whose projective closure has at least three points at infinity, every subset of $X(K)$ which is quasi-integral relative to $A_S$ is finite.
It turns out that these conditions on $X$ are the best possible: in the case where $X$ is genus zero and has only one point at infinity, such as the line $x = 0$ over $\mathbb{Q}$, we see that it is possible for $X$ to have infinitely many integral points. When $X$ has only two points at infinity, we can find examples such as the Pell equations $y^2 - Dx^2 = 1$, where $D$ is square free, which are classically known to have infinitely many integral solutions.

The proof of Siegel relies on the following theorem.

**Theorem 4.** Let $X$ be a smooth projective irreducible curve over $K$ of genus greater than or equal to 1. Let $v$ be a place of $K$. Suppose $P_n \in X(K)$ is a sequence of distinct points whose heights tend to infinity. Let $\phi \in \text{Frac}_K(X)$ be a rational function on $X$ defined over $K$ which is nonconstant. Without loss of generality, assume $P_n$ are not poles of $\phi$, and set $\phi(P_n) = z_n$. Then

$$\lim_{n \to \infty} \frac{\log |z_n|_v}{\log H_K(z_n)} = 0.$$ 

The idea of the proof of this theorem is to assume that instead some subsequence converges to some negative number $\lambda$ (by replacing $\phi$ by $1/\phi$ as necessary.) Then the $z_n$ go to zero in the completion $K_v$, and we can take a subsequence so as to assume that $P_n$ converge to $P$ a zero of $\phi$. Then $P$ is algebraic, as $X$ is a curve. However, this violates Roth’s theorem, as $P_n$ prove to be too good an approximation for $P_0$.

**Corollary 1.** If $X$ is a smooth projective irreducible curve over $\mathbb{Q}$ of genus greater than or equal to 1, then the ratio of the number of digits in the numerators and denominators of rational points tends to 1.

**Proof.** By letting $K = \mathbb{Q}$ and $v = |\cdot|_\infty$ the usual absolute value, we see that

$$\lim_{n \to \infty} \frac{\log |p_n|}{\log |q_n|} = 1$$

where $z_n = p_n/q_n$ picks out a specified coordinate of a sequence of rational points $P_n$.

Let $X, \phi, P_n$ and $z_n$ be as in the above theorem. Suppose $S \subset M_K$ is a finite set of places containing the archimedian places, and let $A_S$ be the ring of $S$-integers of $K$. Then, using Theorem 4, we prove a slightly stronger version of Siegel’s theorem for curves of genus $\geq 1$, that there are only finitely many $n$ such that $\phi(P_n) \in A_S$. The following proof comes from Serre at [4].

**Proof.** Suppose not. Then by taking a subsequence, we can let $z_n \in A_S$ for all $n$, so $|z_n|_v \leq 1$ for $v \notin S$ and for all $n$. The height of $z_n$ is defined as

$$H(z_n) = \prod_{v \in M_K} \sup(1, |z_n|_v) = \prod_{v \in S} \sup(1, |z_n|_v)$$
\[
\log H_K(z_n) = \sum_{v \in S} \sup(0, \log |z_n|_v)
\]

and dividing through we get
\[
1 = \sum_{v \in S} \sup(0, \frac{\log |z_n|_v}{\log H_K(z_n)}) \leq \sum_{v \in S} \frac{\log |z_n|_v}{\log H_K(z_n)}
\]

which is a contradiction, because this goes to 0 as \(n\) goes to infinity.

To finish the proof of Siegel, we need to show it for an affine curve of genus zero whose projective closure has at least 3 points at infinity. It suffices to consider the case of exactly three points at infinity, because any curve with more points at infinity has an injection into a curve with three points at infinity, which, clearing denominators, preserves \(S\)-integral points. Then \(X\) is isomorphic to \(\mathbb{P}^1 \setminus \{0, 1, \infty\}\). Consider the following theorem.

**Theorem 5 (S-unit Equation).** Let \(S \subset M_K\) be a finite set of place and suppose \(a\) and \(b\) are units in \(K\). Then the equation
\[
ax + by = 1
\]
has only a finite number of solutions in \(S\)-units \(x, y \in A_S^*\).

**Proof.** Due to Serre [4].

Suppose there are infinitely many solutions \((x_n, y_n) \in A_S^*\) of the equation \(ax + by = 1\). Then by Dirichlet’s \(S\)-unit theorem, the group \(A_S^*/A_S^m\) is finite for \(m \geq 3\) an integer. Taking a subsequence, we may assume that our \(x_n\) and \(y_n\) each have the same coset representatives, \(c_0\) and \(c_1\) respectively, that is, \(x_n = X_n c_0, y_n = Y_n c_1\) with \(c_0, c_1 \in A_S^*\) fixed coset representatives. Then letting \(\alpha = ac_0, \beta = bc_1\) and \(\gamma = c\) we see that
\[
\alpha X^m + \beta Y^m = \gamma
\]
has infinitely many quasi integral points given by \((X_n, Y_n)\). But since \(m \geq 3\), the genus of this curve is greater than 0, so we have a contradiction by the other case of Siegel’s theorem.

Note that solutions to the \(S\)-unit equation are integer points on the curve \(ax + by = c, xz = 1, yt = 1\), which is isomorphic to \(\mathbb{P}^1\) minus three points, where the isomorphism is given by projection to the \(x\)-coordinate. Thus this concludes the proof of Siegel’s theorem.

Note that when \(K = \mathbb{Q}\), then \(S\) is a finite set of primes, and \(a, b \in \{-1, 1\}\), so the \(S\)-unit equation asks for the solutions to \(\pm x \pm y = 1\) where \(x, y\) have prime factors restricted to \(S\). If we instead clear denominators and write this as \(A + B = C\) with \(A, B, C\) coprime
integers, then we can see that solutions to $A + B = C$ are the same as solutions to the $S$-unit equation when $S$ is the set of primes dividing $\text{rad}(ABC)$. The $S$-unit theorem implies that there are only finitely many such solutions, and we can also get a bound on the number of solutions, but the ABC conjecture also seeks to control the size of the largest solution.

From here we can derive a fun corollary:

**Corollary 2** (Siegel). Let $f$ be a polynomial with integer coefficients having at least two distinct zeroes over $\mathbb{C}$. Then the largest prime factor of $f(n)$ goes to infinity as $n$ goes to infinity.

**Proof.** Due to Serre at [4]. Suppose not. Then taking subsequences, we can find infinitely many $n_i$ such that $f(n_i)$ has largest prime factor less than $M$. We will also throw out any zeroes, so that $f(n_i) \neq 0$. Then suppose $S$ is the set of all prime numbers less than or equal to $M$. Then $1/f(n_i)$ are $S$-integers so the variety $X = Z[T, 1/f(T)] \subset \mathbb{P}^1\mathbb{C}$ is an affine curve of genus zero where at least three points have been removed (infinity and the two distinct zeroes of $f$.) By Siegel’s theorem, the set of $S$-integral points on $X$ is finite, a contradiction.

The importance of Siegel’s theorem extends beyond just finding integral points on curves. Using Siegel’s theorem, we can prove that there are only finitely many curves with good reduction away from some specific finite set of primes. Furthermore, an effective proof of Siegel’s theorem gives us an effective way of finding these curves. While the proof we provided above is not effective, there are effective proofs for certain classes of curves. For example, Baker’s method was the first to give explicit methods in this area. Also, Noam Elkies in [1] shows that ABC implies an effective proof of Mordell’s theorem, and Andrea Surroca uses a similar method in [6] to show that ABC implies an effective proof of Siegel’s theorem.

### 4 Further Problems

A major open question that remains is whether there are effective proofs of Siegel’s theorem: can we find all of the integral points on a particular affine model of a curve? For the reader interested in a longer discussion of Siegel’s theorem or Diophantine problems, see Serre [4] or Lang [3].

**References**


