Belyi Maps, Elliptic Curves and the ABC Conjecture
Lily Khadjavi, Victor Scharaschkin

1. Introduction

If \( n \) is a non-zero integer, let \( \text{rad}(n) \) denote the product of distinct primes dividing \( n \), not counting multiplicity. For example, \( \text{rad}(24) = 6 \). An \( abc \) triple is a triple \((a, b, c)\) of pairwise relatively prime (hence non-zero) integers satisfying

\[
a + b = c.
\]

The quality of an \( abc \) triple \( q(a, b, c) \) is

\[
q(a, b, c) = \frac{\log \max\{|a|, |b|, |c|\}}{\log \text{rad}(abc)}.
\]

Definition 1.1. The \( abc \) conjecture is the statement that as \( \max\{|a|, |b|, |c|\} \to \infty \), the lim sup of \( q(a, b, c) \) is 1. It will be convenient to let \( q' = 1 - \frac{1}{q} \). Thus \( q > 1 \) iff \( q' > 0 \) and \( q \to 1 \) iff \( q' \to 0 \).

To specify an \( abc \) triple we need only give \( b \) and \( c \), which we can encode as a single point \( c/b \in \mathbb{P}^1 \), the projective line over \( \mathbb{Q} \). We often normalize our \( abc \) triples by relabelling the variables so that \( a, b, c > 0 \). Let us say that two triples \((a, b, c), (a', b', c')\) are equivalent if \( \{ |a|, |b|, |c| \} = \{ |a'|, |b'|, |c'| \} \). Then we often choose an equivalence class representative with all variables positive.

Let \( S \) be the set of limit points of all qualities of \( abc \) triples. It is known that \( [1/3, 1 - \delta) \subseteq S \) for some small \( \delta > 0 \). Currently one may take \( \delta = 1/36 \) [7]. Furthermore it is known that \( S \cap [1, 3/2) \neq \emptyset \). However to date it is not known that \( 1 \in S \). That is, no example of a sequence of \( abc \) triples whose qualities have limit 1 is known.

Conjecture 1.2 (Weak ABC Conjecture). Some sequence of \( abc \) triples has quality approaching 1.

As a first approach towards constructing such triple, fix \( a, b \in \mathbb{N} \) with \( \gcd(a, b) = 1 \). Consider triples of the form

\[
(a^n - b) + b = a^n
\]

with \( n \) varying. Let

\[
r = \log \left( \frac{a^n - b}{\text{rad}(a^n - b)} \right).
\]

We have trivially

\[
0 \leq r \leq n \log a.
\]

A small calculation of the quality of the triples (3), shows there exists a positive constant \( C = C(a, b) \) such that for all large \( n \)

\[
\frac{r - C}{n \log a} < q' < \frac{r}{n \log a}.
\]

Recall that a prime \( p \) is called a Wieferich prime to base \( a \) if \( a^{p-1} \equiv 1 \pmod{p^2} \).

\[\text{More formally, let } G = \text{the group freely generated by } r \text{ and } s \text{ modulo relations } r^2 = 1, s^2 = 1, (rs)^3 = 1 \text{ (} G \text{ is the symmetric group on 3 letters). Then } G \text{ acts on } \mathbb{P}^1 \setminus \{0, 1, \infty\} \text{ by } r \cdot q = 1/q, s \cdot q = 1 - q, \text{ and points in the same } G\text{-orbit give rise to equivalent } abc \text{ triples.}\]
Corollary 1.3. For the triples (3),

(a) For any $\epsilon > 0$, $q > 1 - \epsilon$ for all $n$ sufficiently large.

(b) If $r = 0$ infinitely often then $q < 1$ infinitely often.

(c) If $a^n - b$ is divisible by some non-Wieferich prime then $q > 1$ infinitely often.

(d) $q \to 1$ iff $r = o(n)$.

Proof. Only (c) needs proof. But if $p$ is a non-Wieferich prime for $a^n \equiv b \pmod{p}$ then $a^n - b$ is divisible by arbitrarily high powers of $p$ for appropriate $n$ [?] so $r \to \infty$. \hfill \Box

Notice that if $b = 1$ the condition in (c) just becomes: there exists a non-Wieferich prime $p$ to base $a$.

We generalize this approach. Let $A$ be a commutative algebraic group defined over $\mathbb{Q}$, and suppose $a$ is an element of $A$. For all but finitely many primes $p$ the reduction $\tilde{A}$ of $A$ modulo $p$ and $p^2$ is defined. We may thus form the set

$$W = W_{A,a} = \{p \mid \#(\tilde{A}(\mathbb{F}_p)) \cdot a \equiv 0 \pmod{p^2}\}$$

and its complement

$$W' = W'_{A,a} = \{p \mid \#(\tilde{A}(\mathbb{F}_p)) \cdot a \not\equiv 0 \pmod{p^2}\}$$

The sets $W$ and $W'$ are dependent on the model of $A$, but changing the model of $A$ only changes $W$ and $W'$ by only a finite set, and we shall only be only interested in asymptotics. See Silverman [?] for further discussion. (His $W$ is our $W'$.) Define

$$w(x) = w_{A,a}(x) = \#\{p \in W_{A,a} \mid p \leq x\}$$

and $w'(x)$ similarly.

Definition 1.4. The set $W_{A,a}$ is called the set of Wieferich primes for $a$ on $A$. The set $W'_{A,a}$ is the set of non-Wieferich primes.

There are cohomological formulations of $W_E$, including one involving the Brauer-Manin obstruction. See Section 7 for details.

Example 1.5. Let $A = \mathbb{G}_m$ and let $a = 2$. Then $W = W_{\mathbb{G}_m,2} = \{p \mid 2^{p-1} \equiv 1 \pmod{p^2}\}$, which is the set of (classical) Wieferich primes to base 2. It is known that $w(10^{14}) = 2$. Indeed 1093 and 3511 are the only such primes up to $10^{14}$ [?].

Example 1.6. Let $E$ be an elliptic curve and suppose $P_0 \in E(\mathbb{Q})$ is a point of infinite order. Let $m_p$ be its order in $\tilde{E}(\mathbb{F}_p)$. In terms of the canonical $p$-adic filtration on $E(\mathbb{Q}_p)$

$$W = W_{E,P_0} = \{p \mid m_pP_0 \in E_2\}$$

Heuristically $w(x) \ll \log \log x$ in these two cases. No unconditional results are known.

The abc conjecture implies that non-Wieferich primes are common in both situations.

Theorem 1.7. Suppose the abc conjecture holds. Then

(a) If $A = \mathbb{G}_m$ then $w'_{A,a}(x) \gg_a \log x$.

(b) If $A = E$ is an elliptic curve then $w'_{E,P_0}(x) \gg_{E,P_0} (\log x)^{1/2}$.
In this paper we examine a converse: if Wieferich primes are rare, then the weak abc conjecture is true. Given an elliptic curve $E$ we construct such triples using Belyi maps. This approach is discussed by Elkies [1].

The abc conjecture can naturally be stated in terms of rational numbers. In view of equation (1), to give an abc triple we need only $b$ and $c$, which we can encode as a rational number $q = c/b$, considered as a point in $\mathbb{P}^1$, the projective line over $\mathbb{Q}$. Since $a, b, c \neq 0$, $q$ can be any point of $\mathbb{P}^1$ except 0, 1 and $\infty$.

If $C$ is a curve, a Belyi map $\beta$ is a finite morphism $C \to \mathbb{P}^1$ whose ramified points in $\mathbb{P}^1$ are a subset of $\{0, 1, \infty\}$. Given a curve defined over $\mathbb{Q}$ and a Belyi map, each rational point $P$ on the curve gives rise to a rational number $q = c/b$. Abusing notation, we write $q(P)$ for the quality of the triple produced in this way. To obtain an infinite sequence of abc triples from a curve we are forced to choose $C$ of genus 0 or 1 by Faltings’ Theorem.

Thus let $E$ be an elliptic curve defined over $\mathbb{Q}$, with $E(\mathbb{Q})$ infinite, and fix a Belyi map. Our basic plan is to choose a point $P \in E(\mathbb{Q})$ and consider the sequence $nP$. Applying $\beta$ we recover abc triples, and these can satisfy generalized Fermat equations, so could be expected to be of high quality. This may seem unduly restrictive, but it is easy to see (Theorem (4.1)) that every abc triple actually arises in this way.

Elkies proved the following.

**Theorem 1.8.** Let $\epsilon > 0$. Then for almost all points $Q \in E(\mathbb{Q})$ the inequality $q(Q) > 1 - \epsilon$ holds.

**Proof** [1, Formula (24), p. 105].

We extend this result.

Let $E_0$ and $E_{1728}$ be the elliptic surface $y^2 = x^3 + tx$ and $y^2 = x^3 + t$ respectively (elliptic curve over $\mathbb{Q}(t)$). The fibres of these surfaces are the curves of $j$-invariant 0 or 1728. Theorem ?? gives a condition for the fibres to produce abc sequences with limit point 1. Proving the abc conjecture is equivalent to being able to give an upper bound for the limit points across either surface at once, not just fibre by fibre.

**Theorem 1.9.** Suppose either of the following is true.

(a) If $A = \mathbb{G}_m$, assume $w_{A,a}(x) = o((\log x)/\log \log x)$.

(b) If $A = E$ is an elliptic curve, assume there exists $\delta > 0$ with $w_{E,P_0}(x) \ll_{E,P_0} (\log x)^{\frac{1}{2} - \delta}$.

Then 1 is a limit point of the abc conjecture: there is a sequence of abc triples whose quality approaches exactly 1.

If the hypothesis of (b) is modified to be true across an entire family of elliptic curves, with uniform bound then the full abc conjecture follows.

**Corollary 1.10.** Let $E$ be the elliptic surface with fibre $E_t$: $y^2 = x^3 + tx$, or the surface with fibre $y^2 = x^3 + t$. Suppose $P_t$ is a point on each $E_t$. Suppose

$$w(x) = \# \{ p | \exists t \ p \in W_{E,P_t}, \ p \leq x \} \ll_{E} (\log x)^{\frac{3}{2}}.$$ 

Note that the bound is independent of $t$. Then the abc conjecture holds.
2. Notation

If $A$ is an abelian group $A[p]$ denotes the kernel of $A \xrightarrow{p} A$, and $A/p$ the cokernel. If $A \subseteq B$ then $1_A/A$ denotes $\{b \in B \mid pb \in A\}$ (with $B$ specified by context). That is, $1_A/A$ is the kernel of the composite map $B \to B/A \xrightarrow{p} B/A$. All diagrams are commutative with exact rows and columns, unless stated otherwise. The adeles are denoted by $\mathbb{A}$.

We say $f = o(g)$ if $f(x)/g(x)$ approaches 0 as $x \to \infty$. We write $f = O(g)$ or $f \ll g$ if $f(x)/g(x)$ is bounded as $x \to \infty$.

Elliptic curve calculations given in this paper were performed using the programs GP-Pari and mwrank. We also made use of elliptic curve data supplied by Tom Womack in section 9.

3. Heights and Belyi maps

The proof of 1.9(a) is elementary:

Let $S$ be the set of prime divisors of $a - 1$. Let $\ell$ range across the primes outside $S$ up to some large bound $x$. Consider abc triples of the form

$$1 + (a^\ell - 1) = a^\ell.$$

If $p$ divides $a^{\ell_1} - 1$ and $a^{\ell_2} - 1$ then the order of $a$ modulo $p$ divides $\gcd(\ell_1, \ell_2)$. Thus the $a^\ell - 1$ have no common prime divisors outside $S$. Furthermore, if $p \mid (a-1)$ then $1+a+a^2+\cdots+a^{\ell-1} \equiv \ell \not\equiv 0 \pmod{p}$ since $\ell \not\in S$. This shows that only the primes in $S$ divide more than one of the $a^\ell - 1$, and that exponents of these primes in each $a^\ell - 1$ are absolutely bounded. We now show that at least some of the $a^\ell - 1$ have no other repeated prime factors.

Suppose $p \not\in S$ and $p^2 \mid a^\ell - 1$. Since $p \not\in S$, the order of $a$ in $(\mathbb{Z}/p^2)^\times$ is $\ell$, so $\ell \mid p(p-1)$. But $\ell \neq p$ by Fermat’s Little Theorem, so $\ell \mid p-1$, and $a^{p-1} \equiv 1 \pmod{p^2}$. That is, $p$ is a Wieferich prime with $p < a^x$.

By hypothesis there are $o(x/\log x)$ such primes up to $a^x$ but according to the Prime Number Theorem, we have written down $O(x/\log x)$ triples. Letting $x \to \infty$, there are infinitely many $\ell$ not divisible by any Wieferich prime, and hence such that the powerful part of $a^\ell - 1$ is absolutely bounded. The qualities of these triples clearly approach 1.

We modify this proof for abc triple constructed from an elliptic curve via a Belyi map $\beta$. This involves estimating the local height of $\beta(P)$.

To distinguish between addition of divisors, and addition on $E$, denote elliptic curve addition/subtraction by $P \oplus Q$, respectively $P \ominus Q$ and write $\mathcal{O}$ for the point at infinity.

For abelian varieties the local and global height machines of Weil take a simplified form. For each divisor $D$ there is a canonical local height function corresponding to $D$, called the Néron height function $[?, p. 242$ Thm 9.3], denoted $\lambda_D$.

Using linearity and translation, we obtain a formula for $\lambda_D$. Write $D$ as a sum of points. By additivity

$$\lambda_D = \sum_i \lambda_{D_i},$$

up to a constant $c_0$. Now translate $Q$ to $\mathcal{O}$, i.e. compare $\lambda_Q$ to $\lambda_\mathcal{O}$ by using the translation map $E \to E$ given by $P \mapsto P \ominus Q$. See $[?, p242, 9.3(e)]$. This gives (up to constants)

$$\lambda_D + Q(P) = \lambda_D(P \ominus Q).$$
On putting $D = \mathcal{O}$ and using linearity, and writing $\lambda$ for $\lambda_{\mathcal{O}}$ we get

$$\lambda_Q(P) = \lambda(P \oplus Q) - \lambda(P)$$

up to a constant. So we just need a formula for $\lambda$. This can be found in [?, p.470, Remark 4.1.1]. Namely with $p$ a prime of good reduction and $P = (s/d^2, t/d^3)$ on $E$, then

$$\lambda(P) = \text{ord}_p(d)$$

up to multiplication by a positive constant. In terms of the canonical $p$-adic filtration $E_n$ on $E(\mathbb{Q}_p)$, $\lambda(P)$ is the largest $n$ such that $P \in E_n$.) So

$$\lambda_Q(P) = \text{ord}_p(d(P \oplus Q)) - \text{ord}_p(d(P)).$$

Finally, if $D = \text{div}(f)$ and $w$ is a prime then $\lambda_D(P) = v(f(P)) + c_w$, for some fixed constant $c_w$, independent of $P$ (in fact the $c_w$ are 0 except for finitely many $w$). See [?, p. 242 Thm 9.3(c)] or [?, p.87] with [?, pp. 266–67].

Thus to estimate rad $c$, Elkies’ observes that

$$\log(\text{rad } c) = \sum_{p \mid c} 1 \cdot \log p \leq \sum_{p \mid c} \lambda_{D_0,p}(P_0) = \lambda_{D_0}(P_0).$$

We refine this bound.

Let $\beta : E \to \mathbb{P}^1$, let $\beta(P_0) = c/b$, let $D = \text{div}(\beta) = D_0 - D_\infty$. Let $D_0 = \sum_i m_i D_i$ and let $D_0' = \sum D_i$, that is, $D_0$ with the multiplicities removed. Let $\lambda_{D,p}$ be the canonical (Néron) local height on $E$ at $p$ associated to $D$, so $\lambda_{D,p} : (E \setminus \text{supp} D)(\mathbb{Q}_p) \to \mathbb{R}$. In particular for our divisors the associated $\lambda$ will always be defined outside $\beta^{-1}\{0,1,\infty\}$. Let $\alpha_{D,p} = \lambda_{D,p}/\log p$.

Let $D_0 = \sum m_i D_i$, $D_\infty = \sum n_i R_j$. We evaluate $\beta$ at $P \notin \beta^{-1}\{0,1,\infty\}$, and $P_0$ a point of infinite order, so $P_0 \neq Q_i, R_j, \mathcal{O}$. From above (for $P_0 \neq \mathcal{O}, P_0 \neq Q_i$) we have

$$\alpha_{Q_i,p}(P_0) = \text{ord}_p d(P_0 \oplus Q_i) - \text{ord}_p d(P_0).$$

This is a difference of two non-negative integers.

For $p$ outside a finite set $S$ if $\text{ord}_p d(P_0 \oplus Q_i) \geq 1$ for any $i$ then this happens for exactly one $i$, $\text{ord}_p d(P_0) = 0$, and $\text{ord}_p d(P_0 \oplus R_j) = 0$ for all $j$. Now $\lambda_{D_0,p}(P_0) = \sum_i m_i \lambda_{Q_i,p}(P_0)$, so $\lambda_{D_0,p}(P_0) > 0$ iff $\lambda_{D_0',p}(P_0) > 0$ and this implies $\lambda_{D_\infty,p}(P_0) = 0$.

$$\text{ord}_p(c/b) = \alpha_{D,p}(P_0) = \alpha_{D_0,p}(P_0) - \alpha_{D_\infty,p}(P_0)$$

Thus for $p$ outside a finite set, $p \mid c$ iff $\alpha_{D_0,p}(P_0) > 0$ if $\alpha_{D_0',p}(P_0) > 0$, if $P_0 \equiv Q_i$ in $E/E_1$.

Want to write $\log \text{rad } c = \lambda_{D}(P_0) + S(P_0) + C$, where $S(P_0)$ is a sum of all $(n-1)\log p$ for all primes $p$ for which $P_0 \oplus Q_i \in E_n$ with $n \geq 2$, plus a contribution from infinite primes.

Hence $p$ occurs in $\beta(P)$ iff it contributes to $\lambda_{D,p}(P)$, since the latter is just $v(\beta(P)) = \text{ord}_p(\beta(P))$.

The relation between being $P$ and $Q$ being $p$-adically close and $P \oplus Q$ being close to $\mathcal{O}$ is the parallelogram law [S2, p. 476 Ex 6.3]

$$\lambda(P \oplus Q) + \lambda(P \oplus Q) - 2\lambda(P) - 2\lambda(Q) = \text{ord}_p(x(P) - x(Q)).$$

Applying this we see that if $Q$ is fixed, say $Q \in E_n$ but not in $E_{n+1}$, and we choose $P$ so that $\lambda(P \oplus Q) \to \infty$ then $\text{ord}_p(x(P) - x(Q)) \to \infty$ also, unless $\lambda(P) \to \infty$. But $P \oplus Q \in E_m$
for \( m > n \) implies \( P \notin E_{n+1} \) so \( \lambda(P) \) is bounded. So \( \lambda(P \ominus Q) \to \infty \) implies that \( p \)-adically \( x(P) - x(Q) \to 0 \) so \( x(P) \to x(Q) \).

Similarly, as we choose \( P \) to make \( \lambda(P \ominus Q) \to \infty, \lambda_Q(P) \to \infty \).

That is: Fix \( Q \in E(\mathbb{Q}_p) \), and consider a sequence of \( P \). Then \( \text{ord}_p(x(P) - x(Q)) \to \infty \) iff \( P \ominus Q \) or \( P \ominus Q \) falls into higher and higher \( E_m \).

Fix \( Q \) lying in \( E(\overline{\mathbb{Q}}) \).

**Proposition 3.1.** Assume that we can find \( x \in \mathbb{N} \) such that \( 6 \) is what Elkies uses. But more accurately we have

\[
\sum_{\text{infinitely many primes } p} D
\]

So for each \( p \), \( \lambda p \) and \( \lambda\) is what Elkies uses. But more accurately we have

\[
\sum_{\text{infinitely many primes } p} D
\]

Eventually we exhaust the integer points on \( E(\mathbb{Q}) \), so \( NP \ominus Q \) is a point with primes dividing the denominator; it lies in \( E_1 \) for some \( p \).

Now let \( R = Q \ominus NP \). For every \( m \) we can now find \( N' \) with \( N'P \ominus R \in E_m \), so \( nP \ominus Q \in E_m \) where \( n = N + N' \), and we are done. \( \square \)

We have

\[
\text{ord}_p(c/b) \log(p) = \lambda_{D,p}(P_0) + \gamma_p = \lambda_{D_0,p}(P_0) - \lambda_{D_{\infty},p}(P_0) + \gamma_p
\]

Since \( D_0, D_{\infty} \geq 0 \) their associated \( \lambda \) are both non-negative, so we see that \( \text{ord}_p(\beta(P_0)) \log(p) = \lambda_{D_0,p}(P_0) \) for those \( p \) dividing the numerator \( c \), and is \( -\lambda_{D_{\infty},p}(P_0) \) for those in the denominator. So for each \( p \)

\[
\text{ord}_p(c) \log(p) = \lambda_{D_0,p}(P_0) = \sum_i m_i \lambda_{D_1,p}(P_0) = \sum_i m_i \alpha_{i,p} \log p
\]

so

\[
\sum_i m_i \alpha_{i,p} = \text{ord}_p(c)
\]

while

\[
\lambda_{D_0,p}(P_0) \overset{1}{=} \sum_i \lambda_{D_1,p}(P_0) = \sum_i \alpha_{i,p} \log p.
\]

Note that since all the \( \alpha_{i,p} \geq 0 \) and the \( m_i > 0, \alpha_{i,p} = 0 \) for any \( p \) not dividing \( c \).

For \( p \) dividing \( c \), let \( S_{D_0,p}(P_0) = \sum_i \alpha_{i,p} - 1 \). Otherwise let it be 0. Similarly define \( S_{D_{\infty},p}(P_0) \) to be the corresponding sum for the zero divisor of \( 1/\beta \) and \( S_{D_1,p}(P_0) \) for \( \beta - 1 \) and let \( S_p(P_0) \) the be sum of these three. Let \( S(P_0) = \sum_p S_p(P_0) \).

\[
\log \left( \text{rad}(c) \right) = \sum_{p | c} \log p \leq \sum_{p | c} \left( \sum_i \alpha_{i,p} \right) \log p = \sum_{p | c} \lambda_{D_0,p}(P_0) \overset{2}{=} \lambda_{D_0}(P_0).
\]

For (2), note that the sum can be extended over all \( p \), since \( \alpha_{i,p} = 0 \) for \( p \) not dividing \( c \). This is what Elkies uses. But more accurately we have

\[
\log \left( \text{rad}(c) \right) = \lambda_{D,p}(P_0) - S_{D_0,p}(P_0).
\]

Now continue using Elkies’ argument. Compare \( \lambda_D \) to \( \lambda_D' \) to obtain

\[
\frac{1}{q} = 1 + \frac{C - S(P_0)}{h(P_0)}
\]
where now all the constants omitted have been wrapped up into $C$ (possibly negative), independent of $P_0$.

Elkies omits the correction term $S$, so just has

$$\frac{1}{q} \leq 1 + \frac{C}{h(P_0)}$$

which leads to $q \geq 1 - \epsilon$.

In summary:

If we can find a sequence of $n$ such that $nP_0$ approaches one of the divisors $D_i$ in the $p$-adic topology, then $S(nP_0) \to \infty$ for these $n$, and thus $q > 1$ infinitely often.

Such a sequence of $n$ exists provided that for one of the fixed $Q_i$ in the divisors there exists $p$ with $nP_0 - Q \in E_1(\mathbb{Q}_p)$ and some multiple of $P_0$ is non-zero in $E_1/E_2$. [The former always happens, but it we need it for a non-Weiferich prime.]

Thus, if Wieferich primes are rare, 1 is a limit point of abc.

4. Special j invariants

Recall that any affine rational point on an elliptic curve given in Weierstraß form may be written in the form $(s/d^2, t/d^3)$ for integers $s, d, t$ with $\gcd(s, d) = \gcd(t, d) = 1$.

**Theorem 4.1.**

(a) Let $D$ be a fourth-power free (hence non-zero) integer, let $E_D$ be the elliptic curve $y^2 = x^3 + Dx$ and let $\beta$ be the degree 4 Belyi map $\beta(x, y) = -x^2/D = c/b$. The triple $(a, b, c)$ obtained from $E_D$ satisfies a generalized Fermat equation with exponents $(2, 4, 4)$ and coefficients bounded by $|D|$, and satisfies conditions (??) and (??).

(b) Similarly the curves $y^2 = x^3 + D^2$, $D$ cube-free, with Belyi maps $(x, y) \mapsto (y + D)/2D$ produce triples satisfying these conditions and generalized Fermat equations with exponents $(3, 3, 3)$.

(c) The curves $y^2 = x^3 + D$, $D$ sixth power free, with Belyi maps $(x, y) \mapsto y^2/D$ produce triples satisfying these conditions and equations with exponents $(2, 3, 6)$.

(d) Every abc triple arises from all three types of curve.

**Proof**

(a) Any rational point on an elliptic curve in Weierstraß form can be written $(x, y) = (S/d^2, T/d^3)$ where the fractions are reduced. Let $S = As^2$ with $A$ square-free; note that $\gcd(A, d) = 1$. Then

$$T^2 = As^2(A^2s^4 + Dd^4).$$

Suppose $p \mid A$. Since $A$ is square-free, but the left hand side of equation (4) is a square, $\text{ord}_p(A^2s^4 + Dd^4)$ is odd, so $p \mid Dd^4$ and hence $D$. Thus every prime factor of the square-free $A$ divides $D$, so $A \mid D$. Let $D = AB$. Then $As \mid T$, so let $T = Ast$. This gives generalized Fermat equation

$$As^4 + Bd^4 = t^2.$$

By construction $\gcd(s, d) = 1$, verifying condition (??). Finally the log condition follows from (the quantitative version of) Siegel’s Theorem. See [4, p. 250].

(b) Consider the curve $E: y^2 = x^3 + D^2$ and degree 3 map $\beta(x, y) = (y + D)/2D$. This is a Belyi map. (In fact a calculation with the Hurwitz formula shows that this is the lowest
possible degree Belyi map defined over $\mathbb{Q}$ from an elliptic curve; see [10] for more discussion of the bounds on the degree of such a map.)

Let $(x, y) = (s/d^2, t/d^3)$. Then $(t - Dd^3)(t + Dd^3) = s^3$ but $\gcd(t - Dd^3, t + Dd^3)$ divides $2D$, so $t - Dd^3 = As^3$ and $t + Dd^3 = Bs^3$ for some factors $A$, $B$ of $2D$ and $s_1$, $s_2$ of $s$. Thus $c/b = \beta(x, y) = (t + Dd^3)/2Dd^3$ so the $(3, 3, 3)$ generalized Fermat equation is satisfied: $A^3 + 2Dd^3 = Bs^3$.

Note also that $\gcd(s_1, d) = 1$, in line with condition (??).

(c) This is the easiest case. The curve $E: y^2 = x^3 + D$ and degree 6 Belyi map $\beta(x, y) = y^2/D$. Let $x = s/d^2$, $y = t/d^3$ with $\gcd(s, d) = \gcd(t, d) = 1$. Then $t^2 = s^3 + Dd^6$.

(d) In case (a), multiply the equation $c - b = a$ through by $a^3c^2$. Let $x = ac$, $y = a^2c$ and $D = -a^2bc$. Then $(x, y) \in E_D(\mathbb{Q})$ and $\beta(x, y) = c/b$, recovering the triple $(a, b, c)$. Now divide through to make $D$ fourth power free.

Case (b) Similar.

Case (c) Take $D = abc/2$ (note that at least one of $a$, $b$, $c$ is even), $x = ac$, $y = ac(2c - b)/2$. Divide through to make $D$ cube-free.

Example 4.2. The abc triple of highest known quality is $(2, 3^{10} \cdot 109, 23^5)$. See [6]. Here $D$ is the fourth power free part of $-2^4 \cdot 3^{10} \cdot 23^3 \cdot 109$, i.e. $D = -2^2 \cdot 3^2 \cdot 3 \cdot 109 = -90252$. Then $P$ is obtained from $(2 \cdot 23^3, 3^{10} \cdot 23^3)$, so $P = (2 \cdot 23^3/3^4, 2^2 \cdot 23^3/3^4)$.

Note: According to mwrank [9] this curve has rank 2, with $E$/torsion probably generated by $P$ and $Q = (414, 5796)$.

Taking triples equivalent to this one, the other possible $D$ values are $-2 \cdot 23 \cdot 109^2$ (rank 1, generator $(-2 \cdot 109/23^2, 2 \cdot 3^5 \cdot 109^2/23^3)$) and $2 \cdot 3^2 \cdot 23^2 \cdot 109$ (rank 2, generators $(3 \cdot 13^2, 3 \cdot 13 \cdot 73)$ and $(2 \cdot 23^3/3^4, 2 \cdot 23^3/3^6)$).

For simplicity, from now on, let $E$ be an elliptic curve of rank 1 with a torsion-free generator $P_0$. Generate a sequence of abc triples by taking $\beta(nP_0)$. Let $nP_0 = (s(n)/d(n)^2, t(n)/d(n)^3)$, let $r(nP_0)$ be the coradical of the triple obtained from $nP_0$.

The theory of heights gives the following. Or something like this.

Theorem 4.3. Up to a bounded error $d$ is a quadratic form in $n$.

Corollary 4.4. (a) In each of the three cases, for any $\epsilon > 0$, almost all points on the curve give rise to triples of quality $q > 1 - \epsilon$.

(b) In each case, if $E(\mathbb{Q})$ is infinite and the coradical $r$ is unbounded then $q > 1 - \epsilon$ infinitely often.

(c) If $\log(r(n)) = o(n^2)$ then the weak abc conjecture holds.

It is not difficult to show that the coradical is unbounded. To understand the primes appearing in the coordinates of a point we could modulo $p$, so let $\tilde{E}$ be the reduction of $E$ modulo $p$. If $p$ is a prime of good reduction then a point $P = (s/d^2, t/d^3) \in E(\mathbb{Q})$ reduces to the 0 element in the group $\tilde{E}(\mathbb{F}_p)$ if and only if $p \mid d$. Similarly $p \mid t$ if and only if $P$ has exact order 2 in $\tilde{E}(\mathbb{F}_p)$, and $p \mid s$ if and only if $P$ has order 3 in $\tilde{E}(\mathbb{F}_p)$. To estimate the power of $p$ dividing the coordinates we work over $\mathbb{Q}_p$ instead of $\mathbb{F}_p$. 
Fix a minimal model of $E$ over $\mathbb{Q}_p$ for each $p$. (For example $E = E_D$ for any fourth power free integer $D$.) We then have a canonical filtration on $E(\mathbb{Q}_p)$, given for all $n \geq 1$ by
\begin{equation}
E_n = E_n(\mathbb{Q}_p) = \{(x, y) \in E(\mathbb{Q}_p) \mid \text{ord}_p(x) \leq -2n\} \cup \{0\}.
\end{equation}
Note that for primes of good reduction $E_1$ is the kernel of reduction modulo $p$. In general, let $\tilde{E}_{ns}(\mathbb{F}_p)$ be the set of non-singular points modulo $p$, and $E_0 = E_0(\mathbb{Q}_p)$ be the subset of $E(\mathbb{Q}_p)$ mapping to $\tilde{E}_{ns}(\mathbb{F}_p)$. Thus for all $p$ of good reduction, $E_0 = E(\mathbb{Q}_p)$ and $\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)$. Using the formal group law interpretation of $E_1$ one shows that the filtration
\begin{equation}
E(\mathbb{Q}_p) \supseteq E_0 \supseteq E_1 \supseteq E_2 \supseteq \cdots
\end{equation}
is exhaustive, where
\begin{align}
E(\mathbb{Q}_p)/E_0 &= \text{finite} \quad \text{if } E \text{ has bad reduction at } p \\
E(\mathbb{Q}_p)/E_0 &= 0 \quad \text{if } E \text{ has good reduction at } p \\
E_0/E_1 &\simeq \tilde{E}_{ns}(\mathbb{F}_p) \\
E_n/E_{n+1} &\simeq \mathbb{F}_p \quad \text{if } n \geq 1.
\end{align}
See [4, Ex 7.4 p. 187].

Let $m_P$ be the order of $P$ in $\tilde{E}(\mathbb{F}_p)$. It then follows that $p^k$ divides the denominator of the every multiple of the point $(p^{k-1}m_p)P$. We immediately see

**Corollary 4.5.** $\limsup r(nP_0) = \infty$. 

**Corollary 4.6.** $q(Q) > 1$ for infinitely many $Q$. 

The only difficulty with this approach to bounding $r$ is that a larger than expected power of $p$ may creep in. That is taking a multiple of $P_0$ may put us in a higher filtrant than we expected. We discuss this in Section 7. It turns out a higher than expected power of $p$ can occur only at the very first appearance of $p$, namely the multiple $m_P0$. Primes for which $m_P0$ is divisible by $p^2$ are called Wieferich primes. These are the primes that cause us all the difficulties.

Consider $nP_0$. If $p$ is non-Wieferich $\text{ord}_p(r) \leq \text{ord}_p(n)$ if $m_p \mid 2n$ and is 0 otherwise; hence if no Wieferich prime $p$ divides $r$ then $r \leq n$ and certainly $\log(r) = o(n^2)$ is true!

5. TORSION

In this section we note that the torsion of our curves plays little role in generating interesting triples.

**Lemma 5.1.** The torsion of the curve $y^2 = x^3 + Dx$ is given by
\begin{align}
\begin{cases}
\mathbb{Z}/4 & \text{if } D = 4 \\
\mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } -D \text{ is a square} \\
\mathbb{Z}/2 & \text{otherwise}.
\end{cases}
\end{align}
The torsion of $y^2 = x^3 + D$ is given by
\begin{align}
\begin{cases}
\mathbb{Z}/6 & \text{if } D = 1 \\
\mathbb{Z}/3 & \text{if } D \neq 1 \text{ is a square} \\
\mathbb{Z}/2 & \text{if } D = -432 \text{ or } D \neq 1 \text{ is a cube} \\
0 & \text{otherwise}.
\end{cases}
\end{align}
The torsion points on the curves $E_D$ do not produce abc triples.

**Proof** See [4, 10.6 Prop 6.1, p. 323] for the torsion (the statement on p. 323 has two lines interchanged). A one line calculation then shows that in each case the torsion points map under $\beta$ into \{0, 1, $\infty$\}.

Thus rank 0 curves do not produce any abc triples. The cases $D = 4$ and $D = 1$, $D = -432$ have rank 0 (the last statement being Fermat’s Last Theorem for exponent 3!) so our torsion is always 0, $\mathbb{Z}/2$ or $\mathbb{Z}/3$.

**Lemma 5.2.** (a) Suppose $E$ is the curve $y^2 = x^3 + Dx$. Let $T = (0, 0)$ be the 2-torsion point. If $P$ is a rational point on $E$ with $P \neq 0$, $P \neq (0, 0)$ then $P$ and $P + T$ give the same abc triple.

(b) If $-D = e^2$ then the abc triples produced by $P$ and $P + \pm(e, 0)$ contain the same list of primes, and hence have the same radical, although they need be equivalent triples.

**Proof** An explicit calculation shows that if $P = (x, y)$ then

$$P + (0, 0) = (D/x, -Dy/x^2)$$

Thus $\beta(P + (0, 0))$ is the reciprocal of $\beta(P)$, hence produces the same abc triple.

If $D > 0$ and $(x, y)$ is a point with $x \geq \sqrt{D}$ then $\tau(x) \leq \sqrt{D}$, so $\tau(y) \leq \sqrt{2D}^{5/4}$. If $D < 0$ then $E$ has two connected components. If $P = (x, y)$ is a (non-zero) point on the unbounded component $x \geq \sqrt{D}$, so $\tau(P)$ lies on the bounded component (the “egg”). Thus $-\sqrt{D} \leq \tau(x) < 0$ and $0 < y < \sqrt{2D}/3^{3/4}$. In particular, by applying $\tau$, we may always assume that $|x| < \sqrt{D}$, or $|x| > \sqrt{D}$. For example, we may always assume that the naive height of $x$ is the absolute value of its numerator.

We sketch (b). If $-D = e^2$ and $P = (x, y)$ is a non-torsion point, let $P' = P + (e, 0)$. Let $P$ give rise to triple $(a, b, c)$ and $P'$ to $(a', b', c')$. We may write $x = s/d^2$ for relatively prime $s$ and $d$. A calculation gives $\beta(P) = x^2/e^2$ and $\beta(P') = (x+e)^2/(x-e)^2$. Let $g = \gcd(s, e)$ and $g' = \gcd(s + ed^2, s - ed^2)$. Since $\gcd(s, d) = 1$, we see that $g' = 2^h g$ for some $h \geq 0$. Then $a = (s^2 - d^4 e^2)/g^2$, $b = d^4 e^2/g^2$, $c = s^2/g^2$, while $a' = 4sed^2/g^2 4^h$, $b' = (s - ed^2)^2/g^2 4^h$, $c' = (s + ed^2)^2/g^2 4^h$, so $4^h a^2 b' c' = 16a^2 bc$. But $a + b = c$ and $a' + b' = c'$ so (exactly) one of each of $a, b, c$ and of $a', b', c'$ are even. Taking radicals of the previous equation we have $\text{rad}(a'b'c') = \text{rad}(abc)$.

In (b) the triples need not be of identical quality. For example, assume $g = g' = 1$ for simplicity. Without loss of generality, by adding $(0, 0)$ if necessary, we may assume that $P$ lies on the unbounded component of the curve with $x > e$. Then the formulas given above show that $q(a, b, c) = 2 \log(s)/\log(\text{rad}(abc))$, and $q(a, b, c)' = 2 \log(s + ed^2)/\log(\text{rad}(abc))$, so $0 < q(a, b, c)' - q(a, b, c) < 2 \log(1+e/x)/\log(\text{rad}(abc)) < \log(4)/\log(\text{rad}(abc))$ which approaches 0 as the height of the point $P$ approaches infinity. Thus, perturbing the point $P$ by adding $(e, 0)$ does improve the quality of the triple, but with less and less effect as the height of $P$ increases.

**Example 5.3.** Let $D = -6^2$, $T = (6, 0)$, $P = (-3, 9)$. The first few triples are
Corollary 5.4. There exist infinitely many pairs \((a, b, c), (a', b', c')\) of non-equivalent abc triples with \(\text{rad}(abc) = \text{rad}(a'b'c')\), and \(q(a, b, c), q(a, b, c)\)' both greater than 1.

Proof We show below that if \(P \in E_D(\mathbb{Q})\) is a non-torsion point then infinitely many multiples of \(P\) produce triples of quality greater than 1. If \(P\) is a point of infinite order on \(E_D\) with \(s(P) > e\) then adding \(T\) to the appropriate multiples of \(P\) gives the result. □

It is an open problem if infinitely many such pairs exist which also have the same quality.

Example 5.5. Let \(D = -2^4 \cdot 5^2 \cdot 7^3 \cdot 11\). Then \(E_D\) is a curve of rank 2, with generators \(P_1 = (5 \cdot 7^3 \cdot 11/3^2, 5^4 \cdot 7^3 \cdot 11/3^3), P_2 = (5 \cdot 7^3 \cdot 11/2^2, 3^2 \cdot 5^2 \cdot 7^3 \cdot 11/2^3)\) giving \((a, b, c) = (5^3, 2^3, 3^2, 7^3, 11)\), of quality \(\log(3773)/\log(2310) \approx 1.06334\), and \((a, b, c) = (3^2, 5, 2^3, 7^3, 11)\) with the same radical and the same quality.

We have \(c = s^2, b = -Dd^4, a = t^2/s\) (up to \(\gcd(s, D)\)), so the infinitely many equal quality > 1 pairs of triples is essentially equivalent to the existence of infinitely many curves \(E_D\) of rank at least 1, with points \(P = (s/d^2, t/d^3)\) and \(P' = (s'/d^2, t'/d^3)\) with \(d \neq d'\) such that (1) \(s = s'\), and (2) \(\text{rad}(Dd^4) = \text{rad}(Dd'^4)\); that is, any prime occurring in \(y\) not occurring in \(x\) or \(D\) must also be in \(y\) i.e. the set of primes \(p\) for which \(P\) has exact order 2 is the same as the set for which \(P'\) has exact order 2.

ie if and only if \(s = s'\) and for every prime \(p\) of good reduction, \(2P = 0\) in \(\mathbb{F}_p\) \(\iff\) \(2P' = 0\) in \(\mathbb{F}_p\).

Corollary 5.6. It seems we can show that there exist infinitely many pairs of high quality triples if and only if there exist infinitely many curves \(E_{-6}\) with distinct non-torsion points \(P\) and \(P'\) such that for every prime \(p\) of good reduction, \(2P = 0\) in \(\mathbb{F}_p\) \(\iff\) \(2P' = 0\) in \(\mathbb{F}_p\).

6. Some Examples

In this section we give a numerical example of each type of curve.

Example 6.1. (a) with \(D = -6\). The structure of \(E(\mathbb{Q})\) is easily found. The torsion subgroup of \(E(\mathbb{Q})\) is of order 2, generated by \((0, 0)\). Since \(E\) admits a 2-isogeny to the curve \(E': y^2 = x^3 + 24x\), a standard 2-descent shows that the Mordell-Weil group \(E(\mathbb{Q})\) has rank 1. A generator is the point \(P = (3, 3)\).

Let \(\beta: E \to \mathbb{P}^1\) be the Belyi map \((x, y) \mapsto -x^2/6\). We give a table of \(q(nP)\) for small \(n\) calculated using GP-Pari. Note that \(a, b, c\) satisfy generalized Fermat equation with coefficients dividing 6 and exponents \((2, 4, 4)\). Note also that \(q\) appears to approach 1.
Example 6.2. In (b) if \( D = 3 \) then

\[ E(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}/3 \]

generated by \( P = (6, 15) \) of infinite order and \( T = (0, 3) \) of order 3. The map is

\[ \phi(x, y) = (y + 3)/6 = c/b. \]

Below is a table of abc triples obtained from \( nP \) for small \( n \). Note that up to factors of \( 2D = 6 \) each of \( a, b, c \) is a cube and that \( q(a, b, c) \) appears to approach 1.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( a )</th>
<th>( b )</th>
<th>( c )</th>
<th>( q(a, b, c) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0.61315</td>
</tr>
<tr>
<td>2</td>
<td>23^2</td>
<td>2^5 \cdot 3</td>
<td>5^4</td>
<td>0.98486</td>
</tr>
<tr>
<td>3</td>
<td>187^2</td>
<td>2 \cdot 13^4</td>
<td>3^5 \cdot 11^4</td>
<td>1.05569</td>
</tr>
<tr>
<td>4</td>
<td>39841^2</td>
<td>2^6 \cdot 3^4 \cdot 23^4</td>
<td>7^4 \cdot 103^4</td>
<td>1.11019</td>
</tr>
<tr>
<td>5</td>
<td>19^2 \cdot 29^2 \cdot 101^2 \cdot 253^2</td>
<td>2 \cdot 37^4 \cdot 239^4</td>
<td>3 \cdot 17^4 \cdot 41^8</td>
<td>1.09475</td>
</tr>
<tr>
<td>6</td>
<td>23^2 \cdot 1607^2 \cdot 14159^2 \cdot 21863^2</td>
<td>2^6 \cdot 3^3 \cdot 11^4 \cdot 13^4 \cdot 187^4</td>
<td>5^4 \cdot 722977^4</td>
<td>1.01589</td>
</tr>
</tbody>
</table>

Example 6.3. (c) The same curve as above \( y^2 = x^3 + 9 \), but this time with map \( (x, y) \mapsto y^2/9 = c/b \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( a )</th>
<th>( b )</th>
<th>( c )</th>
<th>( q(a, b, c) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2^1 \cdot 3</td>
<td>1</td>
<td>5^2</td>
<td>0.94639</td>
</tr>
<tr>
<td>2</td>
<td>2^6 \cdot 3</td>
<td>131^2</td>
<td>1.17810</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1^7 \cdot 37^3</td>
<td>3^8 \cdot 7^6</td>
<td>1.04804</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2^{12} \cdot 3 \cdot 11^3 \cdot 23^3 \cdot 61^3</td>
<td>191^2 \cdot 962543^2</td>
<td>5^6 \cdot 131^6</td>
<td>1.05298</td>
</tr>
<tr>
<td>5</td>
<td>2^3 \cdot 3 \cdot 3449^3 \cdot 18269^3</td>
<td>26309^6</td>
<td>54 \cdot 734969629321^2</td>
<td>1.03777</td>
</tr>
<tr>
<td>6</td>
<td>1^7 \cdot 37^3 \cdot 197^3 \cdot 307^3 \cdot 106219^3</td>
<td>2^{12} \cdot 3^8 \cdot 5^6 \cdot 7^6 \cdot 2287^6</td>
<td>11^2 \cdot 23^2 \cdot 61^2 \cdot 131^2 \cdot 140617^2</td>
<td>1.01730</td>
</tr>
<tr>
<td>7</td>
<td>2^3 \cdot 3 \cdot 67^3 \cdot 83^3 \cdot 127^3 \cdot 461^3</td>
<td>13^6 \cdot 19^6 \cdot 23007^6</td>
<td>30062737^2</td>
<td>5^4 \cdot 41^2 \cdot 28433^2 \cdot 332641^2 \cdot 96811^2</td>
</tr>
<tr>
<td>8</td>
<td>2^{12} \cdot 3 \cdot 11^3 \cdot 23^3 \cdot 61^3 \cdot 167^3 \cdot 193^3 \cdot 511^3</td>
<td>5^6 \cdot 131^6 \cdot 191^6 \cdot 962543^6</td>
<td>106977777^2</td>
<td>14639^2 \cdot 59868047^2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( n )</th>
<th>( a )</th>
<th>( b )</th>
<th>( c )</th>
<th>( q(a, b, c) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0.61315</td>
</tr>
<tr>
<td>2</td>
<td>23^2</td>
<td>2^5 \cdot 3</td>
<td>5^4</td>
<td>0.98486</td>
</tr>
<tr>
<td>3</td>
<td>187^2</td>
<td>2 \cdot 13^4</td>
<td>3^5 \cdot 11^4</td>
<td>1.05569</td>
</tr>
<tr>
<td>4</td>
<td>39841^2</td>
<td>2^6 \cdot 3^4 \cdot 23^4</td>
<td>7^4 \cdot 103^4</td>
<td>1.11019</td>
</tr>
<tr>
<td>5</td>
<td>19^2 \cdot 29^2 \cdot 101^2 \cdot 253^2</td>
<td>2 \cdot 37^4 \cdot 239^4</td>
<td>3 \cdot 17^4 \cdot 41^8</td>
<td>1.09475</td>
</tr>
<tr>
<td>6</td>
<td>23^2 \cdot 1607^2 \cdot 14159^2 \cdot 21863^2</td>
<td>2^6 \cdot 3^3 \cdot 11^4 \cdot 13^4 \cdot 187^4</td>
<td>5^4 \cdot 722977^4</td>
<td>1.01589</td>
</tr>
</tbody>
</table>

7. Elliptic Wieferich Primes

In this section we define the set \( \mathcal{W}_E \) of primes that causes difficulty. For later reference, recall that a rational point on an elliptic curve defined over \( \mathbb{Q} \) may be written in the form \( (S/d^2, T/d^3) \) where \( S, T \) and \( d \) are integers with \( \gcd(S,d) = \gcd(T,d) = 1 \).

Recall that a Wieferich prime \( p \) to base \( a \) is a prime number satisfying \( a^{p-1} \equiv 1 \pmod{p^2} \). That is, on \( \mathbb{Z} \) we have a filtration

\[ \mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset \cdots \]

Each filtration quotient is \( \mathbb{F}_p \). Each \( p^n\mathbb{Z} \) with \( n \geq 1 \) maps to \( p^{n+1}\mathbb{Z} \) by multiplication by \( p \) while the Fermat map \( f(a) = a^{p-1} - 1 \) provides the map \( \mathbb{Z} \xrightarrow{f} p\mathbb{Z} \). Fix \( a > 1 \). Then \( p \) is a Wieferich prime to base \( a \) if and only if \( a \in \mathbb{Z} \) maps under the Fermat map \( f \) to \( p^2\mathbb{Z} \), i.e., if and only if \( a \)

\[ \text{It may then be necessary to permute } a, b, c \text{ and take absolute values.} \]
lands in an unexpectedly high filtrant. Although Wieferich primes are expected to be very rare, it is not even known that the set of non-Wieferich primes is infinite.

Now, by analogy, let $E$ be an elliptic curve defined over $\mathbb{Q}$. Fix a minimal model of $E$ over $\mathbb{Q}_p$ for each $p$. (For example $E = E_D$ for any fourth power free integer $D$.) Let $\tilde{E}$ be the reduction of $E$ modulo $p$. We then have a canonical filtration on $E(\mathbb{Q}_p)$. Namely, for each $n \geq 1$, let

$$E_n = E_n(\mathbb{Q}_p) = \{(x, y) \in E(\mathbb{Q}_p) \mid \text{ord}_p(x) \leq -2n\} \cup \{0\}.$$ (13)

Note that for primes of good reduction $E_1$ is the kernel of reduction modulo $p$. In general, let $\tilde{E}_{ns}(\mathbb{F}_p)$ be the set of non-singular points modulo $p$, and $E_0 = E_0(\mathbb{Q}_p)$ be the subset of $E(\mathbb{Q}_p)$ mapping to $\tilde{E}_{ns}(\mathbb{F}_p)$. Thus for all $p$ of good reduction, $E_0 = E(\mathbb{Q}_p)$ and $\tilde{E}_{ns}(\mathbb{F}_p) = \tilde{E}(\mathbb{F}_p)$. Using the formal group law interpretation of $E_1$ one shows that the filtration

$$(14)\quad E(\mathbb{Q}_p) \supset E_0 \supset E_1 \supset E_2 \supset \cdots$$

is exhaustive, where

$$E_0/E_1 \simeq \tilde{E}_{ns}(\mathbb{F}_p)$$

$$E_n/E_{n+1} \simeq \mathbb{F}_p \quad \text{if } n \geq 1.$$ (15)

See [4, Ex 7.4 p. 187]. Let

$$(16)\quad E_n(\mathbb{Q}) = E_n \cap E(\mathbb{Q}).$$

(Of course, $E_n(\mathbb{Q})$ depends on the prime $p$, but the value of $p$ is usually clear from the context.) This gives a filtration on $E(\mathbb{Q})$, and each quotient is a sub-group of corresponding quotient from the filtration on $E(\mathbb{Q}_p)$.

**Lemma 7.1.** Let $p$ be a prime. If $p = 2$ assume that the Weierstraß coefficient $a_1$ in the minimal equation for $E$ is 0. Let $n$ and $k$ be positive integers. If $Q \in E(\mathbb{Q})$ gives rise to a non-zero class in $E_n/E_{n+1}$ then $p^kQ$ gives a non-zero class in $E_{n+k}/E_{n+k+1}$. (In particular, $Q$ has infinite order.) Hence there exists $m \geq 0$ such that the filtration on $E(\mathbb{Q})$ is strictly decreasing at every stage from $E_{m+1}(\mathbb{Q})$ onwards.

**Proof** Using induction, it suffices to prove the case $k = 1$. There is an isomorphism $E_n \rightarrow p^n\mathbb{Z}_p$ given by $(x, y) \mapsto z = -y/x$, where the addition on $\mathbb{Z}_p$ is given by the formal group law (power series in two variables) associated with $E$. Multiplication by $p$ in $E$ can be calculated in $E_n$ using appropriate power series $F_p$. By [4, 2.3(a) p. 116 & 4.4 p. 120] $F_p(T) = pT + apT^2 + O(T^3)$ for some coefficient $a$, provided $p \neq 2$. Let $Q = (x, y) \in E_n$ satisfy the hypothesis of the Lemma. Then $Q$ maps to $z \in p^n\mathbb{Z}_p$, i.e. $z = a_n p^n + \cdots$ with $a_n \neq 0$. One then checks that the leading term of $F_p(z)$ is $a_n p^{n+1}$, which comes from $E_{n+1}$ but not $E_{n+2}$. If $p = 2$ then $F_2(T) = 2T - a_1T^2 - 2a_2T^3 + O(T^4)$ [4, p.121], and the same proof works, provided $a_1 = 0$, but if $a_1 = 0$ there may be cancellation in the leading term.

Now for each $m \geq 1$, $E_m(\mathbb{Q})/E_{m+1}(\mathbb{Q})$ is either 0 or $\mathbb{F}_p$. If it is not 0 then it contains some non-zero element $Q$, and then every subsequent quotient contains non-zero element, hence is isomorphic to $\mathbb{F}_p$.

Note that the proof fails for points in $E_0$, because there is no formal group law interpretation; $Q$ now maps to a unit in $\mathbb{Z}_p$ and the power series $F_p(z)$ does not converge in $\mathbb{Z}_p$. \hfill \Box
Definition 7.2. For each prime $p$ let
\[ f_p = \begin{cases} 0 & \text{if } E_1(Q) \neq E_2(Q) \\ \max\{n \mid E_n(Q) = E_{n+1}(Q)\} & \text{otherwise} \end{cases} \]
This is well defined, by the Lemma above. If $f_p > 0$ we say that $p$ is an \textit{(elliptic) Wieferich prime} for $E$. Let $W_E$ be the set of Wieferich primes of $E$.

The canonical filtration is really giving topological information in the $p$-adic topology. We can therefore reformulate the definition in topological terms (this is the definition given in the introduction). Let $\overline{E(Q)}$ denote the closure of $E(Q)$ in $E(Q_p)$.

Lemma 7.3. Suppose $E(Q)$ is infinite and let $p$ be a prime. Then for some $m > 1$, $E_m(Q)$ is dense in $E_m(Q_p)$ (in the $p$-adic topology on $E(Q_p)$).

Let $m$ be the smallest positive integer with this property. Then $m = f_p + 1$. Thus $p$ is Wieferich if and only if the kernel of reduction modulo $p$ of $E(Q)$ is not dense in the kernel of reduction modulo $p$ of $E(Q_p)$.

Proof Fix $p$ and let $E_1(Q) = E_2(Q) = \cdots = E_n(Q) \supset E_{n+1}(Q) \supset E_{n+2}(Q) \supset \cdots$, where the inclusions are all strict. By definition, $p$ is Wieferich if and only if $n > 1$.

The containment $E_n(Q) \subseteq E_n(Q_p)$ is clear, since $E_n(Q_p)$ is closed.

For the other containment, recall that $(x, y) \mapsto y/x$ is a bijective map from $E_n(Q_p)$ to $p^n\mathbb{Z}_p$. Let $R_n \in E_n(Q_p)$ map to $a_n p^n + O(p^{n+1})$, with $a_i \in \mathbb{F}_p$. The key point is that $E_n(Q)/E_{n+1}(Q) \cong \mathbb{F}_p$, so there exists $S_n \in E_n(Q)$ mapping to $-a_n p^n + O(p^{n+1})$. Then adding $R_n$ and $S_n$ in $E_n(Q_p)$ using the formal group law, we see that $R_n + S_n \in E_{n+1}(Q_p)$. Let $R_n = S_n + R_{n+1}$, with $R_{n+1} \in E_{n+1}(Q_p)$. Since the filtration on $E(Q)$ is infinite we may repeat this process and obtain $R_n$ as the limit of a sequence (of partial sums) of points in $E_n(Q)$, converging in the $p$-adic topology on $E(Q_p)$. The limit is a point of $\overline{E_n(Q)}$.

Let $m$ be as described. If $0 < r < n$ we know $E_r(Q_p)/E_{r+1}(Q_p) \cong \mathbb{F}_p$, so let $R_r \in E_r(Q_p) \setminus E_{r+1}(Q_p)$, and let $R_r \mapsto a_r p^r + O(p^{r+1})$ with $a_r \neq 0$. Since $E_r(Q)/E_{r+1}(Q) = 0$, elements in $E_r(Q)$ are not arbitrarily $p$-adically close to $R_r$. So $E_r(Q)$ is not dense. Thus $m = n$. \hfill \Box

Note: Assume that $E(Q)$ is infinite. We give a heuristic argument below that for most primes $E_1(Q)$ is dense in $E_1(Q_p)$. However $E(Q)$ is often not dense in $E(Q_p)$ because the reduction map $E(Q) \to E(F_p)$ is often not surjective. See [3].

Ultimately we care only about the asymptotic size of the set $W_E$, so we can simplify calculations by ignoring small primes and primes of bad reduction. We give a reformulation sufficient for our needs.

Corollary 7.4. Suppose $E(Q)$ is infinite with $E(Q)_\text{tors} \neq 0$ and let $p > 7$ be a prime of good reduction. Then $p$ is a Wieferich prime for $E$ if and only if
\[ \left(\frac{E(Q_p)}{E(Q)}\right)[p] \neq 0 \]
Thus up to a finite set, $W_E$ is the set of primes occurring as orders of group elements in $\prod_p \left(\frac{E(Q_p)}{E(Q)}\right)_\text{tors}$. 


Proof. Examining the filtration, we have

\begin{equation}
[E(Q_p) : E(Q)] = \frac{|E(Q_p) : E_0|}{|E(Q) : E_0(Q)|} \cdot \frac{|\tilde{E}_{ns}(\mathbb{F}_p)|}{|E_0(Q) : E_1(Q)|} \cdot p^r.
\end{equation}

(The right hand side is a product of three integers.) If \( p > 7 \) is a prime of good reduction then we have \([E(Q_p) : E_0] = 1\) and the Weil bound ensures that \( 0 < |\tilde{E}(\mathbb{F}_p)| < 2p \). But \(|\tilde{E}(\mathbb{F}_p)| \neq p\) because the group \( E(Q)_{tors} \) injects into \( \tilde{E}(\mathbb{F}_p) \), and since the former is non-zero its order is divisible by \( 2, 3, 5 \) or \( 7 \). So the same must be true of the order of \( \tilde{E}(\mathbb{F}_p) \). \( \square \)

If \( p = 7 \) is a prime of good reduction then the result still holds unless \( E(Q)_{tors} \) and \( \tilde{E}(\mathbb{F}_p) \) are both cyclic of order 7. For \( p = 2, 3 \) or 5 of good reduction the result holds unless (a) \( \tilde{E}(\mathbb{F}_p) \) and \( E(Q)_{tors} \) are both of order \( p \), or (b) \( \tilde{E}(\mathbb{F}_p) \) is of order \( 2p \) and \( E(Q)_{tors} \) is of order 2, \( p \) or \( 2p \).

Note that this argument shows that for \( p > 7 \),

\begin{equation}
E(Q_p)[p] = 0
\end{equation}

since \( E_1(Q_p)[p] = 0 \) using the formal group argument [4, p. 124] and \( \tilde{E}(\mathbb{F}_p)[p] = 0 \).

We use the following criterion for numerical calculations.

**Lemma 7.5.** Suppose \( E(Q) \) is infinite with \( E(Q)_{tors} \neq 0 \) and let \( p > 7 \) be a prime of good reduction. Let \( P_1, \ldots, P_n \) be generators of \( E(Q) \) and let \( m_i \) be the order of \( \tilde{P}_i \) in \( \tilde{E}(\mathbb{F}_p) \). Then \( p \) is Wieferich if and only if \( m_iP_i \in E_2(Q) \) for every \( i \).

**Proof.** As noted, for such \( p \) we have \( |\tilde{E}(\mathbb{F}_p)| \neq p \), i.e. \( \gcd(m_i, p) = 1 \). If \( p \) is Wieferich then \( E_1(Q) = E_2(Q) \) so \( m_iP_i \in E_2(Q) \) by definition of \( m_i \). We next prove the converse. Consider the contrapositive statement. That is, suppose \( p \) is not Wieferich. Then some point \( R = \sum a_iP_i \) has non-zero image \( \overline{R} \) in \( E_1/E_2 \cong \mathbb{F}_p \). Thus \( m_1m_2 \ldots m_kP_k \overline{R} \neq 0 \), so some \( m_iP_i \) is not in \( E_2 \). \( \square \)

**Remark 7.6.** In the rank one case, this is particularly simple. If \( P \) is a generator of the torsion-free part of \( E(Q) \), \( p \) a prime of good reduction and \( m_p \) the order of \( P \) in \( \tilde{E}(\mathbb{F}_p) \), then \( p \) is Wieferich if and only if the denominator of \( m_pP \) is divisible by \( p^2 \).

**Remark 7.7.** If we assume that for non-torsion \( P_i \) the classes \( m_iP_i \in E_1(Q_p)/E_2(Q_p) \simeq \mathbb{F}_p \) are distributed “randomly” and independently as we vary \( p \) and \( i \) then the chance that \( m_iP_i \) falls into \( E_2(Q_p) \) is about \( 1/p \). If \( E \) has rank \( n \) then the chance that \( p \) is Wieferich for \( E \) is about \( 1/p^2 \). If \( n = 1 \) the number of elliptic Wieferich primes up to a bound \( x \) should grow like \( \sum_{p \leq x} 1/p^2 \ll \log \log x \), just as is conjectured for the usual Wieferich primes. Thus the condition required in Theorem ?? is much weaker than what we would expect heuristically to be true. For a numerical example, see section 9.

We can reformulate Theorem 7.4 in cohomological language. We use the following many times.

**Lemma 7.8.** Suppose

\[
\begin{array}{c}
0 \to A \to B \to C \to 0
\end{array}
\]

is a short exact sequence of abelian groups. Then there is a long exact sequence

\begin{equation}
\begin{array}{cccccccc}
0 & \to & A[p] & \to & B[p] & \to & C[p] & \to & A/p \\
& & \to & \to & \to & \to & \to & \to
\end{array}
\end{equation}

\begin{equation}
\begin{array}{cccccccc}
& \to & B/p & \to & C/p & \to & 0
\end{array}
\end{equation}
Now we introduce the cohomology. Tate local-duality gives a bilinear perfect pairing
\[ H^0(Q_p, E) \times H^1(Q_p, E) \rightarrow \text{Br}(Q_p)^{\text{inv}} \cong Q/Z. \]
For all finite \( p \) the map \( \text{inv} \) is an isomorphism, and \( H^0(Q_p, E) = E(Q_p) \). At the real place \( H^0(\mathbb{R}, E) \) is 0 or \( \mathbb{Z}/2 \), depending on whether or not \( E(\mathbb{R}) \) is connected. Since \( H^1(Q, E) \) maps into the direct sum of the local groups \( H^1(Q_p, E) \) and for any \( x, \text{inv}(x) = 0 \) for almost all \( p \), the pairing above extends to a global pairing:
\[ \prod_p H^0(Q_p, E) \times H^1(Q, E) \rightarrow \bigoplus \text{Br}(Q_p) \cong Q/Z. \]

Let \( p \) be a (finite) prime. Suppose that \( \text{III}(E) \) is finite. We are interested in an asymptotic condition, so we may disregard finitely many primes; hence assume that \( p \) does not divide the order of \( \text{III}(E) \), that \( p > 7 \) and that \( p \) is a prime of good reduction. Assume further that \( E(Q)_{\text{tors}} \neq 0 \). Then \( E(Q_p)[p] = 0 \) (equation 20).

Let \( A_p = E(Q_p)/\overline{E(Q)} \) and let \( E(Q)^\times \) be the profinite completion of \( E(Q) \)—this is also the closure of \( E(Q) \) after diagonally embedding in the product \( \prod_p H^0(Q_p, E) \). That is, if we let \( \pi \) be the projection map onto the \( p \)-th coordinate, and let \( \alpha \) be the diagonal embedding \( E(Q) \rightarrow \prod_p H^0(Q_p, E) \), then \( \pi(\alpha E(Q)^\times) = \pi(\alpha E(Q)) \) \( \cong (\pi \circ \alpha)(E(Q)) \cong E(Q) \) where the closure before equality (a) is closure in the product and equality (b) follows because \( \pi \) is a continuous closed map and hence commutes with the closure operator. The Tate pairing fits into the following diagram (Cassels-Tate duality), where \( X \) is the indicated cokernel:

\[ 0 \rightarrow E(Q)^\times \xrightarrow{\alpha} \prod_p H^0(Q_p, E) \xrightarrow{\beta} H^1(Q, E)^{\times} \rightarrow \text{III}^{\times} \rightarrow 0. \]

By Corollary 7.4 \( p \) is Wieferich if and only if \( X[p] \neq 0 \). We shall rewrite this condition in terms of \( \beta \). Let \( Y = \ker \beta \), and let \( Z = \ker \pi \). Note that \( E(Q_p)[p] = 0 \) by equation 20 so \( E(Q)^\times[p] = 0 \), while \( p \) does not divide the order of \( \text{III}^{\times} \).

We now have several short exact sequences. Truncating the top row of the diagram above and using the Snake Lemma we have
\[ 0 \rightarrow Z \rightarrow Y \rightarrow X \rightarrow 0. \]
From the definition of \( Z \) we have
\[ 0 \rightarrow Z \rightarrow \prod_p H^0(Q_p, E) \rightarrow E(Q_p) \rightarrow 0. \]
while from the definition of \( Y \) we have
\[ 0 \rightarrow E(Q)^\times \rightarrow \prod_p H^0(Q_p, E) \rightarrow Y \rightarrow 0. \]
and
\[ 0 \rightarrow Y \rightarrow H^1(Q, E)^{\times} \rightarrow \text{III}^{\times} \rightarrow 0. \]
so that applying Lemma 7.8 to all of the above short exact sequences and stitching everything together we obtain the following diagram:

\[(25)\]

\[
\begin{array}{cccccccccc}
0 & \to & Z[p] & \zeta & Y[p] & \to & X[p] & \eta & Y/p & \to & X/p & \to & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \prod_p H^0(Q_p, E)[p] & \beta' & H^1(Q, E)^*[p] & \to & E(Q)/p & \overline{\pi} & \prod_p H^0(Q_p, E)/p & \overline{\pi} & H^1(Q, E)^*/p & \to & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
& & E(Q_p)/p & \overline{\pi} & E(Q_p)/p & & & & & & & & \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
& & X/p & 0 & 0 & & & & & & & & \\
\end{array}
\]

Here \(\beta'\) is the restriction of \(\beta\), and \(\overline{\pi}\) is the map induced by \(\pi\) and similarly for other overlined maps.

We thus have the following chain of equivalences.

1. \(p \not\in \mathcal{W}\) \(\iff\) \(\zeta\) is surjective and \(\eta\) is injective.
2. \(\iff\) \(\beta'\) is surjective and \(\overline{\pi}(\ker \overline{\beta}) = E(Q_p)/p\)
3. \(\iff\) \(\frac{1}{p} \ker \beta = \prod_p H^0(Q_p, E)[p] + \ker \beta\) and \(E(Q_p) = pE(Q_p) + \pi(\ker \beta)\).

Equivalence (1) follows from Corollary 7.4. (2) Follows by a diagram chase.

Each part of condition (3) follows from a small calculation. For example, assume \(\frac{1}{p} \ker \beta = \prod_p H^0(Q_p, E)[p] + \ker \beta\). We show that \(\beta'\) is surjective. Let \(c \in H^1(Q, E)^*[p]\). Then the image of \(c\) in \(\prod_p H^0(Q_p, E)[p]\) is 0 so there exists \(b \in \prod_p H^0(Q_p, E)\) with \(\beta(b) = c\). Here \(b\) may not have order \(p\), but \(p\beta(b) = 0\), so \(b \in \frac{1}{p} \ker \beta\), so, by the hypothesis, \(b = b_1 + \alpha(a_1)\) for some \(a_1 \in E(Q)^*\) and \(b_1 \in \prod_p H^0(Q_p, E)[p]\). Thus \(\beta'(b_1) = c\), and so \(\beta'\) is surjective. The converse direction is similar.

Using exactness at \(\prod_p H^0(Q_p, E)/p\) we see that if \(\pi(\ker \overline{\beta}) = E(Q_p)/p\) then for every \(e \in E(Q_p)\) there exists \(a \in E(Q)^*\) satisfying \(e \in pE(Q_p) + \pi \circ \alpha(a)\), so \(E(Q_p) = pE(Q_p) + \pi(\ker \beta)\). The converse is again similar.

The reason for introducing \(\ker \beta\) is that it is closely related to the Brauer-Manin obstruction for \(E\), which we now define. The long exact sequence of low degree terms obtained from the Leray spectral sequence for the structure morphism \(\pi: E \to \text{Spec } \mathbb{Q}\)

\[
\begin{array}{c}
H^r(\text{Spec } \mathbb{Q}, R^s\pi_* \mathbb{G}_m) \Rightarrow H^{r+s}(E, \mathbb{G}_m)
\end{array}
\]
yield an isomorphism $H^1(\mathbb{Q}, E) \cong \text{Br}(E)/\text{Br}(\mathbb{Q})$. After composing pairing 23 with this isomorphism in the second variable, we define the Brauer-Manin pairing:

$$(26) \quad \prod_p H^0(\mathbb{Q}_p, E) \times \text{Br}E/\text{Br}(\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}.$$ 

We thus have a (non-exact) diagram

$$(27) \quad E(\mathbb{A}) \xrightarrow{\theta} \prod_p H^0(\mathbb{Q}_p, E) \xrightarrow{\beta} H^1(\mathbb{Q}, E)^* \xrightarrow{\sim} \left(\text{Br}(E)/\text{Br}(\mathbb{Q})\right)^*.$$ 

**Definition 7.9.** The Brauer-Manin obstruction $E^{\text{Br}}$ is defined to be the kernel of $\theta$.

Of course we have $E^{\text{Br}} \subseteq E(\mathbb{A})$.

Furthermore if we let $E(\mathbb{R})^0$ denote the connected component subgroup of the identity in $E(\mathbb{R})$ we have

$$(28) \quad \ker \beta = E^{\text{Br}} / E(\mathbb{R})^0.$$ 

A more detailed discussion may be found in [12] [13].

It follows that we may rewrite equivalence (4) above in terms of $E^{\text{Br}}$ instead of ker $\beta$. The formulation is:

$$p \not\in W \iff \frac{1}{p}E^{\text{Br}} = E(\mathbb{A})[p] + E^{\text{Br}} \quad \text{and} \quad E(\mathbb{Q}_p) = pE(\mathbb{Q}_p) + \pi(E^{\text{Br}}).$$

In view of equation 28 it is immediate that $E(\mathbb{Q}_p) = pE(\mathbb{Q}_p) + \pi(E^{\text{Br}})$ if and only if $E(\mathbb{Q}_p) = pE(\mathbb{Q}_p) + \pi(\ker \beta)$. It is also clear $\frac{1}{p}E^{\text{Br}} = E(\mathbb{A})[p] + E^{\text{Br}}$ implies $\frac{1}{p} \ker \beta = \prod_p H^0(\mathbb{Q}_p, E)[p] + \ker \beta$. For the converse, observe that since the Brauer-Manin pairing depends only on the connected component of the coordinate in the real place (or in other words, because $\text{Br}(\mathbb{R}) \cong \mathbb{Z}/2$) any point in $E(\mathbb{A})$ representing a class in $\ker \beta$ will automatically lie in $E^{\text{Br}}$. Thus we need only to be able to lift classes class in $(\ker \beta)[p] = \left(E(\mathbb{A})/E(\mathbb{R})^0\right)[p]$ to representatives in $E(\mathbb{A})[p]$. But we can, because $E(\mathbb{R})^0$ is isomorphic to the circle group $S^1$, while $E(\mathbb{R}) \cong S^1 \times \mathbb{Z}/2$. In particular $E(\mathbb{R})^0[p] \neq 0$, while if $p$ is odd, $y_\infty \in E(\mathbb{R})$, and $py_\infty \in E(\mathbb{R})^0$ implies $y_\infty \in E(\mathbb{R})$. Thus with such $p$ and $y_\infty$ there exists $y_\prime \in E(\mathbb{R})^0[p]$ with $y_\prime$ and $y_\infty$ representing the same class (namely 0) in $E(\mathbb{R})/E(\mathbb{R})^0$. Thus any class in $(\ker \beta)[p] = \left(E(\mathbb{A})/E(\mathbb{R})^0\right)[p]$ is represented by an element in $E(\mathbb{A})[p]$.

In summary, we have proved the following:

**Theorem 7.10.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$, with rank at least one and non-zero torsion subgroup. Assume that $\text{III}(E)$ is finite. Let $p > 7$ be a prime of good reduction not dividing the order of $\text{III}(E)$. Then the following are equivalent:

(a) $p$ is not Wieferich.

(b) $\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q})}[p] = 0$.

(c) The natural map $\prod_p H^0(\mathbb{Q}_p, E)[p] \to H^1(Q, E)^*[p]$ is surjective and $\pi\left(\ker(\prod_p H^0(\mathbb{Q}_p, E)/p \to H^1(Q, E)^*/p)\right) = E(\mathbb{Q}_p)/p$.

(d) $\frac{1}{p}E^{\text{Br}} = E(\mathbb{A})[p] + E^{\text{Br}}$ and $E(\mathbb{Q}_p) = pE(\mathbb{Q}_p) + \pi(E^{\text{Br}})$. 


The last condition can be restated: if \( px \) is a Brauer point then \( x \) is a Brauer point, up to an element in \( E(\mathbb{A})[p] \). Secondly, any point in \( E(\mathbb{Q}_p) \) becomes \( p \)-divisible, after adjusting by a suitable Brauer point.

8. The Weak ABC Conjecture

We show that if \( W_E \) is not too large then the weak abc conjecture holds.

The main point is that \( \log(w) \) is essentially a quadratic form in \( n \), while \( r < n \) unless Wieferich primes interfere.

Let \( E \) be an elliptic curve of \( j \)-invariant 1728. Assume that \( X(E) \) is finite. In the following \( p \) will denote a prime of good reduction not dividing the order of \( X(E) \), with \( p > 7 \).

We translate the filtration information on \( E \) into a bound for \( r \). Unfortunately the mysterious elliptic Wieferich primes contribute to \( r \), and we have not been able to control them sufficiently.

Let \( E \) be an elliptic curve of \( j \)-invariant 1728. Assume that \( X(E) \) is finite. In the following \( p \) will denote a prime of good reduction not dividing the order of \( X(E) \), with \( p > 7 \).

For simplicity, assume that \( E \) has rank 1, generated by \( P \). The sequence of points we examine is then \( kP \) for \( k = 1, 2, \ldots \). Let \( m_p \) be the order of \( P \) in \( \tilde{E}(\mathbb{F}_p) \).

Recall that \( r \) measures repeated factors in the coordinates \( d, s \) and so on. The denominator of \( kP \) is divisible by \( p \) if and only if \( kP \) reduces to 0 in \( \tilde{E}(\mathbb{F}_p) \). The exact power of \( p \) that occurs can be read from the filtration.

\[
\text{ord}_p(d(kP)) = \begin{cases} 
0 & \text{if } m_p \text{ does not divide } k \\
\text{ord}_p(k/m_p) + f_p & \text{if } m_p | k.
\end{cases}
\]

That is, each \( m_pP \) gains another factor of \( p \) in its denominator, whenever it is multiplied by \( p \). Further multiples of \( p \) occur if \( m_pP \) lands in \( E_2(\mathbb{Q}) \) or a higher filtrant.

Under the assumptions on \( p \) above, \( p \) and \( m_p \) are relatively prime, so if \( p \) is non-Wieferich,

\[
\text{ord}_p(d(kP)) = \begin{cases} 
0 & \text{if } m_p \text{ does not divide } k \\
\text{ord}_p(k) & \text{if } m_p | k.
\end{cases}
\]

Similarly, to test if \( s(kP) \) or \( t(kP) \) are divisible by \( p \) we can instead test \( d(2kP) \). Finally for the primes of bad reduction we also need to keep track of the \( E/E_0 \) filtration quotient and any factors of \( A \).

**Theorem 8.1.** Let \( k \) be a positive integer, \( P \) a point on \( E \), let \( r = r(kP) \) and let \( p \) be a prime. Suppose the coordinates of \( kP \) are not divisible by any Wieferich primes. Then

\[
r(kP) \leq Ck \prod_{m_p|2k} p^{f_p}
\]

where \( C \) is a constant.

However the height function is quadratic: \( \log s \) grows like \( k^2 \). So the required bound is easily satisfied, unless the \( f_p \) contribute enormously.

Thus, let \( \mathcal{F} \) be the set of positive integers \( k \) such that the coordinates of \( kP \) are not divisible by any Wieferich prime. Since we expect \( W \) to be extremely sparse, \( \mathcal{F} \) should a large subset of integers. In particular it should be infinite!

\[\text{3}\] i.e., at all
Theorem 8.2. Assume that \( F \) is infinite. Then
\[
\lim_{k \in F, k \to \infty} q(kP) = 1
\]

*Proof* This follows from the bound on \( r \) and the Theorem above. \( \square \)

Corollary 8.3. If \( F \) is infinite then 1 is a limit point of \( abc \).

The bound given in Theorem ?? is sufficient to ensure that \( F \) is infinite. Unfortunately we do not know how to bound \( W \).

All we can prove currently is the feeble:

Proposition 8.4. We have \( f_p \neq 1 \) infinitely often.

*Proof* As noted, \( s, t \) and \( d \) can only be perfect powers finitely often.

Next observe that as \( q \) runs through the primes, the smallest prime factor of \( d(qP) \) approaches infinity, since the factors appearing in \( d(qP) \) have appeared in no smaller multiple of \( P \). If from some point onwards all the exponents \( f_p + 1 \) are divisible by some \( n > 1 \) then eventually \( d(qP) \) is always a perfect \( n \)th power, which is impossible. Hence for every \( n \), infinitely many \( f_p \) satisfy
\[
f_p \not\equiv -1 \pmod{n}.
\]

In particular taking \( n = 2 \) we see that infinitely often \( f_p \neq 1 \). \( \square \)

The analogous result for ordinary Wieferich primes was proved by Powell [5, p339]. Since heuristically we believe there are only finitely many primes with \( f_p \geq 2 \) then the Proposition indicates that there should be infinitely many non-Wieferich primes for \( P \) on \( E \). Even if this is true, it still does not prove that \( F \) is infinite because the map \( p \mapsto m_p \) is not injective. However if Conjecture ?? holds, the elliptic Wieferich primes grow so fast (even in comparison to the coordinates on the curve) that most points \( kP \) do not contain any elliptic Wieferich divisors.

Lemma 8.5. If Conjecture ?? holds then \( F \) is infinite.

*Proof* We show that under the hypothesis \( F \) contains infinitely many primes. Consider the multiples \( qP \) of \( P \) with \( 1 \leq q \leq N \) and \( q \) prime. By the Prime Number Theorem there are \( \gg N/\log N \) of these. Next observe that the \( d(qP) \) are pairwise relatively prime: if \( p \mid d(q_1P) \) and \( p \mid d(q_2P) \) then \( m_p \) divides \( q_1 \) and \( q_2 \) which is impossible.

Since \( d < s \) then (extending Lemma 4.3 \( \log(d(NP)) < N^2 \), all the \( d(qP) \) values satisfy \( \log d(\delta < N^{25} \ll N/\log(N) \). That is roughly speaking there are only about \( N^{25} \) elliptic Wieferich primes to be distributed among the approximately \( N/\log N \) pairwise relatively prime values \( d \). So some \( d \)'s must not contain any elliptic Wieferich prime divisor. Similarly for \( t \) and \( s \). \( \square \)

Let \( M \) be the set of integers \( m_p \) for Wieferich primes \( p \). It would be sufficient for our purposes to bound the entries in \( M \).

Lemma 8.6. Suppose \( c < 1 \) is a constant and \( S \) is a set of positive integers not containing 1 such that for all \( x \) sufficiently large \( \# \{ y \in S \mid y \leq x \} < c(x/\log x) \). Then there are infinitely many positive integers not divisible by any element of \( S \).

*Proof* By the Prime Number Theorem there are infinitely many primes which do not occur in \( S \). \( \square \)

If we take \( S = \{ m \mid m \in M \text{, } m \text{ is odd} \} \cup \{ m/2 \mid m \in M \text{, } m \text{ is even} \} \) in the above, we have
Corollary 8.7. If there exists $c < 1$ such that for all sufficiently large $x$ \[ \# \{ p \leq x \mid p \text{ or } 2p \in \mathcal{M} \} < cx / \log x \] then $\mathcal{F}$ is infinite.

\[
\]