

# Power integral points on elliptic curves

Jonathan Reynolds

Mathematics Institute  
Utrecht University

December 2009

Let  $x(P)$  denote the  $x$ -coordinate of a point  $P$  on a Weierstrass equation for an elliptic curve  $E/\mathbb{Q}$  which has coefficients in  $\mathbb{Z}$ . If  $P \in E(\mathbb{Q})$  is non-zero then

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

where  $A_P, B_P \in \mathbb{Z}$  are coprime.

Let  $x(P)$  denote the  $x$ -coordinate of a point  $P$  on a Weierstrass equation for an elliptic curve  $E/\mathbb{Q}$  which has coefficients in  $\mathbb{Z}$ . If  $P \in E(\mathbb{Q})$  is non-zero then

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

where  $A_P, B_P \in \mathbb{Z}$  are coprime.

Definition: If  $B_P$  is a perfect power then call  $P$  *power integral*.

# Why study power integral points?

(1929) Siegel: There are finitely many  $P \in E(\mathbb{Q})$  with  $B_P = 1$ .

# Why study power integral points?

(1929) Siegel: There are finitely many  $P \in E(\mathbb{Q})$  with  $B_P = 1$ .

(1934) Mahler: Let  $S \subset \mathbb{Z}$  be a finite set of primes. There are finitely many  $P \in E(\mathbb{Q})$  with  $B_P$  only divisible by primes from  $S$ .

# Why study power integral points?

The multiples  $mP$  of a non-torsion point  $P \in E(\mathbb{Q})$  produce an *elliptic divisibility sequence* (EDS)  $B_P, B_{2P}, B_{3P}, \dots$

# Why study power integral points?

The multiples  $mP$  of a non-torsion point  $P \in E(\mathbb{Q})$  produce an *elliptic divisibility sequence* (EDS)  $B_P, B_{2P}, B_{3P}, \dots$

Example: When  $E : y^2 + xy = x^3 + x^2 - 7x + 5$ ,  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (2, -3)$ ,  $B_{mP} = 1$  for  $m = 1, 2, 3, 4, 7$  and  $B_{12P} = 2^7$ .

# Why study power integral points?

The multiples  $mP$  of a non-torsion point  $P \in E(\mathbb{Q})$  produce an *elliptic divisibility sequence* (EDS)  $B_P, B_{2P}, B_{3P}, \dots$

Example: When  $E : y^2 + xy = x^3 + x^2 - 7x + 5$ ,  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (2, -3)$ ,  $B_{mP} = 1$  for  $m = 1, 2, 3, 4, 7$  and  $B_{12P} = 2^7$ .

An EDS is a “genus-1 analogue” of the Fibonacci sequence ( $F_m$ ):  
The genus-0 curve  $C : y^2 + xy + y = x^3 - 2x^2$  has  $F_m = B_{m(0,0)}$ .

# Why study power integral points?

The multiples  $mP$  of a non-torsion point  $P \in E(\mathbb{Q})$  produce an *elliptic divisibility sequence* (EDS)  $B_P, B_{2P}, B_{3P}, \dots$

Example: When  $E : y^2 + xy = x^3 + x^2 - 7x + 5$ ,  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (2, -3)$ ,  $B_{mP} = 1$  for  $m = 1, 2, 3, 4, 7$  and  $B_{12P} = 2^7$ .

An EDS is a “genus-1 analogue” of the Fibonacci sequence  $(F_m)$ :  
The genus-0 curve  $C : y^2 + xy + y = x^3 - 2x^2$  has  $F_m = B_{m(0,0)}$ .

(2006) Bugeaud, Mignotte and Siksek: If  $F_m$  is a perfect power then  $m = 1, 2, 6$  or  $12$ .

Theorem(JR): For fixed  $n > 1$ , there are finitely many  $P \in E(\mathbb{Q})$  with  $B_P = Z^n$  for some  $Z \in \mathbb{Z}$ .

Theorem(JR): For fixed  $n > 1$ , there are finitely many  $P \in E(\mathbb{Q})$  with  $B_P = Z^n$  for some  $Z \in \mathbb{Z}$ .

Let  $K$  be a number field and  $S$  a finite set of prime ideals of  $\mathcal{O}_K$ .

Theorem(JR): Let  $x(P)$  denote the  $x$ -coordinate of a  $K$ -rational point  $P$  on a Weierstrass equation for an elliptic curve  $E/K$ . Suppose that for some fixed  $n > 2$ ,  $n \mid \text{ord}_{\mathfrak{p}}(x(P))$  for all  $\mathfrak{p} \notin S$  with  $\text{ord}_{\mathfrak{p}}(x(P)) < 0$ . Then there are finitely many choices for  $P$ .

# Proving the theorem

We can assume that our Weierstrass equation is of the form

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $x^3 + B_2x^2 + B_4x + B_6$ .

# Proving the theorem

We can assume that our Weierstrass equation is of the form

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $x^3 + B_2x^2 + B_4x + B_6$ . Without loss of generality we extend  $K$  and  $S$  by a finite amount so that:

- ▶  $\alpha_1, \alpha_2, \alpha_3 \in K$ ;

# Proving the theorem

We can assume that our Weierstrass equation is of the form

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $x^3 + B_2x^2 + B_4x + B_6$ . Without loss of generality we extend  $K$  and  $S$  by a finite amount so that:

- ▶  $\alpha_1, \alpha_2, \alpha_3 \in K$ ;
- ▶  $B_2, B_4, B_6$  belong to the ring of  $S$ -integers  $\mathcal{O}_{KS}$ ;

# Proving the theorem

We can assume that our Weierstrass equation is of the form

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $x^3 + B_2x^2 + B_4x + B_6$ . Without loss of generality we extend  $K$  and  $S$  by a finite amount so that:

- ▶  $\alpha_1, \alpha_2, \alpha_3 \in K$ ;
- ▶  $B_2, B_4, B_6$  belong to the ring of  $S$ -integers  $\mathcal{O}_{KS}$ ;
- ▶ for all  $i \neq j$ ,  $\alpha_i - \alpha_j$  belong to the group of  $S$ -units  $\mathcal{O}_{KS}^*$ ;

# Proving the theorem

We can assume that our Weierstrass equation is of the form

$$y^2 = x^3 + B_2x^2 + B_4x + B_6.$$

Let  $\alpha_1, \alpha_2, \alpha_3$  be the roots of  $x^3 + B_2x^2 + B_4x + B_6$ . Without loss of generality we extend  $K$  and  $S$  by a finite amount so that:

- ▶  $\alpha_1, \alpha_2, \alpha_3 \in K$ ;
- ▶  $B_2, B_4, B_6$  belong to the ring of  $S$ -integers  $\mathcal{O}_{KS}$ ;
- ▶ for all  $i \neq j$ ,  $\alpha_i - \alpha_j$  belong to the group of  $S$ -units  $\mathcal{O}_{KS}^*$ ;
- ▶  $\mathcal{O}_{KS}$  is a principal ideal domain.

# Proving the theorem

Then by substituting in our point  $P$  and factorizing we have

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

is a square in  $\mathcal{O}_{KS}$ , where  $A_P B_P$  are coprime in  $\mathcal{O}_{KS}$ .

# Proving the theorem

Then by substituting in our point  $P$  and factorizing we have

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

is a square in  $\mathcal{O}_{KS}$ , where  $A_P, B_P$  are coprime in  $\mathcal{O}_{KS}$ . Moreover,

$$A_P - \alpha_i B_P^2$$

are squares in  $\mathcal{O}_{KS}$  up to  $S$ -units.

# Dirichlet's $S$ -unit Theorem

Fix a positive integer  $m$ . The set of cosets  $\mathcal{O}_{KS}^*/(\mathcal{O}_{KS}^*)^m$  is finite.

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

Put

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

# Forcing $A_P - \alpha_j B_P^2$ to be square

Let  $T$  be a fixed finite set of prime ideals of  $\mathcal{O}_L$  containing:

1. the prime ideals which divide the ideals in  $S$ ;
2. the prime ideals which divide 2;
3. the finitely many prime ideals required to make  $\mathcal{O}_{LT}$  a PID.

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

Then  $A_P - \alpha_i B_P^2 = z_i^2$ , where  $z_i \in \mathcal{O}_{LT}$ .

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

Then  $A_P - \alpha_i B_P^2 = z_i^2$ , where  $z_i \in \mathcal{O}_{LT}$ . 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  $z_i \pm z_j$  divide  $B_P^2$  and are coprime in  $\mathcal{O}_{LT}$ .

Fix  $n > 1$  and suppose that  $B_P$  is an  $n$ th power.

# Siegel's identity

Siegel's identity:

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

Siegel's identity:

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

gives

$$\alpha u^{2n} + \beta v^{2n} = 1, \quad u, v \in L$$

where, using Dirichlet's theorem, there are finitely many choices for  $\alpha, \beta \in \mathcal{O}_{LT}^*$ .

# The genus

For any fixed non-zero  $\alpha, \beta \in L$ , the curve given by

$$\alpha u^{2n} + \beta v^{2n} = 1$$

has genus

$$\frac{(2n-1)(2n-2)}{2} > 1.$$

# Getting back to the point

So by Faltings' Theorem, there are finitely many choices for  $u \in L$ , hence finitely many for choices for

$$\alpha u^{2n} = \frac{z_1 \pm z_2}{z_1 - z_3}.$$

## Getting back to the point

Multiplying these two numbers, there are finitely many choices for

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

hence finitely many for

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

# Getting back to the point

Multiplying these two numbers, there are finitely many choices for

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

hence finitely many for

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

But

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

and

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

Let  $K$  be a number field and  $S$  a finite set of prime ideals of  $\mathcal{O}_K$ .

Theorem(JR): Let  $x(P)$  denote the  $x$ -coordinate of a  $K$ -rational point  $P$  on a Weierstrass equation for an elliptic curve  $E/K$ . Suppose that for some fixed  $n > 2$ ,  $n \mid \text{ord}_{\mathfrak{p}}(x(P))$  for all  $\mathfrak{p} \notin S$  with  $\text{ord}_{\mathfrak{p}}(x(P)) < 0$ . Then there are finitely many choices for  $P$ .

Let  $K$  be a number field and  $S$  a finite set of prime ideals of  $\mathcal{O}_K$ .

Theorem(JR): Let  $x(P)$  denote the  $x$ -coordinate of a  $K$ -rational point  $P$  on a Weierstrass equation for an elliptic curve  $E/K$ . Suppose that for some fixed  $n > 2$ ,  $n \mid \text{ord}_{\mathfrak{p}}(x(P))$  for all  $\mathfrak{p} \notin S$  with  $\text{ord}_{\mathfrak{p}}(x(P)) < 0$ . Then there are finitely many choices for  $P$ .

Corollary(JR): Let  $C/K$  be a smooth curve of genus 1,  $P \in C(K)$  and let  $f \in K(C)$  have a pole at  $O \in C$ . Suppose that for some fixed  $n \nmid \text{ord}_O(f)$ ,  $n \mid \text{ord}_{\mathfrak{p}}(f(P))$  for all  $\mathfrak{p} \notin S$  with  $\text{ord}_{\mathfrak{p}}(f(P)) < 0$ . Then there are finitely many choices for  $P$ .

Comments:

- ▶ In general, the proof is ineffective.

## Comments:

- ▶ In general, the proof is ineffective.
- ▶ Can we find non-trivial (positive rank) examples of a curve where all of the power integral points are known?

## Comments:

- ▶ In general, the proof is ineffective.
- ▶ Can we find non-trivial (positive rank) examples of a curve where all of the power integral points are known?
- ▶ For (S-)integral points, effective methods are known.

## Comments:

- ▶ In general, the proof is ineffective.
- ▶ Can we find non-trivial (positive rank) examples of a curve where all of the power integral points are known?
- ▶ For (S-)integral points, effective methods are known.
- ▶ Are there “interesting” examples of power integral points which are not integral?

## Example where all $S$ -integer points are known

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

(1999) Pethő, Zimmer, Gebel and Herrmann proved that

- ▶ there are exactly 58 integer points on  $E$  and
- ▶ exactly 144  $S$ -integer points on  $E$  when  $S = \{3, 5, 7\}$ .

Amongst the largest are

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

- ▶ They build upon work of Baker-Coates and Lang-Zagier.

## Example where all $S$ -integer points are known

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

(1999) Pethő, Zimmer, Gebel and Herrmann proved that

- ▶ there are exactly 58 integer points on  $E$  and
- ▶ exactly 144  $S$ -integer points on  $E$  when  $S = \{3, 5, 7\}$ .

Amongst the largest are

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

- ▶ They build upon work of Baker-Coates and Lang-Zagier.
- ▶  $E(\mathbb{Q}) = \langle (12, 13), (-14, 13), (-1, 26), (38, 221) \rangle$ .
- ▶  $B_{3(12,13)} = 2^5$ ,  $B_{2(-1,26)} = 2^2$  are not  $S$ -integral.

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Let  $p$  be an odd prime.

(2002) Samuel: If  $P$  is a non-torsion integral point on  $E : y^2 = x^3 - p^2x$  and  $p \neq 5, 29$  then

$$x(P) \subset \left\{ \frac{p^2 + 1}{2}, w_p \right\},$$

where  $w_p = u_p^2 - v_p^2$  or  $2u_p v_p$  can only exist when  $p = u_p^2 + v_p^2$ .

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Let  $p$  be an odd prime.

(2002) Samuel: If  $P$  is a non-torsion integral point on  $E : y^2 = x^3 - p^2x$  and  $p \neq 5, 29$  then

$$x(P) \subset \left\{ \frac{p^2 + 1}{2}, w_p \right\},$$

where  $w_p = u_p^2 - v_p^2$  or  $2u_p v_p$  can only exist when  $p = u_p^2 + v_p^2$ .

(2006) Draziotis and Poulakis reduce the problem of finding all integral points on  $E : y^2 = x^3 - (2p)^2x$  to the solution of the unit equation  $u + \sqrt{2}v = 1$  over  $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ .

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Theorem(JR): Let  $\delta \in \{0, 1\}$  and  $E : y^2 = x^3 - (2^\delta p)^2x$ . If  $P \in 2E(\mathbb{Q})$  then  $P$  is not power integral.

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Theorem(JR): Let  $\delta \in \{0, 1\}$  and  $E : y^2 = x^3 - (2^\delta p)^2x$ . If  $P \in 2E(\mathbb{Q})$  then  $P$  is not power integral.

Proof: We have that  $A_P = z_1^2$ ,  $A_P + 2^\delta p B_P^2 = z_2^2$  and  $A_P - 2^\delta p B_P^2 = z_3^2$ , where  $z_1, z_2, z_3$  are all integers.

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Theorem(JR): Let  $\delta \in \{0, 1\}$  and  $E : y^2 = x^3 - (2^\delta p)^2x$ . If  $P \in 2E(\mathbb{Q})$  then  $P$  is not power integral.

Proof: We have that  $A_P = z_1^2$ ,  $A_P + 2^\delta p B_P^2 = z_2^2$  and  $A_P - 2^\delta p B_P^2 = z_3^2$ , where  $z_1, z_2, z_3$  are all integers. If  $B_P$  is an  $n$ th power Siegel's identity yields

$$\alpha U^{2n} + \beta V^{2n} = 2^r W^{2n},$$

where  $U, V, W$  are pairwise coprime integers,  $\alpha, \beta \in \{\pm 1\}$  and  $r \geq 0$ . This was solved by Wiles, Ribet and Darmon and Merel.

# Congruent number curves $y^2 = x^3 - N^2x$ , $N = 2^\delta p$

Theorem(JR): Let  $\delta \in \{0, 1\}$ ,  $E : y^2 = x^3 - (2^\delta p)^2 x$  and  $S = \{2, p\}$ . If  $P \in 2E(\mathbb{Q})$  is power  $S$ -integral then  $\delta = 1$ ,  $p = 3$ ,

$$P = \pm \left( \frac{25}{2^2}, \frac{35}{2^3} \right).$$

# When $P$ on $y^2 = x^3 - p^2x$ does not belong to $2E(\mathbb{Q})$

Suppose that  $\delta = 0$  and

$$A_P = -z_1^2; \quad (1)$$

$$A_P + pB_P^2 = 2pz_2^2; \quad (2)$$

$$A_P - pB_P^2 = -2pz_3^2, \quad (3)$$

where  $z_1, z_2, z_3$  are non-zero integers. Adding these equations gives

$$z_2^2 + p(z_1/p)^2 = z_3^2.$$

# When $P$ on $y^2 = x^3 - p^2x$ does not belong to $2E(\mathbb{Q})$

Suppose that  $\delta = 0$  and

$$A_P = -z_1^2; \quad (1)$$

$$A_P + pB_P^2 = 2pz_2^2; \quad (2)$$

$$A_P - pB_P^2 = -2pz_3^2, \quad (3)$$

where  $z_1, z_2, z_3$  are non-zero integers. Adding these equations gives

$$z_2^2 + p(z_1/p)^2 = z_3^2.$$

This equation can be parametrized. In particular,  $z_1 = pst$  and substituting the parameterizations into (2) or (3) gives

$$s^4 + p^2t^4 = 2B_P^2$$

where  $s$  and  $t$  are odd coprime integers with  $p \nmid s$ .

When  $P$  on  $y^2 = x^3 - p^2x$  does not belong to  $2E(\mathbb{Q})$

So in this case when  $B_P = Y^q$  it is enough to solve

$$s^4 + p^2t^4 = 2Y^{2q},$$

where  $s, t, Y$  are pairwise coprime integers such that  $2p \nmid Y$ .

# Solving $s^4 + p^2 t^4 = 2Y^4$

When  $q = 2$ ,

$$Q = \left( -\frac{s^2}{Y^2}, \frac{spt^2}{Y^3} \right)$$

is a point on  $F : y'^2 = x'^3 - 2x'$ . But  $F(\mathbb{Q}) = \langle (-1, 1), (0, 0) \rangle$  so it follows that  $Q$  is an odd multiple of  $(-1, 1)$ .

# Solving $s^4 + p^2 t^4 = 2Y^4$

When  $q = 2$ ,

$$Q = \left( -\frac{s^2}{Y^2}, \frac{spt^2}{Y^3} \right)$$

is a point on  $F : y'^2 = x'^3 - 2x'$ . But  $F(\mathbb{Q}) = \langle (-1, 1), (0, 0) \rangle$  so it follows that  $Q$  is an odd multiple of  $(-1, 1)$ . Let  $m$  be odd and

$$m(-1, 1) = \left( -\frac{A_m^2}{B_m^2}, \frac{A_m C_m}{B_m^3} \right).$$

Hence when  $C_m$  is prime we get solutions with  $t = 1$ ,  $p = C_m$ ,  $s = A_m$  and  $Y = B_m$ .

# Some large non-integral power integral points

Example: Taking  $m = 7$  we get a non-integral power integral point  $P$  on  $E_p : y^2 = x^3 - p^2x$  with  $p = C_7 = 3503833734241$  and

$$x(P) = -\frac{(1009 \cdot 2351 \cdot p)^2}{2165017^4}.$$

# Some large non-integral power integral points

Example: Taking  $m = 7$  we get a non-integral power integral point  $P$  on  $E_p : y^2 = x^3 - p^2x$  with  $p = C_7 = 3503833734241$  and

$$x(P) = -\frac{(1009 \cdot 2351 \cdot p)^2}{2165017^4}.$$

Conjecture: There are finitely many odd  $m$  for which  $C_m$  is prime. Moreover, if  $C_m$  is prime then  $m = 3, 7$  or  $23$ .

# Solving $s^4 + p^2 t^4 = 2Y^{2q}$ when $q$ is an odd prime

Let  $q$  be an odd prime. Is there a solution to

$$s^4 + p^2 t^4 = 2Y^{2q} \tag{4}$$

where  $s, t, Y$  pairwise coprime integers such that  $2p \nmid Y$ ?

# Solving $s^4 + p^2 t^4 = 2Y^{2q}$ when $q$ is an odd prime

Let  $q$  be an odd prime. Is there a solution to

$$s^4 + p^2 t^4 = 2Y^{2q} \tag{4}$$

where  $s, t, Y$  pairwise coprime integers such that  $2p \nmid Y$ ?

- ▶ A good approach is to factorize over  $\mathbb{Z}[i]$ .

Lemma: When  $q = 3$  there are no solutions to (4).

# Solving $s^4 + p^2 t^4 = 2Y^{2q}$ when $q$ is an odd prime

Let  $q$  be an odd prime. Is there a solution to

$$s^4 + p^2 t^4 = 2Y^{2q} \quad (4)$$

where  $s, t, Y$  pairwise coprime integers such that  $2p \nmid Y$ ?

- ▶ A good approach is to factorize over  $\mathbb{Z}[i]$ .

Lemma: When  $q = 3$  there are no solutions to (4).

- ▶ When  $t = 1$  we are looking for solutions to the much studied equation  $s'^2 + p^2 = 2Y'^q$  with  $s', Y'$  squares.

Lemma (using the work of Siksek and Tengely): If (4) has a solution with  $t = 1$  and  $q \equiv 3$  or  $5$  modulo  $8$  then  $q \leq 443$ .

When  $P$  on  $y^2 = x^3 - (2p)^2x$  does not belong to  $2E(\mathbb{Q})$

Another case:

$$\begin{aligned}A_P &= -z_1^2; \\A_P + pB_P^2 &= 2z_2^2; \\A_P - pB_P^2 &= -2z_3^2.\end{aligned}$$

For  $B_P = Y^q$  this reduces to  $z_1 = 2st$  and

$$s^4 + t^4 = pY^{2q}, \tag{5}$$

where  $s$  and  $t$  are coprime integers of opposite parity.

# When $P$ on $y^2 = x^3 - (2p)^2x$ does not belong to $2E(\mathbb{Q})$

Another case:

$$\begin{aligned}A_P &= -z_1^2; \\A_P + pB_P^2 &= 2z_2^2; \\A_P - pB_P^2 &= -2z_3^2.\end{aligned}$$

For  $B_P = Y^q$  this reduces to  $z_1 = 2st$  and

$$s^4 + t^4 = pY^{2q}, \tag{5}$$

where  $s$  and  $t$  are coprime integers of opposite parity.

Does (5) have a solution with  $Y \neq 1$ ?

(1999) Flynn and Wetherell: (5) has no solution with  $Y \neq 1$  when  $p = 17$  and  $q = 2$ . (They reduce to a genus 2 hyperelliptic curve.)

# The Mordell curve $E : y^2 = x^3 - 2$

Long before the work of Siegel, Fermat showed that the only integral solutions to

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

are  $(3, \pm 5)$ .

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

▶  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (3, 5)$ .

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

- ▶  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (3, 5)$ .
- ▶ So it is enough to consider  $(Z_m)$ , where  $Z_m = B_m P$ .

# The curve $E : y^2 = x^3 - 2$

- ▶  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (3, 5)$ .
- ▶ So it is enough to consider  $(Z_m)$ , where  $Z_m = B_m P$ .
- ▶  $(Z_m)$  is a divisibility sequence:  $m_1 | m_2 \implies Z_{m_1} | Z_{m_2}$ .

# The curve $E : y^2 = x^3 - 2$

- ▶  $E(\mathbb{Q}) = \langle P \rangle$  where  $P = (3, 5)$ .
- ▶ So it is enough to consider  $(Z_m)$ , where  $Z_m = B_{mP}$ .
- ▶  $(Z_m)$  is a divisibility sequence:  $m_1 | m_2 \implies Z_{m_1} | Z_{m_2}$ .
- ▶  $Z_{2^k}$  is even since  $Z_2 = B_{2P}$  is even.

Conjecture: The only power integral points on

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

are  $(3, \pm 5)$ .

Equivalently: If  $Z_m$  is a perfect power then  $m = 1$ .

$m$	$Z_m$
2	$2 \cdot 5$
3	$3^2 \cdot 19$
5	$29 \cdot 211 \cdot 2069$
7	$7^2 \cdot 769 \cdot 1049 \cdot 1487809$

# Finding the power integral points on $y^2 = x^3 - 2$

Suppose that  $x = X/Z_m^{2n}$  and  $y = Y/Z_m^{3n}$  where  $(XY, Z_m) = 1$ .

# Finding the power integral points on $y^2 = x^3 - 2$

Suppose that  $x = X/Z_m^{2n}$  and  $y = Y/Z_m^{3n}$  where  $(XY, Z_m) = 1$ .  
Substituting and factorizing over  $\mathbb{Z}[\sqrt{-2}]$  gives:

$$X^3 = Y^2 + 2Z_m^{6n} = (Y + \sqrt{-2}Z_m^{3n})(Y - \sqrt{-2}Z_m^{3n}).$$

# Finding the power integral points on $y^2 = x^3 - 2$

Suppose that  $x = X/Z_m^{2n}$  and  $y = Y/Z_m^{3n}$  where  $(XY, Z_m) = 1$ .  
Substituting and factorizing over  $\mathbb{Z}[\sqrt{-2}]$  gives:

$$X^3 = Y^2 + 2Z_m^{6n} = (Y + \sqrt{-2}Z_m^{3n})(Y - \sqrt{-2}Z_m^{3n}).$$

The gcd of the two factors in  $\mathbb{Z}[\sqrt{-2}]$  divides  $2\sqrt{-2} = -(\sqrt{-2})^3$ .

# Finding the power integral points on $y^2 = x^3 - 2$

Suppose that  $x = X/Z_m^{2n}$  and  $y = Y/Z_m^{3n}$  where  $(XY, Z_m) = 1$ .  
Substituting and factorizing over  $\mathbb{Z}[\sqrt{-2}]$  gives:

$$X^3 = Y^2 + 2Z_m^{6n} = (Y + \sqrt{-2}Z_m^{3n})(Y - \sqrt{-2}Z_m^{3n}).$$

The gcd of the two factors in  $\mathbb{Z}[\sqrt{-2}]$  divides  $2\sqrt{-2} = -(\sqrt{-2})^3$ .  
Hence

$$Y + \sqrt{-2}Z_m^{3n} = \zeta^3$$

for some  $\zeta \in \mathbb{Z}[\sqrt{-2}]$ .

# Finding the power integral points on $y^2 = x^3 - 2$

Substituting  $\zeta = a + b\sqrt{-2}$ , where  $a, b \in \mathbb{Z}$ , gives:

$$(2\sqrt{-2})Z_m^{3n} = \zeta^3 - \bar{\zeta}^3 = (\zeta - \bar{\zeta})(\zeta^2 + \zeta\bar{\zeta} + \bar{\zeta}^2).$$

Hence:

$$Z_m^{3n} = b(3a^2 - 2b^2) \tag{6}$$

$$Y = a(a^2 - 6b^2) \tag{7}$$

$$X = a^2 + 2b^2. \tag{8}$$

# Showing that $Z_{2k}$ is not a perfect power

Some properties of  $(Z_m)$ :

- ▶  $Z_{2k}$  is even.
- ▶  $3|Z_3$  and  $3|Z_m$  if and only if  $3|m$ .
- ▶ If  $3|k$  then there exists  $k'$  not divisible by 3 so that  $\text{ord}_p B_{2k'} = \text{ord}_p B_{2k}$  for all primes  $p|B_{2k'}$ .

# Showing that $Z_{2k}$ is not a perfect power

Some properties of  $(Z_m)$ :

- ▶  $Z_{2k}$  is even.
- ▶  $3|Z_3$  and  $3|Z_m$  if and only if  $3|m$ .
- ▶ If  $3|k$  then there exists  $k'$  not divisible by 3 so that  $\text{ord}_p B_{2k'} = \text{ord}_p B_{2k}$  for all primes  $p|B_{2k'}$ .

So if  $m = 2k$  we can assume that  $3 \nmid b$ ,  $b = U^{3n}$  is even and

$$3a^2 - 2(U^{3n})^2 = V^{3n}.$$

# Showing that $Z_{2k}$ is not a perfect power

Thus:

$$V^{3n} + 2U^{6n} = 3a^2$$

where  $UV \neq \pm 1$ ,  $U$  is even and  $V, 2U, 3a$  are pairwise coprime.

# Showing that $Z_{2k}$ is not a perfect power

Thus:

$$V^{3n} + 2U^{6n} = 3a^2$$

where  $UV \neq \pm 1$ ,  $U$  is even and  $V, 2U, 3a$  are pairwise coprime.

Bennett and Skinner (2004): If  $n > 5$  is prime then there exists a cuspidal newform of weight 2 and level 18.

Theorem: There are no such newforms.

# Finding the power integral points on $y^2 = x^3 - 2$

Theorem: For any  $k > 0$ ,  $Z_{2k}$  is not an integer raised to the power  $n$  for any prime  $n > 5$ .

# Finding the power integral points on $y^2 = x^3 - 2$

Theorem: For any  $k > 0$ ,  $Z_{2k}$  is not an integer raised to the power  $n$  for any prime  $n > 5$ .

Conjecture: For any  $k > 0$ ,  $Z_{2k}$  is not a perfect power.

# 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:

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

where  $I$  denotes the set of prime ideals  $\wp$  such that  $|\alpha|_{\wp}, |\beta|_{\wp}, |\gamma|_{\wp}$  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.

# Prime values of $B_P$

If  $B_P = \pi$  is a prime in  $\mathcal{O}_{KS}$  then Siegel's identity gives

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

where  $\rho_1, \rho_2, \rho_3 \in \mathcal{O}_{LT}$  divide  $\pi$  and are pairwise coprime.

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