

# Heights and highly effective elliptic Zsigmondy theorems

(Graham Everest, Gerry McLaren)

SECANTS RHUL 5/3/05

Let  $A = (A_n)$  be an integer sequence. A *primitive divisor* of  $A_n$  is a prime that divides  $A_n$  but does not divide any  $A_m$  with  $m < n$ . In the list of  $A_n$ s and their factorization into primes, it is a new prime.

Let

$$Z(A) = \max\{n \mid A_n \text{ has no primitive divisor}\}$$

if this set is finite, and  $Z(A) = \infty$  if not. The number  $Z(A)$  will be called the *Zsigmondy bound* for  $A$ .

Zsigmondy showed in 1892 that

$$Z((2^n - 1)) = 6$$

and more generally

$$Z((a^n - b^n)) \leq 6$$

for coprime  $a, b$ .

Bilu, Hanrot and Voutier showed in 2001 that for a non-trivial Lucas or Lehmer sequence  $L$ ,

$$Z(L) \leq 30.$$

These results are not just effective: they are *highly* effective in that the bounds are so small that for any given example the terms below the bound can be factorized quickly.

The arithmetic of linear recurrence sequences has a *bilinear* or *elliptic* analogue\*.

Let  $E$  denote an elliptic curve defined over  $\mathbb{Q}$ , in generalized Weierstrass form, and  $P = (x(P), y(P))$  a non-torsion rational point on  $E$ . For  $n \geq 1$ , write

$$x(nP) = \frac{A_n}{B_n},$$

in lowest terms, with  $A_n \in \mathbb{Z}$  and  $B_n \in \mathbb{N}$ . The sequence  $B_{E,P} = (B_n)$  is a divisibility sequence:

$$m \mid n \implies B_m \mid B_n.$$

The sequence  $B_{E,P}$  is an example of an *elliptic divisibility sequence*.

Silverman showed an elliptic analogue of Zsigmondy:

$$Z(B_{E,P}) < \infty.$$

\*Shameless plug: see Chapter 10 of '*Recurrence Sequences*', Amer. Math Soc. Surveys and Monographs (2003) by Everest, van der Poorten, Shparlinski and Ward.

Good bounds for the canonical height and for the gap between the Weil height and the canonical height allow Silverman's result to be rendered effective, and with a bit of luck highly effective.

To describe a sample result, we need to follow the odd and even terms separately:

$$Z_e(A) = \max\{2n \mid A_{2n} \text{ has no p.d.}\}$$

if this set is finite, and  $Z_e(A) = \infty$  if not. Similarly,

$$Z_o(A) = \max\{2n - 1 \mid A_{2n-1} \text{ has no p.d.}\}$$

if this set is finite, and  $Z_o(A) = \infty$  if not. These are the *even* and *odd* Zsigmondy bounds respectively.

**Theorem.** Consider the curve

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

with  $T > 0$  square-free. Suppose  $E$  has a non-torsion rational point  $P$  (so  $T \geq 5$ ). Then

$$Z_e(B_{E,P}) \leq 18.$$

If  $x(P) < 0$ , then

$$Z_o(B_{E,P}) \leq 3.$$

If  $x(P)$  is a square, then

$$Z_o(B_{E,P}) \leq 21.$$

These are highly effective – even with the rapid growth in  $B_n$ , for any given sequence the first 21 terms can be factorized (in fact less than factorization is needed).

## Arithmetic

Silverman: if  $p \mid B_n$  then

$$\text{ord}_p(B_{nk}) = \text{ord}_p(B_n) + 2\text{ord}_p(k). \quad (1)$$

Corollary:  $B_{\text{gcd}(m,n)}$  divides  $\text{gcd}(B_n, B_m)$ .

If  $p$  divides  $B_n$  and  $B_m$ , then on the curve reduced modulo  $p$ ,  $mP$  and  $nP$  are the identity, so  $dP$  is also, hence  $p \mid B_d$ .

Conclusion:

$$B_{\text{gcd}(m,n)} = \text{gcd}(B_n, B_m). \quad (2)$$

Hence: If  $B_n$  does not have a primitive divisor then

$$B_n \mid \prod_{p \mid n} p^2 B_{n/p}. \quad (3)$$

## Heights

Write  $h(\frac{a}{b}) = \log \max\{|a|, |b|\}$  for the Weil height of a rational number, so

$$h(x(nP)) = \log \max\{|A_n|, B_n\}.$$

Let  $\hat{h}(P)$  denote the global canonical height of  $P$ . Then by work of Bremner, Silverman and Tzanakis,

$$\begin{aligned} n^2 \hat{h}(P) - \frac{1}{2} \log(T^2 + 1) - 0.116 \\ \leq h(x(nP)) \\ \leq n^2 \hat{h}(P) + \log T + 0.347, \end{aligned} \quad (4)$$

and

$$\hat{h}(P) \geq \frac{1}{4} \log T. \quad (5)$$

## Rough idea

Assume  $B_n$  does not have a primitive divisor.

Taking logarithms in (3) gives

$$\log B_n \leq 2 \sum_{p|n} \log p + \sum_{p|n} \log B_{n/p}. \quad (6)$$

Idea: if  $B_n$  were equal to  $(e^C)^{n^2}$ , then (6) bounds  $n$ :

$$n^2 \leq \frac{2}{C} \sum_{p|n} \log p + \sum_{p|n} \left(\frac{n}{p}\right)^2$$

so  $n$  is uniformly and effectively bounded as long as  $C$  is not too small...

The estimate (4) gives some relation between  $B_n$  (or at least  $\max\{|A_n|, B_n\}$ ) and  $\exp(n^2 \hat{h}(P))$ , while (5) says  $\hat{h}(P)$  is not too small.

## Elliptic transcendence

Deep general results from elliptic transcendence theory give

$$\log B_n \geq n^2 \hat{h}(P) - O(\log n \log \log n). \quad (7)$$

Inserting this into (6) shows that  $Z(B_{E,P})$  is finite because the right-hand side is bounded by  $cn^2$  with  $c < 1$ . However, the constants involved are big and vary in the wrong way with the parameter  $T$  to get uniform results.

Our approach uses a much worse bound in the lead term, something like  $\frac{1}{2}n^2 \hat{h}(P)$ , in return for a more controlled error term, that is in particular linear in  $\log T$ .

## Bounds

The details are messy...

By (4), if  $p|n$  then

$$\begin{aligned}\log B_{n/p} &\leq h(x(\frac{n}{p}P)) \\ &\leq \hat{h}(\frac{n}{p}P) + \log T + 0.347 \\ &= \frac{n^2}{p^2} \hat{h}(P) + \log T + 0.347. \quad (8)\end{aligned}$$

Define

$$\omega(n) = \# \text{ primes dividing } n,$$

$$\rho(n) = \sum_{p|n} \frac{1}{p^2},$$

and

$$\eta(n) = 2 \sum_{p|n} \log p.$$

Notice  $\rho(n) \leq 0.453$  for  $n \geq 1$  and (this really matters)  $\rho(n) \leq 0.203$  for odd  $n \geq 1$ .

This gives

$$\begin{aligned} \log B_n &\leq \eta(n) + n^2 \rho(n) \hat{h}(P) \\ &\quad + \omega(n) (\log T + 0.347) \end{aligned} \quad (9)$$

Assume  $n = 2m$  is even. Then

$$\frac{A_n}{B_n} = \frac{(A_m^2 + T^2 B_m^2)^2}{4A_m B_m (A_m^2 - T^2 B_m^2)}. \quad (10)$$

Careful counting implies that

$$\text{gcd} \leq 4T^4,$$

which bounds how much smaller  $B_n$  is than the denominator of (10).

A simple calculation shows that

$$\begin{aligned} &2 \log \max\{|A_m|, B_m\} - \log T - 0.0954 \\ &\leq \log |A_m| + \log B_m + \log |A_m^2 - T^2 B_m^2|. \end{aligned}$$

These (and some similar arguments) combine to give

$$n^2 \left( \frac{1}{2} - \rho(n) \right) \\ \leq 4 \left( 0.621\eta(n) + 1.216\omega(n) + 7.3714 \right).$$

This implies that  $n \leq 18$ , so  $Z_e(B_{E,P}) \leq 18$ .

The odd case is simpler, and dramatically better bounds are found mainly because of the much larger gap between  $\rho(n)$  and  $\frac{1}{2}$  when  $n$  is odd.

## Examples

1. For  $P = (-4, 6)$  on  $E : y^2 = x^3 - 25x$ , checking the remaining cases gives

$$Z(B_{E,P}) = 1.$$

2. For other elliptic surfaces without a rational 2-torsion point life is more complicated. For  $P = (0, 0)$  on  $E : y^2 + y = x^3 - x$ , these methods show that  $Z_o(B_{E,P}) = 3$ . Here  $nP$  is integral for  $n = 1, 2, 3, 4, 6$  so we could not expect the bound to be any smaller. We are unable to prove that the even Zsigmondy bound is 6.

The *odd* terms comprise the Somos-4 sequence

$$1, 1, 1, 1, 2, 3, 7, 23, \dots$$

This sequence satisfies the bilinear recurrence

$$u_n u_{n-4} = u_{n-1} u_{n-3} + u_{n-2}^2.$$

The bound for  $Z_o$  shows that every term beyond the fourth term has a primitive divisor.