

# Divisibility Sequences for Elliptic Curves with Complex Multiplication

Master's thesis, Universiteit Utrecht  
supervisor: Gunther Cornelissen

Marco Streng

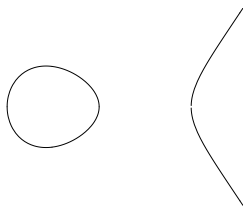
Universiteit Leiden

Irvine Number Theory Seminar, January 2008

# Elliptic Curves

An *elliptic curve*  $E$  is a non-singular projective curve  $E$  given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$



- ▶ It has a natural algebraic group structure with neutral element  $O = (0 : 1 : 0)$  at infinity.

## Elliptic Divisibility Sequences

Let  $E$  be an elliptic curve, given by an equation with coefficients in  $\mathbb{Z}$ . Let  $P \in E(\mathbb{Q})$  be a point of infinite order.

- ▶ Every point  $nP \in E(\mathbb{Q})$  can be written uniquely in the form

$$nP = \left( \frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right)$$

with integers  $A_n, B_n, C_n$  such that  $A_n$  and  $C_n$  are both coprime to  $B_n$ .

- ▶  $B_n$  is the largest integer such that  $nP$  reduces to  $(0 : 1 : 0)$  modulo  $B_n$ .
- ▶ We get a sequence  $B_1, B_2, B_3, \dots$ , which we call an *elliptic divisibility sequence*.

## Recurrent sequences

The terminology comes from a related type of sequence, studied by **Morgan Ward** in the 1940's:

- ▶ An **elliptic divisibility sequence** is a sequence of integers  $h_1, h_2, \dots$ , satisfying

$$h_{m+n}h_{m-n}h_1^2 = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2,$$

and some initial conditions on  $h_1, h_2, h_3, h_4$ .

- ▶ For any such sequence, there exist an elliptic curve  $E$  and a rational point  $P$  such that for the division polynomials  $\psi_n = \psi_{E,n}$ , we have  $h_n = \psi_n(P)$ . (**Ward**)
- ▶ We have  $B_n = \pm h_n$  up to primes  $p$  such that  $P$  reduces to a singular point modulo  $p$ . (**Ayad, 1992**)
- ▶ If not all initial conditions are satisfied, we get for example  $1, 2, 3, 4, \dots$  or a Lucas sequence.

# Applications

- ▶ Source of large primes ...  
(Chudnovsky and Chudnovsky, 1986)
- ▶ ... or not.  
(Everest, King, Miller, Reynolds, Stephens & Stevens)
- ▶ Connection to Hilbert's Tenth Problem:  
*Is there an algorithm that decides whether a polynomial equation  $P(X_1, \dots, X_n) = 0$  has a solution  $(X_1, \dots, X_n) \in \mathbb{Z}^n$ ?*
  - ▶ **No.** (Davis, Putnam, Robinson, Matiyasevich 1970)
  - ▶ But what about other rings?  
With  $\mathbb{Z}$  replaced by  $\mathbb{Q}$ , still an open problem.
- ▶ Learn about elliptic curves.

Example:  $E : y^2 = x^3 - 2x$ ,  $P = (2, 2)$

growth:

$B_1$	- 1
$B_2$	- 2
$B_3$	- 1
$B_4$	- 84
$B_5$	- 1343
$B_6$	- 6214
$B_7$	- 2372159
$B_8$	- 151245528
$B_9$	- 9788425919
$B_{10}$	- 11265465210550
$B_{11}$	- 5705771236038721
$B_{12}$	- 2316186053639990532
$B_{13}$	- 17999572487701067948161
$B_{14}$	- 35989730244828830296744846
$B_{15}$	- 173658539553825212149513251457
$B_{16}$	- 4838927849738289074690192087973888
$B_{17}$	- 75727152767742719949099952561136336896
$B_{18}$	- 2112210601043831815941470427608507178024960
$B_{19}$	- 437825148963391521638828389137155451835696283648
$B_{20}$	- 2648511780315371950034986532978362522386424041570304
$B_{21}$	- 84411998926603535512544634573788037136446095298648761958400
$B_{22}$	- 666676747561498894094226045560233548174764204251787655655413760
$B_{23}$	- 3063568009309298931959856378863776177340999596868565798461674272849920
$B_{24}$	- 5583760264100680237381129136333973574659847646394871628459380791514448789504
$B_{25}$	- 34168080993535113552180464917361262048721737746681574602280069300150039406884945920
$B_{26}$	- 581281081447099968999027703165590575729534780876243950008806563961635496889500622468939776
$B_{27}$	- 1228647482683315378634052011737122211307277977517770914268249674009473286529843656589397261811712
$B_{28}$	- 29468175935974646521240728047319242694637960620437029709703184798221397605426305573782447476979888291840
$B_{29}$	- 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112
$B_{30}$	- 45112182062693748035626811754858027951758898756454294004133102442005976934377844886077402074532318126274500915888128

▶  $\log B_m \sim \widehat{h}(P) m^2.$

(Weil, Siegel)

▶  $\log B_m \leq \widehat{h}(P) m^2 + C.$

▶  $\log B_m = \widehat{h}(P) m^2 + O((\log m)(\log \log m)^3).$

(Linear forms in elliptic logarithms,  
David, 1995)

Example:  $E : y^2 = x^3 - 2x, P = (2, 2)$

$$B_1 = 1$$

$$B_2 = 2$$

$$B_3 = 1$$

$$B_4 = 2^2 \cdot 3 \cdot 7$$

$$B_5 = 17 \cdot 79$$

$$B_6 = 2 \cdot 13 \cdot 239$$

$$B_7 = 1009 \cdot 2351$$

$$B_8 = 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257$$

$$B_9 = 9788425919$$

$$B_{10} = 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161$$

- ▶ divisibility:  
if  $m|n$ , then  $B_m|B_n$ .
- ▶ strong divisibility:  
 $\gcd(B_m, B_n) = B_{\gcd(m,n)}$ .
- ▶ if  $\text{ord}_p(B_m) \gg 0$ , then  
 $\text{ord}_p(B_{mn}) =$   
 $\text{ord}_p(B_m) + \text{ord}_p(n)$ .  
(formal groups / reduction)
- ▶ all but finitely many terms  
have a new prime factor  
(Silverman, 1988)

## Proof of Silverman (1)

- ▶ A *primitive divisor* of the term  $B_n$  is a prime  $q|B_n$  such that for every  $m$ , if  $q|B_m$ , then  $n|m$ .
- ▶ The *primitive part*  $D_n$  of  $B_n$  is the largest divisor of  $B_n$  such that all primes dividing  $D_n$  are primitive divisors of  $B_n$ .

### Lemma

There is a constant  $C \neq 0$  in  $\mathbb{Z}$  such that

$$\frac{B_n}{D_n} \mid C \prod_{p|n} p^{B_n/p}.$$

## Proof of Silverman (2)

$$\frac{B_n}{D_n} \leq C \prod_{p|n} p B_{n/p},$$

so

$$\begin{aligned} \log D_n &\geq \log B_n - \sum_{p|n} (\log B_{n/p} + \log p) - \log C \\ &\geq \hat{h}(P) n^2 - \sum_{p|n} \hat{h}(P) (n/p)^2 - o(1) n^2 \\ &= \hat{h}(P) n^2 \left( 1 - \sum_{p|n} p^{-2} - o(1) \right) \\ &\geq \hat{h}(P) n^2 (0.547 - o(1)) \rightarrow \infty. \quad \square \end{aligned}$$

## Elliptic divisibility sequences with CM

Look at  $\alpha P$  for all  $\alpha \in \text{End}(E)$  to get  $B_\alpha$ .

- ▶ The ring of  $\mathbb{Q}$ -endomorphisms is just  $\mathbb{Z}$ , so look at points and curves over number fields.
- ▶ Unique factorization in number fields only for ideals, so  $B_\alpha$  is an ideal.
- ▶ Do all properties generalize?
  - ▶ Growth. **yes, with norms  $N(\alpha)$  instead of squares  $n^2$**
  - ▶ Divisibility: if  $\alpha|\beta$ , then  $B_\alpha|B_\beta$ .  
**yes, but some work or use Néron models**
  - ▶ Strong divisibility:  $\gcd(B_\alpha, B_\beta) = B_{\gcd(\alpha, \beta)}$ . **yes**
  - ▶ If  $v(B_\alpha) \gg 0$ , then  $v(B_{\alpha\beta}) = v(B_\alpha) + v(B_\beta)$ . **yes**
  - ▶ Primitive divisors. **?**

## Silverman's proof?

Assume that  $\mathcal{O}$  is a principal ring.

- ▶ The original proof gives at best

$$\log D_\alpha \geq \widehat{h}(P) N(\alpha) \left( 1 - \sum_{\pi|\alpha} N(\pi)^{-1} - o(1) \right).$$

There are now too many small primes, because half of the primes split.

- ▶ Solution: Inclusion-exclusion.

## The proof (1)

- ▶ Inclusion-exclusion works best with unique factorization.
- ▶ The ring  $\mathcal{O} = \text{End}(E)$  does not always have unique factorization, but the set of ideals of  $\mathcal{O}$  coprime to the conductor of  $\mathcal{O}$  does.
- ▶ Define  $B_{\alpha}$  for every ideal  $\alpha$  by

$$B_{\alpha} = \gcd_{\alpha \in \mathfrak{a}} B_{\alpha}.$$

In other words,  $B_{\alpha}$  is the largest ideal such that  $\alpha P$  reduces to  $(0 : 1 : 0)$  modulo  $B_{\alpha}$  for all  $\alpha \in \mathfrak{a}$ .

- ▶ Then generalize the properties.

## The proof (2)

- ▶ For the growth, we need points.
- ▶ There is a natural way to associate to every  $\alpha$  a homomorphism of elliptic curves  $\alpha : E \rightarrow E'$ .
- ▶ Its image  $E'$  depends only on the ideal class of  $\alpha$ , so we get points  $\alpha P$  on a finite set of elliptic curves.
- ▶ Their denominators are almost equal to the  $B_\alpha^2$ 's and we can apply David's theorem to each of the (finitely many) curves.

Inclusion-exclusion and Mertens' theorem then prove the existence of primitive divisors.

## Results (1)

### Theorem

*For all ideals  $\mathfrak{a} \subset \mathcal{O}$  coprime to the conductor of  $\mathcal{O}$ , except finitely many, the term  $B_{\mathfrak{a}}$  has a primitive divisor.*

## Results (2)

For  $\mathbb{Z}$ -indexed sequences, the methods give the following:

### Theorem

$$\log D_n = \widehat{h}(P) n^2 \prod_{p|n} (1 - p^{-2}) + O(n^\epsilon),$$

where  $\prod_{p|n} (1 - p^{-2})$  is between  $\zeta(2)^{-1} > 0.6079$  and 1.

(Compare to  $\log D_n \geq \widehat{h}(P) n^2 (0.547 - o(1))$ .)

## Results (3)

Suppose that  $E$  and  $P$  are defined over a number field  $L$  and that not all endomorphisms of  $E$  are defined over  $L$ . Then they are defined over a quadratic extension  $M/L$ . Consider the  $\mathbb{Z}$ -indexed sequence of  $L$ -ideals  $B_1, B_2, B_3, \dots$

### Corollary

*Define for all  $n \in \mathbb{Z}$ , the numbers*

$$r_n = \#\{p|n \text{ prime} : p \text{ ramifies in } \text{End}(E)\},$$

$$s_n = \#\{p|n \text{ prime} : p \text{ splits in } \text{End}(E)\}.$$

*Then for all but finitely many  $n$ , the term  $B_n$  has at least  $r_n + s_n + 1$  primitive divisors, of which at least  $s_n$  split in  $M/L$ .*

## Open problems

- ▶ Prove the conjectures of Gunther Cornelissen and Karim Zahidi.
- ▶ Give a good definition of divisibility sequence for an abelian variety ...
- ▶ ... indexed by (a subring of) the endomorphism ring.

preprint:

<http://www.math.leidenuniv.nl/~streng>  
(to be published by Algebra and Number Theory)