

# Divisibility Sequences for Elliptic Curves with Complex Multiplication

Master's thesis, Universiteit Utrecht

Marco Streng

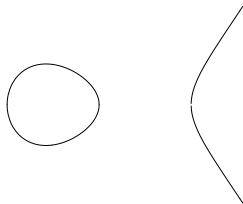
Universiteit Leiden

Diamant/EIDMA Conference, May 2007

# Elliptic Curves

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

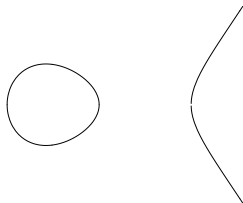
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$



# Elliptic Curves

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

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

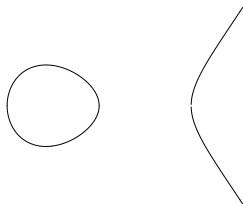


- ▶ It has a natural group law, given by rational functions.

# Elliptic Curves

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

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



- ▶ It has a natural group law, given by rational functions.
- ▶ So we can look at multiples of a point:

$$nP = \underbrace{P + \dots + P}_{n \times}$$

# Divisibility Sequences for Elliptic Curves

Let  $E$  be an elliptic curve, given by an equation with coefficients in  $\mathbb{Z}$ .

## Divisibility Sequences for Elliptic Curves

Let  $E$  be an elliptic curve, given by an equation with coefficients in  $\mathbb{Z}$ .

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

$$Q = \left( \frac{A}{B^2}, \frac{C}{B^3} \right)$$

with integers  $A, B, C$  such that  $A$  and  $C$  are both coprime to  $B$ .

# Divisibility Sequences for Elliptic Curves

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  $Q \in E(\mathbb{Q})$  can be written uniquely in the form

$$Q = \left( \frac{A}{B^2}, \frac{C}{B^3} \right)$$

with integers  $A, B, C$  such that  $A$  and  $C$  are both coprime to  $B$ .

# Divisibility Sequences for Elliptic Curves

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  $B_n$ .

# Divisibility Sequences for Elliptic Curves

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  $B_n$ .

- ▶ We get a sequence  $B_1, B_2, B_3, \dots$ , which we call an *elliptic divisibility sequence*.

# Applications

# Applications

- ▶ Source of large primes ...  
(Chudnovsky and Chudnovsky, 1986)

# Applications

- ▶ Source of large primes ...  
(Chudnovsky and Chudnovsky, 1986)
- ▶ ... or not.  
(Everest, King, Miller, Reynolds, Stephens & Stevens)

# 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  $(X_1, \dots, X_n) \in \mathbb{Z}^n$ ?*

# 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)

# 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?  
(recall: talk of Gunther Cornelissen in Vught)

# 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?  
(recall: talk of Gunther Cornelissen in Vught)
- ▶ Learn about elliptic curves.

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

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

$B_1$  - 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  
 $B_{20}$  - 26485117803153719500349865329783625522386424041570304  
 $B_{21}$  - 84411998926603535512544634573788037136446095298648761958400  
 $B_{22}$  - 6666767475614988940942260455602335481747642042517876555655413760  
 $B_{23}$  - 3063568009309298931959856378863776177340999596868565798461674272849920  
 $B_{24}$  - 5583760264100680273381129136333973574659847646394871628459380791514448789504  
 $B_{25}$  - 34168080993353113552180464917361262048721737746681574602280069300150039406884945920  
 $B_{26}$  - 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776  
 $B_{27}$  - 122864748268331537863405201173712221130727797517770914268249674009473286529843656589397261811712  
 $B_{28}$  - 29468175935974646521240728047319242694637960620437029709703184798221397605426305573782447476979888291840  
 $B_{29}$  - 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112  
 $B_{30}$  - 4511218206629374803566268117548580279517588967564542940040133102442005976934377844886077402074532318126274500915888128

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

growth:

►  $\log B_m \sim \hat{h}(P) m^2$ .  
(Siegel)

$B_1 = 1$   
 $B_2 = 2$   
 $B_3 = 1$   
 $B_4 = 84$   
 $B_5 = 1343$   
 $B_6 = 6214$   
 $B_7 = 2372159$   
 $B_8 = 151245528$   
 $B_9 = 9788425919$   
 $B_{10} = 11265465210550$   
 $B_{11} = 5705771236038721$   
 $B_{12} = 2316186053639990532$   
 $B_{13} = 17999572487701067948161$   
 $B_{14} = 35989730244828830296744846$   
 $B_{15} = 173658539553825212149513251457$   
 $B_{16} = 4838927849738289074690192087973888$   
 $B_{17} = 75727152767742719949099952561136336896$   
 $B_{18} = 2112210601043831815941470427608507178024960$   
 $B_{19} = 437825148963391521638828389137155451835696283648$   
 $B_{20} = 26485117803153719500349865329783625522386424041570304$   
 $B_{21} = 84411998926603535512544634573788037136446095298648761958400$   
 $B_{22} = 666676747561496894094226045560233548174764204251787655655413760$   
 $B_{23} = 3063568009309298931959856378863776177340999596868565798461674272849920$   
 $B_{24} = 5583760264100680237381129136333973574659847646394871628459380791514448789504$   
 $B_{25} = 34168080993535113552180464917361262048721737746681574602280069300150039406884945920$   
 $B_{26} = 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776$   
 $B_{27} = 1228647482683315378634052011737122211307277977517770914268249674009473286529843656589397261811712$   
 $B_{28} = 29468175935974646521240728047319242694637960620437029709703184798221397605426305573782447476979888291840$   
 $B_{29} = 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112$   
 $B_{30} = 4511218206629374803566268117548580279517588967564542940040133102442005976934377844886077402074532318126274500915888128$

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

growth:

$B_1 = 1$

$B_2 = 2$

$B_3 = 1$

$B_4 = 84$

$B_5 = 1343$

$B_6 = 6214$

$B_7 = 2372159$

$B_8 = 151245528$

$B_9 = 9788425919$

$B_{10} = 11265465210550$

$B_{11} = 5705771236038721$

$B_{12} = 2316186053639990532$

$B_{13} = 17999572487701067948161$

$B_{14} = 35989730244828830296744846$

$B_{15} = 173658539553825212149513251457$

$B_{16} = 4838927849738289074690192087973888$

$B_{17} = 75727152767742719949099952561136336896$

$B_{18} = 2112210601043831815941470427608507178024960$

$B_{19} = 437825148963391521638828389137155451835696283648$

$B_{20} = 26485117803153719500349865329783625522386424041570304$

$B_{21} = 84411998926603535512544634573788037136446095298648761958400$

$B_{22} = 66667674561498894094226045560233548174764204251787655655413760$

$B_{23} = 3063568009309298931959856378863776177340999596868565798461674272849920$

$B_{24} = 5583760264100680237381129136333973574659847646394871628459380791514448789504$

$B_{25} = 34168080993353113552180464917361262048721737746681574602280069300150039406884945920$

$B_{26} = 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776$

$B_{27} = 1228647482683315378634052011737122211307277977517770914268249674009473286529843656589397261811712$

$B_{28} = 29468175935974646521240728047319242694637960620437029709703184798221397605426305573782447476979888291840$

$B_{29} = 356876687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112$

$B_{30} = 45112182066293748035662681175485802795175889875645429400401331024420059769343778444886077402074532318126274500915888128$

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

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

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
$B_{22}$	- 66667674561498894094226045560233548174764204251787655655413760
$B_{23}$	- 3063568009309298931959856378863776177340999596868565798461674272849920
$B_{24}$	- 5583760264100680237381129136333973574659847646394871628459380791514448789504
$B_{25}$	- 34168080993535113552180464917361262048721737746681574602280069300150039406884945920
$B_{26}$	- 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776
$B_{27}$	- 1228647482683315378634052011737122211307277977517770914268249874009473286529843656589397261811712
$B_{28}$	- 29468175935974646521240728047319242694637960620437029709703184798221397605426305573782447476979888291840
$B_{29}$	- 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112
$B_{30}$	- 45112182062937480356268117548580279517588987564542940041331024420059769343778444886077402074532318126274500915888128

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

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

▶  $\log B_m = \hat{h}(P) m^2 + O((\log m)(\log \log m)^3)$ .  
(Linear forms in elliptic logarithms, David, 1995)

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

$$B_1 = 1$$

$$B_2 = 2$$

$$B_3 = 1$$

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

$$B_5 = 17 \cdot 79$$

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

$$B_7 = 1009 \cdot 2351$$

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

$$B_9 = 9788425919$$

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

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

► divisibility:  
if  $m|n$ , then  $B_m|B_n$ .

$$B_1 = 1$$

$$B_2 = 2$$

$$B_3 = 1$$

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

$$B_5 = 17 \cdot 79$$

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

$$B_7 = 1009 \cdot 2351$$

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

$$B_9 = 9788425919$$

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

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:  
 $\gcd(B_m, B_n) = B_{\gcd(m,n)}$ .

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  $v(B_m) \gg 0$ , then  
 $v(B_{mn}) = v(B_m) + v(B_n)$ .  
(formal groups / reduction)

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  $v(B_m) \gg 0$ , then  
 $v(B_{mn}) = v(B_m) + v(n)$ .  
(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  $q|B_n$  that does not divide any  $B_m$  with  $0 < m < n$ .

## Proof of Silverman (1)

- ▶ A *primitive divisor* of the term  $B_n$  is a prime  $q|B_n$  that does not divide any  $B_m$  with  $0 < m < n$ .
- ▶ The *primitive part*  $D_n$  is the largest divisor of  $B_n$  such that the only primes dividing  $D_n$  are primitive divisors of  $B_n$ .

## Proof of Silverman (1)

- ▶ A *primitive divisor* of the term  $B_n$  is a prime  $q|B_n$  that does not divide any  $B_m$  with  $0 < m < n$ .
- ▶ The *primitive part*  $D_n$  is the largest divisor of  $B_n$  such that the only 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

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

## Proof of Silverman (2)

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

so

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

## Proof of Silverman (2)

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

so

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

## Proof of Silverman (2)

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

so

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

## Proof of Silverman (2)

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

so

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

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.
- ▶ Example: multiplication by  $n \in \mathbb{Z}$

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.
- ▶ Example: multiplication by  $n \in \mathbb{Z}$
- ▶ Example: If  $E : y^2 = x^3 + ax$ , then  $(x, y) \rightarrow (-x, iy)$ .

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.
- ▶ Example: multiplication by  $n \in \mathbb{Z}$
- ▶ Example: If  $E : y^2 = x^3 + ax$ , then  $(x, y) \rightarrow (-x, iy)$ .
- ▶ The endomorphisms form a ring  $\text{End}(E)$ .

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.
- ▶ Example: multiplication by  $n \in \mathbb{Z}$
- ▶ Example: If  $E : y^2 = x^3 + ax$ , then  $(x, y) \rightarrow (-x, iy)$ .
- ▶ The endomorphisms form a ring  $\text{End}(E)$ .
- ▶  $\text{End}(E)$  is either  $\mathbb{Z}$  or  $\mathbb{Z}[\omega]$ , where  $\omega \in \mathbb{C} \setminus \mathbb{R}$  is a zero of a polynomial  $X^2 + aX + b$  with  $a, b \in \mathbb{Z}$ .

# Complex Multiplication

- ▶ An *endomorphism* of  $E$  is a group homomorphism  $E \rightarrow E$  that is given by rational functions.
- ▶ Example: multiplication by  $n \in \mathbb{Z}$
- ▶ Example: If  $E : y^2 = x^3 + ax$ , then  $(x, y) \rightarrow (-x, iy)$ .
- ▶ The endomorphisms form a ring  $\text{End}(E)$ .
- ▶  $\text{End}(E)$  is either  $\mathbb{Z}$  or  $\mathbb{Z}[\omega]$ , where  $\omega \in \mathbb{C} \setminus \mathbb{R}$  is a zero of a polynomial  $X^2 + aX + b$  with  $a, b \in \mathbb{Z}$ .
- ▶ If  $\text{End}(E) \neq \mathbb{Z}$ , then we say that  $E$  has *Complex Multiplication*.

# Elliptic divisibility sequences with CM

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

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ Unique factorization in number fields only for ideals, so  $B_\alpha$  is an ideal.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ Unique factorization in number fields only for ideals, so  $B_\alpha$  is an ideal.
- ▶ Do all properties generalize?
  - ▶ Growth.
  - ▶ Divisibility: if  $\alpha|\beta$ , then  $B_\alpha|B_\beta$ .
  - ▶ Strong divisibility:  $\gcd(B_\alpha, B_\beta) = B_{\gcd(\alpha, \beta)}$ .
  - ▶ If  $v(B_\alpha) \gg 0$ , then  $v(B_{\alpha\beta}) = v(B_\alpha) + v(B_\beta)$ .
  - ▶ Primitive divisors.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ 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  $B_\alpha|B_\beta$ .
  - ▶ Strong divisibility:  $\text{gcd}(B_\alpha, B_\beta) = B_{\text{gcd}(\alpha, \beta)}$ .
  - ▶ If  $v(B_\alpha) \gg 0$ , then  $v(B_{\alpha\beta}) = v(B_\alpha) + v(B_\beta)$ .
  - ▶ Primitive divisors.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ 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:  $\text{gcd}(B_\alpha, B_\beta) = B_{\text{gcd}(\alpha, \beta)}$ .
  - ▶ If  $v(B_\alpha) \gg 0$ , then  $v(B_{\alpha\beta}) = v(B_\alpha) + v(B_\beta)$ .
  - ▶ Primitive divisors.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ 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:  $\text{gcd}(B_\alpha, B_\beta) = B_{\text{gcd}(\alpha, \beta)}$ . **yes**
  - ▶ If  $v(B_\alpha) \gg 0$ , then  $v(B_{\alpha\beta}) = v(B_\alpha) + v(B_\beta)$ .
  - ▶ Primitive divisors.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ 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.

# Elliptic divisibility sequences with CM

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

- ▶  $\alpha P$  is not always a rational point, so look at points over a number field.
- ▶ 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?

- ▶ Silverman 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. Example: if  $\text{End}(E) = \mathbb{Z}[i]$  and  $30|\alpha$ , then

$$1 + i, 3, 2 + i, 2 - i \mid \alpha \quad \text{and} \quad \frac{1}{2} + \frac{1}{9} + \frac{1}{5} + \frac{1}{5} > 1.$$

## Silverman's proof?

- ▶ Silverman 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. Example: if  $\text{End}(E) = \mathbb{Z}[i]$  and  $30|\alpha$ , then

$$1 + i, 3, 2 + i, 2 - i \mid \alpha \quad \text{and} \quad \frac{1}{2} + \frac{1}{9} + \frac{1}{5} + \frac{1}{5} > 1.$$

- ▶ Solution: Inclusion-exclusion.

# The proof

- ▶ Inclusion-exclusion works best with unique factorization.

## The proof

- ▶ Inclusion-exclusion works best with unique factorization.
- ▶ The ring  $\mathcal{O} = \text{End}(E)$  does not always have unique factorization, but

## The proof

- ▶ 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.

## The proof

- ▶ 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.
- ▶ Use the strong divisibility property as a definition of  $B_{\mathfrak{a}}$  for ideals  $\mathfrak{a}$ , so

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

## The proof

- ▶ 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.
- ▶ Use the strong divisibility property as a definition of  $B_\alpha$  for ideals  $\alpha$ , so

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

- ▶ Use CM theory to get points  $\alpha P$  on a finite set of elliptic curves for the growth.

## The proof

- ▶ 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.
- ▶ Use the strong divisibility property as a definition of  $B_{\mathfrak{a}}$  for ideals  $\mathfrak{a}$ , so

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

- ▶ Use CM theory to get points  $\alpha P$  on a finite set of elliptic curves for the growth.
- ▶ Generalize the other properties.

## The proof

- ▶ 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.
- ▶ Use the strong divisibility property as a definition of  $B_{\mathfrak{a}}$  for ideals  $\mathfrak{a}$ , so

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

- ▶ Use CM theory to get points  $\alpha P$  on a finite set of elliptic curves for the growth.
- ▶ Generalize the other properties.
- ▶ Use Mertens' Theorem to estimate the size of the primitive part.

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

## 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  $B_1, B_2, B_3, \dots$

### Theorem

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

$$\begin{aligned}r_n &= \#\{p \mid n \text{ prime} : p \text{ ramifies in } \text{End}(E)\}, \\s_n &= \#\{p \mid n \text{ prime} : p \text{ splits in } \text{End}(E)\}.\end{aligned}$$

*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.