Divisibility Sequences for Elliptic Curves with Complex Multiplication

Master's thesis, Universiteit Utrecht
supervisor: Gunther Cornelissen

Marco Streng

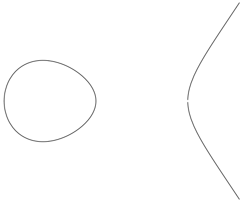
Universiteit Leiden

Journées Arithmétiques, Edinburgh, July 2007

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 (1)

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.

Elliptic Divisibility Sequences (1)

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.
- B is the largest integer such that Q reduces to $(0 : 1 : 0)$ modulo B.

Elliptic Divisibility Sequences (1)

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.
- B is the largest integer such that Q reduces to $(0 : 1 : 0)$ modulo B.

Elliptic Divisibility Sequences (1)

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 $B_1, B_2, B_3, \ldots$, which we call an *elliptic divisibility sequence*.

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 $P(X_1, \ldots, X_n) = 0$ has a solution $(X_1, \ldots, X_n) \in \mathbb{Z}^n$?

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 $P(X_1, \ldots, X_n) = 0$ *has a solution* $(X_1, \ldots, X_n) \in \mathbb{Z}^n$*?*
  - *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 $P(X_1, \ldots, X_n) = 0$ *has a solution* $(X_1, \ldots, X_n) \in \mathbb{Z}^n$*?*
  - *No.* (Davis, Putnam, Robinson, Matiyasevich 1970)
  - But what about other rings?
    With $\mathbb{Z}$ replaced by $\mathbb{Q}$, still an open problem.

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 $P(X_1, \ldots, X_n) = 0$ *has a solution* $(X_1, \ldots, X_n) \in \mathbb{Z}^n$*?*
  - *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: $E : y^2 = x^3 - 2x, P = (2, 2)$

$$
\begin{aligned}
B_1 &= 1\\
B_2 &= 2\\
B_3 &= 1\\
B_4 &= 84\\
B_5 &= 1343\\
B_6 &= 6214\\
B_7 &= 2372159\\
B_8 &= 151245528\\
B_9 &= 9788425919\\
B_{10} &= 11265465210550\\
B_{11} &= 5705771236038721\\
B_{12} &= 2316186053639990532\\
B_{13} &= 17999572487701067948161\\
B_{14} &= 35989730244828830296744846\\
B_{15} &= 173658539553825212149513251457\\
B_{16} &= 4838927849738289074690192087973888\\
B_{17} &= 75727152767742719949099952561136336896\\
B_{18} &= 2112210601043831815941470427608507178024960\\
B_{19} &= 437825148963391521638828389137155451835696283648\\
B_{20} &= 26485117803153719500349865329783625522386424041570304\\
B_{21} &= 8441199892660353551254463457378803713646095298648761958400\\
B_{22} &= 666676747561498894094226045560233548174764204251787655565413760\\
B_{23} &= 3063568009309298931959856378863776177340999596868565798461674272849920\\
B_{24} &= 5583760264100680237381129136333973574659847646394871628459380791514448789504\\
B_{25} &= 34168080993535113552180464917361262048721737746681574602280069300150039406884945920\\
B_{26} &= 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776\\
B_{27} &= 1228647482683315378634052011737122211307277977517770914268249874009473286529843656589397261811712\\
B_{28} &= 29468175935974646521240728047319242694637960820437029709703184798221397605426305573782447476979888291840\\
B_{29} &= 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112\\
B_{30} &= 45112182066293748035662681175485802795175889875645429400401331024420059769343777844886077402074532318126274500915888128
\end{aligned}
$$

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

growth:

$$
\begin{aligned}
B_{1} &= 1\\
B_{2} &= 2\\
B_{3} &= 1\\
B_{4} &= 84\\
B_{5} &= 1343\\
B_{6} &= 6214\\
B_{7} &= 2372159\\
B_{8} &= 151245528\\
B_{9} &= 9788425919\\
B_{10} &= 11265465210550\\
B_{11} &= 5705771236038721\\
B_{12} &= 2316186053639990532\\
B_{13} &= 1799957248770106794816 1\\
B_{14} &= 3598973024482883029674484 6\\
B_{15} &= 173658539553825212149513251457\\
B_{16} &= 483892784973828907469019208797388 8\\
B_{17} &= 757271527677427199490999525611363368 96\\
B_{18} &= 2112210601043831815941470427608507178024960\\
B_{19} &= 4378251489633915216388283891371554518356962836 48\\
B_{20} &= 2648511780315371950034986532978362552238642404157030 4\\
B_{21} &= 844119989266035355125446345737880371364609529864876195840 0\\
B_{22} &= 666676747561498894094226045560233548174764204251787655565541376 0\\
B_{23} &= 3063568009309298931959856378863776177340999596868565798461674272849920\\
B_{24} &= 558376026410068023738112913633397357465984764639487162845938079151444878950 4\\
B_{25} &= 341680809935351135521804649173612620487217377466815746022800693001500394068849459 20\\
B_{26} &= 58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776\\
B_{27} &= 122864748268331537863405201173712221130727797751777091426824987400947328652984365658939726181171 2\\
B_{28} &= 294681759359746465212407280473192426946379608204370297097031847982213976054263055737824474769798882918 40\\
B_{29} &= 356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112\\
B_{30} &= 451121820662937480356626811754858027951758898756454294004013310244200597693437778448860774020745323181262745009158881 28
\end{aligned}
$$

- $\log B_m \sim \widehat{h}(P)\ m^2$. (Weil, Siegel)

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

growth:

$B_1 = 1$
$B_2 = 2$
$B_3 = 1$
$B_4 = 84$
$B_5 = 1343$
$B_6 = 6214$
$B_7 = 2372159$
$B_8 = 151245528$
$B_9 = 9788425919$
$B_{10} = 11265465210550$
$B_{11} = 5705771236038721$
$B_{12} = 2316186053639990532$
$B_{13} = 1799957248770106794 8161$
$B_{14} = 359897302448288302967448 46$
$B_{15} = 173658539553825212149513251457$
$B_{16} = 483892784973828907469019208 7973888$
$B_{17} = 757271527677427199490999525611 36336896$
$B_{18} = 211221060104383181594147042760850717 8024960$
$B_{19} = 437825148963391521638828389137155451835696283648$
$B_{20} = 264851178031537195003498653297836255223864240415 70304$
$B_{21} = 844119989266035355125446345737880371364609529864 8761958400$
$B_{22} = 666676747561498894094226045560233548174764204251787655 5655413760$
$B_{23} = 306356800930929893195985637886377617734099959686856579846167427 2849920$
$B_{24} = 558376026410068023738112913633397357465984764639487162845938079151 4448789504$
$B_{25} = 341680809935351135521804649173612620487217377466815746022800693001 5003940688 4945920$
$B_{26} = 581281081447099968999027703165590575729534780876243950008806563961 63549689500622468939776$
$B_{27} = 122864748268331537863405201173712221130727797751777091426824987400947 32865298436565893972618 11712$
$B_{28} = 294681759359746465212407280473192426946379608204370297097031847982213 97605426305573782447476979888291840$
$B_{29} = 356878687646301597118830109548723651778237805769218351288805337153805 28523759851524564322184590214502 6221146112$
$B_{30} = 451121820662937480356626811754858027951758898756454294004013310244200 5976934377784488607740207453231812627450091 5888128$

- $\log B_m \sim \widehat{h}(P)\ m^2$.
  (Weil, Siegel)
- $\log B_m \leq \widehat{h}(P)\ m^2 + C$.

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}	$=$	1799957248770106794816 1
B_{14}	$=$	35989730244828830296744846
B_{15}	$=$	173658539553825212149513251457
B_{16}	$=$	4838927849738289074690192087973888
B_{17}	$=$	757271527677427199490999525611363368 96
B_{18}	$=$	211221060104383181594147042760850717802 4960
B_{19}	$=$	4378251489633915216388283891371554518356962836 48
B_{20}	$=$	26485117803153719500349865329783625522386424041570304
B_{21}	$=$	844119989266035355125446345737880371364609529864876195840 0
B_{22}	$=$	666676747561498894094226045560233548174764204251787655565541376 0
B_{23}	$=$	306356800930929893195985637886377617734099959686856579846167427284992 0
B_{24}	$=$	55837602641006802373811291363339735746598476463948716284593807915144487895 04
B_{25}	$=$	34168080993535113552180464917361262048721737746681574602280069300150039406884945920
B_{26}	$=$	58128108144709996899902770316559057572953478087624395000880656396163549689500622468939776
B_{27}	$=$	1228647482683315378634052011737122211307277977517770914268249874009473286529843656589397261811712
B_{28}	$=$	29468175935974646521240728047319242694637960820437029709703184798221397605426305573782447476979888291840
B_{29}	$=$	356878687646301597118830109548723651778237805769218351288805337153805285237598515245643221845902145026221146112
B_{30}	$=$	45112182066293748035662681175485802795175889875645429400401331024420059769343777844886077402074532318126274500915888128

- $\log B_m \sim \hat{h}(P)\ m^2$. (Weil, Siegel)
- $\log B_m \leq \hat{h}(P)\ m^2 + C$.
- $\log B_m = \hat{h}(P)\ m^2 + O\left((\log m)(\log\log m)^3\right)$. (Linear forms in elliptic logarithms, David, 1995)

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

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 2 \\
B_3 &= 1 \\
B_4 &= 2^2 \cdot 3 \cdot 7 \\
B_5 &= 17 \cdot 79 \\
B_6 &= 2 \cdot 13 \cdot 239 \\
B_7 &= 1009 \cdot 2351 \\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \\
B_9 &= 9788425919 \\
B_{10} &= 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161
\end{aligned}
$$

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

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 2 \\
B_3 &= 1 \\
B_4 &= 2^2 \cdot 3 \cdot 7 \\
B_5 &= 17 \cdot 79 \\
B_6 &= 2 \cdot 13 \cdot 239 \\
B_7 &= 1009 \cdot 2351 \\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \\
B_9 &= 9788425919 \\
B_{10} &= 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161
\end{aligned}
$$

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

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

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 2 \\
B_3 &= 1 \\
B_4 &= 2^2 \cdot 3 \cdot 7 \\
B_5 &= 17 \cdot 79 \\
B_6 &= 2 \cdot 13 \cdot 239 \\
B_7 &= 1009 \cdot 2351 \\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \\
B_9 &= 9788425919 \\
B_{10} &= 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161
\end{aligned}
$$

- divisibility:
  if $m|n$, then $B_m|B_n$.
- strong divisibility:
  $\gcd(B_m, B_n) = B_{\gcd(m,n)}$.

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

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 2 \\
B_3 &= 1 \\
B_4 &= 2^2 \cdot 3 \cdot 7 \\
B_5 &= 17 \cdot 79 \\
B_6 &= 2 \cdot 13 \cdot 239 \\
B_7 &= 1009 \cdot 2351 \\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \\
B_9 &= 9788425919 \\
B_{10} &= 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161
\end{aligned}
$$

- divisibility: if $m|n$, then $B_m|B_n$.
- strong divisibility: $\gcd(B_m, B_n) = B_{\gcd(m,n)}$.
- if $\mathrm{ord}_{\mathfrak{p}}(B_m) >> 0$, then $\mathrm{ord}_{\mathfrak{p}}(B_{mn}) = \mathrm{ord}_{\mathfrak{p}}(B_m) + \mathrm{ord}_{\mathfrak{p}}(n)$. (formal groups / reduction)

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

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 2 \\
B_3 &= 1 \\
B_4 &= 2^2 \cdot 3 \cdot 7 \\
B_5 &= 17 \cdot 79 \\
B_6 &= 2 \cdot 13 \cdot 239 \\
B_7 &= 1009 \cdot 2351 \\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \\
B_9 &= 9788425919 \\
B_{10} &= 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 79 \cdot 337 \cdot 8161
\end{aligned}
$$

- divisibility:
  if $m|n$, then $B_m|B_n$.
- strong divisibility:
  $\gcd(B_m, B_n) = B_{\gcd(m,n)}$.
- if $\mathrm{ord}_{\mathfrak{p}}(B_m) >> 0$, then
  $\mathrm{ord}_{\mathfrak{p}}(B_{mn}) =$
  $\mathrm{ord}_{\mathfrak{p}}(B_m) + \mathrm{ord}_{\mathfrak{p}}(n)$.
  (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 $n|m$.

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.

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

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

Proof of Silverman (2)

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

so

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

Proof of Silverman (2)

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

so

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

Proof of Silverman (2)

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

so

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

Proof of Silverman (2)

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

so

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

Complex Multiplication

- An *endomorphism* of E is an algebraic group homomorphism $E \to E$.

Complex Multiplication

- An *endomorphism* of E is an algebraic group homomorphism $E \to E$.
- Example: multiplication by $n \in \mathbb{Z}$

Complex Multiplication

- An *endomorphism* of E is an algebraic group homomorphism $E \to E$.
- Example: multiplication by $n \in \mathbb{Z}$
- Example: If $E : y^2 = x^3 + ax$, then $(x, y) \to (-x, iy)$.

Complex Multiplication

- An *endomorphism* of E is an algebraic group homomorphism $E \to E$.
- Example: multiplication by $n \in \mathbb{Z}$
- Example: If $E : y^2 = x^3 + ax$, then $(x, y) \to (-x, iy)$.
- The endomorphisms form a ring $\mathrm{End}(E)$.

Complex Multiplication

- An *endomorphism* of E is an algebraic group homomorphism $E \to E$.
- Example: multiplication by $n \in \mathbb{Z}$
- Example: If $E : y^2 = x^3 + ax$, then $(x, y) \to (-x, iy)$.
- The endomorphisms form a ring $\mathrm{End}(E)$.
- $\mathrm{End}(E)$ 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 an algebraic group homomorphism $E \to E$.
- Example: multiplication by $n \in \mathbb{Z}$
- Example: If $E : y^2 = x^3 + ax$, then $(x, y) \to (-x, iy)$.
- The endomorphisms form a ring $\mathrm{End}(E)$.
- $\mathrm{End}(E)$ 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 $\mathrm{End}(E) \neq \mathbb{Z}$, then we say that E has *Complex Multiplication*.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α is an ideal.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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 $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$.
  - Primitive divisors.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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: $\gcd(B_\alpha, B_\beta) = B_{\gcd(\alpha,\beta)}$.
  - If $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$.
  - Primitive divisors.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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: $\gcd(B_\alpha, B_\beta) = B_{\gcd(\alpha,\beta)}$.
  - If $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$.
  - Primitive divisors.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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 $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$.
  - Primitive divisors.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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 $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$. yes
  - Primitive divisors.

Elliptic divisibility sequences with CM

Look at αP for all $\alpha \in \mathrm{End}(E)$ to get B_α.

- αP is not always a rational point, so look at points and curves over number fields.
- Unique factorization in number fields only for ideals, so B_α 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 $v(B_\alpha) >> 0$, then $v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$. 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.

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 proof (1)

- Inclusion-exclusion works best with unique factorization.
- The ring $\mathcal{O} = \mathrm{End}(E)$ does not always have unique factorization, but the set of ideals of $\mathcal{O}$ coprime to the conductor of $\mathcal{O}$ does.

The proof (1)

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

$$B_{\mathfrak{a}} = \mathrm{gcd}_{\alpha \in \mathfrak{a}} B_{\alpha}.$$

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

The proof (1)

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

$$B_{\mathfrak{a}} = \mathrm{gcd}_{\alpha \in \mathfrak{a}} B_{\alpha}.$$

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

The proof (2)

- For the growth, we need points.

The proof (2)

- For the growth, we need points.
- There is a natural way to associate to every $\mathfrak{a}$ a homomorphism of elliptic curves $\mathfrak{a} : E \longrightarrow E'$.

The proof (2)

- For the growth, we need points.
- There is a natural way to associate to every $\mathfrak{a}$ a homomorphism of elliptic curves $\mathfrak{a} : E \longrightarrow E'$.
- Its image E' depends only on the ideal class of $\mathfrak{a}$, so we get points $\mathfrak{a}P$ on a finite set of elliptic curves.

The proof (2)

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

The proof (2)

- For the growth, we need points.
- There is a natural way to associate to every $\mathfrak{a}$ a homomorphism of elliptic curves $\mathfrak{a} : E \longrightarrow E'$.
- Its image E' depends only on the ideal class of $\mathfrak{a}$, so we get points $\mathfrak{a}P$ on a finite set of elliptic curves.
- Their denominators are almost equal to the $B_{\mathfrak{a}}^2$'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 $B_1, B_2, B_3, \ldots$.

Corollary

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

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

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.

preprint:

`http://www.math.leidenuniv.nl/~streng`