Abelian Divisibility Sequences

Joseph H. Silverman

Brown University

Arithmetic of Low-Dimensional Abelian Varietes

ICERM, June 3–7 2019

Divisibility Sequences

A **divisibility sequence** is a sequence of (positive) integers

$$(D_n)_{n\geq 1} \quad \text{such that} \quad m \mid n \implies D_m \mid D_n.$$

Divisibility Sequences

A **divisibility sequence** is a sequence of (positive) integers

$$(D_n)_{n\ge 1} \quad \text{such that} \quad m \mid n \implies D_m \mid D_n.$$

Classical examples divisibility sequences include:

$D_n = a^n - b^n, \quad$ where $a > b \ge 1$;

the Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, \ldots$.

Divisibility Sequences

A **divisibility sequence** is a sequence of (positive) integers

$$(D_n)_{n\ge 1} \quad \text{such that} \quad m \mid n \implies D_m \mid D_n.$$

Classical examples divisibility sequences include:

$$D_n = a^n - b^n, \quad \text{where } a > b \ge 1;$$
the Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, \ldots$.

An **elliptic divisibility sequence** (**EDS**) is formed from an elliptic curve $E/\mathbb{Q}$ and a non-torsion point $P \in E(\mathbb{Q})$ by writing

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

The sequence $\big(D_n(P)\big)_{n\ge 1}$ is an EDS.

Divisibility Sequences over Dedekind Domains

More generally, if R is a Dedekind domain, we define an R**-divisibility sequence** to be a sequence of ideals

$$(\mathfrak{D}_n)_{n\geq 1} \quad \text{such that} \quad m \mid n \implies \mathfrak{D}_m \mid \mathfrak{D}_n.$$

Divisibility Sequences over Dedekind Domains

More generally, if R is a Dedekind domain, we define an ***R*-divisibility sequence** to be a sequence of ideals

$$(\mathfrak{D}_n)_{n\ge1} \quad \text{such that} \quad m \mid n \implies \mathfrak{D}_m \mid \mathfrak{D}_n.$$

In this way we can define an EDS, for example, by factoring the ideal generated by $x(nP)$ in the form

$$x(nP)R = \mathfrak{A}_n(P)\mathfrak{D}_n(P)^{-2}$$

and taking the sequence

$$\big(\mathfrak{D}_n(P)\big)_{n\ge1}.$$

Reformulating EDS

Let E/K be an elliptic curve, let $P \in E(K)$, and let $\mathcal{E}/R$ be a Néron model for E/K. Then the EDS

$$\boxed{\bigl(\mathfrak{D}_n(P)\bigr)_{n\ge 1}}$$

is characterized by noting that for each prime ideal $\mathfrak{p}$ of R, we have*

$$\boxed{\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_n(P) = \Bigl(\text{largest } k \text{ so that } nP \equiv \mathcal{O} \pmod{\mathfrak{p}^k}\Bigr).}$$

* Maybe not quite right at primes of bad reduction.

Reformulating EDS

Let E/K be an elliptic curve, let $P \in E(K)$, and let $\mathcal{E}/R$ be a Néron model for E/K. Then the EDS

$$\big(\mathfrak{D}_n(P)\big)_{n \ge 1}$$

is characterized by noting that for each prime ideal $\mathfrak{p}$ of R, we have*

$$\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_n(P) = \Big(\text{largest } k \text{ so that } nP \equiv \mathcal{O} \pmod{\mathfrak{p}^k}\Big).$$

* Maybe not quite right at primes of bad reduction.

Or we can simply say that $\mathfrak{D}_n(P)$ is the largest ideal (ordered by divisibility) such that

$$nP \equiv \mathcal{O} \pmod{\mathfrak{D}_n(P)}.$$

Abelian Divisibility Sequences: Type I

In general:

R	a Dedekind domain.
K	the fraction field of R.
A/K	an abelian variety.
$\mathcal{A}/R$	a Néron model for A/K.
$P \in A(K)$	a non-torsion point.

The **abelian divisibility sequence** (**ADS**) for the pair (A, P) is the sequence of ideals $\bigl(\mathfrak{D}_n(P)\bigr)_{n\ge1}$ defined by the property that $\mathfrak{D}_n(P)$ is the largest ideal satisfying

$$nP \equiv \mathcal{O} \pmod{\mathfrak{D}_n(P)}.$$

Abelian Divisibility Sequences: Type I

In general:

R	a Dedekind domain.
K	the fraction field of R.
A/K	an abelian variety.
$\mathcal{A}/R$	a Néron model for A/K.
$P \in A(K)$	a non-torsion point.

The **abelian divisibility sequence** (**ADS**) for the pair (A, P) is the sequence of ideals $\big(\mathfrak{D}_n(P)\big)_{n\ge1}$ defined by the property that $\mathfrak{D}_n(P)$ is the largest ideal satisfying

$$nP \equiv \mathcal{O} \pmod{\mathfrak{D}_n(P)}.$$

Alternatively, letting $\pi : \mathcal{A} \to \operatorname{Spec}(R)$, we can define $\mathfrak{D}_n(P)$ via arithmetic intersection theory,

$$\mathfrak{D}_n(P) := \pi_*(nP \cdot \mathcal{O}) = (nP)^*(\mathcal{O}) \in \operatorname{Div}\big(\operatorname{Spec}(R)\big).$$

Abelian Divisibility Sequences: Type I

In general:

R	a Dedekind domain.
K	the fraction field of R.
A/K	an abelian variety.
$\mathcal{A}/R$	a Néron model for A/K.
$P \in A(K)$	a non-torsion point.

The **abelian divisibility sequence** (**ADS**) for the pair (A, P) is the sequence of ideals $\bigl(\mathfrak{D}_n(P)\bigr)_{n\ge1}$ defined by the property that $\mathfrak{D}_n(P)$ is the largest ideal satisfying

$$nP \equiv \mathcal{O} \pmod{\mathfrak{D}_n(P)}.$$

Alternatively, letting $\pi : \mathcal{A} \to \operatorname{Spec}(R)$, we can define $\mathfrak{D}_n(P)$ via arithmetic intersection theory,

$$\mathfrak{D}_n(P) := \pi_*(nP \cdot \mathcal{O}) = (nP)^*(\mathcal{O}) \in \operatorname{Div}\bigl(\operatorname{Spec}(R)\bigr).$$

Exercise: Prove that $\bigl(\mathfrak{D}_n(P)\bigr)$ is a divisibility sequence.

Growth Rates

A $\mathbb{G}_m$-divisibility sequence $\mathcal{D} = (D_n)$ such as $a^n - b^n$ or the Fibonacci sequence grows exponentially,

$$\lim_{n\to\infty} |D_n|^{1/n} > 1.$$

Growth Rates

A $\mathbb{G}_m$-divisibility sequence $\mathcal{D} = (D_n)$ such as $a^n - b^n$ or the Fibonacci sequence grows exponentially,

$$\lim_{n\to\infty} |D_n|^{1/n} > 1.$$

Elliptic divisiblity sequences $\mathcal{D} = \bigl(\mathfrak{D}_n(P)\bigr)$ grow even faster,

$$\lim_{n\to\infty} \bigl(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P)\bigr)^{1/n^2} > 1. \qquad (*)$$

Two remarks about elliptic divisibility sequences:

- The limit in $(*)$ is $\hat{H}_E(P)$, i.e.,

$$\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P) \approx \hat{H}_E(P)^{n^2} = \hat{H}_E(nP).$$

- The proof uses a deep, ineffective theorem of Siegel.

Growth Rates

A $\mathbb{G}_m$-divisibility sequence $\mathcal{D} = (D_n)$ such as $a^n - b^n$ or the Fibonacci sequence grows exponentially,

$$\lim_{n\to\infty} |D_n|^{1/n} > 1.$$

Elliptic divisiblity sequences $\mathcal{D} = \bigl(\mathfrak{D}_n(P)\bigr)$ grow even faster,

$$\lim_{n\to\infty} \bigl(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P)\bigr)^{1/n^2} > 1. \qquad (*)$$

Two remarks about elliptic divisibility sequences:

- The limit in $(*)$ is $\hat{H}_E(P)$, i.e.,

$$\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P) \approx \hat{H}_E(P)^{n^2} = \hat{H}_E(nP).$$

- The proof uses a deep, ineffective theorem of Siegel.

The height of nP on an abelian variety grows at a similar rate, but co-dimension considerations suggest that $\mathfrak{D}_n(P)$ might not grow that fast.

Growth Rates of ADS: A Conjecture

Conjecture 1. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then

$$\lim_{n\to\infty} \bigl(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P)\bigr)^{1/n^2} = 1.$$

Growth Rates of ADS: A Conjecture

Conjecture 1. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then

$$\lim_{n\to\infty} \bigl(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{D}_n(P)\bigr)^{1/n^2} = 1.$$

The conjecture says that in dimension ≥ 2, an ADS grows more slowly than the heights of the points in the sequence nP.

Growth Rates of ADS: A Conjecture

Conjecture 1. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then

$$\lim_{n\to\infty}\left(\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P)\right)^{1/n^2} = 1.$$

The conjecture says that in dimension ≥ 2, an ADS grows more slowly than the heights of the points in the sequence nP.

Theorem. Conjecture 1 follows from Vojta's conjecture applied to A blown up at $\mathcal{O}$.

A Multiplicative Analogue to Conjecture 1

Here is a $\mathbb{G}_m$ analogue. We replace A by $\mathbb{G}_m^2$ and $P \in A(K)$ with $(a, b) \in \mathbb{G}_m^2(\mathbb{Q})$. The associated divisibility sequence

$$\gcd(a^n - 1, b^n - 1)$$

measures the "arithmetic distance" from $(a, b)^n$ to $(1, 1)$.

A Multiplicative Analogue to Conjecture 1

Here is a $\mathbb{G}_m$ analogue. We replace A by $\mathbb{G}_m^2$ and $P \in A(K)$ with $(a,b) \in \mathbb{G}_m^2(\mathbb{Q})$. The associated divisibility sequence

$$\gcd(a^n - 1, b^n - 1)$$

measures the "arithmetic distance" from $(a,b)^n$ to $(1,1)$.

Theorem. (Bugeaud–Corvaja–Zannier 2003) Let $a, b \in \mathbb{Z}$ with $|a| > |b| > 1$. Then

$$\lim_{n\to\infty} \gcd(a^n - 1, b^n - 1)^{1/n} = 1.$$

([BCZ] result is more general. See also work of A. Levin.)

A Multiplicative Analogue to Conjecture 1

Here is a $\mathbb{G}_m$ analogue. We replace A by $\mathbb{G}_m^2$ and $P \in A(K)$ with $(a,b) \in \mathbb{G}_m^2(\mathbb{Q})$. The associated divisibility sequence

$$\gcd(a^n - 1, b^n - 1)$$

measures the "arithmetic distance" from $(a,b)^n$ to $(1,1)$.

Theorem. (Bugeaud–Corvaja–Zannier 2003) Let $a, b \in \mathbb{Z}$ with $|a| > |b| > 1$. Then

$$\lim_{n\to\infty} \gcd(a^n - 1, b^n - 1)^{1/n} = 1.$$

([BCZ] result is more general. See also work of A. Levin.)

The proof uses Schmidt's subspace theorem and is surprisingly intricate, even for $a = 3$ and $b = 2$.

Challenge: Give an elementary proof that

$$\gcd(3^n - 1, 2^n - 1)^{1/n} \longrightarrow 1.$$

Growth Rates of ADS: Another Conjecture

Conjecture 1 says that an ADS does not grow too fast. The next conjecture says that for many n, it doesn't grow at all!

Growth Rates of ADS: Another Conjecture

Conjecture 1 says that an ADS does not grow too fast. The next conjecture says that for many n, it doesn't grow at all!

Conjecture 2. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then there is a constant $C = C(A/K, P)$ with the property that

$$(*) \quad \left|\mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n(P)\right| \leq C \quad \text{for infinitely many } n \geq 1.$$

Growth Rates of ADS: Another Conjecture

Conjecture 1 says that an ADS does not grow too fast. The next conjecture says that for many n, it doesn't grow at all!

Conjecture 2. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then there is a constant $C = C(A/K, P)$ with the property that

$$(*) \quad \left|\mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n(P)\right| \leq C \quad \text{for infinitely many } n \geq 1.$$

Bolder Conjecture: The set of *primes* n such that the inequality $(*)$ holds is a set of positive density.

Growth Rates of ADS: Another Conjecture

Conjecture 1 says that an ADS does not grow too fast. The next conjecture says that for many n, it doesn't grow at all!

Conjecture 2. Let A/K be an abelian variety of dimension ≥ 2, and let $P \in A(K)$ be a point such that $\mathbb{Z}P$ is Zariski dense in A. Then there is a constant $C = C(A/K, P)$ with the property that

$$(*) \quad \left|\mathrm{N}_{K/\mathbb{Q}}\mathfrak{D}_n(P)\right| \leq C \quad \text{for infinitely many } n \geq 1.$$

Bolder Conjecture: The set of *primes* n such that the inequality $(*)$ holds is a set of positive density.

Even Bolder ~~Conjecture~~ Question: The set of *primes* n such that the inequality $(*)$ holds is a set of density 1.

A Multiplicative Analogue to Conjecture 2

It is surprising to me that this conjecture wasn't formulated until quite recently.

Conjecture. (Ailon–Rudnick 2004) Let $a, b \in \mathbb{Z}$ with $|a| > |b| > 1$. Then there are infinitely many values of $n \geq 1$ such that

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1).$$

A Multiplicative Analogue to Conjecture 2

It is surprising to me that this conjecture wasn't formulated until quite recently.

Conjecture. (Ailon–Rudnick 2004) Let $a, b \in \mathbb{Z}$ with $|a| > |b| > 1$. Then there are infinitely many values of $n \geq 1$ such that

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1).$$

Even for $\gcd(3^n - 1, 2^n - 1)$, there seem to be no tools to attack the problem. However, we do have:

A Multiplicative Analogue to Conjecture 2

It is surprising to me that this conjecture wasn't formulated until quite recently.

Conjecture. (Ailon–Rudnick 2004) Let $a, b \in \mathbb{Z}$ with $|a| > |b| > 1$. Then there are infinitely many values of $n \geq 1$ such that

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1).$$

Even for $\gcd(3^n - 1, 2^n - 1)$, there seem to be no tools to attack the problem. However, we do have:

Theorem. (Ailon–Rudnick 2004) Let $a(T), b(T) \in \mathbb{C}[T]$ be multiplicatively independent modulo $\mathbb{C}^*$. Then there is a $c(T) \in \mathbb{C}[t]$ such that

$$\gcd\bigl(a(T)^n - 1, b(T)^n - 1\bigr) \mid c(T) \quad \text{for all } n \geq 1.$$

Experiments

I've gathered a fair amount of data for the $\mathbb{G}_m^2$ conjecture, i.e., Ailon–Rudnick's conjecture for

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1),$$

which I will display on the next slide.

Experiments

I've gathered a fair amount of data for the $\mathbb{G}_m^2$ conjecture, i.e., Ailon–Rudnick's conjecture for

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1),$$

which I will display on the next slide.

I've also gathered some data for Conjecture 2 when

$$A = E_1 \times E_2$$

is a product of elliptic curves.

Experiments

I've gathered a fair amount of data for the $\mathbb{G}_m^2$ conjecture, i.e., Ailon–Rudnick's conjecture for

$$\gcd(a^n - 1, b^n - 1) = \gcd(a - 1, b - 1),$$

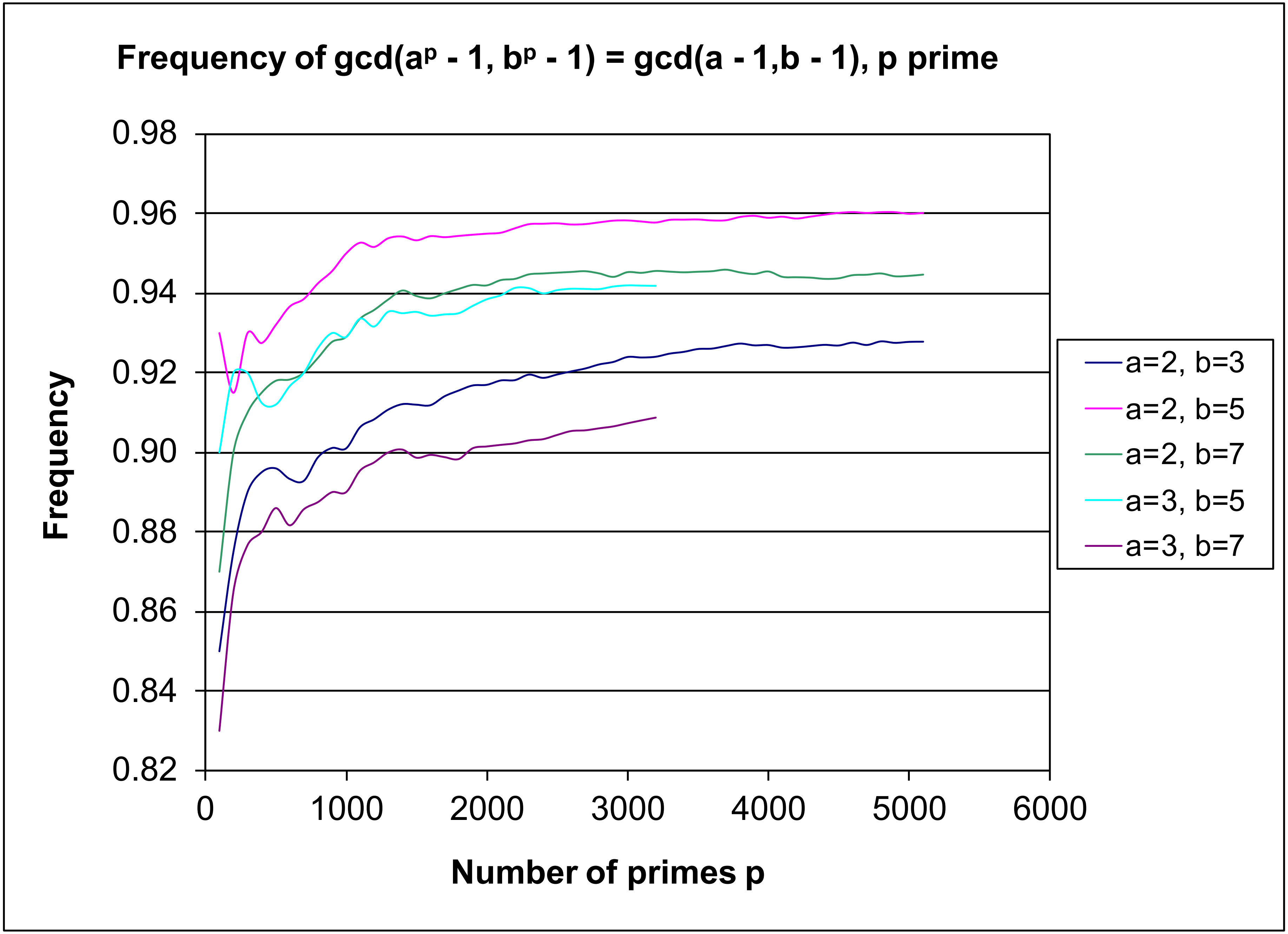
which I will display on the next slide.

I've also gathered some data for Conjecture 2 when

$$A = E_1 \times E_2$$

is a product of elliptic curves.

It would be interesting to do some experiments using simple abelian surfaces.



Question: Does the frequency go to 100%?

Fast Growth Versus Slow Growth

As we have seen the growth rate of the ADS associated to an abelian variety A is

$$\boxed{\begin{array}{ll} \textbf{Fast} & \text{if } \dim(A) = 1; \\ \textbf{Slow} & \text{if } \dim(A) \ge 2 \text{ (conjecturally).} \end{array}}$$

Fast Growth Versus Slow Growth

As we have seen the growth rate of the ADS associated to an abelian variety A is

$$\boxed{\begin{array}{rl} \textbf{Fast} & \text{if } \dim(A) = 1; \\ \textbf{Slow} & \text{if } \dim(A) \geq 2 \text{ (conjecturally).} \end{array}}$$

There are a number of reasons why fast-growing divisibility sequences are useful, including:

- Existence of primitive prime divisors (defined later);
- Applications to logic, Hilbert's 10th problem;
- Applications to cryptography based on discrete logarithms and/or pairings.

Fast Growth Versus Slow Growth

As we have seen the growth rate of the ADS associated to an abelian variety A is

$$\boxed{\begin{array}{rl} \textbf{Fast} & \text{if } \dim(A) = 1; \\ \textbf{Slow} & \text{if } \dim(A) \ge 2 \text{ (conjecturally).} \end{array}}$$

There are a number of reasons why fast-growing divisibility sequences are useful, including:

- Existence of primitive prime divisors (defined later);
- Applications to logic, Hilbert's 10th problem;
- Applications to cryptography based on discrete logarithms and/or pairings.

How can we get fast-growing, geometrically defined, abelian divisibility sequences in high dimension?

Abelian Divisibility Sequences: Type II

Let $\pi : \mathcal{A} \to \operatorname{Spec}(R)$ be a Néron model for A/K. For a point $P \in A(K)$ on the generic fiber, let $\overline{P} \subset \mathcal{A}$ be the closure of P. We defined the Type I ADS for (A, P) to be the sequence of ideals

$$\mathfrak{D}_n(P) := \pi_*\bigl(\overline{[n]P} \cdot \overline{\mathcal{O}}\bigr) = \pi_*\bigl(\overline{P} \cdot [n]^*\overline{\mathcal{O}}\bigr).$$

This is small when $\dim(A) \geq 2$ because

$$\dim(\mathcal{A}) \geq 3, \quad \text{while} \quad \dim \overline{P} = \dim \overline{\mathcal{O}} = 1.$$

Abelian Divisibility Sequences: Type II

Let $\pi : \mathcal{A} \to \operatorname{Spec}(R)$ be a Néron model for A/K. For a point $P \in A(K)$ on the generic fiber, let $\overline{P} \subset \mathcal{A}$ be the closure of P. We defined the Type I ADS for (A, P) to be the sequence of ideals

$$\mathfrak{D}_n(P) := \pi_*\bigl(\overline{[n]P} \cdot \overline{\mathcal{O}}\bigr) = \pi_*\bigl(\overline{P} \cdot [n]^*\overline{\mathcal{O}}\bigr).$$

This is small when $\dim(A) \geq 2$ because

$$\dim(\mathcal{A}) \geq 3, \quad \text{while} \quad \dim \overline{P} = \dim \overline{\mathcal{O}} = 1.$$

To obtain a *fast-growing sequence*, we should replace P and/or $\mathcal{O}$ with a higher-dimensional variety.

Abelian Divisibility Sequences: Type II

Let $\pi : \mathcal{A} \to \operatorname{Spec}(R)$ be a Néron model for A/K. For a point $P \in A(K)$ on the generic fiber, let $\overline{P} \subset \mathcal{A}$ be the closure of P. We defined the Type I ADS for (A, P) to be the sequence of ideals

$$\mathfrak{D}_n(P) := \pi_*\bigl(\overline{[n]P} \cdot \overline{\mathcal{O}}\bigr) = \pi_*\bigl(\overline{P} \cdot [n]^*\overline{\mathcal{O}}\bigr).$$

This is small when $\dim(A) \geq 2$ because

$$\dim(\mathcal{A}) \geq 3, \quad \text{while} \quad \dim \overline{P} = \dim \overline{\mathcal{O}} = 1.$$

To obtain a *fast-growing sequence*, we should replace P and/or $\mathcal{O}$ with a higher-dimensional variety.

And in order to get a *divisibility sequence*, we need to replace P, not $\mathcal{O}$.

Abelian Divisibility Sequences: Type II

Definition: Let $X \subset A_K$ be an irreducible codimension 1 subvariety defined over K, and let $\overline{X}$ be its closure in $\mathcal{A}$. The **abelian divisibility sequence** for the pair (A, X) is the sequence of ideals*

$$\mathfrak{D}_n(X) := \pi_*\bigl(\overline{X} \cdot [n]^*\overline{\mathcal{O}}\bigr).$$

* Need to be a bit careful if $\overline{X}$ contains a component of $[n]^*\overline{\mathcal{O}}$.

Abelian Divisibility Sequences: Type II

Definition: Let $X \subset A_K$ be an irreducible codimension 1 subvariety defined over K, and let $\overline{X}$ be its closure in $\mathcal{A}$. The **abelian divisibility sequence** for the pair (A, X) is the sequence of ideals*

$$\mathfrak{D}_n(X) := \pi_*\bigl(\overline{X} \cdot [n]^*\overline{\mathcal{O}}\bigr).$$

* Need to be a bit careful if $\overline{X}$ contains a component of $[n]^*\overline{\mathcal{O}}$.

Conjecture. If A is simple, or more generally if X contains no translates of abelian subvarieties, then $\mathfrak{D}_n(X)$ is fast-growing:

$$\liminf_{n\to\infty} \left|\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{D}_n(X)\right|^{1/n^{2\dim A}} > 1.$$

Tori Divisibility Sequences: Type II

The analogous problem for $\mathbb{G}_m^N$ is solved.

Theorem. (Habegger, Dimitrov, 2016) Let $f \in R[T_1^{\pm 1}, \dots, T_N^{\pm 1}]$ be a Laurent polynomial, and let $X_f \subset \mathbb{G}_m^N$ be the associated divisor. Then

$$\lim_{n\to\infty} \left| \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n(X_f) \right|^{1/n^N} = \mathrm{MahlerMeasure}(f).$$

Tori Divisibility Sequences: Type II

The analogous problem for $\mathbb{G}_m^N$ is solved.

Theorem. (Habegger, Dimitrov, 2016) Let $f \in R[T_1^{\pm 1}, \ldots, T_N^{\pm 1}]$ be a Laurent polynomial, and let $X_f \subset \mathbb{G}_m^N$ be the associated divisor. Then

$$\lim_{n\to\infty} \left| \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n(X_f) \right|^{1/n^N} = \mathrm{MahlerMeasure}(f).$$

$$\mathfrak{D}_n(X_f) := \prod_{\zeta_1,\ldots,\zeta_N \in \boldsymbol{\mu}_n} f(\zeta_1, \ldots, \zeta_N).$$

Tori Divisibility Sequences: Type II

The analogous problem for $\mathbb{G}_m^N$ is solved.

Theorem. (Habegger, Dimitrov, 2016) Let $f \in R[T_1^{\pm 1}, \dots, T_N^{\pm 1}]$ be a Laurent polynomial, and let $X_f \subset \mathbb{G}_m^N$ be the associated divisor. Then

$$\lim_{n\to\infty} \left| \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n(X_f) \right|^{1/n^N} = \mathrm{MahlerMeasure}(f).$$

$$\mathfrak{D}_n(X_f) := \prod_{\zeta_1,\dots,\zeta_N \in \boldsymbol{\mu}_n} f(\zeta_1, \dots, \zeta_N).$$

Remark. The theorem is false if we allow f to have $\mathbb{C}$ coefficients. Even for $N = 1$, the theorem requires some sort of estimate coming from linear-forms-in-logarithms, because we need to know that algebraic numbers cannot be too closely approximated by roots of unity.

Primitive Prime Divisors and Zsigmondy Sets

Question: Which terms contain a "new" prime divisor?

Definition: Let $\mathcal{D} := (\mathfrak{D}_n)_{n \geq 1}$ be a sequence of ideals. A **primitive prime divisor of $\mathfrak{D}_n$** is a prime ideal $\mathfrak{p}$ satisfying

$$\mathfrak{p} \mid \mathfrak{D}_n \quad \text{and} \quad \mathfrak{p} \nmid \mathfrak{D}_m \quad \text{for all } m < n.$$

Primitive Prime Divisors and Zsigmondy Sets

Question: Which terms contain a "new" prime divisor?

Definition: Let $\mathcal{D} := (\mathfrak{D}_n)_{n\geq 1}$ be a sequence of ideals. A **primitive prime divisor of $\mathfrak{D}_n$** is a prime ideal $\mathfrak{p}$ satisfying

$$\mathfrak{p} \mid \mathfrak{D}_n \quad \text{and} \quad \mathfrak{p} \nmid \mathfrak{D}_m \quad \text{for all } m < n.$$

The **Zsigmondy set of $\mathcal{D}$** specifies the terms that do not have a primitive prime divisor:

$$\mathcal{Z}(\mathcal{D}) := \{n \geq 1 : \mathfrak{D}_n \text{ has no primitive prime divisors}\}.$$

Primitive Prime Divisors and Zsigmondy Sets

Question: Which terms contain a "new" prime divisor?

Definition: Let $\mathcal{D} := (\mathfrak{D}_n)_{n\ge1}$ be a sequence of ideals. A **primitive prime divisor of $\mathfrak{D}_n$** is a prime ideal $\mathfrak{p}$ satisfying

$$\mathfrak{p} \mid \mathfrak{D}_n \quad \text{and} \quad \mathfrak{p} \nmid \mathfrak{D}_m \quad \text{for all } m < n.$$

The **Zsigmondy set of $\mathcal{D}$** specifies the terms that do not have a primitive prime divisor:

$$\mathcal{Z}(\mathcal{D}) := \{n \ge 1 : \mathfrak{D}_n \text{ has no primitive prime divisors}\}.$$

Some Sample Results:

- Bang/Zsigmondy (1886/92): $\mathcal{Z}(a^n - b^n) \subseteq \{1, 2, 6\}$.
- Carmichael (1913): $\mathcal{Z}(\text{Fibonacci sequence}) = \{1, 2, 6, 12\}$.
- Bilu–Hanrot–Voutier (2001):
  $$\mathcal{Z}(\text{Lucas/Lehmer sequence}) \subset \{1, 2, \dots, 30\}.$$
- JS (1988): $\mathcal{Z}(\text{elliptic divisibility sequence})$ is finite.

Primitive Prime Divisors in Abelian Divisibility Sequences

There are two ingredients that go into proofs that the Zsigmondy set of a sequence $\mathcal{D} = (\mathfrak{D}_n)_{n\ge 1}$ is finite:

- The sequence grows rapidly in norm, e.g.,
$$\log \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n \gg n^{\delta} \quad \text{for some } \delta > 1.$$
- The $\mathfrak{p}$-divisiblity does not grow too rapidly, e.g., let r be the smallest index with $\mathfrak{p} \mid \mathfrak{D}_r$, then
$$\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_{nr} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_r + O\big(\operatorname{ord}_{\mathfrak{p}}(n)\big).$$

Primitive Prime Divisors in Abelian Divisibility Sequences

There are two ingredients that go into proofs that the Zsigmondy set of a sequence $\mathcal{D} = (\mathfrak{D}_n)_{n\ge 1}$ is finite:

- The sequence grows rapidly in norm, e.g.,

$$\log \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n \gg n^\delta \quad \text{for some } \delta > 1.$$

- The $\mathfrak{p}$-divisiblity does not grow too rapidly, e.g., let r be the smallest index with $\mathfrak{p} \mid \mathfrak{D}_r$, then

$$\operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_{nr} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{D}_r + O\big(\operatorname{ord}_{\mathfrak{p}}(n)\big).$$

For ADS of Type I, the Ailon–Rudnick conjecture implies that $\mathcal{Z}(\mathcal{D})$ is infinite.

Primitive Prime Divisors in Abelian Divisibility Sequences

There are two ingredients that go into proofs that the Zsigmondy set of a sequence $\mathcal{D} = (\mathfrak{D}_n)_{n\ge1}$ is finite:

- The sequence grows rapidly in norm, e.g.,

$$\log \mathrm{N}_{K/\mathbb{Q}} \mathfrak{D}_n \gg n^\delta \quad \text{for some } \delta > 1.$$

- The $\mathfrak{p}$-divisiblity does not grow too rapidly, e.g., let r be the smallest index with $\mathfrak{p} \mid \mathfrak{D}_r$, then

$$\operatorname{ord}_\mathfrak{p} \mathfrak{D}_{nr} = \operatorname{ord}_\mathfrak{p} \mathfrak{D}_r + O\bigl(\operatorname{ord}_\mathfrak{p}(n)\bigr).$$

For ADS of Type I, the Ailon–Rudnick conjecture implies that $\mathcal{Z}(\mathcal{D})$ is infinite.

For ADS of Type II, we conjecturally have rapid norm growth, but $\mathfrak{p}$-divisibility when $\dim \ge 2$ is much less regular than for $\dim = 1$. Again, I've done experiments and have weak partial results for $\mathbb{G}_m^2$, but it would be very interesting to gather data for abelian surfaces.

Primes in Divisibility Sequences

Let $\mathcal{D} = (D_n)_{n\geq 1}$ be a divisibility sequence in $\mathbb{Z}$.

Natual Question: Are there infinitely many primes in the sequence $|D_n/D_1|$?

Primes in Divisibility Sequences

Let $\mathcal{D} = (D_n)_{n\geq 1}$ be a divisibility sequence in $\mathbb{Z}$.

Natual Question: Are there infinitely many primes in the sequence $|D_n/D_1|$?

Since $D_k \mid D_{mk}$, should consider $|D_p/D_1|$ with p prime.

Primes in Divisibility Sequences

Let $\mathcal{D} = (D_n)_{n\geq 1}$ be a divisibility sequence in $\mathbb{Z}$.

Natual Question: Are there infinitely many primes in the sequence $|D_n/D_1|$?

Since $D_k \mid D_{mk}$, should consider $|D_p/D_1|$ with p prime.

Three Guesses:

- For a $\mathbb{G}_m$-sequence, which typically satisfies

$$\log |D_n| \gg\ll n,$$

  we expect D_p/D_1 to be prime for infinitely many p.
  Example: Mersenne sequence $D_n = 2^n - 1$.

- For an EDS , which typically satisfies

$$\log |D_n| \gg\ll n^2,$$

  we expect D_p/D_1 to be prime for only finitely many p.

- Ditto for higher dimensional Type II ADS with

$$\log |D_n| \gg\ll n^d.$$

I want to thank the organizers,

Jenn, Noam, Brendan,

Bjorn, Drew, and John,

for inviting me to speak, and to thank you for your attention.

Abelian Divisibility Sequences

Joseph H. Silverman

Brown University

Arithmetic of Low-Dimensional Abelian Varietes

ICERM, June 3–7 2019