Greatest common divisors and Diophantine approximation

Aaron Levin

Michigan State University

The First JNT Biennial Conference
Cetraro, Italy

Greatest Common Divisors

- We'll be interested in greatest common divisors like

$$\gcd(2^n - 1, 3^n - 1), \quad n = 1, 2, 3, \ldots$$

- Let's compute some values:

n	$2^n - 1$	$3^n - 1$	$\gcd(2^n - 1, 3^n - 1)$
1	1	2	1
2	3	8	1
3	7	26	1
4	15	80	5
5	31	242	1
6	63	728	7
7	127	2186	1
8	255	6560	5
9	511	19862	1
10	1023	59048	11

$\gcd(2^n - 1, 3^n - 1)$

- We'll be interested in greatest common divisors like

$$\gcd(2^n - 1, 3^n - 1), \quad n = 1, 2, 3, \ldots$$

- Let's compute some values:

n	$2^n - 1$	$3^n - 1$	$\gcd(2^n - 1, 3^n - 1)$
1	1	2	1
2	3	8	1
3	7	26	1
4	15	80	5
5	31	242	1
6	63	728	7
7	127	2186	1
8	255	6560	5
9	511	19862	1
10	1023	59048	11

A question

- First question: Are there infinitely many $n \geq 1$ such that
$$\gcd(2^n - 1, 3^n - 1) = 1?$$
- Not known! Conjectured answer: yes.
- For integers a, b, let's look more generally at
$$\gcd(a^n - 1, b^n - 1).$$
- Note that $\gcd(a - 1, b - 1)$ divides $\gcd(a^n - 1, b^n - 1)$ for all positive n.

A question

- First question: Are there infinitely many $n \geq 1$ such that

$$\gcd(2^n - 1, 3^n - 1) = 1?$$

- Not known! Conjectured answer: yes.
- For integers a, b, let's look more generally at

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

- Note that $\gcd(a-1, b-1)$ divides $\gcd(a^n - 1, b^n - 1)$ for all positive n.

A question

- First question: Are there infinitely many $n \geq 1$ such that
$$\gcd(2^n - 1, 3^n - 1) = 1?$$
- Not known! Conjectured answer: yes.
- For integers a, b, let's look more generally at
$$\gcd(a^n - 1, b^n - 1).$$
- Note that $\gcd(a - 1, b - 1)$ divides $\gcd(a^n - 1, b^n - 1)$ for all positive n.

A question

- First question: Are there infinitely many $n \geq 1$ such that
$$\gcd(2^n - 1, 3^n - 1) = 1?$$
- Not known! Conjectured answer: yes.
- For integers a, b, let's look more generally at
$$\gcd(a^n - 1, b^n - 1).$$
- Note that $\gcd(a-1, b-1)$ divides $\gcd(a^n - 1, b^n - 1)$ for all positive n.

Multiplicative dependence

- Another observation: If $a = c^i$ and $b = c^j$ for some $i, j \geq 1$, then

$$a^n - 1 = (c^n)^i - 1,$$
$$b^n - 1 = (c^n)^j - 1,$$

and

$$(c^n - 1) \mid \gcd(a^n - 1, b^n - 1), \quad n \geq 1.$$

- In this case, a and b are multiplicatively dependent:

$$a^r = b^s$$

for some integers r, s, not both 0.

- Thus, if a, b are multiplicatively dependent then $\gcd(a^n - 1, b^n - 1)$ can grow exponentially.

Multiplicative dependence

- Another observation: If $a = c^i$ and $b = c^j$ for some $i, j \geq 1$, then

$$a^n - 1 = (c^n)^i - 1,$$
$$b^n - 1 = (c^n)^j - 1,$$

and

$$(c^n - 1) | \gcd(a^n - 1, b^n - 1), \quad n \geq 1.$$

- In this case, a and b are multiplicatively dependent:

$$a^r = b^s$$

for some integers r, s, not both 0.

- Thus, if a, b are multiplicatively dependent then $\gcd(a^n - 1, b^n - 1)$ can grow exponentially.

Multiplicative dependence

- Another observation: If $a = c^i$ and $b = c^j$ for some $i, j \geq 1$, then

$$a^n - 1 = (c^n)^i - 1,$$
$$b^n - 1 = (c^n)^j - 1,$$

and

$$(c^n - 1) | \gcd(a^n - 1, b^n - 1), \quad n \geq 1.$$

- In this case, a and b are multiplicatively dependent:

$$a^r = b^s$$

for some integers r, s, not both 0.

- Thus, if a, b are multiplicatively dependent then $\gcd(a^n - 1, b^n - 1)$ can grow exponentially.

Ailon-Rudnick Conjecture

Conjecture (Ailon-Rudnick)

If $a, b \in \mathbb{Z}$ are multiplicatively independent then there exist infinitely many $n \geq 1$ such that

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

- In particular, there should be infinitely many $n \geq 1$ such that

$$\gcd(2^n - 1, 3^n - 1) = 1.$$

- Conjecture seems very difficult. Ailon and Rudnick proved the analogous conjecture for polynomials $f, g \in \mathbb{C}[x]$.

Ailon-Rudnick Conjecture

Conjecture (Ailon-Rudnick)

If $a, b \in \mathbb{Z}$ are multiplicatively independent then there exist infinitely many $n \geq 1$ such that

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

- In particular, there should be infinitely many $n \geq 1$ such that

$$\gcd(2^n - 1, 3^n - 1) = 1.$$

- Conjecture seems very difficult. Ailon and Rudnick proved the analogous conjecture for polynomials $f, g \in \mathbb{C}[x]$.

Ailon-Rudnick Conjecture

Conjecture (Ailon-Rudnick)

If $a, b \in \mathbb{Z}$ are multiplicatively independent then there exist infinitely many $n \geq 1$ such that

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

- In particular, there should be infinitely many $n \geq 1$ such that

$$\gcd(2^n - 1, 3^n - 1) = 1.$$

- Conjecture seems very difficult. Ailon and Rudnick proved the analogous conjecture for polynomials $f, g \in \mathbb{C}[x]$.

Upper bounds for $\gcd(2^n - 1, 3^n - 1)$

- Now look at upper bounds.
- How large can $\gcd(2^n - 1, 3^n - 1)$ be?
- Let's look at entries from our table with $\gcd(2^n - 1, 3^n - 1) > 1$:

n	$2^n - 1$	$3^n - 1$	$\gcd(2^n - 1, 3^n - 1)$
4	15	80	5
6	63	728	7
8	255	6560	5
10	1023	59048	11

Upper bounds for $\gcd(2^n - 1, 3^n - 1)$

- Now look at upper bounds.
- How large can $\gcd(2^n - 1, 3^n - 1)$ be?
- Let's look at entries from our table with $\gcd(2^n - 1, 3^n - 1) > 1$:

n	$2^n - 1$	$3^n - 1$	$\gcd(2^n - 1, 3^n - 1)$
4	15	80	5
6	63	728	7
8	255	6560	5
10	1023	59048	11

Upper bounds for $\gcd(2^n - 1, 3^n - 1)$

- Now look at upper bounds.
- How large can $\gcd(2^n - 1, 3^n - 1)$ be?
- Let's look at entries from our table with $\gcd(2^n - 1, 3^n - 1) > 1$:

n	$2^n - 1$	$3^n - 1$	$\gcd(2^n - 1, 3^n - 1)$
4	15	80	5
6	63	728	7
8	255	6560	5
10	1023	59048	11

Fermat's little theorem

- All the nontrivial gcds in the table come from Fermat's little theorem:

$$n^{p-1} \equiv 1 \pmod{p}$$

for any prime p and integer n with $p \nmid n$.

- So for any prime $p \neq 2, 3$,

$$p | \gcd(2^{p-1} - 1, 3^{p-1} - 1).$$

- We can try to make $\gcd(2^n - 1, 3^n - 1)$ large by finding n so that $p - 1$ divides n for many primes p.

Fermat's little theorem

- All the nontrivial gcds in the table come from Fermat's little theorem:

$$n^{p-1} \equiv 1 \pmod{p}$$

for any prime p and integer n with $p \nmid n$.

- So for any prime $p \neq 2, 3$,

$$p \mid \gcd(2^{p-1} - 1, 3^{p-1} - 1).$$

- We can try to make $\gcd(2^n - 1, 3^n - 1)$ large by finding n so that $p - 1$ divides n for many primes p.

Fermat's little theorem

- All the nontrivial gcds in the table come from Fermat's little theorem:

$$n^{p-1} \equiv 1 \pmod{p}$$

  for any prime p and integer n with $p \nmid n$.
- So for any prime $p \neq 2, 3$,

$$p \mid \gcd(2^{p-1} - 1, 3^{p-1} - 1).$$

- We can try to make $\gcd(2^n - 1, 3^n - 1)$ large by finding n so that $p - 1$ divides n for many primes p.

- In this direction, we have:

Theorem (Adleman, Pomerance, Rumely)

There exists a constant $C > 0$ such that

$$\#\{p : p \text{ is prime, } (p-1)|n\} > e^{C \log n / \log\log n}$$

holds for infinitely many positive integers n.

- Using Fermat's theorem this easily gives:

$$\log \gcd(2^n - 1, 3^n - 1) > e^{C \log n / \log\log n}$$

for infinitely many positive integers n and some constant $C > 0$.

A lower bound

- In this direction, we have:

Theorem (Adleman, Pomerance, Rumely)

There exists a constant $C > 0$ such that

$$\#\{p : p \text{ is prime, } (p-1)|n\} > e^{C \log n / \log \log n}$$

holds for infinitely many positive integers n.

- Using Fermat's theorem this easily gives:

$$\log \gcd(2^n - 1, 3^n - 1) > e^{C \log n / \log \log n}$$

for infinitely many positive integers n and some constant $C > 0$.

A lower bound

- In this direction, we have:

Theorem (Adleman, Pomerance, Rumely)

There exists a constant $C > 0$ such that

$$\#\{p : p \text{ is prime, } (p-1)|n\} > e^{C \log n / \log\log n}$$

holds for infinitely many positive integers n.

- Using Fermat's theorem this easily gives:

$$\log \gcd(2^n - 1, 3^n - 1) > e^{C \log n / \log\log n}$$

for infinitely many positive integers n and some constant $C > 0$.

Bugeaud-Corvaja-Zannier theorem

- In the other direction, an upper bound was given by Bugeaud, Corvaja, and Zannier in 2003.

Theorem (Bugeaud, Corvaja, Zannier)

Let $a, b \in \mathbb{Z}$ be multiplicatively independent integers. Then for every $\epsilon > 0$,

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

for all but finitely many positive integers n.

- In view of the previous lower bound, the result is reasonably close to optimal.
- Proof uses the deep Schmidt Subspace Theorem from Diophantine approximation.

Bugeaud-Corvaja-Zannier theorem

- In the other direction, an upper bound was given by Bugeaud, Corvaja, and Zannier in 2003.

Theorem (Bugeaud, Corvaja, Zannier)

Let $a, b \in \mathbb{Z}$ be multiplicatively independent integers. Then for every $\epsilon > 0$,

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

for all but finitely many positive integers n.

- In view of the previous lower bound, the result is reasonably close to optimal.
- Proof uses the deep Schmidt Subspace Theorem from Diophantine approximation.

Bugeaud-Corvaja-Zannier theorem

- In the other direction, an upper bound was given by Bugeaud, Corvaja, and Zannier in 2003.

Theorem (Bugeaud, Corvaja, Zannier)

Let $a, b \in \mathbb{Z}$ be multiplicatively independent integers. Then for every $\epsilon > 0$,

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

for all but finitely many positive integers n.

- In view of the previous lower bound, the result is reasonably close to optimal.
- Proof uses the deep Schmidt Subspace Theorem from Diophantine approximation.

Bugeaud-Corvaja-Zannier theorem

- In the other direction, an upper bound was given by Bugeaud, Corvaja, and Zannier in 2003.

Theorem (Bugeaud, Corvaja, Zannier)

Let $a, b \in \mathbb{Z}$ be multiplicatively independent integers. Then for every $\epsilon > 0$,

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

for all but finitely many positive integers n.

- In view of the previous lower bound, the result is reasonably close to optimal.
- Proof uses the deep Schmidt Subspace Theorem from Diophantine approximation.

$\gcd(u-1, v-1)$

- Now discuss several generalizations.
- First, let $S = \{\infty, p_1, \ldots, p_m\}$ be a set of primes and

$$\mathbb{Z}_S^* = \{\pm p_1^{i_1} \cdots p_m^{i_m} \mid i_1, \ldots, i_m \in \mathbb{Z}\}$$

  be the group of S-units in $\mathbb{Q}$.
- Corvaja and Zannier and, independently, Hernández and Luca, generalized Bugeaud-Corvaja-Zannier's result:

Theorem (Corvaja-Zannier, Hernández-Luca)

For every $\epsilon > 0$,

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

for all but finitely many multiplicatively independent S-unit integers $u, v \in \mathbb{Z}_S^*$.

$\gcd(u-1, v-1)$

- Now discuss several generalizations.
- First, let $S = \{\infty, p_1, \ldots, p_m\}$ be a set of primes and

$$\mathbb{Z}_S^* = \{\pm p_1^{i_1} \cdots p_m^{i_m} \mid i_1, \ldots, i_m \in \mathbb{Z}\}$$

  be the group of S-units in $\mathbb{Q}$.
- Corvaja and Zannier and, independently, Hernández and Luca, generalized Bugeaud-Corvaja-Zannier's result:

Theorem (Corvaja-Zannier, Hernández-Luca)

For every $\epsilon > 0$,

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

for all but finitely many multiplicatively independent S-unit integers $u, v \in \mathbb{Z}_S^*$.

$\gcd(u-1, v-1)$

- Now discuss several generalizations.
- First, let $S = \{\infty, p_1, \ldots, p_m\}$ be a set of primes and

$$\mathbb{Z}_S^* = \{\pm p_1^{i_1} \cdots p_m^{i_m} \mid i_1, \ldots, i_m \in \mathbb{Z}\}$$

  be the group of S-units in $\mathbb{Q}$.
- Corvaja and Zannier and, independently, Hernández and Luca, generalized Bugeaud-Corvaja-Zannier's result:

Theorem (Corvaja-Zannier, Hernández-Luca)

For every $\epsilon > 0$,

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

for all but finitely many multiplicatively independent S-unit integers $u, v \in \mathbb{Z}_S^*$.

- Now discuss several generalizations.
- First, let $S = \{\infty, p_1, \ldots, p_m\}$ be a set of primes and

$$\mathbb{Z}_S^* = \{\pm p_1^{i_1} \cdots p_m^{i_m} \mid i_1, \ldots, i_m \in \mathbb{Z}\}$$

  be the group of S-units in $\mathbb{Q}$.
- Corvaja and Zannier and, independently, Hernández and Luca, generalized Bugeaud-Corvaja-Zannier's result:

Theorem (Corvaja-Zannier, Hernández-Luca)

For every $\epsilon > 0$,

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

for all but finitely many multiplicatively independent S-unit integers $u, v \in \mathbb{Z}_S^*$.

Generalized logarithmic greatest common divisor

- Define the (generalized) logarithmic greatest common divisor of $\alpha, \beta \in \bar{\mathbb{Q}}$ (not both zero) by

$$\log \gcd(\alpha, \beta) = h([1 : \alpha : \beta]) - h([\alpha : \beta]),$$

where h is the usual absolute logarithmic height on projective space.

- Alternatively, if α and β are in a number field k:

$$\log \gcd(\alpha, \beta) = -\sum_{v \in M_k} \log^- \max\{|\alpha|_v, |\beta|_v\},$$

where $\log^- z = \min\{0, \log z\}$ and $M_k =$ set of places of k.

- This generalizes the gcd for integers, and notably includes an archimedean contribution.

Generalized logarithmic greatest common divisor

- Define the (generalized) logarithmic greatest common divisor of $\alpha, \beta \in \bar{\mathbb{Q}}$ (not both zero) by

$$\log \gcd(\alpha, \beta) = h([1 : \alpha : \beta]) - h([\alpha : \beta]),$$

  where h is the usual absolute logarithmic height on projective space.
- Alternatively, if α and β are in a number field k:

$$\log \gcd(\alpha, \beta) = -\sum_{v \in M_k} \log^- \max\{|\alpha|_v, |\beta|_v\},$$

  where $\log^- z = \min\{0, \log z\}$ and $M_k =$ set of places of k.
- This generalizes the gcd for integers, and notably includes an archimedean contribution.

Generalized logarithmic greatest common divisor

- Define the (generalized) logarithmic greatest common divisor of $\alpha, \beta \in \bar{\mathbb{Q}}$ (not both zero) by

$$\log \gcd(\alpha, \beta) = h([1 : \alpha : \beta]) - h([\alpha : \beta]),$$

  where h is the usual absolute logarithmic height on projective space.
- Alternatively, if α and β are in a number field k:

$$\log \gcd(\alpha, \beta) = -\sum_{v \in M_k} \log^- \max\{|\alpha|_v, |\beta|_v\},$$

  where $\log^- z = \min\{0, \log z\}$ and M_k = set of places of k.
- This generalizes the gcd for integers, and notably includes an archimedean contribution.

Multiplicative independence

- Also want to rephrase the multiplicative independence condition.
- Let $\mathbb{G}_m^n$ denote the n-dimensional algebraic torus, where $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{A}^1 \setminus \{0\}$.
- Then $\mathbb{G}_m^n(k) \cong (k^*)^n$ with the obvious group structure coming from coordinate-wise multiplication.
- The condition that u and v are multiplicatively independent can be rephrased as saying that (u, v) is not an element of a proper algebraic subgroup of $\mathbb{G}_m^2$ (subtorus).

Multiplicative independence

- Also want to rephrase the multiplicative independence condition.
- Let $\mathbb{G}_m^n$ denote the n-dimensional algebraic torus, where $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{A}^1 \setminus \{0\}$.
- Then $\mathbb{G}_m^n(k) \cong (k^*)^n$ with the obvious group structure coming from coordinate-wise multiplication.
- The condition that u and v are multiplicatively independent can be rephrased as saying that (u, v) is not an element of a proper algebraic subgroup of $\mathbb{G}_m^2$ (subtorus).

Multiplicative independence

- Also want to rephrase the multiplicative independence condition.
- Let $\mathbb{G}_m^n$ denote the n-dimensional algebraic torus, where $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{A}^1 \setminus \{0\}$.
- Then $\mathbb{G}_m^n(k) \cong (k^*)^n$ with the obvious group structure coming from coordinate-wise multiplication.
- The condition that u and v are multiplicatively independent can be rephrased as saying that (u, v) is not an element of a proper algebraic subgroup of $\mathbb{G}_m^2$ (subtorus).

Multiplicative independence

- Also want to rephrase the multiplicative independence condition.
- Let $\mathbb{G}_m^n$ denote the n-dimensional algebraic torus, where $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{A}^1 \setminus \{0\}$.
- Then $\mathbb{G}_m^n(k) \cong (k^*)^n$ with the obvious group structure coming from coordinate-wise multiplication.
- The condition that u and v are multiplicatively independent can be rephrased as saying that (u, v) is not an element of a proper algebraic subgroup of $\mathbb{G}_m^2$ (subtorus).

An explicit result

- In fact, Corvaja and Zannier show that

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

holds outside of the union of finitely many proper subtori of $\mathbb{G}_m^2$ along with a finite number of exceptions.

- Explicitly, one needs to exclude subgroups given by an equation $u^p = v^q$ with p and q coprime integers satisfying $|p|, |q| \leq 1/\epsilon$.

An explicit result

- In fact, Corvaja and Zannier show that

$$\log \gcd(u-1, v-1) \leq \epsilon \max\{\log |u|, \log |v|\}$$

holds outside of the union of finitely many proper subtori of $\mathbb{G}_m^2$ along with a finite number of exceptions.

- Explicitly, one needs to exclude subgroups given by an equation $u^p = v^q$ with p and q coprime integers satisfying $|p|, |q| \leq 1/\epsilon$.

Corvaja-Zannier theorem

- Corvaja and Zannier generalized their result to:
  - Arbitrary number fields.
  - Polynomials in u and v.

Theorem (Corvaja, Zannier)

Let $\Gamma \subset \mathbb{G}_m^2(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x,y), g(x,y) \in \bar{\mathbb{Q}}[x,y]$ be coprime polynomials such that not both of them vanish at $(0,0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^2$ such that

$$\log \gcd(f(u,v), g(u,v)) < \epsilon \max\{h(u), h(v)\}$$

for all $(u,v) \in \Gamma \setminus Z$.

Corvaja-Zannier theorem

- Corvaja and Zannier generalized their result to:
  - Arbitrary number fields.
  - Polynomials in u and v.

Theorem (Corvaja, Zannier)

Let $\Gamma \subset \mathbb{G}_m^2(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x,y), g(x,y) \in \bar{\mathbb{Q}}[x,y]$ be coprime polynomials such that not both of them vanish at $(0,0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^2$ such that

$$\log \gcd(f(u,v), g(u,v)) < \epsilon \max\{h(u), h(v)\}$$

for all $(u,v) \in \Gamma \setminus Z$.

Corvaja-Zannier theorem

- Corvaja and Zannier generalized their result to:
  - Arbitrary number fields.
  - Polynomials in u and v.

Theorem (Corvaja, Zannier)

Let $\Gamma \subset \mathbb{G}_m^2(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x,y), g(x,y) \in \bar{\mathbb{Q}}[x,y]$ be coprime polynomials such that not both of them vanish at $(0,0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^2$ such that

$$\log \gcd(f(u,v), g(u,v)) < \epsilon \max\{h(u), h(v)\}$$

for all $(u,v) \in \Gamma \setminus Z$.

Corvaja-Zannier theorem

- Corvaja and Zannier generalized their result to:
  - Arbitrary number fields.
  - Polynomials in u and v.

Theorem (Corvaja, Zannier)

Let $\Gamma \subset \mathbb{G}_m^2(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x,y), g(x,y) \in \bar{\mathbb{Q}}[x,y]$ be coprime polynomials such that not both of them vanish at $(0,0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^2$ such that

$$\log \gcd(f(u,v), g(u,v)) < \epsilon \max\{h(u), h(v)\}$$

for all $(u,v) \in \Gamma \setminus Z$.

A generalization to several variables

- Main result:

Theorem (L.)

Let n be a positive integer. Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in \bar{\mathbb{Q}}[x_1, \dots, x_n]$ be coprime polynomials such that not both of them vanish at $(0, 0, \dots, 0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$\log \gcd(f(u_1, \dots, u_n), g(u_1, \dots, u_n)) < \epsilon \max\{h(u_1), \dots, h(u_n)\}$$

for all $(u_1, \dots, u_n) \in \Gamma \setminus Z$.

- Can avoid nonvanishing hypothesis: if $u_1, \dots, u_n$ are S-units, replace the gcd by the “gcd outside S”.

A generalization to several variables

- Main result:

Theorem (L.)

Let n be a positive integer. Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in \bar{\mathbb{Q}}[x_1, \dots, x_n]$ be coprime polynomials such that not both of them vanish at $(0, 0, \dots, 0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$\log \gcd(f(u_1, \dots, u_n), g(u_1, \dots, u_n)) < \epsilon \max\{h(u_1), \dots, h(u_n)\}$$

for all $(u_1, \dots, u_n) \in \Gamma \setminus Z$.

- Can avoid nonvanishing hypothesis: if $u_1, \dots, u_n$ are S-units, replace the gcd by the "gcd outside S".

A generalization to several variables

- Main result:

Theorem (L.)

Let n be a positive integer. Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group. Let $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \bar{\mathbb{Q}}[x_1, \ldots, x_n]$ be coprime polynomials such that not both of them vanish at $(0, 0, \ldots, 0)$. For all $\epsilon > 0$, there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$\log \gcd(f(u_1, \ldots, u_n), g(u_1, \ldots, u_n)) < \epsilon \max\{h(u_1), \ldots, h(u_n)\}$$

for all $(u_1, \ldots, u_n) \in \Gamma \setminus Z$.

- Can avoid nonvanishing hypothesis: if $u_1, \ldots, u_n$ are S-units, replace the gcd by the "gcd outside S".

Height interpretation

Height reformulation

- Classically, a height function h_D and local height functions $h_{D,v}$, $v \in M_k$, can be associated to a Cartier divisor D on a projective variety X.
- Let D be a hypersurface over k in $\mathbb{P}^n$ of degree d defined by $f(x_0, \ldots, x_n) = 0$ and let $v \in M_k$.
- A *local height function* with respect to D and v is:

$$h_{D,v}(P) = \log \frac{\max |x_i|_v^d}{|f(x_0, \ldots, x_n)|_v}, \qquad \text{for } P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k).$$

- Roughly, when D is effective:

$$h_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

Height reformulation

- Classically, a height function h_D and local height functions $h_{D,v}$, $v \in M_k$, can be associated to a Cartier divisor D on a projective variety X.
- Let D be a hypersurface over k in $\mathbb{P}^n$ of degree d defined by $f(x_0, \ldots, x_n) = 0$ and let $v \in M_k$.
- A *local height function* with respect to D and v is:

$$h_{D,v}(P) = \log \frac{\max |x_i|_v^d}{|f(x_0, \ldots, x_n)|_v}, \qquad \text{for } P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k).$$

- Roughly, when D is effective:

$$h_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

Height reformulation

- Classically, a height function h_D and local height functions $h_{D,v}$, $v \in M_k$, can be associated to a Cartier divisor D on a projective variety X.
- Let D be a hypersurface over k in $\mathbb{P}^n$ of degree d defined by $f(x_0, \ldots, x_n) = 0$ and let $v \in M_k$.
- A *local height function* with respect to D and v is:

$$h_{D,v}(P) = \log \frac{\max |x_i|_v^d}{|f(x_0, \ldots, x_n)|_v}, \qquad \text{for } P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k).$$

- Roughly, when D is effective:

$$h_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

Height reformulation

- Classically, a height function h_D and local height functions $h_{D,v}$, $v \in M_k$, can be associated to a Cartier divisor D on a projective variety X.
- Let D be a hypersurface over k in $\mathbb{P}^n$ of degree d defined by $f(x_0, \ldots, x_n) = 0$ and let $v \in M_k$.
- A *local height function* with respect to D and v is:

$$h_{D,v}(P) = \log \frac{\max |x_i|_v^d}{|f(x_0, \ldots, x_n)|_v}, \qquad \text{for } P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k).$$

- Roughly, when D is effective:

$$h_{D,v}(P) = -\log(v\text{-adic distance from } P \text{ to } D).$$

Heights associated to closed subschemes

- More generally, can associate heights and local heights to closed subschemes of projective varieties (Silverman).
- For Y, Z closed subschemes, a basic property is that

$$h_{Y\cap Z,v}(P) = \min\{h_{Y,v}(P), h_{Z,v}(P)\}.$$

- So if D_1 and D_2 are hypersurfaces of the same degree d defined by $f_1, f_2 \in k[x_0, \ldots, x_n]$, respectively, then

$$h_{D_1\cap D_2,v}(P) = \log \frac{\max |x_i|_v^d}{\max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}}.$$

Heights associated to closed subschemes

- More generally, can associate heights and local heights to closed subschemes of projective varieties (Silverman).
- For Y, Z closed subschemes, a basic property is that

$$h_{Y\cap Z,v}(P) = \min\{h_{Y,v}(P), h_{Z,v}(P)\}.$$

- So if D_1 and D_2 are hypersurfaces of the same degree d defined by $f_1, f_2 \in k[x_0, \ldots, x_n]$, respectively, then

$$h_{D_1\cap D_2,v}(P) = \log \frac{\max |x_i|_v^d}{\max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}}.$$

Heights associated to closed subschemes

- More generally, can associate heights and local heights to closed subschemes of projective varieties (Silverman).
- For Y, Z closed subschemes, a basic property is that

$$h_{Y\cap Z,v}(P) = \min\{h_{Y,v}(P), h_{Z,v}(P)\}.$$

- So if D_1 and D_2 are hypersurfaces of the same degree d defined by $f_1, f_2 \in k[x_0, \ldots, x_n]$, respectively, then

$$h_{D_1\cap D_2,v}(P) = \log \frac{\max |x_i|_v^d}{\max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}}.$$

Gcd heights

- If $P = [x_0 : \cdots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, then for any prime $v = p$,

$$h_{D_1 \cap D_2, v}(P) = -\log \max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}.$$

- If $Y = D_1 \cap D_2$, the closed subscheme defined by $f_1 = f_2 = 0$, then in this case

$$\sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} h_{Y,v}(P) = \log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n)).$$

- So the height $h_Y(P)$ generalizes $\log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n))$, including a contribution from archimedean places.
- Point: GCDs are heights with respect to closed subschemes of codimension ≥ 2.

Gcd heights

- If $P = [x_0 : \cdots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, then for any prime $v = p$,

$$h_{D_1 \cap D_2, v}(P) = -\log \max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}.$$

- If $Y = D_1 \cap D_2$, the closed subscheme defined by $f_1 = f_2 = 0$, then in this case

$$\sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} h_{Y,v}(P) = \log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n)).$$

- So the height $h_Y(P)$ generalizes $\log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n))$, including a contribution from archimedean places.
- Point: GCDs are heights with respect to closed subschemes of codimension ≥ 2.

Gcd heights

- If $P = [x_0 : \cdots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, then for any prime $v = p$,

$$h_{D_1 \cap D_2, v}(P) = -\log \max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}.$$

- If $Y = D_1 \cap D_2$, the closed subscheme defined by $f_1 = f_2 = 0$, then in this case

$$\sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} h_{Y,v}(P) = \log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n)).$$

- So the height $h_Y(P)$ generalizes $\log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n))$, including a contribution from archimedean places.
- Point: GCDs are heights with respect to closed subschemes of codimension ≥ 2.

Gcd heights

- If $P = [x_0 : \cdots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, then for any prime $v = p$,

$$h_{D_1 \cap D_2, v}(P) = -\log \max\{|f_1(x_0, \ldots, x_n)|_v, |f_2(x_0, \ldots, x_n)|_v\}.$$

- If $Y = D_1 \cap D_2$, the closed subscheme defined by $f_1 = f_2 = 0$, then in this case

$$\sum_{v \in M_{\mathbb{Q}} \setminus \{\infty\}} h_{Y,v}(P) = \log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n)).$$

- So the height $h_Y(P)$ generalizes $\log \gcd(f_1(x_0, \ldots, x_n), f_2(x_0, \ldots, x_n))$, including a contribution from archimedean places.
- Point: GCDs are heights with respect to closed subschemes of codimension ≥ 2.

- We can state a projective version of the main theorem for the “gcd height" h_Y as follows.

Theorem (L.)

Let Y be a closed subscheme of codimension ≥ 2 in $\mathbb{P}^n$ in general position with the coordinate hyperplanes (boundary of $\mathbb{G}_m^n$). Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group and $\epsilon > 0$. Then there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$h_Y(P) \leq \epsilon h(P)$$

for all $P \in \Gamma \setminus Z \subset \mathbb{P}^n(\bar{\mathbb{Q}})$.

- Not quite equivalent to the earlier main theorem, but they're closely related (and the earlier one implies this one).

Height formulation of main theorem

- We can state a projective version of the main theorem for the “gcd height" h_Y as follows.

Theorem (L.)

Let Y be a closed subscheme of codimension ≥ 2 in $\mathbb{P}^n$ in general position with the coordinate hyperplanes (boundary of $\mathbb{G}_m^n$). Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group and $\epsilon > 0$. Then there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$h_Y(P) \leq \epsilon h(P)$$

for all $P \in \Gamma \setminus Z \subset \mathbb{P}^n(\bar{\mathbb{Q}})$.

- Not quite equivalent to the earlier main theorem, but they're closely related (and the earlier one implies this one).

Height formulation of main theorem

- We can state a projective version of the main theorem for the “gcd height" h_Y as follows.

Theorem (L.)

Let Y be a closed subscheme of codimension ≥ 2 in $\mathbb{P}^n$ in general position with the coordinate hyperplanes (boundary of $\mathbb{G}_m^n$). Let $\Gamma \subset \mathbb{G}_m^n(\bar{\mathbb{Q}})$ be a finitely generated group and $\epsilon > 0$. Then there exists a finite union Z of translates of proper subtori of $\mathbb{G}_m^n$ such that

$$h_Y(P) \leq \epsilon h(P)$$

for all $P \in \Gamma \setminus Z \subset \mathbb{P}^n(\bar{\mathbb{Q}})$.

- Not quite equivalent to the earlier main theorem, but they're closely related (and the earlier one implies this one).

- General position condition:

$$[1:0:\cdots:0],\ldots,[0:0:\cdots:0:1]\notin Y.$$

- It is a symmetric version of the earlier condition that the polynomials don't vanish at the origin.
- More generally, prove a completely analogous result for $\mathbb{G}_m^n \subset X$ where X is a nonsingular projective toric variety.

Toric varieties

- General position condition:

$$[1:0:\cdots:0],\ldots,[0:0:\cdots:0:1]\notin Y.$$

- It is a symmetric version of the earlier condition that the polynomials don't vanish at the origin.
- More generally, prove a completely analogous result for $\mathbb{G}_m^n \subset X$ where X is a nonsingular projective toric variety.

Toric varieties

- General position condition:

$$[1:0:\cdots:0],\ldots,[0:0:\cdots:0:1]\notin Y.$$

- It is a symmetric version of the earlier condition that the polynomials don't vanish at the origin.
- More generally, prove a completely analogous result for $\mathbb{G}_m^n \subset X$ where X is a nonsingular projective toric variety.

Blowups and Vojta's conjecture

- Alternatively, if $\pi : X \to \mathbb{P}^n$ is the blowup along Y with exceptional divisor E, then by functoriality of heights

$$h_Y(\pi(P)) = h_E(P) + O(1), \quad \forall P \in X(\bar{\mathbb{Q}}).$$

- One can interpret the main result in terms of heights on blowups.
- GCD inequalities turn out to be cases of Vojta's conjecture applied to blowups (Silverman).

Blowups and Vojta's conjecture

- Alternatively, if $\pi : X \to \mathbb{P}^n$ is the blowup along Y with exceptional divisor E, then by functoriality of heights

$$h_Y(\pi(P)) = h_E(P) + O(1), \quad \forall P \in X(\bar{\mathbb{Q}}).$$

- One can interpret the main result in terms of heights on blowups.
- GCD inequalities turn out to be cases of Vojta's conjecture applied to blowups (Silverman).

- Alternatively, if $\pi : X \to \mathbb{P}^n$ is the blowup along Y with exceptional divisor E, then by functoriality of heights

$$h_Y(\pi(P)) = h_E(P) + O(1), \quad \forall P \in X(\bar{\mathbb{Q}}).$$

- One can interpret the main result in terms of heights on blowups.
- GCD inequalities turn out to be cases of Vojta's conjecture applied to blowups (Silverman).

Application: Greatest common divisors in linear recurrence sequences

Linear recurrence sequences

- Linear recurrence sequence: sequence of complex numbers $F(n)$, $n \in \mathbb{N}$, that satisfies a relation

$$F(n) = a_1 F(n-1) + \cdots + a_r F(n-r), \quad n > r,$$

for some constants $a_i \in \mathbb{C}$.

- $F(n)$ is a linear recurrence sequence if and only if

$$F(n) = \sum_{i=1}^{s} f_i(n) \alpha_i^n, \quad n \in \mathbb{N},$$

for some nonzero polynomials $f_i \in \mathbb{C}[x]$ and distinct $\alpha_i \in \mathbb{C}^*$, classically called the *roots* of F.

- The roots are exactly the distinct roots of the corresponding characteristic polynomial

$$X^r - a_1 X^{r-1} - \cdots - a_r.$$

Linear recurrence sequences

- Linear recurrence sequence: sequence of complex numbers $F(n)$, $n \in \mathbb{N}$, that satisfies a relation

$$F(n) = a_1 F(n-1) + \cdots + a_r F(n-r), \quad n > r,$$

for some constants $a_i \in \mathbb{C}$.

- $F(n)$ is a linear recurrence sequence if and only if

$$F(n) = \sum_{i=1}^{s} f_i(n)\alpha_i^n, \quad n \in \mathbb{N},$$

for some nonzero polynomials $f_i \in \mathbb{C}[x]$ and distinct $\alpha_i \in \mathbb{C}^*$, classically called the *roots* of F.

- The roots are exactly the distinct roots of the corresponding characteristic polynomial

$$X^r - a_1 X^{r-1} - \cdots - a_r.$$

Linear recurrence sequences

- Linear recurrence sequence: sequence of complex numbers $F(n)$, $n \in \mathbb{N}$, that satisfies a relation

$$F(n) = a_1 F(n-1) + \cdots + a_r F(n-r), \quad n > r,$$

  for some constants $a_i \in \mathbb{C}$.
- $F(n)$ is a linear recurrence sequence if and only if

$$F(n) = \sum_{i=1}^{s} f_i(n)\alpha_i^n, \quad n \in \mathbb{N},$$

  for some nonzero polynomials $f_i \in \mathbb{C}[x]$ and distinct $\alpha_i \in \mathbb{C}^*$, classically called the *roots* of F.
- The roots are exactly the distinct roots of the corresponding characteristic polynomial

$$X^r - a_1 X^{r-1} - \cdots - a_r.$$

Simple linear recurrences

- A linear recurrence is called *simple* if it has the form

$$F(n) = \sum_{i=1}^{r} c_i \alpha_i^n, \quad n \in \mathbb{N},$$

  where $\alpha_i, c_i \in \mathbb{C}^*$, $i = 1, \ldots, r$.
- This happens if and only if the roots of the associated characteristic polynomial are distinct (simple roots).
- A simple linear recurrence is *algebraic* if $\alpha_i, c_i \in \bar{\mathbb{Q}}$ for $i = 1, \ldots, n$.

Simple linear recurrences

- A linear recurrence is called *simple* if it has the form

$$F(n) = \sum_{i=1}^{r} c_i \alpha_i^n, \quad n \in \mathbb{N},$$

  where $\alpha_i, c_i \in \mathbb{C}^*$, $i = 1, \ldots, r$.
- This happens if and only if the roots of the associated characteristic polynomial are distinct (simple roots).
- A simple linear recurrence is *algebraic* if $\alpha_i, c_i \in \bar{\mathbb{Q}}$ for $i = 1, \ldots, n$.

Simple linear recurrences

- A linear recurrence is called *simple* if it has the form

$$F(n) = \sum_{i=1}^{r} c_i \alpha_i^n, \quad n \in \mathbb{N},$$

  where $\alpha_i, c_i \in \mathbb{C}^*$, $i = 1, \ldots, r$.
- This happens if and only if the roots of the associated characteristic polynomial are distinct (simple roots).
- A simple linear recurrence is *algebraic* if $\alpha_i, c_i \in \bar{\mathbb{Q}}$ for $i = 1, \ldots, n$.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a "large" gcd.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a “large" gcd.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a "large" gcd.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a "large" gcd.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a "large" gcd.

A philosophy

- Philosophy: Arithmetic properties of $F(n)$ and $G(n)$ holding for all (or infinitely many) n, should be explained by corresponding identities involving F and G (in the ring of linear recurrences).
- Examples include:
  - Divisibility: Hadamard quotient theorem (Pourchet, van der Poorten, Corvaja-Zannier (strong version))
  - Perfect powers: Pisot's dth root conjecture (Zannier)
- Consider this in the context of greatest common divisors.
- Classification of terms from two algebraic simple linear recurrences that have a “large" gcd.

Greatest common divisors of linear recurrence terms

Theorem (L.)

Let F and G be two algebraic simple linear recurrences. Suppose that there is no prime dividing every root of F and G. Let $\epsilon > 0$. Then all but finitely many solutions (m, n) of the inequality

$$\log \gcd(F(m), G(n)) > \epsilon \max\{m, n\}$$

satisfy one of finitely many linear relations

$$(m, n) = (a_i t + b_i, c_i t + d_i), \quad t \in \mathbb{Z}, i = 1, \ldots, r,$$

where $a_i, b_i, c_i, d_i \in \mathbb{Z}$, $a_i c_i \neq 0$, and the linear recurrences $F(a_i n + b_i)$ and $G(c_i n + d_i)$ have a nontrivial common factor for $i = 1, \ldots, r$.

- This result was recently generalized to $\log \gcd(F(n), G(n))$ and general linear recurrences by Grieve and Wang (i.e., without the simple hypothesis).
- Proven as an application of a “moving targets" version of the main result.
- My student Zheng Xiao is currently proving further results for $\log \gcd(F(m), G(n))$ for general linear recurrences.

- This result was recently generalized to $\log \gcd(F(n), G(n))$ and general linear recurrences by Grieve and Wang (i.e., without the simple hypothesis).
- Proven as an application of a “moving targets" version of the main result.
- My student Zheng Xiao is currently proving further results for $\log \gcd(F(m), G(n))$ for general linear recurrences.

- This result was recently generalized to $\log \gcd(F(n), G(n))$ and general linear recurrences by Grieve and Wang (i.e., without the simple hypothesis).
- Proven as an application of a “moving targets" version of the main result.
- My student Zheng Xiao is currently proving further results for $\log \gcd(F(m), G(n))$ for general linear recurrences.

Greatest Common Divisors and Meromorphic Functions

Vojta's dictionary

- Deep analogies between Diophantine approximation and Nevanlinna theory (Vojta's dictionary)
- Qualitative level: infinite set of integral points on a variety X corresponds to a nonconstant holomorphic map $f : \mathbb{C} \to X$.
- Entire functions without zeros are analogous to S-units.

- Deep analogies between Diophantine approximation and Nevanlinna theory (Vojta's dictionary)
- Qualitative level: infinite set of integral points on a variety X corresponds to a nonconstant holomorphic map $f : \mathbb{C} \to X$.
- Entire functions without zeros are analogous to S-units.

Vojta's dictionary

- Deep analogies between Diophantine approximation and Nevanlinna theory (Vojta's dictionary)
- Qualitative level: infinite set of integral points on a variety X corresponds to a nonconstant holomorphic map $f : \mathbb{C} \to X$.
- Entire functions without zeros are analogous to S-units.

GCD Counting Function

- Let f and g be meromorphic functions. Define

$$n(f,g,r) = \sum_{|z|\leq r} \min\{\mathrm{ord}_z^+(f), \mathrm{ord}_z^+(g)\},$$

$$N_{\mathrm{gcd}}(f,g,r) = \int_0^r \frac{n(f,g,t)-n(f,g,0)}{t}\,dt + n(f,g,0)\log r,$$

- The gcd counting function $N_{\mathrm{gcd}}(f,g,r)$ gives a notion analogous to the gcd of two numbers.
- We also need an analogue of the height: the Nevanlinna characteristic function $T_f(r)$.
- For holomorphic f it is given by

$$T_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi},$$

where $\log^+ z = \max\{0, \log z\}$.

GCD Counting Function

- Let f and g be meromorphic functions. Define

$$n(f,g,r) = \sum_{|z|\le r} \min\{\mathrm{ord}_z^+(f), \mathrm{ord}_z^+(g)\},$$

$$N_{\mathrm{gcd}}(f,g,r) = \int_0^r \frac{n(f,g,t)-n(f,g,0)}{t}\,dt + n(f,g,0)\log r,$$

- The gcd counting function $N_{\mathrm{gcd}}(f,g,r)$ gives a notion analogous to the gcd of two numbers.
- We also need an analogue of the height: the Nevanlinna characteristic function $T_f(r)$.
- For holomorphic f it is given by

$$T_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi},$$

where $\log^+ z = \max\{0, \log z\}$.

GCD Counting Function

- Let f and g be meromorphic functions. Define

$$n(f,g,r) = \sum_{|z|\leq r} \min\{\mathrm{ord}_z^+(f), \mathrm{ord}_z^+(g)\},$$

$$N_{\mathrm{gcd}}(f,g,r) = \int_0^r \frac{n(f,g,t) - n(f,g,0)}{t} dt + n(f,g,0)\log r,$$

- The gcd counting function $N_{\mathrm{gcd}}(f,g,r)$ gives a notion analogous to the gcd of two numbers.
- We also need an analogue of the height: the Nevanlinna characteristic function $T_f(r)$.
- For holomorphic f it is given by

$$T_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi},$$

where $\log^+ z = \max\{0, \log z\}$.

GCD Counting Function

- Let f and g be meromorphic functions. Define

$$n(f,g,r) = \sum_{|z|\leq r} \min\{\mathrm{ord}_z^+(f), \mathrm{ord}_z^+(g)\},$$

$$N_{\mathrm{gcd}}(f,g,r) = \int_0^r \frac{n(f,g,t)-n(f,g,0)}{t}\,dt + n(f,g,0)\log r,$$

- The gcd counting function $N_{\mathrm{gcd}}(f,g,r)$ gives a notion analogous to the gcd of two numbers.
- We also need an analogue of the height: the Nevanlinna characteristic function $T_f(r)$.
- For holomorphic f it is given by

$$T_f(r) = \int_0^{2\pi} \log^+ |f(re^{i\theta})| \frac{d\theta}{2\pi},$$

where $\log^+ z = \max\{0, \log z\}$.

- In this language, a Nevanlinna theory analogue of the main result is:

Theorem

Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime polynomials. Let $g_1, \ldots, g_n$ be entire functions without zeros. Assume that $g_1^{i_1} \cdots g_n^{i_n} \notin \mathbb{C}$ for any index set $(i_1, \ldots, i_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$. Let $\epsilon > 0$. Then

$$N_{\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n), r) \leq_{\mathrm{exc}} \epsilon \max_{1 \leq i \leq n} \{T_{g_i}(r)\}.$$

- The theorem is equivalent to a special case of a very general result of Noguchi, Winkelmann, and Yamanoi for semiabelian varieties.

GCD Counting Function Inequality

- In this language, a Nevanlinna theory analogue of the main result is:

Theorem

Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime polynomials. Let $g_1, \ldots, g_n$ be entire functions without zeros. Assume that $g_1^{i_1} \cdots g_n^{i_n} \notin \mathbb{C}$ for any index set $(i_1, \ldots, i_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$. Let $\epsilon > 0$. Then

$$N_{\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n), r) \leq_{\mathrm{exc}} \epsilon \max_{1 \leq i \leq n} \{T_{g_i}(r)\}.$$

- The theorem is equivalent to a special case of a very general result of Noguchi, Winkelmann, and Yamanoi for semiabelian varieties.

GCD Counting Function Inequality

- In this language, a Nevanlinna theory analogue of the main result is:

Theorem

Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime polynomials. Let $g_1, \ldots, g_n$ be entire functions without zeros. Assume that $g_1^{i_1} \cdots g_n^{i_n} \notin \mathbb{C}$ for any index set $(i_1, \ldots, i_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$. Let $\epsilon > 0$. Then

$$N_{\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n), r) \leq_{\mathrm{exc}} \epsilon \max_{1 \leq i \leq n} \{T_{g_i}(r)\}.$$

- The theorem is equivalent to a special case of a very general result of Noguchi, Winkelmann, and Yamanoi for semiabelian varieties.

Asymptotic GCD result

- In recent joint work with Julie Wang we prove “asymptotic" gcd results for *meromorphic* functions:

Theorem (L., Wang)

Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime polynomials such that not both of them vanish at $(0, \ldots, 0)$. Let $g_1, \ldots, g_n$ be meromorphic functions such that $g_1^{i_1} \cdots g_n^{i_n} \notin \mathbb{C}$ for any index set $(i_1, \ldots, i_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$. Then for any $\epsilon > 0$, there exists k_0 such that for all $k \geq k_0$,

$$N_{\mathrm{gcd}}(F(g_1^k, \ldots, g_n^k), G(g_1^k, \ldots, g_n^k), r) \leq_{\mathrm{exc}} \epsilon \max_{1 \leq i \leq n} \{T_{g_i^k}(r)\};$$

Asymptotic GCD result

- In recent joint work with Julie Wang we prove “asymptotic" gcd results for *meromorphic* functions:

Theorem (L., Wang)

Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$ *be coprime polynomials such that not both of them vanish at* $(0, \ldots, 0)$. *Let* $g_1, \ldots, g_n$ *be meromorphic functions such that* $g_1^{i_1} \cdots g_n^{i_n} \notin \mathbb{C}$ *for any index set* $(i_1, \ldots, i_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$. *Then for any* $\epsilon > 0$, *there exists* k_0 *such that for all* $k \geq k_0$,

$$N_{\mathrm{gcd}}(F(g_1^k, \ldots, g_n^k), G(g_1^k, \ldots, g_n^k), r) \leq_{\mathrm{exc}} \epsilon \max_{1 \leq i \leq n} \{T_{g_i^k}(r)\};$$

- In particular, we prove a conjectured inequality of Pasten-Wang:

Corollary (L., Wang)

Let f and g be multiplicatively independent meromorphic functions. Then for any $\epsilon > 0$, there exists k_0 such that for all $k \geq k_0$,

$$N_{\mathrm{gcd}}(f^k - 1, g^k - 1, r) \leq_{\mathrm{exc}} \epsilon \max\{T_{f^k}(r), T_{g^k}(r)\}.$$

- Guo and Wang proved a similar result with $\frac{1}{2} + \epsilon$ instead of ϵ.

Pasten-Wang Conjecture

- In particular, we prove a conjectured inequality of Pasten-Wang:

Corollary (L., Wang)

Let f and g be multiplicatively independent meromorphic functions. Then for any $\epsilon > 0$, there exists k_0 such that for all $k \geq k_0$,

$$N_{\mathrm{gcd}}(f^k - 1, g^k - 1, r) \leq_{\mathrm{exc}} \epsilon \max\{T_{f^k}(r), T_{g^k}(r)\}.$$

- Guo and Wang proved a similar result with $\frac{1}{2} + \epsilon$ instead of ϵ.

Pasten-Wang Conjecture

- In particular, we prove a conjectured inequality of Pasten-Wang:

Corollary (L., Wang)

Let f and g be multiplicatively independent meromorphic functions. Then for any $\epsilon > 0$, there exists k_0 such that for all $k \geq k_0$,

$$N_{\mathrm{gcd}}(f^k - 1, g^k - 1, r) \leq_{\mathrm{exc}} \epsilon \max\{T_{f^k}(r), T_{g^k}(r)\}.$$

- Guo and Wang proved a similar result with $\frac{1}{2} + \epsilon$ instead of ϵ.

Proofs

- The primary tool in the proofs is Schmidt's Subspace Theorem in Diophantine approximation.
- Let's first recall Roth's foundational result in Diophantine approximation.

Theorem (Roth 1955)

Let $\alpha \in \bar{\mathbb{Q}}$. Let $\epsilon > 0$. Then there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

Roth's Theorem

- The primary tool in the proofs is Schmidt's Subspace Theorem in Diophantine approximation.
- Let's first recall Roth's foundational result in Diophantine approximation.

Theorem (Roth 1955)

Let $\alpha \in \bar{\mathbb{Q}}$. Let $\epsilon > 0$. Then there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

- The primary tool in the proofs is Schmidt's Subspace Theorem in Diophantine approximation.
- Let's first recall Roth's foundational result in Diophantine approximation.

Theorem (Roth 1955)

Let $\alpha \in \bar{\mathbb{Q}}$. Let $\epsilon > 0$. Then there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

- Roth's theorem can be generalized to arbitrary number fields and to finite sets of places (including nonarchimedean ones).

Theorem (Ridout-Lang version of Roth)

Let k be a number field and S a finite set of places of k. For each $v \in S$, let $Q_v \in \mathbb{P}^1(k)$. Let $\epsilon > 0$. Then

$$\sum_{v \in S} h_{Q_v,v}(P) \leq (2+\epsilon)h(P)$$

for all but finitely many points $P \in \mathbb{P}^1(k)$.

- Roth's theorem can be generalized to arbitrary number fields and to finite sets of places (including nonarchimedean ones).

Theorem (Ridout-Lang version of Roth)

Let k be a number field and S a finite set of places of k. For each $v \in S$, let $Q_v \in \mathbb{P}^1(k)$. Let $\epsilon > 0$. Then

$$\sum_{v \in S} h_{Q_v,v}(P) \leq (2+\epsilon)h(P)$$

for all but finitely many points $P \in \mathbb{P}^1(k)$.

Schmidt's Theorem

- In 1970 Schmidt gave a deep generalization of Roth's theorem to the setting of approximation of hyperplanes in projective space.
- Schmidt's theorem (as improved by Schlickewei to allow arbitrary finite sets of places):

Theorem (Schmidt's Subspace Theorem)

Let k be a number field. Let S be a finite set of places of k. For each $v \in S$, let $H_{0v}, \ldots, H_{nv}$ be hyperplanes over k in $\mathbb{P}^n$ in general position. Let $\epsilon > 0$. Then there exists a finite union of hyperplanes $Z \subset \mathbb{P}^n$ such that

$$\sum_{v \in S} \sum_{i=0}^{n} h_{H_{iv},v}(P) \leq (n+1+\epsilon)h(P)$$

holds for all $P \in \mathbb{P}^n(k) \backslash Z$.

Schmidt's Theorem

- In 1970 Schmidt gave a deep generalization of Roth's theorem to the setting of approximation of hyperplanes in projective space.
- Schmidt's theorem (as improved by Schlickewei to allow arbitrary finite sets of places):

Theorem (Schmidt's Subspace Theorem)

Let k be a number field. Let S be a finite set of places of k. For each $v \in S$, let $H_{0v}, \ldots, H_{nv}$ be hyperplanes over k in $\mathbb{P}^n$ in general position. Let $\epsilon > 0$. Then there exists a finite union of hyperplanes $Z \subset \mathbb{P}^n$ such that

$$\sum_{v \in S} \sum_{i=0}^{n} h_{H_{iv},v}(P) \leq (n+1+\epsilon)h(P)$$

holds for all $P \in \mathbb{P}^n(k) \setminus Z$.

Schmidt's Theorem

- In 1970 Schmidt gave a deep generalization of Roth's theorem to the setting of approximation of hyperplanes in projective space.
- Schmidt's theorem (as improved by Schlickewei to allow arbitrary finite sets of places):

Theorem (Schmidt's Subspace Theorem)

Let k be a number field. Let S be a finite set of places of k. For each $v \in S$, let $H_{0v}, \ldots, H_{nv}$ be hyperplanes over k in $\mathbb{P}^n$ in general position. Let $\epsilon > 0$. Then there exists a finite union of hyperplanes $Z \subset \mathbb{P}^n$ such that

$$\sum_{v \in S} \sum_{i=0}^{n} h_{H_{iv},v}(P) \leq (n+1+\epsilon)h(P)$$

holds for all $P \in \mathbb{P}^n(k) \setminus Z$.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^*H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^*H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^*H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^*H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^* H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^* H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^* H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^* H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^*H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^*H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Idea of proof

- Briefly describe the idea for proving $h_Y(P) \leq \epsilon h(P)$.
- Let $\pi : X \to \mathbb{P}^n$ be the blowup along Y, let E be the exceptional divisor, and let H be a hyperplane.
- For large enough m, $\mathcal{O}(m\pi^*H - E)$ is generated by global sections and we consider the associated morphism $\phi : X \to \mathbb{P}^N$.
- Idea of proof: Apply Schmidt's theorem to $\mathbb{P}^N$ with a nicely chosen system of hyperplanes $\mathcal{H}_v$, $v \in S$.
- Hyperplanes $\mathcal{H}_v$ are chosen (dependent on $P \in X(k)$) so that the associated sections of $\mathcal{O}(m\pi^*H - E)$ vanish to high order along (pullback of) coordinate hyperplanes v-adically close to P.
- Use functoriality to pull back, via ϕ, the resulting Diophantine approximation statement to X.

Future work

- Current joint work with Corvaja and Zannier exploring function field analogues and applications (after their earlier work in dimension 2).
- This has connections to topics including Vojta's conjecture over function fields, unlikely intersections, lacunary polynomials, etc.

Future work

- Current joint work with Corvaja and Zannier exploring function field analogues and applications (after their earlier work in dimension 2).
- This has connections to topics including Vojta's conjecture over function fields, unlikely intersections, lacunary polynomials, etc.