Multiplicative orders on varieties

Mei-Chu Chang

University of California, Riverside

(joint with B. Kerr, I. E. Shparlinski, U. Zannier)

Poonen Conjecture

$\mathcal{A} =$ semiabelian variety over $\mathbb{F}_q$

$\mathcal{X} < A$ subvariety

Poonen Conjecture

$\mathcal{A} =$ semiabelian variety over $\mathbb{F}_q$

$\mathcal{X} < A$ subvariety

$$\mathcal{Z} = \bigcup_{\substack{a \in \mathcal{X},\ \mathcal{Y} < \mathcal{X} \\ \dim \mathcal{Y} > 0,\ \text{semiabelian over } \overline{\mathbb{F}}_q}} a\mathcal{Y}$$

$x \in (\mathcal{X} - \mathcal{Z})(\overline{\mathbb{F}}_q),\ \deg x = [\mathbb{F}_q(x) : \mathbb{F}_q] = d$

Poonen Conjecture

$\mathcal{A} =$ semiabelian variety over $\mathbb{F}_q$

$\mathcal{X} < A$ subvariety

$$\mathcal{Z} = \bigcup_{\substack{a \in \mathcal{X},\ \mathcal{Y} < \mathcal{X} \\ \dim \mathcal{Y} > 0,\ \text{semiabelian over } \overline{\mathbb{F}}_q}} a\mathcal{Y}$$

$x \in (\mathcal{X} - \mathcal{Z})(\overline{\mathbb{F}}_q),\ \deg x = [\mathbb{F}_q(x) : \mathbb{F}_q] = d$

Then

$$\text{ord } x > q^{dc}$$

for some absolute constant $c > 0$.

Special case: $\mathcal{A} = \mathbb{G}_m(\overline{\mathbb{F}}_p) \times \mathbb{G}_m(\overline{\mathbb{F}}_p)$

Theorem (Voloch)

$f(X, Y) \in \mathbb{F}_p[X, Y]$ absolutely irreducible

(under some natural condition on f)

Special case: $\mathcal{A} = \mathbb{G}_m(\overline{\mathbb{F}}_p) \times \mathbb{G}_m(\overline{\mathbb{F}}_p)$

Theorem (Voloch)

$f(X, Y) \in \mathbb{F}_p[X, Y]$ absolutely irreducible

(under some natural condition on f)

$(x, y) \in V(f)$ such that

$$\deg x = d = [\mathbb{F}_q(x) : \mathbb{F}_q] \gg 0$$

Special case: $\mathcal{A} = \mathbb{G}_m(\overline{\mathbb{F}}_p) \times \mathbb{G}_m(\overline{\mathbb{F}}_p)$

Theorem (Voloch)

$f(X, Y) \in \mathbb{F}_p[X, Y]$ absolutely irreducible

(under some natural condition on f)

$(x, y) \in V(f)$ such that

$$\deg x = d = [\mathbb{F}_q(x) : \mathbb{F}_q] \gg 0$$

Then $\forall \epsilon > 0, \exists \delta > 0$ such that

either $\operatorname{ord} x > d^{2-\epsilon}$ or $\operatorname{ord} y > \exp(\delta(\log d)^2)$

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

for any $f(X, Y) \in \mathbb{F}_p[X, Y]$ irreducible, $\deg f = d$

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

for any $f(X,Y) \in \mathbb{F}_p[X,Y]$ irreducible, $\deg f = d$

$\nexists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$ or $\lambda Y^\beta - X^\alpha$, $\lambda \in \overline{\mathbb{F}}_p$.

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

for any $f(X,Y) \in \mathbb{F}_p[X,Y]$ irreducible, $\deg f = d$

$\nexists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^{\alpha} Y^{\beta} - 1$ or $\lambda Y^{\beta} - X^{\alpha}$, $\lambda \in \overline{\mathbb{F}}_p$. Then

$$\#\Big\{(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p : f(x,y) = 0,$$

$$\operatorname{ord} x + \operatorname{ord} y < p^{2/(89d^2+3d+14)}\Big\} < 11d^3 + d$$

Theorem (Lang-Ihara-Serre-Tate) over $\mathbb{C}$

V: irreducible curve in $A = \mathbb{G}_m \times \mathbb{G}_m$

V has infinitely many torsion points.

Theorem (Lang-Ihara-Serre-Tate) over $\mathbb{C}$

V: irreducible curve in $A = \mathbb{G}_m \times \mathbb{G}_m$

V has infinitely many torsion points.

Then V is a translate of a subgroup of A by a torsion point, i.e.

$$V = \{(x, y) : x^r = \eta\, y^s\}$$

for some root of unity η.

Theorem (Beukers-Smyth)

$f \in \mathbb{C}[X, Y]$, deg $f = d$

$V(f)$ has more than $11d^2$ torsion points

Theorem (Beukers-Smyth)

$f \in \mathbb{C}[X, Y]$, deg $f = d$

$V(f)$ has more than $11d^2$ torsion points

Then $V(f)$ has infinitely many torsion points,

Theorem (Beukers-Smyth)

$f \in \mathbb{C}[X, Y]$, deg $f = d$

$V(f)$ has more than $11d^2$ torsion points

Then $V(f)$ has infinitely many torsion points, hence

$\exists \phi | f(X, Y)$ with $\phi = \phi(X, Y) = \lambda X^\alpha Y^\beta - 1$ or

$\lambda Y^\beta - X^\alpha$ for some $\lambda \in \mathbb{C}$

Theorem (Conway-Jones)

$U = \{\text{roots of unity}\}$

Let $a_1, \cdots, a_n \in \mathbb{Q} \setminus \{0\}$.

Theorem (Conway-Jones)

$U = \{\text{roots of unity}\}$

Let $a_1, \cdots, a_n \in \mathbb{Q} \setminus \{0\}$. Then

$$\#\left\{\text{nondeg solutions of } \sum_{i=1}^{n} a_i x_i = 1 \text{ in } U\right\}$$
$$= O\Big(\exp\left(cn^{3/2}(\log n)^{1/2}\right)\Big).$$

A solution $(x_1, \cdots, x_m)$ of the equation

$$\sum_{i=1}^{m} c_i x_i = 1, c_i \in \mathbb{C}$$

is called *nondegenerate*, if

$$\sum_{i \in I} c_i x_i \neq 0$$

for all subsets $I \subseteq \{1, \cdots, m\}$.

Theorem (Evertse-Schlickewei-Schmidt)

$\Gamma < \langle \mathbb{C}^*, \cdot \rangle$, rank $\Gamma = r$

$c_1, \ldots, c_m \in \mathbb{C} \setminus \{0\}$

Theorem (Evertse-Schlickewei-Schmidt)

$\Gamma < \langle \mathbb{C}^*, \cdot \rangle$, rank $\Gamma = r$

$c_1, \ldots, c_m \in \mathbb{C} \setminus \{0\}$

Then

$$\#\left\{\text{nondeg solutions of } \sum_{i=1}^{m} c_i x_i = 1 \text{ in } \Gamma\right\} < \exp\left((r+1)(6m)^{3m}\right).$$

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

for any $f(X,Y) \in \mathbb{F}_p[X,Y]$ irreducible, $\deg f = d$

$\nexists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^{\alpha} Y^{\beta} - 1$ or

$\lambda Y^{\beta} - X^{\alpha}$, $\lambda \in \overline{\mathbb{F}}_p$. Then

$$\#\Big\{(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p : f(x,y) = 0,$$

$$\operatorname{ord} x + \operatorname{ord} y < p^{2/(89d^2+3d+14)}\Big\} < 11d^3 + d$$

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \mathrm{ord}_p(a)$

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \mathrm{ord}_p(a)$

Artin Conjecture

$f(p) = p - 1$ for infinitely many primes p

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \mathrm{ord}_p(a)$

Artin Conjecture

$f(p) = p - 1$ for infinitely many primes p

Hooley GRH $\Rightarrow$ Artin

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \text{ord}_p(a)$

Artin Conjecture

$f(p) = p - 1$ for infinitely many primes p

Hooley GRH $\Rightarrow$ Artin

Gupta-Murty $\#\{a : \text{Artin fails}\} < \infty$

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \text{ord}_p(a)$

Artin Conjecture

$f(p) = p - 1$ for infinitely many primes p

Hooley GRH $\Rightarrow$ Artin

Gupta-Murty $\#\{a : \text{Artin fails}\} < \infty$

Heath-Brown

$\#\{a : a = \text{prime and Artin fails}\} \leq 2$

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \mathrm{ord}_p(a)$

Artin Conjecture

$f(p) = p - 1$ for infinitely many primes p

Hooley GRH $\Rightarrow$ Artin

Gupta-Murty $\#\{a : \text{Artin fails}\} < \infty$

Heath-Brown

$\#\{a : a = \text{prime and Artin fails}\} \leq 2$

e.g. among $2, 3, 5$, at least one of them is a primitive root for $\gg \frac{x}{(\log x)^2}$ primes $p \leq x$

Fix $a \in \mathbb{N}, \quad a \neq -1$, square

Define $f(p) = \mathrm{ord}_p(a)$

Theorem (Erdős-Murty)

For any function $\varepsilon(z) \to 0$ as $z \to \infty$

$$f(p) \geq \frac{p^{1/2+\epsilon(p)}}{\log p}$$

except for $o\left(\frac{x}{\log x}\right)$ many primes $p \leq x$

Proof of Erdős-Murty .

$$f(p) = \mathrm{ord}_p(a) < z \implies p | \prod_{t<z}(a^t - 1) := B$$

Proof of Erdős-Murty .

$$f(p) = \mathrm{ord}_p(a) < z \implies p | \prod_{t<z}(a^t - 1) := B$$

the number of prime factors of B is bounded by

$$O\left(\frac{\log B}{\log\log B}\right) = O\left(\sum_{t<z}\frac{t}{\log t}\right) = O\left(\frac{z^2}{\log z}\right)$$

Proof of Erdős-Murty .

$$f(p) = \mathrm{ord}_p(a) < z \implies p | \prod_{t<z}(a^t - 1) := B$$

the number of prime factors of B is bounded by

$$O\left(\frac{\log B}{\log\log B}\right) = O\left(\sum_{t<z}\frac{t}{\log t}\right) = O\left(\frac{z^2}{\log z}\right)$$

Take $z = \frac{x^{1/2}}{\log x}$.

Then $f(p) < \frac{x^{1/2}}{\log x}$ holds for $O\left(\frac{x}{(\log x)^3}\right)$ primes

Lemma (Erdős-Murty)

$\delta > 0$ fixed.

$\epsilon(x) =$ any function s. t. $\lim_{x\to\infty} \epsilon(x) = 0$

$$\left|\left\{p < x : \exists d|\ p-1,\ d \in (x^{\delta}, x^{\delta+\epsilon(x)}\right\}\right| = o\left(\frac{x}{\log x}\right)$$

Lemma (Erdős-Murty)

$\delta > 0$ fixed.

$\epsilon(x) =$ any function s. t. $\lim_{x\to\infty} \epsilon(x) = 0$

$$\left|\left\{p < x : \exists d |\ p-1,\ d \in (x^{\delta}, x^{\delta+\epsilon(x)}\right\}\right| = o\left(\frac{x}{\log x}\right)$$

Take $\delta = 1/2$. Then $f(p) < \dfrac{x^{1/2+\epsilon(x)}}{\log x}$ holds for $o\left(\dfrac{x}{\log x}\right)$ primes in $\left[\dfrac{x}{2},\ x\right]$.

Theorem (Bourgain-Garaev-Konyagin-Shparlinski)

$\forall \epsilon > 0$, $\exists m = m(\epsilon)$ such that

for $x \in \mathbb{Z}$ and for $T = T(x) \gg 0$,

Theorem (Bourgain-Garaev-Konyagin-Shparlinski)

$\forall \epsilon > 0$, $\exists m = m(\epsilon)$ such that

for $x \in \mathbb{Z}$ and for $T = T(x) \gg 0$, we have

$$\max\{\mathrm{ord}_p(x+1), \cdots, \mathrm{ord}_p(x+m)\} > T^{1-\epsilon}$$

Theorem (Bourgain-Garaev-Konyagin-Shparlinski)

$\forall \epsilon > 0$, $\exists m = m(\epsilon)$ such that

for $x \in \mathbb{Z}$ and for $T = T(x) \gg 0$, we have

$$\max\{\mathrm{ord}_p(x+1), \cdots, \mathrm{ord}_p(x+m)\} > T^{1-\epsilon}$$

for all primes $p < T$ except $< \epsilon \frac{T}{\log T}$ many exceptions

Theorem (C)

(1). For most primes p, let $q = p^m$ for some m.

Let $\beta \in \mathbb{F}_{q^{2n}}$ satisfy some natural condition.

Then

$$\text{ord}\left(\beta + \frac{1}{\beta}\right) > p^{1-\frac{c}{\log n}} \quad \text{for some } c > 0$$

Theorem (C)

(1). For most primes p, let $q = p^m$ for some m.

Let $\beta \in \mathbb{F}_{q^{2n}}$ satisfy some natural condition.

Then

$$\text{ord}\left(\beta + \frac{1}{\beta}\right) > p^{1-\frac{c}{\log n}} \quad \text{for some } c > 0$$

(2). For almost all primes p,

$\forall s \in \mathbb{F}_p^*$ with $\text{ord}_p(s) > 3$,

$$\max\{\text{ord}_p(s), \text{ord}_p(s+1)\} > p^{1/4+\epsilon},$$

where $\epsilon = \epsilon(p) \to 0$ as $p \to \infty$.

recall

Theorem (C-Kerr-Shparlinski-Zannier)

Fixed d, for almost all prime p,

for any $f(X,Y) \in \mathbb{F}_p[X,Y]$ irreducible, $\deg f = d$

$\nexists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$ or $\lambda Y^\beta - X^\alpha$, $\lambda \in \overline{\mathbb{F}}_p$. Then

$$\#\Big\{(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p : f(x,y) = 0,$$

$$\operatorname{ord} x + \operatorname{ord} y < \varepsilon(p) p^{2/(89d^2+3d+14)}\Big\} < 11d^3 + d$$

for any function $\varepsilon(z) \to 0$ as $z \to \infty$.

$f(X,Y) = \Sigma_{i+j \leq d} a_{i,j} X^i Y^j$

$\exists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$

$f(X,Y) = \Sigma_{i+j \leq d} a_{i,j} X^i Y^j$

$\exists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$

More generally, consider $f(X,Y)$ and $\phi(X,Y)$ with common factor of positive degree in Y

$f(X,Y) = \Sigma_{i+j\leq d}\, a_{i,j} X^i Y^j$

$\exists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$

More generally, consider $f(X,Y)$ and $\phi(X,Y)$ with common factor of positive degree in Y

(new) variables: $\vec{A} = \{A_{i,j}\}_{i+j\leq d},\ X,\ Y,\ \Lambda$

Instead of $f(X,Y) = \Sigma_{i+j\leq d}\, a_{i,j} X^i Y^j$ and

$\phi(X,Y) = \lambda X^\alpha Y^\beta - 1$, we study

$f(X,Y) = \Sigma_{i+j\leq d}\, a_{i,j} X^i Y^j$

$\exists \phi | f(X,Y)$ with $\phi = \phi(X,Y) = \lambda X^\alpha Y^\beta - 1$

More generally, consider $f(X,Y)$ and $\phi(X,Y)$ with common factor of positive degree in Y

(new) variables: $\vec{A} = \{A_{i,j}\}_{i+j\leq d},\ X,\ Y,\ \Lambda$

Instead of $f(X,Y) = \Sigma_{i+j\leq d}\, a_{i,j} X^i Y^j$ and

$\phi(X,Y) = \lambda X^\alpha Y^\beta - 1,$ we study

$$F = F(\vec{A}, X, Y) = \sum_{i+j\leq d} A_{i,j} X^i Y^j$$

$$\Phi = \Phi_{a,b}(X,Y,\Lambda) = \Lambda X^a Y^b - 1$$

variables: $\vec{A} = \{A_{i,j}\}_{i+j \le d},\ X,\ Y,\ \Lambda$

$$F = F(\vec{A}, X, Y) = \sum_{i+j \le d} A_{i,j} X^i Y^j = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j$$

$$\Phi = \Phi_{a,b}(X, Y, \Lambda) = \Lambda X^a Y^b - 1$$

variables: $\vec{A} = \{A_{i,j}\}_{i+j \le d},\ X,\ Y,\ \Lambda$

$$F = F(\vec{A}, X, Y) = \sum_{i+j \le d} A_{i,j} X^i Y^j = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j$$

$$\Phi = \Phi_{a,b}(X, Y, \Lambda) = \Lambda X^a Y^b - 1$$

$$\mathsf{gcd}_Y(F, \Phi) \neq 1 \iff \mathsf{Res}_Y(F, \Phi) = 0$$

$$F = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j, \quad \Phi = \wedge X^a Y^b - 1$$

$$\mathrm{Res}_{\mathsf{Y}}(\mathsf{F}, \Phi)$$

$$= \det \begin{bmatrix}
f_0(\vec{A}, X) & f_1(\vec{A}, X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
0 & f_0(\vec{A}, X) & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdot & \cdot & \cdot & f_0(\vec{A}, X) & \cdot & \cdot & \cdot & \cdot \\
-1 & \cdot & \cdot & \cdot & \cdot & \cdot & \wedge X^a & 0 & \cdot & \cdot \\
0 & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \wedge X^a & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \wedge X^a
\end{bmatrix}$$

variables: $\vec{A} = \{A_{i,j}\}_{i+j \le d},\ X,\ Y,\ \Lambda$

$$F = F(\vec{A}, X, Y) = \sum_{i+j \le d} A_{i,j} X^i Y^j = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j$$

$$\Phi = \Phi_{a,b}(X, Y, \Lambda) = \Lambda X^a Y^b - 1$$

$$\gcd(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$$

Write

$$\mathrm{Res}_Y(F, \Phi) = \Sigma_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,\ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$$

variables: $\vec{A} = \{A_{i,j}\}_{i+j\le d},\ X,\ Y,\ \Lambda$

$$F = F(\vec{A}, X, Y) = \sum_{i+j\le d} A_{i,j} X^i Y^j = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j$$

$$\Phi = \Phi_{a,b}(X, Y, \Lambda) = \Lambda X^a Y^b - 1$$

$$\gcd(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$$

Write

$$\mathrm{Res}_Y(F, \Phi) = \Sigma_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,\ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$$

$$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle$$

variables: $\vec{A} = \{A_{i,j}\}_{i+j\le d},\ X,\ Y,\ \Lambda$

$$F = F(\vec{A}, X, Y) = \sum_{i+j\le d} A_{i,j} X^i Y^j = \sum_{j=0}^{d} f_j(\vec{A}, X) Y^j$$

$$\Phi = \Phi_{a,b}(X, Y, \Lambda) = \Lambda X^a Y^b - 1$$

$$\gcd(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$$

Write

$\mathrm{Res}_Y(F, \Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,a,b} X^r$, $\widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$

$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle$

$I_{a,b} = \langle G_{s,a,b} : s = 0, \cdots, S \rangle$ elimination ideal

$G_{s,a,b} \in \mathbb{Z}[\vec{A}]$

$$F = \sum_{i+j \le d} A_{i,j} X^i Y^j, \quad \Phi = \Lambda X^a Y^b - 1$$

$$\gcd_Y(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$$

$$\mathrm{Res}_Y(F, \Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,$$

$$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle, \ \ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$$

$$I_{a,b} = \langle G_{s,a,b} : s = 0, \cdots, S \rangle, \ \ G_{s,a,b} \in \mathbb{Z}[\vec{A}]$$

$$F = \sum_{i+j \le d} A_{i,j} X^i Y^j, \quad \Phi = \Lambda X^a Y^b - 1$$

$$\gcd_Y(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$$

$$\mathrm{Res}_Y(F, \Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,$$

$$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle, \ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$$

$$I_{a,b} = \langle G_{s,a,b} : s = 0, \cdots, S \rangle, \ G_{s,a,b} \in \mathbb{Z}[\vec{A}]$$

$$\widetilde{V}_{a,b} = V(\tilde{I}_{a,b}), \quad V_{a,b} = V(I_{a,b})$$

$F = \sum_{i+j \le d} A_{i,j} X^i Y^j, \quad \Phi = \Lambda X^a Y^b - 1$

$\gcd_Y(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$

$\mathrm{Res}_Y(F, \Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,$

$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle, \ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$

$I_{a,b} = \langle G_{s,a,b} : s = 0, \cdots, S \rangle, \ G_{s,a,b} \in \mathbb{Z}[\vec{A}]$

$\widetilde{V}_{a,b} = V(\tilde{I}_{a,b}), \quad V_{a,b} = V(I_{a,b})$

$\vec{a} = (a_{i,j})_{i+j \le d} \in V_{a,b}$ lifted to $(\vec{a}, \lambda) \in \widetilde{V}_{a,b}$,

if $\vec{a} \notin V$(leading coeff of $\widetilde{G}_{r,a,b}$ in Λ, $\forall r$)

$F = \Sigma_{i+j\le d} A_{i,j} X^i Y^j, \quad \Phi = \Lambda X^a Y^b - 1$

$\gcd_Y(F, \Phi) \neq 1 \iff \mathrm{Res}_Y(F, \Phi) = 0$

$\mathrm{Res}_Y(F, \Phi) = \Sigma_{r=0}^{R} \widetilde{G}_{r,a,b} X^r,$

$\tilde{I}_{a,b} = \langle \widetilde{G}_{r,a,b} : r = 0, \cdots, R \rangle, \ \widetilde{G}_{r,a,b} \in \mathbb{Z}[\vec{A}, \Lambda]$

$I_{a,b} = \langle G_{s,a,b} : s = 0, \cdots, S \rangle, \ G_{s,a,b} \in \mathbb{Z}[\vec{A}]$

$\widetilde{V}_{a,b} = V(\tilde{I}_{a,b}), \quad V_{a,b} = V(I_{a,b})$

$\vec{a} = (a_{i,j})_{i+j\le d} \in V_{a,b}$ lifted to $(\vec{a}, \lambda) \in \widetilde{V}_{a,b}$,

if $\vec{a} \notin V$(leading coeff of $\widetilde{G}_{r,a,b}$ in Λ, $\forall r$)

$(\vec{a}, \lambda) \in \widetilde{V}_{a,b}$ means

$$\gcd_Y \left(\Sigma_{i+j\le d} a_{i,j} X^i Y^j, \ \lambda X^\alpha Y^\beta - 1 \right) \neq 1$$

Let $f(X,Y) = \sum_{i+j \le d} a_{i,j} X^i Y^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has K solutions $(x_1, y_1), \cdots, (x_K, y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Let $f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has K solutions $(x_1, y_1), \cdots, (x_K, y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Then $((a_{i,j})_{i+j\le d}, (x_h, y_h)_{h=1,\cdots,K})$ is a solution to the system

$$\begin{cases} \sum_{i+j\le d} A_{i,j} X_h^i Y_h^j = 0 \\ \Phi_{m_h}(X_h) = 0 \\ \Phi_{n_h}(Y_h) = 0 \end{cases} \qquad h = 1, \cdots, K$$

mth cyclotomic polynomial

$$\Phi_m = \prod_{\substack{s=1 \\ \gcd(s,m)=1}}^{m} (X - e^{2\pi i \frac{s}{m}})$$

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = x^2 - x + 1$$

Given $K = K(d),\ m_1, \cdots, m_K,\ n_1, \cdots, n_K$

Given $K = K(d),\ m_1, \cdots, m_K,\ n_1, \cdots, n_K$

variables: $\vec{A} = \{A_{i,j}\}_{i+j \le d},\ \{X_h,\ Y_h\}_{h=1,\cdots,K}$

Given $K = K(d),\ m_1, \cdots, m_K,\ n_1, \cdots, n_K$

variables: $\vec{A} = \{A_{i,j}\}_{i+j \le d},\ \{X_h,\ Y_h\}_{h=1,\cdots,K}$

$W = W_{m_1,\cdots,m_K,n_1,\cdots,n_K}$ defined over $\mathbb{C}$ by

$$\begin{cases} \sum_{i+j \le d} A_{i,j} X_h^i Y_h^j = 0 \\ \Phi_{m_h}(X_h) = 0 \qquad\qquad h = 1, \cdots, K \\ \Phi_{n_h}(Y_h) = 0 \end{cases}$$

Given $K = K(d),\ m_1, \cdots, m_K,\ n_1, \cdots, n_K$

variables: $\vec{A} = \{A_{i,j}\}_{i+j\leq d},\ \{X_h,\ Y_h\}_{h=1,\cdots,K}$

$W = W_{m_1,\cdots,m_K,n_1,\cdots,n_K}$ defined over $\mathbb{C}$ by

$$\begin{cases} \sum\limits_{i+j\leq d} A_{i,j} X_h^i Y_h^j = 0 & \\ \Phi_{m_h}(X_h) = 0 & h = 1, \cdots, K \\ \Phi_{n_h}(Y_h) = 0 & \end{cases}$$

If $K > 11d^2$, *then* $W \subset \cup_{a,b\leq d} V_{a,b} \cup V_1$, *where*

$V_{a,b} = V(I_{a,b})$, $V_1 = V(\prod\limits_{h_1<h_2\leq K}(X_{h_1} - X_{h_2}))$

Proof.

Take $P = \left((a_{i,j})_{i+j \leq d},\ (x_h,\ y_h)_{h=1,\cdots,K} \right) \in W$

Proof.

Take $P = \left((a_{i,j})_{i+j \leq d},\ (x_h,\ y_h)_{h=1,\cdots,K} \right) \in W$

Let $f(X,Y) = \sum_{i+j \leq d} a_{i,j} X^i Y^j \in \mathbb{C}[X,Y]$

Proof.

Take $P = \left((a_{i,j})_{i+j\le d},\ (x_h,\ y_h)_{h=1,\cdots,K}\right) \in W$

Let $f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has K solutions $(x_1, y_1), \cdots, (x_K, y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Proof.

Take $P = \left((a_{i,j})_{i+j\leq d},\ (x_h,\ y_h)_{h=1,\cdots,K}\right) \in W$

Let $f(X,Y) = \sum_{i+j\leq d} a_{i,j} X^i Y^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has K solutions $(x_1, y_1), \cdots, (x_K, y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Two possibilities:

- $\exists h_1 \neq h_2$ and $x_{h_1} = x_{h_2} \implies P \in V_1$

Theorem (Beukers-Smyth)

$f \in \mathbb{C}[X, Y]$, deg $f = d$

$V(f)$ has more than $11d^2$ torsion points

Then $V(f)$ has infinitely many torsion points, hence $\exists \phi | f(X, Y)$ with $\phi = \lambda X^\alpha Y^\beta - 1$ or $\lambda Y^\beta - X^\alpha$ for some $\lambda \in \mathbb{C}$

Proof.

Take $P = \left((a_{i,j})_{i+j\le d},\ (x_h,\ y_h)_{h=1,\cdots,K}\right) \in W$

Let $f(X,Y) = \sum_{i+j\le d} a_{i,j}X^iY^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has solutions $(x_1,y_1),\cdots,(x_K,y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Two possibilities:

- $\exists h_1 \neq h_2$ and $x_{h_1} = x_{h_2} \implies P \in V_1$
- Otherwise, $V(f)$ has $> 11d^2$ torsion points hence

$\exists \phi | f(X,Y)$ with $\phi = \lambda X^\alpha Y^\beta - 1$ or $\lambda Y^\beta - X^\alpha$ for some $\lambda \in \mathbb{C}$

Proof.

Take $P = \left((a_{i,j})_{i+j\le d},\ (x_h,\ y_h)_{h=1,\cdots,K}\right) \in W$

Let $f(X,Y) = \sum_{i+j\le d} a_{i,j}X^iY^j \in \mathbb{C}[X,Y]$

$f(X,Y) = 0$ has solutions $(x_1,y_1),\cdots,(x_K,y_K)$

ord $x_h = m_h$, ord $y_h = n_h$

Two possibilities:

- $\exists h_1 \neq h_2$ and $x_{h_1} = x_{h_2} \implies P \in V_1$
- Otherwise, $V(f)$ has $> 11d^2$ torsion points hence

$\exists \phi | f(X,Y)$ with $\phi = \lambda X^\alpha Y^\beta - 1$ or $\lambda Y^\beta - X^\alpha$ for some $\lambda \in \mathbb{C}$

$\mathrm{Res}_Y(f,\phi) = 0$

$$f(X,Y) = \sum_{i+j \le d} a_{i,j} X^i Y^j, \quad \phi = \lambda X^\alpha Y^\beta - 1$$

$$\mathrm{Res}_Y(f,\phi) = 0$$

$$f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j, \quad \phi = \lambda X^\alpha Y^\beta - 1$$

$\mathrm{Res}_Y(f,\phi) = 0$

Write $\mathrm{Res}_Y(f,\phi) = \sum_{r=0}^{R} \widetilde{G}_{r,\alpha,\beta} X^r$

$\widetilde{G}_{r,\alpha,\beta}\left((a_{i,j})_{i+j\le d}, \lambda\right) = 0$ for $r = 0, \cdots, R$.

$f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j, \quad \phi = \lambda X^\alpha Y^\beta - 1$

$\mathrm{Res}_Y(f,\phi) = 0$

Write $\mathrm{Res}_Y(f,\phi) = \sum_{r=0}^{R} \widetilde{G}_{r,\alpha,\beta} X^r$

$\widetilde{G}_{r,\alpha,\beta}\left((a_{i,j})_{i+j\le d}, \lambda\right) = 0$ for $r = 0, \cdots, R$. Hence

$G_{s,\alpha,\beta}\left((a_{i,j})_{i+j\le d}\right) = 0$ for $s = 0, \cdots, S$,

and $P \in V_{\alpha,\beta}$ QED

$$\forall G_{s,a,b} \in I_{a,b}, \quad V_{a,b} \subset V(G_{s,a,b})$$

$$\forall G_{s,a,b} \in I_{a,b}, \quad V_{a,b} \subset V(G_{s,a,b})$$

Define

$$G_\ell = \prod_{a,b \leq d} G_{s,a,b}(\vec{A}) \prod_{h_1 < h_2} (X_{h_1} - X_{h_2}),$$

where $G_{s,a,b}(\vec{A})$ is any generator of $I_{a,b}$

$$\forall G_{s,a,b} \in I_{a,b}, \quad V_{a,b} \subset V(G_{s,a,b})$$

Define

$$G_\ell = \prod_{a,b \le d} G_{s,a,b}(\vec{A}) \prod_{h_1 < h_2} (X_{h_1} - X_{h_2}),$$

where $G_{s,a,b}(\vec{A})$ is any generator of $I_{a,b}$

- G_ℓ vanishes on W

Quantitative Nullstellensatz

((immediate from Krick-Pardo-Sombra)

$F_1, \ldots, F_N,\ G \in \mathbb{Z}[X_1, \ldots, X_n],$

$D = \max \deg F_i \geq 3,\ \ H = \max\ \log\ |\text{coeff}\ F_i|$

Quantitative Nullstellensatz

((immediate from Krick-Pardo-Sombra)

$F_1, \ldots, F_N,\ G \in \mathbb{Z}[X_1, \ldots, X_n],$

$D = \max \deg F_i \geq 3,\ \ H = \max\ \log\ |\text{coeff } F_i|$

G vanishes on the variety

$$F_1(X_1, \ldots, X_n) = \ldots = F_N(X_1, \ldots, X_n) = 0$$

Quantitative Nullstellensatz

((immediate from Krick-Pardo-Sombra)

$F_1, \ldots, F_N,\ G \in \mathbb{Z}[X_1, \ldots, X_n],$

$D = \max \deg F_i \geq 3,\ \ H = \max\ \log\ |\text{coeff } F_i|$

G vanishes on the variety

$$F_1(X_1, \ldots, X_n) = \ldots = F_N(X_1, \ldots, X_n) = 0$$

$$\Longrightarrow \exists\, b, r \in \mathbb{Z}^+, \quad Q_1, \ldots, Q_N \in \mathbb{Z}[X_1, \ldots, X_m]$$

$$bG^r = F_1 Q_1 + \ldots + F_N Q_N$$

$$\log b \leq C(n) D^{n+1} (H + \log N + D)$$

$$\exists\ b_\ell = b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K) \in \mathbb{Z} \setminus \{0\},$$
$$\exists\ r_\ell \in \mathbb{Z}^+$$

$\exists\ b_\ell = b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K) \in \mathbb{Z} \setminus \{0\}$,

$\exists\ r_\ell \in \mathbb{Z}^+$ such that

$$b_\ell G_\ell^{r_\ell} = \sum_{h=1}^{K} (\Psi_h \sum_{i+j \le d} A_{i,j} X_h^i Y_h^j + P_h \Phi m_h(X_h) + Q_h \Phi n_h(Y_h)), \qquad (\clubsuit)$$

$\exists\ b_\ell = b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K) \in \mathbb{Z} \setminus \{0\}$,

$\exists\, r_\ell \in \mathbb{Z}^+$ such that

$$b_\ell G_\ell^{r_\ell} = \sum_{h=1}^{K} (\Psi_h \sum_{i+j \le d} A_{i,j} X_h^i Y_h^j + P_h \Phi m_h(X_h) + Q_h \Phi n_h(Y_h)), \qquad (\clubsuit)$$

where $\Psi_h, P_h, Q_h \in \mathbb{Z}[\vec{A}, \{X_h, Y_h\}_{h=1,\cdots,K}]$.

$$\log b_\ell \le C(d)\ T^{cd^2}$$

with an absolute constant $c > 0$.

For prime p such that

$$\gcd\left(p, b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K)\right) = 1$$

for all $m_1, \cdots, m_K, n_1, \cdots, n_K < T$, and for all ℓ

For prime p such that

$$\gcd\left(p, b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K)\right) = 1$$

for all $m_1, \cdots, m_K, n_1, \cdots, n_K < T$, and for all ℓ

Assume $f = \Sigma_{i+j \le d} a_{i,j} X^i Y^j$ has $K > 11d^2$ solutions $(x_h, y_h) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ with $x_{h_1} \neq x_{h_2}$ and $\mathrm{ord} x_h = m_h, \mathrm{ord} y_h = n_h < T, \quad h = 1, \cdots, K$

For prime p such that

$$\gcd\left(p, b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K)\right) = 1$$

for all $m_1, \cdots, m_K, n_1, \cdots, n_K < T$, and for all ℓ

Assume $f = \Sigma_{i+j\le d} a_{i,j} X^i Y^j$ has $K > 11d^2$ solutions $(x_h, y_h) \in \mathbb{F}_p \times \mathbb{F}_p$ with $x_{h_1} \neq x_{h_2}$ and $\mathrm{ord} x_h = m_h, \mathrm{ord} y_h = n_h < T, \quad h = 1, \cdots, K$

Let $A_{i,j} = a_{i,j}, X_h = x_h, Y_h = y_h$ in

$$b_\ell G_\ell^{r_\ell} = \sum_{h=1}^{K} (\Psi_h \sum_{i+j\le d} A_{i,j} X_h^i Y_h^j \qquad (\clubsuit)$$
$$+ P_h \Phi_{m_h}(X_h) + Q_h \Phi_{n_h}(Y_h)),$$

For prime p such that

$$\gcd\left(p, b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K)\right) = 1$$

for all $m_1, \cdots, m_K, n_1, \cdots, n_K < T$, and for all ℓ

Assume $f = \Sigma_{i+j \le d} a_{i,j} X^i Y^j$ has $K > 11d^2$

solutions $(x_h, y_h) \in \mathbb{F}_p \times \mathbb{F}_p$ with $x_{h_1} \neq x_{h_2}$ and

$\mathrm{ord} x_h = m_h, \mathrm{ord} y_h = n_h < T, \quad h = 1, \cdots, K$

Let $A_{i,j} = a_{i,j}, X_h = x_h, Y_h = y_h$ in (♣)

$\Longrightarrow$ RHS$= 0$

For prime p such that

$$\gcd\left(p, b_\ell(m_1, \cdots, m_K, n_1, \cdots, n_K)\right) = 1$$

for all $m_1, \cdots, m_K, n_1, \cdots, n_K < T$, and for all ℓ

Assume $f = \Sigma_{i+j\le d}\, a_{i,j} X^i Y^j$ has $K > 11d^2$ solutions $(x_h, y_h) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ with $x_{h_1} \neq x_{h_2}$ and $\mathrm{ord} x_h = m_h, \mathrm{ord} y_h = n_h < T, \quad h = 1, \cdots, K$

Let $A_{i,j} = a_{i,j}, X_h = x_h, Y_h = y_h$ in (♣)

$\Longrightarrow$ RHS$= 0$

$\Longrightarrow \quad G_\ell((a_{i,j})_{i+j\le d}, (x_h)_{h=1,\cdots,K}) = 0$

Claim. $\vec{a} = (a_{i,j})_{i+j \leq d} \in V_{a,b}$ for some (a, b)

Claim. $\vec{a} = (a_{i,j})_{i+j \le d} \in V_{a,b}$ for some (a, b)

Proof. If $\vec{a} \notin V_{a,b}, \forall (a, b)$, then

$$\forall (a, b), \quad \exists G_{s,a,b}(\vec{a}) \neq 0 \quad \text{for some } s$$

Claim. $\vec{a} = (a_{i,j})_{i+j \le d} \in V_{a,b}$ for some (a, b)

Proof. If $\vec{a} \notin V_{a,b}, \forall (a, b)$, then

$$\forall (a, b), \quad \exists G_{s,a,b}(\vec{a}) \neq 0 \quad \text{for some } s$$

Let $G_\ell(\vec{A}, \{X_h\}_{h=1,\cdots,K})$

$$= \prod_{a,b \le d} G_{s,a,b}(\vec{A}) \prod_{h_1 < h_2} (X_{h_1} - X_{h_2})$$

Claim. $\vec{a} = (a_{i,j})_{i+j\le d} \in V_{a,b}$ for some (a,b)

Proof. If $\vec{a} \notin V_{a,b}, \forall (a,b)$, then

$$\forall (a,b), \quad \exists G_{s,a,b}(\vec{a}) \neq 0 \quad \text{for some } s$$

Let $G_\ell(\vec{A}, \{X_h\}_{h=1,\cdots,K})$

$$= \prod_{a,b\le d} G_{s,a,b}(\vec{A}) \prod_{h_1<h_2} (X_{h_1} - X_{h_2})$$

Then $G_\ell((a_{i,j})_{i+j\le d}, (x_h)_{h=1,\cdots,K}) \neq 0 \quad \rightarrow\leftarrow$

$$f(X,Y) = \sum_{i+j \le d} a_{i,j} X^i Y^j, \quad \Phi = \lambda X^a Y^b - 1$$

$$\gcd(f, \Phi) \neq 1 \iff \mathrm{Res}_Y(f, \Phi) = 0$$

$$f(X,Y) = \sum_{i+j \le d} a_{i,j} X^i Y^j, \quad \Phi = \lambda X^a Y^b - 1$$

$$\gcd(f, \Phi) \neq 1 \iff \mathrm{Res}_Y(f, \Phi) = 0$$

$$\mathrm{Res}_Y(f, \Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,\alpha,\beta} X^r$$

$$f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j, \quad \Phi = \lambda X^a Y^b - 1$$

$$\gcd(f,\Phi) \neq 1 \iff \mathrm{Res}_Y(f,\Phi) = 0$$

$$\mathrm{Res}_Y(f,\Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,\alpha,\beta} X^r$$

$\vec{a} = (a_{i,j})_{i+j\le d} \in V_{a,b}$ can be lifted to $(\vec{a},\lambda) \in \widetilde{V}_{a,b}$,
if $\vec{a} \notin U_{a,b} = V$(leading coeff of $\widetilde{G}_{r,a,b}$ in Λ, $\forall r$).

$$f(X,Y) = \sum_{i+j\le d} a_{i,j} X^i Y^j, \quad \Phi = \lambda X^a Y^b - 1$$

$$\gcd(f,\Phi) \neq 1 \iff \mathrm{Res}_Y(f,\Phi) = 0$$

$$\mathrm{Res}_Y(f,\Phi) = \sum_{r=0}^{R} \widetilde{G}_{r,\alpha,\beta} X^r$$

$\vec{a} = (a_{i,j})_{i+j\le d} \in V_{a,b}$ can be lifted to $(\vec{a},\lambda) \in \widetilde{V}_{a,b}$,
if $\vec{a} \notin U_{a,b} = V$(leading coeff of $\widetilde{G}_{r,a,b}$ in Λ, $\forall r$).

$(\vec{a},\lambda) \in \widetilde{V}_{a,b}$ means $\Phi | f$ $\quad \to\leftarrow$

Theorem' (C-Kerr-Shparlinski-Zannier)

$f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$

$\mathcal{V} = V(f_1, \ldots, f_m)$ irreducible over $\mathbb{C}$

Theorem' (C-Kerr-Shparlinski-Zannier)

$f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$

$\mathcal{V} = V(f_1, \ldots, f_m)$ irreducible over $\mathbb{C}$

Assume $\mathcal{V}$ does not contain curve parametrized by

$X_1 = \rho_1 T^{k_1}, \ldots, X_n = \rho_n T^{k_n}$, where

$\rho_1, \ldots, \rho_n$ are roots of unity, and $k_1, \ldots, k_n \in \mathbb{Z}$.

Theorem' (C-Kerr-Shparlinski-Zannier)

$f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$

$\mathcal{V} = V(f_1, \ldots, f_m)$ irreducible over $\mathbb{C}$

Assume $\mathcal{V}$ does not contain curve parametrized by $X_1 = \rho_1 T^{k_1}, \ldots, X_n = \rho_n T^{k_n}$, where $\rho_1, \ldots, \rho_n$ are roots of unity, and $k_1, \ldots, k_n \in \mathbb{Z}$.

Then $\exists C = C(\mathcal{V})$ s.t. for almost all p

$$\#\Big\{(x_1, \ldots, x_n) \in \mathcal{V}_p \subset \mathbb{F}_p^n : \max\{\operatorname{ord} x_1, \ldots, \operatorname{ord} x_n\} < \epsilon(p) p^{1/2n}\Big\} < C$$