Roots of Polynomials in Subgroups of $\mathbb{F}_p^*$ and Applications to Congruences

Enrico Bombieri, Jean Bourgain, Sergei Konyagin

IAS, Princeton, IAS Princeton, Moscow State University

The decimation problem

Let $A \in \mathbb{Z}(\text{mod } p) \setminus \{0\}$ and $(d, p-1) = 1$, p an odd prime. Then $x \mapsto Ax^d$ induces a permutation $\pi_{d,A}$ of $\mathbb{Z}(\text{mod } p)$. Consider

$$Even := \{0, 2, 4, \ldots, p-1\} \subset \{0, 1, 2, 3, \ldots, p-1\} \cong \mathbb{Z}\ (\text{mod } p).$$

Then the question is to determine all cases in which $\pi_{d,A}(Even) = Even$. We may assume that $(d, A) \neq (1, 1)$ and $1 < d < p/2$.

The following conjecture is due to Goresky and Kappler.
Conjecture GK *The only cases in which* $\pi_{d,A}(Even) = Even$ *and* $1 < d < p/2$ *are*

$$(p, d, A) = (5, 3, 3), (7, 1, 5), (11, 9, 3), (11, 3, 7), (11, 5, 9), (13, 1, 5).$$

The decimation problem

Let $A \in \mathbb{Z}(\text{mod } p) \setminus \{0\}$ and $(d, p-1) = 1$, p an odd prime. Then $x \mapsto Ax^d$ induces a permutation $\pi_{d,A}$ of $\mathbb{Z}(\text{mod } p)$. Consider

$$Even := \{0, 2, 4, \ldots, p-1\} \subset \{0, 1, 2, 3, \ldots, p-1\} \cong \mathbb{Z}\ (\text{mod } p).$$

Then the question is to determine all cases in which $\pi_{d,A}(Even) = Even$. We may assume that $(d, A) \neq (1, 1)$ and $1 < d < p/2$.

The following conjecture is due to Goresky and Kappler.
Conjecture GK *The only cases in which* $\pi_{d,A}(Even) = Even$ *and* $1 < d < p/2$ *are*

$$(p, d, A) = (5, 3, 3), (7, 1, 5), (11, 9, 3), (11, 3, 7), (11, 5, 9), (13, 1, 5).$$

The conjecture has been verified numerically for $p < 2 \times 10^6$ and recently (preprint 2008) proved for $p > 2.26 \times 10^{55}$ by Bourgain, Cochrane, Paulhus, and Pinner.

A reformulation

The problem is equivalent to showing that the equation

$$A(2x)^d = 2y - 1$$

in $\mathbb{Z}(\mathrm{mod}\ p) \times \mathbb{Z}(\mathrm{mod}\ p)$ has a solution in the box

$$\mathcal{B} = \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

A reformulation

The problem is equivalent to showing that the equation

$$A(2x)^d = 2y - 1$$

in $\mathbb{Z} \pmod{p} \times \mathbb{Z} \pmod{p}$ has a solution in the box

$$\mathcal{B} = \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

If not, then

$$(x, A2^{d-1}x^d) \pmod{p} \in \mathcal{B} + (0, -\overline{2})$$

has no solutions.

A reformulation

The problem is equivalent to showing that the equation

$$A(2x)^d = 2y - 1$$

in $\mathbb{Z}(\text{mod } p) \times \mathbb{Z}(\text{mod } p)$ has a solution in the box

$$\mathcal{B} = \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

If not, then

$$(x, A2^{d-1}x^d) \ (\text{mod } p) \in \mathcal{B} + (0, -\overline{2})$$

has no solutions.

This appears to be very unlikely because on average one expects

$$p \frac{|\mathcal{B}|}{p^2} \sim \frac{1}{4} p$$

solutions.

The Fourier method

The study of the number of solutions of $(ax, bx^d) \in \mathcal{B}$ for a general box $\mathcal{B}$ is easily reduced to the question of bounds for

$$S(u,v) = \sum_{x \in \mathbb{Z} \,(\mathrm{mod}\ p)} e_p(aux^d + vx)$$

with $e_p(x) = e^{2\pi i x/p}$ and $u, v \in \mathbb{Z}\,(\mathrm{mod}\ p)$ not both 0.

If

$$S(u,v) = O\left(\frac{p}{(\log p)^2}\right)$$

then one can prove the asymptotic formula

$$\left|(ax, bx^d) \in \mathcal{B}\right| \sim \frac{|\mathcal{B}|}{p}.$$

By Weil estimate, $|S(u,v)| \le (d-1)\sqrt{p}$. Thus the real difficulties occur if $d \gg \sqrt{p}/(\log p)^2$.

The Sum–Product Method

A new combinatorial method for studying the general exponential sum

$$S = \sum_{x \in \mathbb{Z} \pmod{p}} e_p\Big(\sum_{i=1}^{r} a_i x^{d_i} \Big)$$

has been introduced by Bourgain uses the sum–product theorem: There is an absolute constant $\delta > 0$ such that if $A \subset \mathbb{Z} \pmod{p}$ then

$$\max(|A + A|, |A \cdot A|) \geq \min\left(p, |A|^{1+\delta}\right).$$

The Sum–Product Method

A new combinatorial method for studying the general exponential sum

$$S = \sum_{x \in \mathbb{Z} \pmod{p}} e_p\Big(\sum_{i=1}^{r} a_i x^{d_i}\Big)$$

has been introduced by Bourgain uses the sum–product theorem: There is an absolute constant $\delta > 0$ such that if $A \subset \mathbb{Z} \pmod{p}$ then

$$\max(|A+A|, |A \cdot A|) \geq \min\left(p, |A|^{1+\delta}\right).$$

Proposition 1. *Given $r \in \mathbb{N}$ and $\varepsilon > 0$, there are $\delta > 0$ and C, depending only on r and ε, with the following property. If $p > C$ is a prime and $1 \leq d_1 < \cdots < d_r < p-1$ satisfy*

$$(d_i, p-1) < p^{1-\varepsilon} \quad (1 \leq i \leq r)$$
$$(d_i - d_j, p-1) < p^{1-\varepsilon} \quad (1 \leq j < i \leq r)$$

then for $(a_1, \ldots, a_r) \in (\mathbb{Z} \pmod{p})^r \setminus \{\mathbf{0}\}$ it holds

$$\left|\sum_{x \in \mathbb{Z} \pmod{p}} e_p\left(a_1 x^{d_1} + \cdots + a_r x^{d_r}\right)\right| < p^{1-\delta}.$$

Solution of the decimation problem for large p

This solves the decimation problem for large p provided

$$(d-1,p-1)<p^{1-\varepsilon}.$$

In order to deal with the remaining case, note that if $(d-1,p-1)\geq p^{1-\varepsilon}$ then x^d and x are correlated in the sense that $x^d\equiv xu \pmod p$ where $u^t\equiv 1 \pmod p$ with $t=(d-1)/(d-1,p-1)\leq p^{\varepsilon}$. Now write $x=y^tz$ and get $(x,Ax^d)=(y^tz,Ay^tz^d)$. When varying y and z (not 0), each x occurs exactly $p-1$ times, counting multiplicities.

Let $\mathcal{B}$ be a box $\pmod p$ with sides of length N_1, N_2. For fixed z and varying y, the Fourier method shows that the number of solutions of $(y^tz,Ay^tz^d)\in\mathcal{B}$ is $\sim N_1N_2/p$ (as expected), provided $uz+vAz^d\neq 0$ for $|u|<p^{\delta}$, $|v|<p^{\delta}$, with $(u,v)\neq(0,0)$.

An elementary counting of the exceptional z now yields for some $\delta=\delta(\varepsilon)>0$ the lower bound

$$\Big|(x,Ax^d)\in\mathcal{B}\Big|\geq\Big(1-\frac{2t}{p-1}\Big)\frac{N_1N_2}{p}+O\Big(p^{1-\delta}\Big).$$

The main result

Theorem 1. *Given* $r \geq 2$ *and* $\varepsilon > 0$ *there are* $B = B(r, \varepsilon) > 0$, $c = c(r, \varepsilon) > 0$, $\delta = \delta(r, \varepsilon) > 0$, *such that the following holds. Let* $1 \leq d_1 < \cdots < d_r < p - 1$ *be such that*

$$(d_i, p-1) < p^{1-\varepsilon} \quad (1 \leq i \leq r)$$
$$(d_i - d_j, p-1) < \frac{p}{B} \quad (1 \leq j < i \leq r).$$

Then for $p \geq C(r, \varepsilon)$, *all* $a_1, \ldots, a_r \in [1, p-1]$, *and any rectangular box*

$$\mathcal{B} \subset (\mathbb{Z} \pmod{p})^r$$

it holds

$$\left|\left(a_i x^{d_i},\ (i = 1, \ldots, r)\right) \in \mathcal{B}\right| \geq c\,\frac{|\mathcal{B}|}{p^{r-1}} + O\left(p^{1-\delta}\right).$$

(The result is meaningful only if $|\mathcal{B}| \gg p^{r-\delta}$.)

How hard is to define a subgroup of $\mathbb{F}_p^*$?

Denote by $\overline{X}$ the reduction $\pmod{p}$ of X.

Proposition 2. *Let $d \geq 2$, $H \geq 1$, and q a prime number. Let $G < \mathbb{F}_p^*$ be a subgroup of order coprime with q. Then at least one of the following three statements holds.*

(i) $|G|$ *divides* Δ *for some integer* Δ *with* $\phi(\Delta) \leq d$*, where* $\phi(n)$ *is Euler's function.*

(ii) $p \leq 3^{(q+1)d^2} H^{(q+1)d}$*.*

(iii) *There is* $\gamma \in G$ *such that for* ***every*** *polynomial* $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ *of degree at most* d *and height* $H(f) \leq H$ *it holds* $\bar{f}(\gamma) \neq 0$*.*

How hard is to define a subgroup of $\mathbb{F}_p^*$?

Denote by $\overline{X}$ the reduction $\pmod p$ of X.

Proposition 2. *Let $d \geq 2$, $H \geq 1$, and q a prime number. Let $G < \mathbb{F}_p^*$ be a subgroup of order coprime with q. Then at least one of the following three statements holds.*

(i) $|G|$ *divides* Δ *for some integer* Δ *with* $\phi(\Delta) \leq d$, *where* $\phi(n)$ *is Euler's function.*

(ii) $p \leq 3^{(q+1)d^2} H^{(q+1)d}$.

(iii) *There is* $\gamma \in G$ *such that for* ***every*** *polynomial* $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ *of degree at most* d *and height* $H(f) \leq H$ *it holds* $\bar{f}(\gamma) \neq 0$.

The lower bound (i) for $|G|$ is sharp. Take $p \equiv 1 \pmod m$, $d = \phi(m)$, and G the subgroup of the mth roots of unity. The cyclotomic factors of $x^m - 1$ have height not more than 2^m and degree not more than $\phi(m)$. Now (ii) fails for large p, (iii) fails for every element of G, and (i) holds with equality.

The proof, I

The Mahler measure $M(f)$ of $f \in \mathbb{C}[x]$ with leading coefficient a_0 is

$$M(f) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|f(e^{i\theta})\right| \mathrm{d}\theta\right) = |a_0| \prod_{f(\alpha)=0} \max(1, |\alpha|).$$

Its main properties are:

(m1) *Multiplicativity:* $M(fg) = M(f)M(g)$.

(m2) $M(f(x^n)) = M(f(x))$ *for* $n \in \mathbb{N}$.

(m3) *Comparison: If* $H(f)$ *is the height of* f *of degree* d*, then*

$$(d+1)^{-\frac{1}{2}} M(f) \leq H(f) \leq \binom{d}{\lfloor d/2 \rfloor} M(f).$$

Let γ be a generator of the cyclic group G. Then γ^{q^i}, $i = 0, 1, \ldots$ are all generators of G, because q does not divide $|G|$. Suppose now that (iii) fails and $p > H$. Then for every integer $i \geq 0$ there is a polynomial $f_i(x) \in \mathbb{Z}[x]$, of degree at most d, height $H(f_i) \leq H$, such that

$$\bar{f}_i\left(\gamma^{q^i}\right) = 0$$

and $\bar{f}_i$ not identically 0.

The proof, II

We may further assume that each $f_i(x)$ is irreducible. If not, it factors in $\mathbb{Z}[x]$ (by Gauss Lemma). Then $\bar{g}\left(\gamma^{q^i}\right) = 0$ holds for some irreducible factor $g(x)$ of $f_i(x)$ of degree less than d, again in $\mathbb{Z}[x]$. By (m1) its Mahler measure does not exceed $M(f_i)$; by (m3) it cannot exceed $2^d H$. Thus $\bar{f}_i\left(\gamma^{q^i}\right) = 0$ holds for certain irreducible polynomials with height

$$H(f_i) \leq 2^d H.$$

Consider now the two polynomials $\bar{f}_0(x)$ and $\bar{f}_1(x^q)$. They have the common root γ, hence their resultant R vanishes in $\mathbb{F}_p$:

$$R\Big(\bar{f}_0(x), \bar{f}_1(x^q)\Big) = 0.$$

This simply means that the resultant of $f_0(x)$ and $f_1(x^q)$ is divisible by p. Equivalently, for α a root of $f_0(x)$ and a_0 the leading coefficient of $f_0(x)$, it holds

$$N := a_0^{q\deg(f_1)} \mathrm{Norm}_{\mathbb{Q}(\alpha)/\mathbb{Q}} f_1(\alpha^q) \equiv 0 \pmod{p}.$$

The proof, III

Suppose first that $N \neq 0$. Let a_0 be the leading coefficient of $f_0(x)$ and let $\alpha_1, \ldots, \alpha_r$, where $r = \deg(f_0)$, be a full set of conjugates of α. Then

$$\begin{aligned} p \leq |N| = |a_0|^{q \deg(f_1)} \prod_{i=1}^{r} |f_1(\alpha_i^q)| \\ &\leq (\deg(f_1) + 1)^r H(f_1)^r \left(|a_0| \prod_{i=1}^{r} \max(1, |\alpha_i|) \right)^{q \deg(f_1)} \\ &\leq (d+1)^d (2^d H)^d M(\alpha)^{qd} \leq (d+1)^{(q+2)d/2} (2^d H)^{(q+1)d} \end{aligned}$$

because $H(f) \leq 2^d H$ and $M(\alpha) \leq (d+1)^{\frac{1}{2}} H(f_0)$.

This easily yields (ii) of the proposition.

If instead $N = 0$ the resultant vanishes, thus $f_0(x)$ and $f_1(x^q)$ have a common root. Since f_0 is irreducible, we infer that $f_0(x)$ divides $f_1(x^q)$.

Next, we make the same construction with f_1 and f_2 and again (ii) follows unless $f_1(x)$ divides $f_2(x^q)$. By induction, we get either (ii) or $f_i(x)$ divides $f_{i+1}(x^q)$ for every index i.

The proof, IV

Moreover, if (ii) does not hold the irreducible polynomials $f_i(x)$ are uniquely determined. (Hint: Consider the resultant of f_i and an irreducible polynomial g with $H(g) \leq 2^d H$ and with a same root $\pmod{p}$.)

The proof, IV

Moreover, if (ii) does not hold the irreducible polynomials $f_i(x)$ are uniquely determined. (Hint: Consider the resultant of f_i and an irreducible polynomial g with $H(g) \leq 2^d H$ and with a same root $(\bmod\ p)$.)

Hence if q does not divide $|G|$ the sequence of polynomials $f_i(x)$ is periodic and, by Euler's congruence, the period is a divisor of $\phi(|G|)$.

The proof, IV

Moreover, if (ii) does not hold the irreducible polynomials $f_i(x)$ are uniquely determined. (Hint: Consider the resultant of f_i and an irreducible polynomial g with $H(g) \leq 2^d H$ and with a same root $(\bmod\ p)$.)

Hence if q does not divide $|G|$ the sequence of polynomials $f_i(x)$ is periodic and, by Euler's congruence, the period is a divisor of $\phi(|G|)$.

Since $f_i(x)$ divides $f_{i+1}(x^q)$, the sequence $(M(f_i))_{i=1,2,\ldots}$ is increasing; by periodicity, it must be a constant, say c. Thus the quotient $f_{i+1}(x^q)/f_i(x)$ has Mahler measure 1 and, by Kronecker's characterization of roots of unity, f_{i+1}/f_i is a product of cyclotomic polynomials.

The proof, IV

Moreover, if (ii) does not hold the irreducible polynomials $f_i(x)$ are uniquely determined. (Hint: Consider the resultant of f_i and an irreducible polynomial g with $H(g) \leq 2^d H$ and with a same root $(\bmod\ p)$.)

Hence if q does not divide $|G|$ the sequence of polynomials $f_i(x)$ is periodic and, by Euler's congruence, the period is a divisor of $\phi(|G|)$.

Since $f_i(x)$ divides $f_{i+1}(x^q)$, the sequence $(M(f_i))_{i=1,2,\ldots}$ is increasing; by periodicity, it must be a constant, say c. Thus the quotient $f_{i+1}(x^q)/f_i(x)$ has Mahler measure 1 and, by Kronecker's characterization of roots of unity, f_{i+1}/f_i is a product of cyclotomic polynomials.

By induction, $f_i(x^{q^i})/f_0(x)$ is a product of cyclotomic polynomials. Since the degree of $f_i(x^{q^i})$ is unbounded, f_i must eventually have a root which is a root of unity, whence it is a cyclotomic polynomial because it is irreducible. Thus $c = 1$, hence every f_i is a cyclotomic polynomial. Therefore, $f_0(x)$ divides $x^\Delta - 1$ for some Δ with $\phi(\Delta) = \deg(f_0)$. Hence the generator γ satisfies $\gamma^\Delta = 1$, $|G|$ divides Δ, and (i) holds.

Refinements

Corollary. *Let $d \geq 2$, $H \geq 1$, and let $G < \mathbb{F}_p^*$ be a subgroup. Then at least one of the following three statements holds.*

(i) $|G| \leq \Delta^2$ *for some integer* Δ *with* $\phi(\Delta) \leq d$.

(ii) $p \leq 3^{4d^2} H^{4d}$.

(iii) *There is* $\gamma \in G$ *such that for every polynomial* $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ *of degree at most* d *and height* $H(f) \leq H$ *it holds* $\bar{f}(\gamma) \neq 0$.

Proof. Apply Proposition 2 to the two subgroups of G of elements with order coprime with 2 and 3.

Proposition 3. *Let $d \geq 2$, $0 < \varepsilon < 1$, $H \geq 1$. There are $C_1(d, \varepsilon) > 0$, $C_2(d, \varepsilon) > 0$, depending only on d and ε, with the following property. Let $G < \mathbb{F}_p^*$ be a subgroup. Then at least one of the following three statements holds.*

(i) $|G| \leq C_1(d, \varepsilon)$.

(ii) $p \leq C_2(d, \varepsilon) H^{8d^3/\varepsilon}$.

(iii) *For at least* $(1-\varepsilon)|G|$ *elements* $\gamma \in G$ *and every polynomial* $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ *of degree bounded by* d *and with height* $H(f) \leq H$ *it holds* $\bar{f}(\gamma) \neq 0$.

Idea of proof for Proposition 3

Let $\mathcal{E}$ be the exceptional set of $\gamma \in G$, namely

$$\mathcal{E} = \left\{ \begin{array}{c} \gamma \in G : \quad \bar{f}(\gamma) = 0 \ \textit{for some } f(x) \in \mathbb{Z}[x] \setminus \{0\}, \\ 1 \le \deg(f) \le d,\ H(f) \le H \end{array} \right\}.$$

We want to show that $\mathcal{E}$ has small cardinality. It will suffice to show that there are many translates of $\mathcal{E}$ disjoint from each other.

Idea of proof for Proposition 3

Let $\mathcal{E}$ be the exceptional set of $\gamma \in G$, namely

$$\mathcal{E} = \left\{ \begin{array}{c} \gamma \in G : \quad \bar{f}(\gamma) = 0 \ \textit{ for some } f(x) \in \mathbb{Z}[x] \setminus \{0\}, \\ 1 \leq \deg(f) \leq d, \ H(f) \leq H \end{array} \right\}.$$

We want to show that $\mathcal{E}$ has small cardinality. It will suffice to show that there are many translates of $\mathcal{E}$ disjoint from each other.

We choose translates by powers γ_0^k of a suitable element of G. If two polynomials $A(x)$ and $B(x)$ vanish on the intersection of two different translates, it means that there exists $\gamma \in G$ such that $A(\gamma) = 0$ and $B(\gamma\gamma_0^k) = 0$. Then the resultant $R(y)$ of $A(x)$ and $B(xy^k)$ with respect to x will vanish for $y = \gamma_0$.

The degree and height of $R(x)$ will be controlled by quantities D , H_1 (with approriate bounds), and k. Then if $R(x)$ is not identically 0 we will obtain a contradiction with the corollary to Proposition 2 by choosing γ_0 the element of G whose existence is provided by that corollary. This will show that translates of $\mathcal{E}$ by small powers of γ_0 are disjoint.

Intersections of Fermat varieties

Proposition 4. *Given $r \in \mathbb{N}$, there is $D = D(r) \geq 1$ with the following property. Let $0 \leq d_0 < d_1 < \cdots < d_D$ be integers and let V_{d_μ} be a hypersurface defined by an equation*

$$\sum_{i=0}^{r} a_{\mu i} g_i(\mathbf{x}) x_i^{d_\mu} = 0$$

where the factors $g_i(\mathbf{x})$ are homogeneous polynomials in $\mathbf{x} = (x_0, \ldots, x_r)$, of the same degree and not identically 0, and where for each i the coefficients $a_{\mu i}$ are complex numbers, not all 0. Let W denote the projective variety

$$W := \bigcap_{\mu=0}^{D} V_{d_\mu}.$$

Then every irreducible component Y of W satisfies at least one of:

(i) Y is contained in one of the hypersurfaces $g_i(\mathbf{x}) = 0$.

(ii) Y is contained in some hyperplane $x_i - c x_j = 0$ with $j < i$ and $c \in \mathbb{C}$.

Remark. The proof shows that $D(r) = r(r+1)/2$ is admissible.

Proof of Proposition 4, I

Let Y be an irreducible component of W. If Y is empty or a point this is trivial, hence we may assume that $\dim(Y) \geq 1$.

If a coordinate x_i vanishes identically on Y we simply take $c = 0$. Hence there is no loss of generality in assuming that x_i is not identically 0 on Y.

We pass to inhomogeneous coordinates and work in the function field L of Y. Let $A_i = x_i/x_0$ $(i = 0, \dots, r)$, hence $A_0 = 1$, and write $\mathbf{A} = (A_0, A_1, \dots, A_r)$ where now $A_i \in L^*$. Let $s = \dim(Y)$; then L is a finite extension $L = \mathbb{C}(\xi, \mathbf{t}^{(0)})$ of $\mathbb{C}(\mathbf{t}^{(0)})$ with $\mathbf{t}^{(0)} = (t_1, \dots, t_s)$ purely transcendental over $\mathbb{C}$ and ξ algebraic over $\mathbb{C}(\mathbf{t}^{(0)})$, with $f(\xi, \mathbf{t}^{(0)}) = 0$.

Let δ be a generic derivation δ of $\mathbb{C}(\mathbf{t}^{(0)})$ defined by $\delta\mathbb{C} = 0$ and $\delta\mathbf{t}^{(0)} = \mathbf{t}^{(1)}$ componentwise, where $\mathbf{t}^{(1)}$ is purely transcendental over $\mathbb{C}(\mathbf{t}^{(0)})$, and extend δ by means of $\delta\mathbf{t}^{(l)} = \mathbf{t}^{(l+1)}$ $(l = 0, 1, \dots)$, where $\mathbf{t}^{(l+1)}$ is purely transcendental over $\mathbb{C}(\mathbf{t}^{(0)}, \dots, \mathbf{t}^{(l)})$. Then set

$$\delta\xi = -\frac{1}{f_\xi(\xi, \mathbf{t}^{(0)})} \sum_{i=1}^{s} f_{t_i}(\xi, \mathbf{t}^{(0)}) t_i^{(1)}.$$

Proof of Proposition 4, II

Suppose the functions $g_i(\mathbf{A})A_i^m$ $(i = 0, \ldots, r)$ are linearly dependent over $\mathbb{C}$. Then their Wronskian with respect to δ vanishes:

$$\Psi := \det \begin{pmatrix} g_0(\mathbf{A})A_0^m & g_1(\mathbf{A})A_1^m & \ldots & g_r(\mathbf{A})A_r^m \\ \delta(g_0(\mathbf{A})A_0^m) & \delta(g_1(\mathbf{A})A_1^m) & \ldots & \delta(g_r(\mathbf{A})A_r^m) \\ . & . & \ldots & . \\ \delta^r(g_0(\mathbf{A})A_0^m) & \delta^r(g_1(\mathbf{A})A_1^m) & \ldots & \delta^r(g_r(\mathbf{A})A_r^m) \end{pmatrix} = 0.$$

The function $(A_0 \cdots A_r)^{-m}\Psi$ is the determinant of an $(r+1) \times (r+1)$ matrix with entries a_{ij} $(i, j = 1, \ldots, r+1)$, where a_{ij} is a polynomial in m of degree at most $i-1$, with coefficients in Λ, hence it is a polynomial in m of degree at most $r(r+1)/2$. Thus if the Wronskian Ψ is not identically 0 there are not more than $r(r+1)/2$ possible values of m for which the Wronskian vanishes.

On the other hand, by hypothesis the relation of linear dependence holds for the $r(r+1)/2 + 1$ values $m = d_\mu$ $(\mu = 0, 1, \ldots, r(r+1)/2)$ and we conclude that $\Psi = 0$ identically.

Proof of Proposition 4, III

(A powerful Vandermonde determinant)

A simple calculation shows that the highest power of m in the expansion of $(A_0 \cdots A_r)^{-m}\Psi$ is

$$g_0(\mathbf{A}) \cdots g_r(\mathbf{A}) \mathrm{Vand}\left(\frac{\delta A_0}{A_0}, \frac{\delta A_1}{A_1}, \ldots, \frac{\delta A_r}{A_r}\right) m^{r(r+1)/2}$$

where $\mathrm{Vand}(x_0, \ldots, x_r)$ is the Vandermonde determinant.

Since Y is irreducible, the identical vanishing of this term implies that either $g_i(\mathbf{A}) = 0$ for some i, or $\frac{\delta A_i}{A_i} = \frac{\delta A_j}{A_j}$ for some $i \neq j$.

In the former case, statement (i) of the proposition holds.

In the latter case, it must be the case that $\delta(A_i/A_j) = 0$, hence $A_i/A_j = x_i/x_j$ is in the field of constants for δ. Since δ is a generic derivation, the field of constants for δ is $\mathbb{C}$ and statement (ii) follows.

Controlling degrees and coefficients

Corollary. *In particular, if $D = r(r+1)/2$, $g_i(\mathbf{x}) = 1$, $d_\mu = \mu$, there are finitely many non-zero homogeneous polynomials $p_{ij}(x,y)$, $0 \le j < i \le r$, such that the polynomial*

$$P(\mathbf{x}) := \prod_{j<i} p_{ij}(x_i, x_j)$$

vanishes identically on W. Moreover, if $a_{di} \in \mathbb{Z}$ and $|a_{di}| \le A$ for all coefficients a_{di}, the polynomials $p_{ij}(x,y)$ can be chosen such that it holds

$$p_{ij}(x,y) \in \mathbb{Z}[x,y], \quad \deg(p_{ij}) \le C_3, \quad H(p_{ij}),\, H(P) \le C_4 A^{C_5}$$

for some constants C_3, C_4, C_5, depending only on r.

Controlling degrees and coefficients

Corollary. *In particular, if* $D = r(r+1)/2$, $g_i(\mathbf{x}) = 1$, $d_\mu = \mu$, *there are finitely many non-zero homogeneous polynomials* $p_{ij}(x,y)$, $0 \le j < i \le r$, *such that the polynomial*

$$P(\mathbf{x}) := \prod_{j<i} p_{ij}(x_i, x_j)$$

vanishes identically on W*. Moreover, if* $a_{di} \in \mathbb{Z}$ *and* $|a_{di}| \le A$ *for all coefficients* a_{di}*, the polynomials* $p_{ij}(x,y)$ *can be chosen such that it holds*

$$p_{ij}(x,y) \in \mathbb{Z}[x,y], \quad \deg(p_{ij}) \le C_3, \quad H(p_{ij}),\, H(P) \le C_4 A^{C_5}$$

for some constants C_3, C_4, C_5, *depending only on* r.

Comments for the proof. We may take for $P(x,y) \in Z[x,y]$ the product of the norms $\mathrm{Norm}_{K/\mathbb{Q}}(x_i - \xi x_j)$, for all components of W. Control of degree and heights is best done by using an Arithmetic Bézout Theorem, getting for example

$$h(P) \le D^r \log(r+2)(\log A + 6r).$$

Application of the Arithmetic Nullstellensatz

Arithmetic Hilbert Nullstellensatz. *Let* $\mathbf{x} = (x_1, \ldots, x_n)$. *Let* $f_1, \ldots, f_s \in \mathbb{Z}[\mathbf{x}]$ *be polynomials of degree at most* d *and suppose that* $g \in \mathbb{Z}[\mathbf{x}]$ *vanishes on the zero-set of the polynomials* f_i. *Let* $\Delta = \max(d, \deg(g))$ *and suppose that* $H(g) \le H$, $H(f_1), \ldots, H(f_s) \le H$.
Then there are $g_i \in \mathbb{Z}[\mathbf{x}]$ *and non-zero integers* a, l, *such that:*

(N1) $g_1 f_1 + \cdots + g_s f_s = a\, g^l$.

(N2) $|a| \le C_6 H^{C_7}$, *where* C_6 *and* C_7 *depend only on* n, s, *and* Δ.

Proposition 5. *There are* $\varepsilon_1 > 0$ *and* C_8, C_9, *depending only on* r, *with the following property. Let* $G < (\mathbb{F}_p^*)^r$ *be a subgroup. Let* G_{ij} *be the image of* G *by the homomorphism* $\Phi_{ij}(\boldsymbol{\gamma}) = \gamma_i/\gamma_j$.
Then at least one of the following three statements holds:

(i) *There are two indices* $j < i$ *such* $|G_{ij}| \le C_8$.

(ii) $p \le C_9$.

(iii) *There is* $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in G$ *such that*

$$\overline{a}_1\gamma_1 + \cdots + \overline{a}_r\gamma_r \ne 0$$

whenever $a_1, \ldots, a_r \in \mathbb{Z}$ *and* $0 < \sum |a_i| \le p^{\varepsilon_1}$.

Idea of proof, I

Fix $\gamma \in G$ and assume that (ii) fails. Then it must fail for γ^d, $d = 1, 2, \ldots$ and we obtain a system of equations

$$f_d(\gamma) := \overline{a}_{d1}\gamma_1^d + \cdots + \overline{a}_{dr}\gamma_r^d = 0, \quad (1 \le d \le r(r-1)/2)$$

for certain $a_{ds} \in \mathbb{Z}$ with $0 < \sum_i |a_{di}| \le p^{\varepsilon_1}$.

The polynomials f_i define a variety W. The last part of Corollary of Proposition 4 yields a polynomial $P = \prod p_{ij}(x_i, x_j)$, with $1 \le j < i \le r$ and with controlled degree and height, such that P vanishes on W. By the Arithmetic Nullstellensatz, there are polynomials g_i with integer coefficients such that

$$g_1 f_1 + g_2 f_2 + \cdots + g_D f_D = a P^l$$

with $a \neq 0$ and $|a| < C_6 p^{C_7 \varepsilon_1}$, with C_6 and C_7 depending only on r. We reduce the Hilbert equation $\pmod{p}$ and evaluate it at γ, getting

$$\overline{a}\bar{P}(\gamma)^l = 0.$$

Idea of proof, II

If $p > C_9$ and $\varepsilon_1 < 1/(2C_7)$, then $\overline{a} \neq 0$ and we get $\bar{P}(\boldsymbol{\gamma})^l = 0$. The polynomial $\bar{P}(\boldsymbol{x}) \in \mathbb{F}_p[\mathrm{x}]$ is homogeneous and not identically 0, because p is large and $H(P)$ is small relative to p.

Therefore, $\bar{P}(\boldsymbol{\gamma}) = 0$. Since P factors as a product of homogeneous polynomials p_{ij}, it follows that $\overline{p}_{ij}(\gamma_i/\gamma_j, 1) = 0$ for some choice of indices $j < i$, also depending on $\boldsymbol{\gamma}$.
Since the number of pairs $\{i, j\}$ with $j < i$ is $(r-1)r/2$, there is a pair $\{j, i\}$ such that

$$\left|\left\{\gamma \in G_{ij} \,:\, \overline{p}_{ij}(\gamma, 1) = 0\right\}\right| > \frac{2}{r^2}\,|G_{ij}|.$$

We have the bounds

$$H(p_{ij}),\ H(P) \leq C_4 H^{C_5}.$$

Now we apply Proposition 2 to this situation, taking $\varepsilon = 2/r^2$. Thus if ε_1 is small enough as a function of r alone and p is large enough as a function of r alone then statements (ii) and (iii) of that proposition do not hold. The only possibility left is that $|G_{ij}|$ is bounded as a function of r.

Several variables

Let $\mathfrak{M} \subset \mathbb{Z}^r$. For $\mathfrak{m} = (m_1, \ldots, m_r) \in \mathfrak{M}$ and $\mathbf{x} = (x_1, \ldots, x_r)$ we denote by $\mathbf{x}^{\mathfrak{m}}$ the associated monomial $x_1^{m_1} \cdots x_r^{m_r}$. We also write $|\mathfrak{m}| = |m_1| + \cdots + |m_r|$

Proposition 6. *Let r and $K \geq 1$ be given. Then there are ε_2, ε_3, C_{10}, C_{11}, depending only on K and r, with the following property. Let $G < (\mathbb{F}_p^*)^r$ and $\mathfrak{M} \subset \mathbb{Z}^r$, with $\max |\mathfrak{m}| \leq K$. Let also $\eta_{\mathfrak{m}} \in \mathbb{F}_p^*$, $(\mathfrak{m} \in \mathfrak{M})$. For $\mathfrak{M} \subset \mathbb{Z}^r$ let $G_{\mathfrak{M}}$ denote the image of G by the homomorphism $\Phi_{\mathfrak{M}} : G \to (\mathbb{F}_p^*)^{|\mathfrak{M}|}$ given by $\boldsymbol{\gamma} \mapsto (\boldsymbol{\gamma}^{\mathfrak{m}})_{\mathfrak{m} \in \mathfrak{M}}$.*
Then at least one of the following three statements holds.

(i) There are $\mathfrak{m} \neq \mathfrak{m}' \in \mathfrak{M}$ such that $|G_{\{\mathfrak{m}-\mathfrak{m}'\}}| \leq C_{10}$.

(ii) $p \leq C_{11}$.

(iii) For at least $\varepsilon_2 |G|$ elements $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in G$ it holds

$$\sum_{\mathfrak{m} \in \mathfrak{M}} \bar{a}_{\mathfrak{m}}\, \eta_{\mathfrak{m}} \boldsymbol{\gamma}^{\mathfrak{m}} \neq 0$$

whenever

$$0 < \sum_{\mathfrak{m} \in \mathfrak{M}} |a_{\mathfrak{m}}| \leq p^{\varepsilon_3}.$$

Comments about the proof, I

The proof is long and complicated and is done in several steps, proceeding by contradiction.

Step 0: Choose M' much larger than $M = \max|\mathfrak{m}|$ and d_i, $i = 1, \ldots, M'$ a very lacunary sequence of increasing integers. Take $\gamma \in G$ and assume that γ^{d_i} fails in (iii) for $i = 1, \ldots, M'$.

Step I: This yields a homogeneous linear system of M' equations in the M unknowns $\eta_\mathfrak{m}$:

$$\sum_{\mathfrak{m} \in \mathfrak{M}} \overline{a}_\mathfrak{m} \, \eta_\mathfrak{m} \gamma^{d_i \mathfrak{m}} = 0.$$

Step II: Since there are many equations, one can work with a reduced set $\mathfrak{M}^*$ of exponents for which $a_\mathfrak{m} \neq 0$. Thus we may assume the validity of this condition, which proves to be essential in what follows.

Comments about the proof, II

Step III: We eliminate the coefficients $\eta_{\mathfrak{m}}$ by taking the determinant associated to a subset of equations (Cramer's Rule). Each determinant yields a relation of the same type but relative to a new set of exponents. The lacunarity of the d_i ensures that no new exponent arises twice from the determinant expansion.
Since there is a very large number of such relations, one obtains a large set of relations in which the coefficients $\eta_{\mathfrak{m}}$ are all 1 and in addition all coefficients $a_{\mathfrak{m}}$ are not 0. Thus it suffices to prove the proposition with these additional assumptions.

Step IV: Prove the case $r = 1$ by appealing to a quantitative version of Proposition 5 where the conclusion holds for many $\gamma \in G$.

Step V: Proceed by induction on r by using the homomorphisms $G \to G_{\{\mathfrak{m}-\mathfrak{m}'\}}$ appropriately to show that (i) of Proposition 5 must hold for a non-trivial pair $(\mathfrak{m}, \mathfrak{m}')$.

Step VI: Since now $l = \left|G_{\{\mathfrak{m}-\mathfrak{m}'\}}\right|$ is small, one can kill $G_{\{\mathfrak{m}-\mathfrak{m}'\}}$ by replacing G by G^l. This allows the induction step from $r-1$ to r.

The steps in the proof of Theorem 1

Step I: Apply the circle method in $\mathbb{F}_p$ to compute a smoothed weighted number of solutions of

$$(a_1 x^{d_1} - l_1, \dots, a_r x^{d_r} - l_r) \in \mathcal{B}$$

with $\mathcal{B} = [1, N_1] \times \cdots \times [1, N_r]$. For a given x the weighted counting (with respect to a smooth weight function F with support in $\mathcal{B}$) is

$$\frac{1}{p^r} \sum_{\boldsymbol{\lambda} \in \mathbb{F}_p^r} e_p\Big(- \sum_{i=1}^{r} \lambda_i a_i x^{k_i} \Big) \, e_p\Big(\sum_{i=1}^{r} \lambda_i l_i \Big) \, \widehat{F}(\boldsymbol{\lambda})$$

where $\widehat{F}(\boldsymbol{\lambda})$ is the $\pmod{p}$ Fourier transform.

For any $\eta > 0$ the Fourier transform is essentially supported in the box

$$\mathcal{L} = \Big\{ \boldsymbol{\lambda} \, : \, |\lambda_i| < p^{1+\eta}/N_i \quad (i = 1, \dots, r) \Big\}$$

while outside of this box it is $O(p^{-K})$, for any fixed $K > 0$.

Step II: We want to mimic what was done earlier for the case $r = 2$ when we set $x = y^t z$ and use the Bourgain estimate to conclude with a lower bound. The difficulty is to show that such a t exists.

A finite covering theorem

The key to conclude the proof is a covering theorem for a finite set of points in a metric space X with distance function $\delta(u, v)$ and diameter function $\Delta(Y)$ on subsets $Y \subset X$.

Proposition 7. *Let X be a metric space and let $\mathcal{E}$ be a set of points of X of cardinality $|\mathcal{E}| = r$ and let $\varepsilon > 0$.*
Then there is a partition

$$\mathcal{E} = \mathcal{E}_1 \cup \cdots \cup \mathcal{E}_s$$

such that

$$\max_{\sigma} \Delta(\mathcal{E}_\sigma) \leq \frac{1}{2r} \kappa\varepsilon, \quad \min_{\sigma \neq \tau} \delta(\mathcal{E}_\sigma, \mathcal{E}_\tau) \geq \kappa\varepsilon$$

for some constant

$$(5r^2)^{-r} \leq \kappa \leq 1.$$

Conclusion

We take $\mathcal{E} = \{1, \ldots, r\}$ and write $(d_i - d_j, p-1) = (p-1)^{1-\varepsilon_{ij}}$. Then $\delta(i,j) = \varepsilon_{ij}$ is a distance function on $\mathcal{E}$.

For each σ choose $i_\sigma \in \mathcal{E}_\sigma$ and set

$$t = \prod_{\sigma=1}^{s} \prod_{j \in \mathcal{E}_\sigma} \frac{p-1}{(k_{i_\sigma} - k_j, p-1)}.$$

Then

$$(td_{i_\sigma} - td_j, p-1) = p-1 \quad if \;\; j \in \mathcal{E}_\sigma,$$

$$(td_{i_\sigma} - td_{i_\tau}, p-1) \leq p^{1-\kappa\varepsilon/2} \quad if \;\; \sigma \neq \tau.$$

The first equation shows that the substitution $x = y^t z$ clumps together the terms involving x^{d_i} $(i \in \mathcal{E}_\sigma)$ in the exponential sum as

$$\sum_{\sigma=1}^{s} \left(\sum_{i \in \mathcal{E}_\sigma} \lambda_i a_i z^{d_i} \right) y^{td_{i_\sigma}}.$$

Proposition 6 is essential for proving that for a positive density of z it holds $\sum_{i \in \mathcal{E}_\sigma} \lambda_i a_i z^{d_i} \neq 0$. The second equation shows that the $y^{td_{i_\sigma}}$ are uncorrelated enough to apply the estimate for fixed z. The rest is as for $r = 2$.

THE END