Equidistribution from the Chinese Remainder Theorem

E. Kowalski

ETH Zürich

April 23, 2020

[Joint work with K. Soundararajan, `arXiv:2003.12965`]

Motivation

Hooley (1964): "the fractional parts of the roots modulo $q \leqslant x$ of a fixed irreducible $f \in \mathbf{Z}[X]$ of degree at least 2 become equidistributed in $[0, 1]$ as $x \to +\infty$."

Basic summary of (parts of) our results:

- This sentence is open to different interpretations, and Hooley's is not the most natural;
- But the result has little to do with specific arithmetic properties of roots of polynomial congruences;
- Rather, there is a very natural and very general statement which reveals that the key source of equidistribution here is the "mixing" property of the Chinese Remainder Theorem.

Equidistribution

Equidistribution modulo 1 was defined by Weyl for *sequences* (x_n) of real numbers. For generalizations, it is much better to view it as a special case of convergence in law, or weak convergence of probability measures.

Definition. Let X be a *compact* topological space with a probability measure μ. A sequence (μ_n) of probability measures on X converges to μ if we have

$$\lim_{n\to+\infty} \int_X f(x)d\mu_n(x) = \int_X f(x)d\mu(x)$$

for all continuous functions $f : X \to \mathbf{C}$.

Abstract Weyl Criterion: it is enough to use f that span (algebraically) a dense subset of $\mathcal{C}(X)$.

Hooley's (implicit) measures

- $X = [0,1]$, $\mu =$ Lebesgue measure.
- $f \in \mathbf{Z}[X]$ irreducible of degree $\geqslant 2$.
- For $Q \geqslant 1$, the probability measure $\mu_Q^{(H)}$ is

$$\mu_Q^{(H)} = \frac{1}{M_Q} \sum_{q \leqslant Q} \sum_{\substack{a \bmod q \\ f(a)=0}} \delta_{\{a/q\}}$$

where δ_t is a Dirac mass at t and

$$M_Q = \sum_{q \leqslant Q} \sum_{\substack{a \bmod q \\ f(a)=0}} 1.$$

- (Weyl) It is enough to test equidistribution for the functions

$$f(x) = e(hx) = \exp(2i\pi hx), \qquad h \in \mathbf{Z} \text{ non-zero.}$$

Generalization

The key properties that explain Hooley's result are:

1. There is a positive density of primes p such that f has at least 2 roots modulo p (e.g. totally split primes, by Chebotarev);
2. *The number of roots modulo p is bounded as p varies*;
3. The roots of f modulo q are determined, if q is squarefree, by the Chinese Remainder Theorem and the roots of f modulo prime divisors of q:

$$\{a \in \mathbf{Z}/q\mathbf{Z} \mid f(a) = 0\} = \{a \in \mathbf{Z}/q\mathbf{Z} \mid \text{ for all } p \mid q,\ f(a \bmod p) = 0 \bmod p\}.$$

Condition (2) is an artefact of Hooley's (implicit) choice of measures. Only (1) and (3) are essential.

Equidistribution in $\mathbf{R}/\mathbf{Z}$

For p prime, let $A_p \subset \mathbf{Z}/p\mathbf{Z}$ be given. For q squarefree, let

$$A_q = \{x \in \mathbf{Z}/q\mathbf{Z} \mid x \bmod p \in A_p \text{ for all} p \mid q\}.$$

Let $\varrho(q) = |A_q|$; it is a multiplicative function. Let $\mathcal{Q}$ be the set of squarefree q such that $\varrho(q) \geqslant 1$, i.e., such that A_q is not empty; for $x \geqslant 1$, let $\mathcal{Q}(x)$ be the set of $q \leqslant x$ in $\mathcal{Q}$

Standing Assumption. For a fixed $\alpha > 0$ and $x \geqslant x_0$, we have

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \log p \geqslant \alpha x.$$

For $q \in \mathcal{Q}$, let Δ_q be the probability measure

$$\Delta_q = \frac{1}{\varrho(q)} \sum_{x \in A_q} \delta_{\{x/q\}} \qquad \text{on } \mathbf{R}/\mathbf{Z}.$$

First statement

Theorem. (K–Sound) Assume that $\displaystyle\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}} \frac{1}{p} \to +\infty$. Then the measures

$$\mu_x = \frac{1}{|\mathcal{Q}(x)|} \sum_{q\in\mathcal{Q}(x)} \Delta_q$$

converge to the Lebesgue measure λ on $\mathbf{R}/\mathbf{Z}$ as $x \to +\infty$.
In fact, we have a quantitative discrepancy bound: there exists $C \geqslant 0$, depending on x_0, α, such that for $x \geqslant 2$

$$\operatorname{disc}(\mu_x) \leqslant \frac{1}{|\mathcal{Q}(x)|} \sum_{q\in\mathcal{Q}(x)} \operatorname{disc}(\Delta_q) \leqslant C \exp\Big(-\frac{1}{6} \sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}} \frac{1}{p}\Big).$$

Here $\operatorname{disc}(\mu) = \sup_I |\mu(I) - \lambda(I)|$, where I runs over closed intervals.

Optimality

The discrepancy estimate

$$\frac{1}{|\mathcal{Q}(x)|}\sum_{q\in\mathcal{Q}(x)}\operatorname{disc}(\Delta_q)\leqslant C\exp\Big(-\frac{1}{6}\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}}\frac{1}{p}\Big)$$

shows that for most q, the measure Δ_q is close to the Lebesgue measure.

This statement is not far from sharp: for "random" sets, we can expect that the number of squarefree integers $q\in\mathcal{Q}(x)$ which have no prime divisor p with $\varrho(p)\geqslant 2$ is

$$\asymp|\mathcal{Q}(x)|\prod_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}}\Big(1-\frac{1}{p}\Big)\asymp|\mathcal{Q}(x)|\exp\Big(-\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}}\frac{1}{p}\Big),$$

and we have $\operatorname{disc}(\Delta_q)=1$ for every such q.

Higher-dimensional version

Fix $n \geqslant 1$. We consider now subsets $A_p \subset (\mathbf{Z}/p\mathbf{Z})^n$ and define A_q and $\mathcal{Q}$ as before. There can be further obstructions to equidistribution: it could be, e.g., that A_p is contained in

$$\{(x_1, \ldots, x_n) \in (\mathbf{Z}/p\mathbf{Z})^n \mid x_1 + \cdots + x_n = 1\}$$

for all p, in which case A_q will satisfy the same constraint modulo q, and the fractional parts will be constrained to lie on a subtorus of $(\mathbf{R}/\mathbf{Z})^n$.

Linear conditions like these are the only additional restrictions.

For p prime, let $\lambda(p) = \max_H |H \cap A_p|$, where H runs over affine hyperplanes modulo p.

Example. If $n = 1$, then $\lambda(p) = 1$ if A_p is not empty.

Second statement

Theorem. (K–Sound) For sets in n-dimensional space, we have

$$\frac{1}{|\mathcal{Q}(x)|}\sum_{q\in\mathcal{Q}(x)}\operatorname{disc}(\Delta_q)\leqslant C_n\exp\Bigl(-\frac{1}{3}\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 1}}\Bigl(1-\frac{\lambda(p)}{\varrho(p)}\Bigr)\frac{1}{p}\Bigr).$$

Here the discrepancy is the "box" discrepancy

$$\operatorname{disc}(\mu)=\sup_{B}|\mu(B)-\lambda_n(B)|$$

for measures μ on $(\mathbf{R}/\mathbf{Z})^n$, where B runs over products of closed intervals and λ_n is the Lebesgue measure on $(\mathbf{R}/\mathbf{Z})^n$.

Note that $\lambda(p)=\varrho(p)$ if $0\leqslant\varrho(p)\leqslant n$. Intuitively, we obtain the equidistribution if we have $\varrho(p)\geqslant n+1$ for a positive density of primes, and the points of A_p are in "general position".

Restricting the number of prime factors

Another motivating question is whether equidistribution of roots of polynomial congruences already holds modulo primes.

In our setting, the residue classes modulo primes are chosen arbitrarily, so obviously this cannot be true. But we can show that, if $|A_p| \to +\infty$, then equidistribution will already hold for q with exactly two prime factors. In the general case, we can also fix the number k of prime factors in a wide range, provided $k \to +\infty$ with x.

For $k \geqslant 1$, we denote by $\mathcal{Q}_k$ and $\mathcal{Q}_k(x)$ the elements of $\mathcal{Q}$ and $\mathcal{Q}(x)$ which have exactly k prime factors.

Many prime factors

Theorem. (K–Sound) For sets in n-dimensional space, if

$$\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 1}} \Big(1-\frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p} \geqslant \delta \log\log x,$$

where $\delta > 0$ then we have

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)} \operatorname{disc}(\Delta_q) \leqslant C\Big(e^{-k\delta/18}+(\log x)^{-\alpha\delta/18}\Big)$$

provided $k_0 \leqslant k \leqslant \exp(c\sqrt{\log\log x})$ where $c = c(n,\alpha,\delta) > 0$ et $k_0 = k_0(n,\delta)$.

A fixed number of prime factors

Theorem. (K–Sound) For sets in n-dimensional space, if k is fixed and

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \frac{\lambda(p)}{\varrho(p)} \frac{1}{p} < +\infty$$

then there exists $c > 0$, $C \geqslant 0$ such that

$$\frac{1}{|\mathcal{Q}_k(x)|} \sum_{q \in \mathcal{Q}_k(x)} \operatorname{disc}(\Delta_q) \leqslant C(c \log\log x)^{-(k-1)/10}$$

for $x \geqslant 2$.

In particular, we obtain equidistribution already with $k = 2$.

Application 1: a question of Hrushovski

For *prime moduli*, Hrushovski (`arXiv:1911.01096`) has asked if

$$\left(\left\{\frac{a}{p}\right\},\dots,\left\{\frac{a^{d-1}}{p}\right\}\right)\in(\mathbf{R}/\mathbf{Z})^{d-1},\qquad f(a)=0 \bmod p,$$

where a runs over roots modulo $p\leqslant x$ of an irreducible $f\in\mathbf{Z}[X]$ of degree $d\geqslant 1$ become equidistributed as $x\to+\infty$.

This is indeed the case for the roots modulo squarefree moduli q:

- For a positive proportion of primes, we have $\varrho(p)=d$;
- For any affine hyperplane H modulo p, we have $|H\cap A_p|\leqslant d-1$ so that $\lambda(p)\leqslant d-1$;
- Hence $$\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 1}}\left(1-\frac{\lambda(p)}{\varrho(p)}\right)\frac{1}{p}\gg\log\log x.$$

By projecting to the first coordinate (when $d\geqslant 2$), we obtain our version of Hooley's Theorem.

Application 2: variations around roots of polynomial congruences

- Equidistribution of roots of f modulo q, when q is restricted to have all prime factors in suitable subsets of the primes (it suffices that they are independent enough of the totally split primes to ensure that $\varrho(p) \geqslant 2$ for a positive density of p);
- Equidistribution of roots a of f modulo q, when a is restricted to belong to a subset of $\mathbf{Z}/q\mathbf{Z}$ which has, for q prime, a positive density (again with some minor independence assumption); for instance, a can be assumed to be a value $a = g(b)$ of another (non-constant) polynomial $g \in \mathbf{Z}[X]$, for some $b \in \mathbf{Z}/q\mathbf{Z}$.
- Combinations of these.
- If $f_1, \ldots, f_n$ are distinct irreducible polynomials, each with degree $\geqslant 2$, we get equidistribution in $(\mathbf{R}/\mathbf{Z})^n$ of the fractional parts of $(a_1, \ldots, a_n)$, where a_i mod q runs over roots of f_i mod q.

Application 3: pseudo-polynomials

Definition. (Hall) A *pseudo-polynomial* is a function $f : \mathbf{Z} \to \mathbf{Z}$ such that $a - b \mid f(a) - f(b)$ for all $a \neq b$ in $\mathbf{Z}$. Then f mod q is a well-defined function $\mathbf{Z}/q\mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$ for all $q \geqslant 1$.

There are uncountably many pseudo-polynomials. Examples are

$$f_1(n) = \lfloor en! \rfloor$$
$$f_2(n) = (-1)^n \times |\{\text{derangements } \sigma \in \mathfrak{S}_n\}|.$$

Question. Are the fractional parts of the zeros modulo q of a (genuine) pseudo-polynomial f equidistributed?

For f_1 we don't know – although, experimentally, the number of zeros of f_1 modulo a large prime p seems to behave like a Poisson random variable with parameter 1.
But we can prove it for $f_2 - 1$, because this can be checked to have $\geqslant 2$ zeros modulo any prime $p \geqslant 3$ (namely, $a = 0$ and $a = p - 1$).

Counterexample: Hooley's measures are unnatural

Our basic results involve the probability measures $\frac{1}{|\mathcal{Q}(x)|}\sum_{q\in\mathcal{Q}(x)}\Delta_q$, in contrast with Hooley's (implicit) use of the measures

$$\mu_x^{(H)} = \frac{1}{M_x}\sum_{q\in\mathcal{Q}(x)}\varrho(q)\Delta_q \qquad M_x = \sum_{q\in\mathcal{Q}(x)}\varrho(q).$$

There is no general analogue of our results for these measures.

Example. Let A_p be the set of classes modulo p of the integers such that $1 \leqslant i \leqslant p/\log p$. Define A_q for q squarefree by the Chinese Remainder Theorem.

Then $\mu_x^{(H)}$ *does not converge* to the Lebesgue measure as $x \to +\infty$ (because the primes already contribute a positive proportion of the measure).

Ideas of the proof

- The discrepancy is bounded using the Erdős–Turán inequality; this amounts to taking the test functions

$$f(x) = e(h \cdot x), \quad (h \cdot x = \sum h_i x_i, \quad \text{uniformly with respect to } h);$$

- Cancellation comes from the average

$$\Big(\frac{1}{p}\sum_{a \bmod p}\Big|\frac{1}{\varrho(p)}\sum_{x\in A_p} e\Big(\frac{a\,h\cdot x}{p}\Big)\Big|\Big)^2 \leqslant \frac{1}{p}\sum_{a \bmod p}\Big|\frac{1}{\varrho(p)}\sum_{x\in A_p} e\Big(\frac{a\,h\cdot x}{p}\Big)\Big|^2.$$

The trivial bound is 1; but this is also equal to

$$\frac{1}{\varrho(p)^2}\sum_{\substack{x,y\in A_p\\ h\cdot x = h\cdot y}} 1 = \frac{1}{\varrho(p)^2}\sum_{x\in A_p}\sum_{\substack{y\in A_p\\ h\cdot x = h\cdot y}} 1 \leqslant \frac{\lambda(p)}{\varrho(p)}.$$

So if $\lambda(p) < \varrho(p)$ for sufficiently many primes, using multiplicativity to "amplify" this constant factor, we can obtain cancellation.

Ideas of the proof (cont.)

- Weyl sums for Δ_q:

$$W(h;q) = \frac{1}{\varrho(q)} \sum_{x \in A_q} e\Big(\frac{h \cdot x}{q}\Big).$$

- Factor $q = rs$ where s has all prime factors "small"; then $W(h;rs) = W(\bar{r}h;s)W(\bar{s}h;r)$; bound $W(\bar{s}h;r)$ trivially, then sum over r in arithmetic progressions modulo s:

$$\sum_{q=rs \in \mathcal{Q}(x)} |W(h;q)| \leqslant \sum_{s \leqslant x} \sum_{a \bmod s} |W(\bar{a}h;s)| \sum_{\substack{r \leqslant x/s \\ r \equiv a \bmod s}} 1.$$

- Use Brun–Titchmarsh for the inner sum; then Cauchy–Schwarz and multiplicativity for the first moment of $W(\bar{a}h;s)$.
- We also require upper and lower bounds for $|\mathcal{Q}(x)|$, which are obtained by elementary means.

All moduli

Tentative Theorem. (K-Sound) For primes p and $k \geqslant 1$, let A_{p^k} be a subset of $(\mathbf{Z}/p^k\mathbf{Z})^n$. For $q \geqslant 1$, define

$$A_q = \{x \in (\mathbf{Z}/q\mathbf{Z})^m \mid x \bmod p^k \in A_{p^k} \text{ for all } p^k \mid\mid q\}.$$

Let $\mathcal{Q}$ be the set of q such that $\varrho(q) \geqslant 1$. Assume the same *Standing Assumption* as before:

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \log p \geqslant \alpha x.$$

Define Δ_q for all q. Then all previous results should still hold.

In other words, *no constraint or compatibility condition whatsoever* should be required for the subsets A_{p^k} when $k \geqslant 2$. The previous results correspond to the case when A_{p^k} is empty for $k \geqslant 2$.

Prime moduli

For roots of polynomial congruences $f(a) = 0 \bmod p$ to prime moduli (with f irreducible), the two types of measures lead a priori to different conjectures (except for degree 2, in which case they are the same):

- Convergence of Hooley's measures:

$$\frac{1}{\pi(x)} \sum_{p \leqslant x} \sum_{f(a)=0 \bmod p} \delta_{\{a/p\}}, \quad \pi(x) \sim \sum_{p \leqslant x} \varrho(p)$$

- ... or of the measures

$$\frac{1}{|\mathcal{P}(x)|} \sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \frac{1}{\varrho(p)} \sum_{f(a)=0 \bmod p} \delta_{\{a/p\}}, \quad \mathcal{P}(x) = \{p \leqslant x \mid \varrho(p) \geqslant 1\}.$$

A function field analogue suggests that, in this case, the first statement is more natural. But both should be true.