POISSON STATISTICS VIA THE CHINESE REMAINDER THEOREM

ANDREW GRANVILLE AND PÄR KURLBERG

Abstract. We consider the distribution of spacings between consecutive elements in subsets of $\mathbf{Z}/q\mathbf{Z}$ where q is highly composite and the subsets are defined via the Chinese remainder theorem. We give a sufficient criterion for the spacing distribution to be Poissonian as the number of prime factors of q tends to infinity, and as an application we show that the value set of a generic polynomial modulo q have Poisson spacings. We also study the spacings of subsets of $\mathbf{Z}/q_1q_2\mathbf{Z}$ that are created via the Chinese remainder theorem from subsets of $\mathbf{Z}/q_1\mathbf{Z}$ and $\mathbf{Z}/q_2\mathbf{Z}$ (for q_1, q_2 coprime), and give criteria for when the spacings modulo q_1q_2 are Poisson. Moreover, we also give some examples when the spacings modulo q_1q_2 are not Poisson, even though the spacings modulo q_1 and modulo q_2 are both Poisson.

1. Introduction

Let $1 = x_1 < x_2 < \cdots < x_m < q$ be the set of squares[1] modulo a large integer q. If $q = p$ is prime then $m = (p-1)/2$; that is, roughly half of the integers mod p are squares, so an integer chosen at random is square with probability close to $1/2$. So do the squares appear as if they are "randomly distributed" (if one can appropriately formulate this question)? For instance, if one chooses a random square x_i mod p, what is the probability that $x_{i+1} - x_i = 1$, or 2, or $3, \ldots$? Is it the same as for a random subset of the integers? In 1931 Davenport [4] showed that the answer is "yes" by proving that the probability that $x_{i+1} - x_i = d$ is $1/2^d + o_p(1)$. (Note that if one takes a random subset S of $[1, n]$ of size $n/2$ then the the proportion of $x \in S$ such that the next smallest element of S is $x + d$, is $\sim 1/2^d$ with probability 1.)

Date: February 10, 2005.

1991 *Mathematics Subject Classification.* Primary 11N69, Secondary 11K36.

A.G. has been supported in part by the National Science Foundation and by NSERC (Canada) during the preparation of this paper. P.K. supported in part by the National Science Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council.

[1]An integer x is a square mod q if there exists y for which $y^2 \equiv x \pmod{q}$.

If q is odd with k distinct prime factors, then $m = \phi(q)/2^k$. The average gap, s_q, between these squares is now a little larger than 2^k, which is large if k is large; so we might expect that the probability that $x_{i+1} - x_i = 1$ becomes vanishingly small as k gets larger. Hence, to test whether the squares appear to be "randomly distributed", it is more appropriate to consider $(x_{i+1} - x_i)/s_q$. If we have m integers randomly chosen from $1, 2, \dots, q-1$ then we expect that the probability that $(x_{i+1} - x_i)/s_q > t$ is $\sim e^{-t}$ as $q, s_q \to \infty$. In 1999/2000 Kurlberg and Rudnick [10, 9] proved that this is true for the squares mod q.

To a number theorist this is reminiscent of Hooley's 1965 result [7, 8] in which he proved that the set of integers coprime to q appear to be "randomly distributed" in the same sense, as the average gap $s_q = q/\phi(q)$ gets large[2].

In both of these examples the sets of integers $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ are obtained from sets of integers $\Omega_{p^a} \subset \mathbf{Z}/p^e\mathbf{Z}$ (for each prime power $p^e \| q$) by the Chinese Remainder Theorem (that is $a \in \Omega_q$ if and only if $a \in \Omega_{p^e}$ for all $p^e \| q$). We thus ask whether, in general, sets $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ created from sets $\Omega_{p^a} \subset \mathbf{Z}/p^e\mathbf{Z}$ (for each prime power $p^e \| q$) by the Chinese Remainder Theorem appear (in the above sense) to be "randomly distributed, at least under some reasonable hypotheses? This question is inspired by the Central Limit Theorem which tells us that, incredibly, if we add enough reasonable probability distributions together then we obtain a generic "random" distribution, such as the Poisson or Normal distribution.

Let us be more precise. For simplicity we restrict our attention to squarefree q. Suppose that for each prime p we are given a subset $\Omega_p \subset \mathbf{Z}/p\mathbf{Z}$. For q a squarefree integer, we define $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ using the Chinese remainder theorem; in other words, $x \in \Omega_q$ if and only if $x \in \Omega_p$ for all primes p dividing q. Let $s_q = q/|\Omega_q|$ be the average spacing between elements of Ω_q, and $r_q = 1/s_q = |\Omega_q|/q$ be the probability that a randomly chosen integer belongs to Ω_q. Let $1 = x_1 < x_2 < \cdots < x_m < q$ be the elements of Ω_q, and define $\Delta_j = (x_{j+1} - x_j)/s_q$ for all $1 \le j \le m-1$. For any given real numbers $t_1, t_2, \dots, t_k \ge 0$ define $\mathrm{Prob}_q(t_1, \dots, t_k)$ to be the proportion of these integers j for which $\Delta_{j+i} > t_i$ for each $i = 1, 2, \dots, k$.[3]

[2] Under a similar assumption, namely that $s_p = (p-1)/\phi(p-1)$ tends to infinity, Cobeli and Zaharescu has shown [3] that the spacings between primitive roots modulo p becomes Poissonian as p tends to infinity along primes.

[3] By letting $x_j = x_{j \pmod m}$ and $\Delta_j = \Delta_{j \pmod m}$ for any $j \in \mathbf{Z}$ we obtain the distribution of spacings "with wraparound", but in the limit $|\Omega_q| \to \infty$, $\mathrm{Prob}_q(t_1, \dots, t_k)$ is independent of whether spacings are considered with or without wraparound.

Suppose that Q is an infinite set of squarefree, positive integers which can be ordered in such a way that $s_q \to \infty$. We say that the spacings between elements in the sets Ω_q for $q \in Q$ become *Poisson distributed* if for any $t_1, t_2, \ldots, t_m \geq 0$

$$\mathrm{Prob}_q(t_1, t_2, \ldots, t_m) \to e^{-(t_1+t_2+\ldots+t_m)} \text{ as } s_q \to \infty,\ q \in Q.$$

For a given vector of integers $\mathbf{h} = (h_1, h_2, \ldots, h_{k-1})$, let $h_0 = 0$ and define the counting function[4] for k-tuples mod q as

$$N_k(\mathbf{h}, \Omega_q) = \#\{t \pmod q : \ t + h_i \in \Omega_q \text{ for } 0 \leq i \leq k-1\}.$$

Note that the average of $N_k(\mathbf{h}, \Omega_q)$ (over all possible $\mathbf{h}$) is $r_q^k\, q$.

Our main result shows that if for each fixed k, the k-tuples of elements of Ω_p are well-distributed for all sufficiently large primes p, then indeed the sets Ω_q become Poisson distributed.

Theorem 1. *Suppose that we are given subsets $\Omega_p \subset \mathbf{Z}/p\mathbf{Z}$ for each prime p. For each integer k, assume that*

$$N_k(\mathbf{h}, \Omega_p) = r_p^k \cdot p\ (1 + O_k((1-r_p)p^{-\epsilon})) \tag{1}$$

provided that $0, h_1, h_2, \ldots, h_{k-1}$ are distinct mod p. If $s_p = p^{o(1)}$ for all primes p, then the spacings between elements in the sets Ω_q become Poisson distributed as $s_q \to \infty$.

Remark 1. Theorem 12 in section 4 actually gives something a little more explicit and stronger.

From the theorem, we easily recover the result of Hooley, since for $\Omega_p = \{1, 2, \ldots, p-1\}$ we have $r_p = 1 - 1/p$ and thus

$$N_k(\mathbf{h}, \Omega_p) = p - k = r_p^k \cdot p \left(1 + O_k\left(\frac{1-r_p}{p}\right)\right);$$

and a generalization of the result Kurlberg-Rudnick using Weil's bounds for the number of points on curves:

Corollary 2. *Fix an integer d and let Ω_q be the set of d-th powers modulo q. Then the spacings between elements in the sets Ω_q become Poisson distributed as $s_q \to \infty$.*

Another situation where we may apply Weil's bounds is to the sets $\{x \mod q : \text{There exists } y \mod q \text{ such that } y^2 \equiv x^3+ax+b \pmod q\}$ for any given integers a, b; and indeed to coordinates of any given non-singular hyperelliptic curve. Thus we may deduce the analogy to Corollary 2 in these cases.

[4]The counting function is defined for $\mathbf{h}$ modulo q, so implicitly we consider gaps with wraparound.

In section 4 we also show that the spacings between residues mod q in the image of a polynomial having $n-1$ distinct critical values[5] (a generic condition) become Poisson distributed as $s_q \to \infty$:

Theorem 3. *Let f be a polynomial of degree n with integer coefficients. Regarding f as a map from $\mathbf{Z}/q\mathbf{Z}$ into itself, define Ω_q to be the image of f modulo q, i.e., $\Omega_q := \{x \pmod q : \text{ there exists } y \pmod q \text{ such that } f(y) \equiv x \pmod q\}$. If f has $n-1$ distinct critical values, then the spacings between elements in the sets Ω_q become Poisson distributed as $s_q \to \infty$.*

Remark 2. Theorem 3 is true for all polynomials, but the proof of this is considerably more complicated and will appear in a separate paper. In fact, there are polynomials for which (1) does not hold - see section 4.2 for more details. We also note that if f has $n-1$ distinct critical values, Birch and Swinnerton-Dyer have proved [2] that

$$|\Omega_p| = |\{x \in \mathbb{F}_p : x = f(y) \text{ for some } y \in \mathbb{F}_p\}| = c_n p + O_n(p^{1/2})$$

where

$$c_n = 1 - \frac{1}{2} + \frac{1}{3!} - \ldots - (-1)^n \frac{1}{n!}$$

is the truncated Taylor series for $1 - e^{-1}$. (Note that $n! \cdot (1 - c_n)$ is the "nth derangement number" from combinatorics, so c_n can be interpreted as the probability that a random permutation $\sigma \in S_n$ has at least one fixed point. In fact, this is no coincidence - for these polynomials the Galois group of $f(x) - t$, over $\mathbb{F}_p(t)$, equals S_n, and the proportion of elements in the image of f, up to an error $O(p^{-1/2})$, equals the proportion of elements in the Galois group fixing at least one root.) Since the expected cardinality of the image of a random map from $\mathbb{F}_p$ to $\mathbb{F}_p$ is $p \cdot (1 - e^{-1})$, the above result can be interpreted as saying that the cardinality of the image of a generic polynomial (of large degree) behaves as that of a random map. Their result also implies that $s_q \to \infty$ as the number of prime factors of q tends to infinity.

In Theorem 1 we proved that if *all* k-tuples in Ω_p are "well-distributed" (in the sense of (1)) for all primes p then the Ω_q become Poisson distributed as $s_q \to \infty$. Perhaps though one needs to make less assumption on the sets Ω_p? For example, perhaps it suffices to simply assume an averaged form of (1), like

$$\frac{1}{p^{k-1}} \sum_{\mathbf{h}} \left| \frac{N_k(\mathbf{h}, \Omega_p)}{r_p^k\, p} - 1 \right| \ll_k (1 - r_p) p^{-\epsilon}$$

[5]The critical values of f is the set $\{f(\xi) : \xi \in \mathbf{C}, f'(\xi) = 0\}$.

where the sum is over all $\mathbf{h}$ for which $0, h_1, h_2, \dots h_{k-1}$ are distinct mod p. We have been unable to prove this as yet.

In the central limit theorem, where one adds together lots of distributions to obtain a normal distribution, the hypotheses for the distributions which are summed is very weak. So perhaps in our problem we do not need to make an assumption which is as strong as (1)? In section 5 we suppose that we are given sets Ω_{q_1} and Ω_{q_2} of residues modulo q_1 and q_2 (with $(q_1, q_2) = 1$), and try to determine whether the spacings in Ω_q (where $q = q_1 q_2$) is close to a Poisson distribution. We show that under certain natural hypotheses the answer is "yes". These take the form: If Ω_{q_1} is suitably "strongly Poisson" then Ω_q is Poisson if and only if Ω_{q_2} is Poisson with an appropriate parameter.

On the other hand, if we allow the sets to be correlated, then the answer can be "no". In section 6 we give three examples in which the distribution of points in Ω_q is not consistent with that of a Poisson distribution. The constructions can be roughly described as follows:

- Ω_{q_1} is random and small, and $\Omega_{q_2} = \{a : 1 \le a \le q_2/2\}$.
- $\Omega_{q_2} = \Omega_{q_1}$ is a random subset of $\{1, 2, \dots, q_1\}$ where $q_2 = q_1 + 1$.
- Each Ω_{q_i} is a random subset of $\{a : 1 \le a \le q_i, \ m|a\}$ for $i = 1, 2$, with integer $m \ge 2$.

1.1. **Acknowledgments.** P.K. would like to thank J. Brzeziński, T. Ekedahl, M. Jarden, and Z. Rudnick for helpful discussions.

2. Poisson statistics primer

Given a positive integer q and a subset $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$, let $s_q = q/|\Omega_q|$ be the average gap between consecutive elements in Ω_q. One can view $r_q = 1/s_q$ as the probability that a randomly selected element in $\mathbf{Z}/q\mathbf{Z}$ belongs to Ω_q.

If $0 < x_1 < x_2 < \dots$ are the positive integers belonging to Ω_q then define $\Delta_j = (x_{j+1} - x_j)/s_q$ for all $j \ge 1$; we are interested in the statistical behavior of these gaps as $q \to \infty$, along some subsequence of square free integers. We define the (normalized) *limiting spacing distribution*, if it exists, as a probability measure μ such that

$$\lim_{q \to \infty} \frac{\#\{j : \ 1 \le j \le |\Omega_q|, \ \Delta_j \in I\}}{|\Omega_q|} = \int_I d\mu(x)$$

for all compact intervals $I \subset \mathbf{R}^+$. If $d\mu(x) = e^{-x}\, dx$ and the gaps are independent (i.e., that k consecutive gaps are independent for any k), the limiting spacing distribution is said to be *Poissonian*. This can be characterized (under fairly general conditions) as follows: For any fixed $\lambda > 0$ and integer $k \ge 0$, the probability that there are exactly

k (renormalized) points in a randomly chosen interval of length λ, is given by $\frac{\lambda^k e^{-\lambda}}{k!}$ (see [1], section 23.)

We shall use a characterization of the Poisson distribution which is relatively easy to work with: The *k-level correlation* for a compact set $X \subset \{x \in \mathbf{R}^{k-1} : 0 < x_1 < x_2 < \ldots < x_{k-1}\}$ is defined as

$$R_k(X, \Omega_q) = \frac{1}{|\Omega_q|} \sum_{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1}} N_k(\mathbf{h}, \Omega_q). \tag{2}$$

Note that we ensure that $0 < h_1 < \ldots < h_{k-1}$ else $N_k(\mathbf{h}, \Omega_q) = N_\ell(\mathbf{h}', \Omega_q)$ where $0 < h'_1 < \ldots < h'_{\ell-1}$ are the distinct integers amongst $0, h_1, \ldots, h_{k-1}$.

Now for any positive real numbers $b_1, b_2, \ldots, b_{k-1}$ define

$$B(b_1, b_2, \ldots, b_{k-1}) := \{x \in \mathbf{R}^{k-1} : 0 < x_i - x_{i-1} \le b_i \text{ for } i = 1, 2, \ldots k-1\}$$

where we let $x_0 = 0$. Let $\mathbb{B}_k$ be the set of such (not necessarily rectangular) boxes.

Suppose we are given a sequence of integers $Q = \{q_1, q_2, \ldots\}$ with $s_{q_i} \to \infty$ as $i \to \infty$. Then (e.g., see Appendix A of [10]) the spacings of the elements in Ω_{q_n} become Poisson as $n \to \infty$ if and only if for each integer $k \ge 2$ and box $X \in \mathbb{B}_k$,

$$R_k(X, \Omega_{q_n}) \to \mathrm{vol}(X) \quad \text{as } n \to \infty.$$

It will be useful to include a further definition along similar lines. Suppose θ_n is a positive real number for each n. We say that the spacings of the elements in Ω_{q_n} become Poisson with parameter θ_n as $n \to \infty$ if and only if for each integer $k \ge 2$ and box $X \in \mathbb{B}_k$,

$$R_k(\theta_n X, \Omega_{q_n}) \to \mathrm{vol}(\theta_n X) \quad \text{as } n \to \infty.$$

Notice that “Poisson with parameter 1” is the same thing as “Poisson”. (In fact, Poisson with any bounded parameter is the same as Poisson.)

2.1. **Correlations for randomly selected sets.**

Let $X_1, X_2, \ldots, X_q$ be independent Bernoulli random variables with parameter $1/\sigma \in (0, 1)$. In other words, $X_i = 1$ with probability $1/\sigma$, and $X_i = 0$ with probability $1 - 1/\sigma$. Given an outcome of $X_1, X_2, \ldots, X_q$, we define $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ by letting $i \in \Omega_q$ if and only if $X_i = 1$. Note that the expected average gap is then given by σ. Below we write $R_k(x, q)$ for $R_k(x, \Omega_q)$.

Lemma 4. *As we vary over all subsets of $\mathbf{Z}/q\mathbf{Z}$ with the probability space as above, we have*

$$\mathbb{E}(R_k(X, q)) = \mathrm{vol}(X) + O_k(1/\sigma + \sigma/q)$$

and

$$\mathbb{E}\left(\left(R_k(X,q)-\mathrm{vol}(X)\right)^2\right) \ll_k 1/\sigma + \sigma/q$$

Proof. Using conditional expectations we write

$$\mathbb{E}(R_k(X,q)) = \sum_{r=k}^{q} \mathrm{Prob}(|\Omega_q|=r)\ \mathbb{E}(R_k(X,q) : |\Omega_q|=r)$$

$$= \sum_{h\in\sigma X\cap \mathbf{Z}^{k-1}} \sum_{r=k}^{q} \frac{\mathrm{Prob}(|\Omega_q|=r)}{r} \sum_{i=1}^{q} \mathbb{E}\left(x_i x_{i+h_1}\dots x_{i+h_{k-1}} : |\Omega_q|=r\right)$$

Now, the number of ways to have $|\Omega_q| = r$ is $\binom{q}{r}$, and the number of ways to have $|\Omega_q| = r$ with $i, i+h_1, \dots, i+h_{k-1} \in \Omega_q$ is $\binom{q-k}{r-k}$. Therefore,

$$\mathbb{E}\left(x_i x_{i+h_1}\dots x_{i+h_k} : |\Omega_q|=r\right) = \binom{q-k}{r-k}\Big/\binom{q}{r}$$

Note that $R_k(X,q) = 0$ if $|\Omega_q| \le k-1$, and

$$\mathrm{Prob}(|\Omega_q|=r) = \binom{q}{r}\sigma^{-r}(1-1/\sigma)^{q-r}.$$

Taking $q \ge 4k$ with q/σ large, we obtain

$$\mathbb{E}(R_k(X,q)) = \left|\sigma X\cap \mathbf{Z}^{k-1}\right| \sum_{r=k}^{q} \frac{1}{r}\ \sigma^{-r}(1-1/\sigma)^{q-r} q \cdot \binom{q-k}{r-k}$$

$$= q\sigma^{-k}\left(\sigma^{k-1}\ \mathrm{vol}(X) + O(\sigma^{k-2})\right)\cdot \sum_{r=k}^{q} \frac{\sigma^{k-r}}{r}\ (1-1/\sigma)^{(q-k)-(r-k)}\binom{q-k}{r-k}$$

$$= (q/\sigma)\left(\mathrm{vol}(X)+O(1/\sigma)\right)\cdot \sum_{R=0}^{Q} \frac{1}{R+k}\ (1/\sigma)^R(1-1/\sigma)^{Q-R}\binom{Q}{R}$$

where $Q = q-k$ and $R = r-k$. Now

$$\frac{1}{R+k} = \frac{1}{R+1} + O\left(\frac{k}{(R+1)(R+2)}\right),$$

so the last sum is

$$\frac{\sigma}{(Q+1)}\left(1-(1-1/\sigma)^{Q+1}\right) + O\left(\frac{k\sigma^2}{Q^2}\right) = \frac{\sigma}{q}\left(1+O_k\left(\frac{\sigma}{q}\right)\right),$$

since $(Q/\sigma)^A(1-1/\sigma)^Q \ll_A 1$, and thus

$$\mathbb{E}(R_k(X,q)) = \mathrm{vol}(X) + O\left(1/\sigma + \sigma/q\right).$$

For the variance, note that

$$\mathbb{E}\left(R_k(X,q)^2\right) = \sum_{r=k}^{q} \mathrm{Prob}\left(|\Omega_q|=r\right)\mathbb{E}\left(R_k(X,q)^2 : |\Omega_q|=r\right)$$

$$= \sum_{r=k}^{q} \binom{q}{r} \sigma^{-r}(1-1/\sigma)^{q-r}\frac{1}{r^2}\cdot$$

$$\cdot \sum_{h,H\in\sigma X\cap\mathbf{Z}^{k-1}} \sum_{i,j=1}^{q} \mathbb{E}\left(x_i x_{i+h_1} x_{i+h_2}\dots x_{i+h_{k-1}} x_j x_{j+H_1}\dots x_{j+H_{k-1}} : |\Omega_q|=r\right)$$

If there are l distinct elements in $\{i, i+h_1, \dots, h_{k-1}, j, j+H_1, \dots, j+H_{k-1}\}$ then the expectation is

$$\binom{q-l}{r-l}\Big/\binom{q}{r}.$$

Given α, β, h and H there is a solution to $i+h_\alpha = j+H_\beta$ for $O(k^2 q)$ values of i and j. Thus our main term is

$$\left(q^2+O_k(q)\right)\binom{q-2k}{r-2k}\Big/\binom{q}{r}.$$

We treat the other terms as follows: Fix d and consider i and j with $j \equiv i+d \pmod q$. Select $u_1, \dots, u_m, v_1, \dots, v_m$ with $h_{u_t} \equiv H_{v_t} + d \pmod q$. The number of choices for i and j is q. H can be chosen freely and so can $k-m-1$ of the coordinates of h. The total number of choices is thus

$$\asymp_{X,k} q\sigma^{k-1}\sigma^{k-m-1}$$

Moreover the number of choices for d is $\asymp_X \sigma$. Therefore, since $l = 2k - m$, we have[6]

$$\mathbb{E}\left(R_k(X,q)^2\right) = \sum_{r=k}^{q} \frac{\sigma^{-r}(1-1/\sigma)^{q-r}}{r^2} \times$$

$$\times\left(\left|\sigma X \cap \mathbf{Z}^{k-1}\right|^2 \binom{q-2k}{r-2k} \left(q^2+O(q)\right) + O\left(\sum_{m=1}^{k} \binom{q-2k+m}{r-2k+m} q\sigma^{2k-1-m}\right)\right)$$

$$= \left(q^2+O(q)\right)\left(\sigma^{k-1}\operatorname{vol}(X)+O(\sigma^{k-2})\right)^2 \sum_{r=2k}^{q} \binom{q-2k}{r-2k} \frac{1}{r^2}\, \sigma^{-r}(1-1/\sigma)^{q-r}$$

$$+ O\left(\sum_{m=1}^{k} q\sigma^{2k-1-m} \sum_{r=2k-m}^{q} \binom{q-2k+m}{r-2k+m} \frac{\sigma^{-r}(1-1/\sigma)^{q-r}}{r^2}\right).$$

Now, for $k \le \ell \le 2k$ take $Q = q - \ell$ and $R = r - \ell$, and note that

$$\frac{1}{(R+\ell)^2} = \frac{1}{(R+1)(R+2)} + O_k\left(\frac{1}{(R+1)(R+2)(R+3)}\right),$$

to obtain

$$\sum_{r=\ell}^{q} \binom{q-\ell}{r-\ell} \frac{1}{r^2}\, \sigma^{-r}(1-1/\sigma)^{q-r}$$

$$= \sigma^{-\ell} \sum_{R=0}^{Q} \binom{Q}{R} \frac{1}{(R+\ell)^2}\, (1/\sigma)^R (1-1/\sigma)^{Q-R} \sigma^{-\ell} \cdot$$

$$\cdot \left(\frac{\sigma^2}{(Q+1)(Q+2)} + O_k\left(\frac{\sigma^3}{q^3}\right)\right)$$

$$= \frac{\sigma^{2+2k-\ell}}{\sigma^{2k} q^2}\left(1 + O_k\left(\frac{\sigma}{q}\right)\right)$$

Substituting this in above gives

$$\mathbb{E}\left(R_k(X,q)^2\right) = \operatorname{vol}(X)^2 + O\left(1/\sigma + \sigma/q\right),$$

and hence

$$\mathbb{E}\left(\left(R_k(X,q) - \operatorname{vol}(X)\right)^2\right) = \mathbb{E}\left(\left(R_k(X,q)\right)^2\right) - \operatorname{vol}(X)^2$$

$$= O\left(1/\sigma + \sigma/q\right).$$

□

One can interpret this result as saying that almost all sets have Poisson spacings.

[6] We use the convention that $\binom{n}{k} = 0$ if $k < 0$.

3. Correlations via the Chinese remainder theorem

3.1. **Counting solutions to congruences.** Suppose that $\Gamma = \{\gamma_{i,j} : 0 \leq i \neq j \leq k-1 \text{ with } \gamma_{i,j} = \gamma_{j,i}\}$ is a given set of positive squarefree integers for which

$$\gcd(\gamma_{i,j}, \gamma_{j,l}) \text{ divides } \gamma_{i,l} \text{ for any distinct } i, j, l \tag{3}$$

Define

$$\gamma_j := \underset{0 \leq i \leq j-1}{\mathrm{LCM}} \gamma_{i,j}$$

and let

$$\gamma(\Gamma) := \gamma_1 \dots \gamma_{k-1}$$

Once one understands all this terminology one easily sees that

Lemma 5. *If σ is a permutation of $\{1, \dots, k-1\}$ and $\sigma(0) = 0$ define $\gamma_{i,j}^{(\sigma)} = \gamma_{\sigma(i),\sigma(j)}$. Then $\gamma^{(\sigma)}(\Gamma) = \gamma(\Gamma)$.*

Define $c(\Gamma)$ to be the squarefree product of the primes dividing $\gamma(\Gamma)$, so that $c(\Gamma)$ divides $\gamma(\Gamma)$, which divides $c(\Gamma)^{k-1}$.

Given a squarefree positive integer c, and a set of distinct non-negative integers $h_0 = 0, h_1, h_2, \dots, h_{k-1}$ let $\mathbf{h} = (h_1, \dots, h_{k-1})$ and define

$$\gamma_{i,j}(\mathbf{h}) := \gcd(c, h_j - h_i) \text{ for } 0 \leq i \neq j \leq k-1,$$

and then $\Gamma(\mathbf{h})$ accordingly.

For a given set Γ and integer $c = c(\Gamma)$ define

$$\begin{aligned} M_\Gamma(H) := \#\{&(h_0 = 0, h_1, \dots, h_{k-1}) \in \mathbb{Z}^k : \\ &h_i \neq h_j \text{ for } i \neq j,\ 0 \leq h_i \leq H \text{ for all } 0 \leq i \leq k-1 \text{ and } \Gamma(\mathbf{h}) = \Gamma\} \end{aligned} \tag{4}$$

Finally for given integers γ and c, with $c|\gamma|c^{k-1}$, define

$$M_\gamma(H) := \sum_{\Gamma : \gamma(\Gamma) = \gamma} M_\Gamma(H). \tag{5}$$

We wish to give good upper bounds of $M_\gamma(H)$. First note that if $\gamma_{i,j} > H$, then $M_\Gamma(H) = 0$ else $\gamma_{i,j} | h_i - h_j$ and so $H < \gamma_{i,j} \leq |h_i - h_j| \leq H$. Thus if $\gamma > H^{\binom{k}{2}}$ then $M_\gamma(H) = 0$ else $\max \gamma_{i,j} \geq \gamma^{1/\binom{k}{2}} > H$.

The Stirling number of the second kind, $S(k, \ell)$, is defined to be the number of ways of partitioning a k element set into ℓ non-empty subsets, and may be evaluated as

$$S(k, \ell) = \frac{1}{(\ell-1)!} \sum_{j=1}^{\ell} (-1)^{\ell-j} \binom{\ell-1}{j-1} j^{k-1}.$$

One can show that $S(k, k-e) \leq \binom{k}{2}^e$.

Lemma 6. $\#\{\Gamma : \gamma(\Gamma) = \gamma\} \leq \prod_{p^e \| \gamma} S(k, k-e) \leq \binom{k}{2}^{\#\{p^e : p^e | \gamma\}}$.

Proof. For each prime p dividing γ, we partition $\{0, \dots, k-1\}$ into subsets where i and j are in the same subset if $p | \gamma_{i,j}$ (by (3) this is consistent). The bound follows. □

Now we wish to bound $M_\Gamma(H)$.

Proposition 7. *We have*

$$M_\Gamma(H) \leq \prod_{i=1}^{k-1} \Big(\frac{H}{\gamma_i^{(\sigma)}} + 1 \Big) \text{ for any } \sigma \in S_{k-1}.$$

Proof. Certainly we may rearrange the order, using σ, without changing the question; so relabel $\sigma(i)$ as i. Now by induction on $k \geq 1$, we have, for each given $(h_1, \dots, h_{k-2}) \in M_{\Gamma'}(H)$ where Γ' is Γ less all elements of the form $\gamma_{i,k-1}$ or $\gamma_{k-1,i}$ for $0 \leq i \leq k-1$, that if $(h_1, \dots, h_{k-1}) \in M_\Gamma(H)$, then $h_{k-1} \equiv h_i \bmod \gamma_{i,k-1}$ for each i, $0 \leq i \leq k-2$ and so h_{k-1} is determined modulo γ_{k-1}. Thus the number of possibilities for h_{k-1} is $\leq H/\gamma_{k-1} + 1$, and the result follows. □

Corollary 8. *We have*

$$M_\Gamma(H) \leq 2^{k-1} H^{k-1} / \prod_{i=1}^{k} \min(\gamma_i, H)$$

In particular,

$$M_\Gamma(H) \leq \begin{cases} 2^{k-1} H^{k-1}/\gamma & \text{if each } \gamma_i \leq H \\ 2^{k-1} H^{k-2} & \text{if any } \gamma_j \geq H \end{cases} \tag{6}$$

Remark: When $k = 2$ the first bound in (6) is up to the constant best possible. For $k = 3$ things are immediately more complicated. For suppose $\gamma_{0,1}, \gamma_{0,2}, \gamma_{1,2}$ are all coprime and each lies in the interval $(T, 2T)$ with $T > \sqrt{H}$. Then $\gamma_1 \approx T, \gamma_2 > H$ and so $M_\Gamma(H) \leq 4H/T$ is what the corollary yields, rather than what we might predict, $\approx H^2/T^3$. Thus this "prediction" cannot be true if $T > H^{2/3+\epsilon}$.

Next we look for a "good" re-ordering σ; select $\sigma(1)$ so as to maximize $\gamma_{\sigma(1),0}$. Now swap $\sigma(1)$ and 1 and then swap $\sigma(2)$ and 2 so as to maximize $\text{LCM}(\gamma_{\sigma(2),1}, \gamma_{\sigma(2),0})$. Proceeding like this we obtain

$$\gamma_r = LCM[\gamma_{r,0}, \gamma_{r,1}, \dots, \gamma_{r,r-1}] \geq LCM[\gamma_{j,0}, \gamma_{j,1}, \dots \gamma_{j,r-1}] \text{ for all } j \geq r.$$

Note that

$$\gamma_{r+1} \leq LCM[\gamma_{r,0}, \dots, \gamma_{r,r-1}] \gamma_{r+1,r} = \gamma_r \gamma_{r+1,r} \leq H \gamma_r. \tag{7}$$

Now in our general construction let $I = \{i \in [1, \ldots, k-1] : \gamma_i \le H\}$ and write $D(\Gamma) = \prod_{i=1}^{k-1} \min(\gamma_i, H)$ so that $M_\Gamma(H) \le (2H)^{k-1}/D(\Gamma)$, and $D(\Gamma) = H^{k-|I|-1} D_I(\Gamma)$ where $D_I(\Gamma) = \prod_{i \in I} \gamma_i$. Also, by (7) we have $\gamma_{r+1} \le H\gamma_r$, and thus

$$\gamma = \gamma_1 \ldots \gamma_{k-1} \le \prod_{i \in I} \gamma_i \cdot \prod_{j=1}^{k-|I|-1} H^{1+j} = D_I(\Gamma) H^{\frac{1}{2}(k-|I|-1)(k-|I|+2)}.$$

Let us suppose $|I| = \rho$ where $1 \le \rho \le k-1$ (note that we always have $\gamma_1 \le H$). Then $1 \le D_I(\Gamma) \le H^\rho$. Write $D_I(\Gamma) = H^{\rho\theta}$ for some $0 \le \theta \le 1$. Thus

$$D(\Gamma) = H^{k-1-\rho+\rho\theta} \tag{8}$$

and

$$\gamma \le H^{\rho\theta + \frac{1}{2}(k-\rho-1)(k-\rho+2)} \le H^{\frac{1}{2}(k-\rho-1)(k-\rho+2)+\rho} \tag{9}$$

We note that $\frac{1}{2}(k-\rho-1)(k-\rho+2)+\rho$ is decreasing in the range $1 \le \rho \le k-1$. Therefore if we choose τ in the range $1 \le \tau \le k-1$ so that

$$H^{\frac{1}{2}(\tau-2)(\tau+1)+k+1-\tau} < \gamma \le H^{\frac{1}{2}(\tau-1)(\tau+2)+k-\tau} \tag{10}$$

then $\rho \le k - \tau$.

We wish to bound $D(\Gamma)$ from below. By (8), we immediately get

$$D(\Gamma) \ge H^{k-1-\rho}$$

Moreover, if for a given $\rho \le k-\tau$, we have $\gamma \le H^{\frac{1}{2}(k-\rho-1)(k-\rho+2)+\rho\theta}$ then

$$H^{\rho\theta} \ge \frac{\gamma}{H^{\frac{1}{2}(k-\rho-1)(k-\rho+2)}}$$

and thus

$$D(\Gamma) = H^{k-1-\rho} \cdot H^{\rho\theta} \ge \frac{\gamma H^{k-1-\rho}}{H^{\frac{1}{2}(k-\rho-1)(k-\rho+2)}} = \frac{\gamma}{H^{\frac{1}{2}(k-\rho-1)(k-\rho)}}.$$

Since we are going to relinquish control of γ, other than the size, we obtain the bound from the worst case. To facilitate the calculation, we write $\gamma = H^\lambda, D(\Gamma) = H^\Delta$ and $\mu = k-1-\rho$ so that $k-2 \ge \mu \ge \tau - 1$. With this notation, (10) is equivalent to

$$\frac{\tau^2}{2} - \frac{3\tau}{2} + k < \lambda \le \frac{\tau^2}{2} - \frac{\tau}{2} + k - 1.$$

For a given λ in our range we thus have, from the bounds above,

$$\Delta \ge \min_{\mu \ge \tau} \left(\max \left\{ \min_{\substack{\mu: \\ \frac{1}{2}\mu(\mu+3) \ge \lambda}} \mu, \min_{\substack{\mu: \\ \frac{1}{2}\mu(\mu+3) \le \lambda}} \lambda - \frac{1}{2}\mu(\mu+1) \right\} \right) \ge u$$

where we define u to be the positive real number for which

$$\frac{1}{2}u(u+3) = \lambda$$

so that

$$\left(u+\frac{3}{2}\right)^2 = u(u+3)+\frac{9}{4} = 2\lambda+\frac{9}{4} > \left(\tau-\frac{3}{2}\right)^2 + 2k \geq 2k+\frac{1}{4},$$

if τ is an integer. Note also that $H^\Delta = D(\Gamma) \geq H^{k-1-\rho} \geq H^{k-1-(k-\tau)}$ so that $\Delta \geq \tau - 1$. Therefore $\Delta \geq \max(\tau-1, \sqrt{2k+1/4}-3/2)$. Thus we have proved the following:

Corollary 9. *Let τ be an integer $1 \leq \tau \leq k$, and define $w(\tau) = \frac{1}{2}(\tau-\frac{1}{2})^2 + k - \frac{9}{8}$. If $H^{w(\tau-1)} < \gamma \leq H^{w(\tau)}$ then*

$$M_\Gamma(H) \ll_k H^{k-\max\{\tau, \sqrt{2k+1/4}-1/2\}}.$$

Note that $w(k-1) = k(k-1)/2$, and let $\tau_1 = [\sqrt{2k+1/4}-\frac{1}{2}]$. Combining this with Lemma 6 and Corollary 8 gives that

$$M_\gamma(H) \ll_k \prod_{p^e \| \gamma} S(k, k-e) \cdot$$

$$\cdot \begin{cases} H^{k-1}/\gamma & \text{for} \qquad \gamma \leq H, \\ H^{k-2} & \text{for} \qquad H < \gamma \leq H^{\omega(0)} \\ H^{k+1/2-\sqrt{2k+1/4}} & \text{for } H^{w(0)} < \gamma \leq H^{w(\tau_1)} \\ H^{k-\tau} & \text{for } H^{w(\tau-1)} < \gamma \leq H^{w(\tau)} \ \tau_1+1 \leq \tau \leq k-1 \end{cases}$$

3.2. **Proof of Theorem 1.** For $\mathbf{h} \in \mathbf{Z}^{k-1}$, define the "error term" $\varepsilon_k(\mathbf{h}, q)$ by

$$N_k(\mathbf{h}, q) = r_q^{k-1}|\Omega_q|(1+\varepsilon_k(\mathbf{h}, q)).$$

We will need to use bounds on the size of $|\varepsilon_k(\mathbf{h}, p)|$, so select $A_{p,k}$ so that

$$|\varepsilon_k(\mathbf{h}, p)| \leq A_{p,k}$$

for all $\mathbf{h}$ for which $0, h_1, \ldots h_{k-1}$ are distinct mod p. If $0, h_1, \ldots h_{k-1}$ are not all distinct mod p then let $\mathbf{h}'$ be the set of distinct residues amongst $0, h_1, \ldots, h_{k-1}$ mod p; if $\mathbf{h}'$ contains $\ell \geq 1$ elements, then $N_k(\mathbf{h}, p) = N_\ell(\mathbf{h}', p)$ so that

$$\varepsilon_k(\mathbf{h}, p) = s_p^{k-\ell} - 1 + s_p^{k-\ell}\varepsilon_\ell(\mathbf{h}', p). \tag{11}$$

We will assume that $A_{p,k}$ is non-decreasing as k increases[7].

[7]This is a benign assumption since we may replace each $A_{p,k}$ by $\max_{\ell \leq k} A_{p,\ell}$.

For $d > 1$ a square free integer, put $e_k(\mathbf{h}, 1) = 1$ and

$$e_k(\mathbf{h}, d) = \prod_{p|d} \varepsilon_k(\mathbf{h}, p),$$

so that

$$N_k(\mathbf{h}, q) = \prod_{p|q} r_p^{k-1}|\Omega_p|\,(1 + e_k(\mathbf{h}, p)) = r_q^{k-1}|\Omega_q| \sum_{d|q} e_k(\mathbf{h}, d).$$

With this notation

$$R_k(X, \Omega_q) = \frac{1}{|\Omega_q|} \sum_{\mathbf{h}\in s_qX\cap\mathbf{Z}^{k-1}} N_k(\mathbf{h}, q) = r_q^{k-1} \sum_{\mathbf{h}\in s_qX\cap\mathbf{Z}^{k-1}} 1 + \text{Error}.$$

where

$$\text{Error} = r_q^{k-1} \sum_{\substack{d|q\\ d>1}} \sum_{\mathbf{h}\in s_qX\cap\mathbf{Z}^{k-1}} e_k(\mathbf{h}, d) \tag{12}$$

Since $s_q = 1/r_q$, the main term equals

$$r_q^{k-1} \sum_{\mathbf{h}\in s_qX\cap\mathbf{Z}^{k-1}} 1 = r_q^{k-1}\left(\text{vol}(s_qX) + O(s_q^{k-2})\right) = \text{vol}(X) + O(1/s_q).$$

To prove the theorem we wish to show that Error$= o(1)$. To begin with we show that the average of $e_k(\mathbf{h}, d)$, over a full set of residues modulo d, equals zero for $d > 1$:

Lemma 10. *If $d > 1$ then*

$$\sum_{\mathbf{h}\in(\mathbf{Z}/d\mathbf{Z})^{k-1}} e_k(\mathbf{h}, d) = 0$$

Proof. For any prime p we have

$$\begin{aligned}|\Omega_p|^k = \sum_{\mathbf{h}\in(\mathbf{Z}/p\mathbf{Z})^{k-1}} N_k(\mathbf{h}, p) &= r_p^{k-1}|\Omega_p| \sum_{\mathbf{h}\in(\mathbf{Z}/p\mathbf{Z})^{k-1}} (1 + \varepsilon_k(\mathbf{h}, p))\\ &= p^{k-1}r_p^{k-1}|\Omega_p| + pr_p^k \sum_{\mathbf{h}\in(\mathbf{Z}/p\mathbf{Z})^{k-1}} e_k(\mathbf{h}, p)\end{aligned}$$

so that $\sum_{\mathbf{h}\in(\mathbf{Z}/p\mathbf{Z})^{k-1}} e_k(\mathbf{h}, p) = 0$. The result follows as $e_k(\mathbf{h}, d)$ is multiplicative. $\square$

Throughout this section we shall take $\tau_1 = [\sqrt{2k + 1/4} - \frac{1}{2}]$, $v(0) = k - 2$, $v(\tau_1) = k + \frac{1}{2} - \sqrt{2k + 1/4}$, $v(\tau) = k - \tau$ for $\tau_1 + 1 \le \tau \le k - 1$ and $w(\tau) = k - 9/8 + (\tau - 1/2)^2/2$.

Proposition 11. *Suppose that we are given $R \in [0,1]$, as well as $\alpha_0, \alpha_1, \beta_1, \alpha(\tau), \beta(\tau) > 0$, for $\tau_1 \leq \tau \leq k-1$. Assume that $|\Omega_p| > p^{1-\alpha(\tau)}$ for all τ and all primes p (so that $s_p \leq p^{\alpha(\tau)}$). Then*

$$\begin{aligned}
\text{Error} \ll\, & s_q^{\alpha_0 R-1} \prod_{p|q} \Big(1 + O_k(p^{1-\alpha_0}(A_{p,k} + (s_p-1)/p))\Big) \\
& + s_q^{\alpha_1-\beta_1 R} \prod_{p|q} \Big(1 + O_k(p^{\beta_1}(A_{p,k} + (s_p-1)/p^{1+\alpha_1})\Big) \\
& + \sum_{\substack{\tau=0 \text{ or} \\ \tau_1 \leq \tau \leq k-1}} s_q^{v(\tau)+\alpha(\tau)w(\tau)-(k-1)-\beta(\tau)R} \prod_{p|q} \left(1 + p^{\beta(\tau)} O_k\Big(A_{p,k} + \frac{s_p-1}{p^{\alpha(\tau)}}\Big)\right).
\end{aligned}$$

Proof. We split the divisor sum in (12) into two parts depending on the size of the divisor d.

Small d: We first consider $d \leq s_q^R$. A point $\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1}$ is contained in a unique cube $C_{\mathbf{h},d} \subset \mathbf{R}^{k-1}$ of the form

$$C_{\mathbf{h},d} = \{(x_1, x_2, \ldots, x_{k-1}) : dt_i \leq x_i < d(t_i+1), t_i \in \mathbf{Z},\ i = 1, 2, \ldots, k-1\}$$

We say that $\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1}$ is a *d-interior* point of $s_q X$ if $C_{\mathbf{h},d} \subset s_q X$, and if $C_{\mathbf{h},d}$ intersects the boundary of $s_q X$, we say that h is a *d-boundary point* of $s_q X$.

By Lemma 10, the sum over the d-interior points is zero, and hence

$$r_q^{k-1} \sum_{\substack{d|q \\ 1<d\leq s_q^R}} \sum_{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1}} e_k(\mathbf{h}, d) = r_q^{k-1} \sum_{\substack{d|q \\ 1<d\leq s_q^R}} \sum_{\substack{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1} \\ \mathbf{h} \text{ is } d\text{-boundary point}}} e_k(\mathbf{h}, d) \tag{13}$$

Now, the number of cubes $C_{\mathbf{h},d}$ intersecting the boundary of $s_q X$ is $\ll (s_q/d)^{k-2}$, and hence (13) is

$$\ll r_q^{k-1} \sum_{\substack{d|q \\ 1<d\leq s_q^R}} (s_q/d)^{k-2} \sum_{\mathbf{h} \in (\mathbf{Z}/d\mathbf{Z})^{k-1}} |e_k(\mathbf{h}, d)|$$

$$= \frac{1}{s_q} \sum_{\substack{d|q \\ 1<d\leq s_q^R}} \frac{1}{d^{k-2}} \sum_{\mathbf{h} \in (\mathbf{Z}/d\mathbf{Z})^{k-1}} |e_k(\mathbf{h}, d)| \tag{14}$$

Further,

$$\sum_{\mathbf{h} \in (\mathbf{Z}/d\mathbf{Z})^{k-1}} |e_k(\mathbf{h}, d)| = \prod_{p|d} \sum_{\mathbf{h} \in (\mathbf{Z}/p\mathbf{Z})^{k-1}} |e_k(\mathbf{h}, p)|$$

By assumption, $|e_\ell(\mathbf{h}', p)| \le A_{p,\ell} \le A_{p,k}$ whenever $\mathbf{h}'$ has $\ell \le k$ distinct elements mod p. Therefore, by (11),

$$|e_k(\mathbf{h}, p)| \le s^{k-\ell} - 1 + s_p^{k-\ell} A_{p,k}, \tag{15}$$

for all $\mathbf{h}$ with ℓ distinct entries modulo p, and so

$$\sum_{\mathbf{h} \in (\mathbf{Z}/p\mathbf{Z})^{k-1}} |e_k(\mathbf{h}, p)| \le p^{k-1} A_{p,k} + O_k\Big(\sum_{\ell=1}^{k-1} p^{k-\ell-1}(s_p^\ell - 1 + s_p^\ell A_{p,k})\Big).$$

Now $s_p/p \le 1/2$ for p large, so this error term is $\ll_k p^{k-2}(s_p - 1 + s_p A_{p,k})$, and so the equation implies that

$$\sum_{\mathbf{h} \in (\mathbf{Z}/d\mathbf{Z})^{k-1}} |e_k(h, d)| \le d^{k-2} \prod_{p|d} \Big(pA_{p,k} + O_k(s_p - 1 + s_p A_{p,k})\Big).$$

Now, $1 \le (s_q^r/d)^{\alpha_0}$ for any $\alpha_0 > 0$, for all $d \le s_q^r$, and therefore (14) is, for any $\alpha_0 > 0$,

$$\le s_q^{\alpha_0 R - 1} \prod_{p|q} \Big(1 + p^{-\alpha_0}\Big(pA_{p,k} + O_k(s_p - 1 + s_p A_{p,k})\Big)\Big), \tag{16}$$

and we get the first term in the upper bound.

Large d: We now consider $d > s_q^R$. Define $\Gamma(\mathbf{h})$ as in 3.1. By (15),

$$|e_k(\mathbf{h}, d)| \le \prod_{p|d/c} A_{p,k} \prod_{p^e \| \gamma} (s_p^e - 1 + s_p^e A_{p,k}),$$

(note that $\#\{h_0 = 0, h_1, \dots, h_{k-1} \mod p\} = k - e$ if $p|c$ but $= k$ if $p|(d/c)$), and hence

$$\sum_{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1}} |e_k(\mathbf{h}, d)|$$
$$\le \sum_{c|d} (\prod_{p|d/c} A_{p,k}) \sum_{\substack{\gamma: \\ c|\gamma|c^{k-1}}} \prod_{p^e \| \gamma} (s_p^e - 1 + s_p^e A_{p,k}) \cdot \sum_{\substack{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1} \\ \gamma(\mathbf{h}) = \gamma}} 1.$$

Now $\displaystyle\sum_{\substack{\mathbf{h} \in s_q X \cap \mathbf{Z}^{k-1} \\ \gamma(\mathbf{h}) = \gamma}} 1 \le M_\gamma(H)$ as defined earlier, where $H = O(s_q)$. Using Corollary 9 we bound this in various ranges: For $\gamma \le H$ we obtain

$$\ll_k H^{k-1} \sum_{c|d} (\prod_{p|d/c} A_{p,k}) \sum_{\substack{\gamma \le H \\ c|\gamma|c^{k-1}}} \frac{1}{\gamma} \prod_{p^e \| \gamma} S(k, k-e)(s_p^e - 1 + s_p^e A_{p,k}). \tag{17}$$

Now, for any $\alpha_1 > 0$, the last sum here is

$$\leq \sum_{\substack{\gamma\geq 1\\ c|\gamma|c^{k-1}}} \Big(\frac{H}{\gamma}\Big)^{\alpha_1} \frac{1}{\gamma} \prod_{p^e\|\gamma} \big(S(k,k-e)(s_p^e - 1 + s_p^e A_{p,k})\big)$$

$$= H^{\alpha_1} \prod_{p|c} \left(\sum_{e=1}^{k-1} S(k,k-e) \frac{s_p^e - 1 + s_p^e A_{p,k}}{p^{e(1+\alpha_1)}} \right)$$

and substituting this above gives that (17) is

$$\ll_k H^{k-1+\alpha_1} \prod_{p|d} \Big(A_{p,k} + O_k\Big(\frac{s_p - 1 + s_p A_{p,k}}{p^{1+\alpha_1}}\Big)\Big) \tag{18}$$

The other ranges for γ take the form $\gamma \leq H^{w(\tau)}$ (and $\gamma > H^{w(\tau')}$) giving a bound $M_\gamma(H) \ll_k H^{v(\tau)} \prod_{p^e\|\gamma} S(k,k-e)$, and the analogous argument then gives that the sums are, for any $\alpha(\tau) > 0$,

$$\ll_k H^{v(\tau)+\alpha(\tau)w(\tau)} \prod_{p|d} \Big(A_{p,k} + O_k\Big(\frac{s_p - 1 + s_p A_{p,k}}{p^{\alpha(\tau)}}\Big)\Big) \tag{19}$$

where $\tau = 0, \tau_1$ or $\tau_1+1 \leq \tau \leq k-1$. We need to bound $r_q^{k-1} \sum_{\substack{d|q\\ d>s_q^R}} \rho(d)$ with $\rho(d)$ as in (18) or (19). Clearly this is

$$\leq r_q^{k-1} \sum_{\substack{d|q\\ d\geq 1}} \rho(d)(d/s_q^R)^\beta$$

for any $\beta > 0$, and recalling that $H = O(s_q)$, we obtain the bounds

$$\ll_k s_q^{\alpha_1-\beta_1 R} \prod_{p|q} \Big(1 + p^{\beta_1}\Big(A_{p,k} + O_k\Big(\frac{s_p - 1 + s_p A_{p,k}}{p^{1+\alpha_1}}\Big)\Big)\Big) \tag{20}$$

and

$$\ll_k s_q^{\nu(\tau)+\alpha(\tau)w(\tau)-(k-1)-\beta(\tau)R} \cdot \tag{21}$$

$$\cdot \prod_{p|q} \Big(1 + p^{\beta(\tau)}\Big(A_{p,k} + O_k\Big(\frac{s_p - 1 + s_p A_{p,k}}{p^{\alpha(\tau)}}\Big)\Big)\Big)$$

for any $\alpha(\tau), \beta(\tau) > 0$, where τ runs through the relevant ranges, and the result follows. $\square$

Define $\lambda_k := \min_\tau (k-1-v(\tau))/w(\tau)$ so that $\lambda_2 = (\sqrt{17}-3)/2 = .56155\ldots$, $\lambda_3 = 1/3$, and $\lambda_k = \frac{1}{k-1}$ for all $k \geq 4$.

We will deduce the following theorem from Proposition 11, which implies Theorem 1 after the discussion in section 2.

Theorem 12. *Fix $\epsilon > 0$ and integer K. Suppose that we are given subsets $\Omega_p \subset \mathbf{Z}/p\mathbf{Z}$ for each prime p with $s_p \ll_K p^{\lambda_K - \epsilon}$. Moreover assume that (1) holds for each $k \le K$ provided that $0, h_1, h_2, \dots h_{k-1}$ are distinct mod p. Then, for $X \subset \{x \in \mathbf{R}^{k-1} : 0 < x_1 < x_2 < \dots < x_{k-1}\}$, the k-level correlation function satisfies*

$$R_k(X, \Omega_q) = \mathrm{vol}(X) + o_{X,k}(1)$$

as $s_q = q/|\Omega_q|$ tends to infinity.

This follows immediately from Proposition 11 and the following:

Lemma 13. *Fix $\epsilon > 0$ and assume that*

$$A_{p,k} \ll_k (1 - r_p)p^{-\epsilon} \text{ with } s_p \ll_k p^{\lambda_k - 2\epsilon}.$$

Then there exists $\delta = \delta_\epsilon > 0$ such that Error $\ll s_q^{-\delta}$.

Proof. Taking $\alpha_0 = 1, \alpha_1 \le R\beta_1 - 2\delta$ where $0 < \beta_1 < \epsilon/2$, $\beta(\tau) = 0$ and $\alpha(\tau) = \lambda_k - \epsilon$ (so that $s_p \le p^{\alpha(\tau)-\epsilon}$) in Proposition 11, we find that the p-th term in each Euler product is $\le 1 + O((1 - r_p)/p^{\epsilon/2})$. Now if $1 \le s_p \le 2$ then this is $\le 1 + O((s_p - 1)/p^{\epsilon/2}) = s_p^{O(1/p^{\epsilon/2})} = s_p^{o(1)}$, and if $s_p > 2$ this is $1 + O(1/p^{\epsilon/2}) = s_p^{O(1/p^{\epsilon/2})} = s_p^{o(1)}$. Thus each of the Euler products is $s_q^{o(1)}$ and the result follows. □

4. Poisson spacings for values taken by generic polynomials

Let f be a polynomial of degree n with integer coefficients, and assume that f has $n - 1$ distinct critical values, i.e., that

$$\{f(\xi) : f'(\xi) = 0,\ \xi \in \overline{\mathbf{Q}}\}$$

has $n - 1$ elements. Then, for all but finitely many p, the set

$$\{f(\xi) : f'(\xi) = 0,\ \xi \in \overline{\mathbb{F}_p}\}$$

also has $n - 1$ elements.

We will deduce Theorem 3 from Theorem 1 together with the following result:

Theorem 14. *Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree $n < p$, and let*

$$R := \{f(\xi) : \xi \in \overline{\mathbb{F}_p}, f'(\xi) = 0\}.$$

Assume that $|R| = n - 1$. If $0, h_1, h_2, \dots h_{k-1}$ are distinct modulo p, then

$$N_k((h_1, h_2, \dots, h_{k-1}), p) = r_p^k \cdot p + O_{k,n}(\sqrt{p}).$$

Remark 3. Theorem 14 is not true for all polynomials. For example, if we take $f(x) = x^4 - 2x^2$, then the critical values of f are $0, -1$, and for certain primes p, $N_2(1,p) = 3/32 \cdot p + O(\sqrt{p})$, rather than the expected answer $(3/8)^2 \cdot p + O(\sqrt{p})$. See Section 4.2 for more details.

4.1. **Proof of Theorem 14.** Assume that n and k are given and that p is a sufficiently large prime (in terms of n and k). We wish to count the number of t for which there exists $x_0, x_1, \dots x_{k-1} \in \mathbb{F}_p$ such that

$$f(x_i) = t + h_i \text{ for } 0 \leq i \leq k-1.$$

In order to study this, let $X_{k,\mathbf{h}}$ be the affine curve

$$X_{k,\mathbf{h}} := \{f(x_0) = t,\ f(x_1) = t + h_1, \dots, f(x_{k-1}) = t + h_{k-1}\}.$$

and let $\mathbb{F}_p[X_{k,\mathbf{h}}]$ be the coordinate ring of $X_{k,\mathbf{h}}$. We then have

$$\begin{aligned} (22) \quad & N_k((h_1, h_2, \dots, h_{k-1}), p) \\ & = |\{\mathfrak{m} \in \mathbb{F}_p[t] : \mathfrak{M}|\mathfrak{m} \text{ for some degree one prime } \mathfrak{M} \in \mathbb{F}_p[X_{k,\mathbf{h}}]\ \}| \end{aligned}$$

In order to estimate the size of this set, we will use the Chebotarev density theorem, made effective via the Riemann hypothesis for curves, for the Galois closure of $\mathbb{F}_p[X_{k,\mathbf{h}}]$. Thus, define a curve $Y_{k,\mathbf{h}}$ by letting $\mathbb{F}_p(Y_{k,\mathbf{h}})$ correspond to the Galois closure of the extension $\mathbb{F}_p(X_{k,\mathbf{h}})/\mathbb{F}_p(t)$. In order to study this extension we introduce some notation: Given $h \in \mathbb{F}_p$, define a polynomial $F_h \in \mathbb{F}_p[x,t]$ by

$$F_h(x,t) := f(x) - (t+h).$$

Since the t-degree of F_h is one, it is irreducible, and thus

$$K_h := \mathbb{F}_p[x,t]/F_h(x,t)$$

is a field. Let L_h be the Galois closure of K_h, and let

$$G_h := \mathrm{Gal}(L_h/\mathbb{F}_p(t)).$$

(Note that all field extensions considered are separable since $p > n$.)

Hilbert has shown [6] (e.g., see Serre [12], chapter 4.4) that $G_h \cong S_n$ for all h. Our first goal is to show that the field extensions $L_{h_0}, \dots, L_{h_{k-1}}$ are linearly disjoint, or equivalently, if we let

$$E := L_{h_0} L_{h_1} \cdots L_{h_{k-1}}$$

be the compositum of the fields $L_{h_0}, \dots, L_{h_{k-1}}$, that $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong S_n^k$.

We begin with the following consequence of Goursat's Lemma:

Lemma 15. *Given a subset $I = \{i_1, i_2, \dots, i_l\}$ of $\{1, 2, \dots, k\}$, define a projection $P_I : S_n^k \to S_n^l$ by*

$$P_I((\sigma_1, \sigma_2, \dots, \sigma_k)) = (\sigma_{i_1}, \sigma_{i_2}, \dots, \sigma_{i_l}).$$

Let K be a subgroup of S_n^k, and assume that the restriction of P_I to K is surjective for all $I \subsetneq \{1, 2, \dots, k\}$. If $k > 2$ then either $K = S_n^k$ or

$$K = \{\sigma \in S_n^k : \operatorname{sgn}(\sigma) = 1\}.$$

If $k = 2$, there is the additional possibility that

$$K = \{(\sigma_1, \sigma_2) \in S_n \times S_n : \sigma_1 = \sigma_2\},$$

and if $k = 2$ and $n = 4$, we also have the possibility that

$$K = \{(\sigma_1, \sigma_2) \in S_4 \times S_4 : \sigma_1 H = \sigma_2 H\}$$

where $H = \{1, (12)(34), (13)(24), (14)(23)\}$ is the unique nontrivial normal subgroup of A_4. In particular, we note that if K contains an odd permutation, then $K = S_n^k$.

Proof. Let $P_1 = P_{\{1\}}$ be the projection on the first coordinate, put $P_2 = P_{\{2,3,\dots k\}}$, and let N_i be the kernel of P_i restricted to K for $i = 1, 2$. We may then regard N_1 as a normal subgroup of S_n^{k-1}, and N_2 as a normal subgroup of S_n. By Goursat's lemma (e.g. see exercise 5 of ch. 1 in [11]), K may be described as follows (were we have identified S_n^k with $S_n^{k-1} \times S_n$):

$$K = \{(x, y) \in S_n^{k-1} \times S_n : f_1(x) = f_2(y)\}$$

where $f_1 : S_n^{k-1} \to S_n^{k-1}/N_1$ and $f_2 : S_n \to S_n/N_2$ are the canonical projections, and S_n^{k-1}/N_1 and S_n/N_2 are identified via an isomorphism.

We first consider the case $k > 2$. Now, if $(\sigma_1, \sigma_2, \dots \sigma_{k-1}) \in N_1 \lhd S_n^{k-1}$ and σ_j is a transposition we find that N_1 contains the subgroup

$$\{(\sigma_1, \sigma_2, \dots, \sigma_{k-1}) : \sigma_j \in A_n \text{ and } \sigma_i = 1 \text{ for } i \neq j\}.$$

Hence, since P_I is surjective for all $I \subsetneq \{1, 2, \dots, k\}$, we have $A_n^{k-1} \subset N_1$. Thus f_1 factors through $S_n^{k-1}/A_n^{k-1} \cong \mathbb{F}_2^{k-1}$ and hence $S_n^{k-1}/N_1 \cong \mathbb{F}_2^{k'}$ for some $k' < k$. But if $\mathbb{F}_2^{k'} \cong S_n/N_2$ then either $N_2 = S_n$ and $k' = 0$, or $N_2 = A_n$ and $k' = 1$. In the first case, we find that f_1 and f_2 both are constant, and thus $K = S_n^k$. As for the second case, we note that $f_2(\sigma) = \operatorname{sgn}(\sigma)$ and that f_1 must be of the form

$$f_1((\sigma_1, \sigma_2, \dots, \sigma_{k-1})) = \prod_{i=1}^{k-1} \operatorname{sgn}(\sigma_i)^{\epsilon_i}$$

for some choice of $\epsilon_i \in \{0,1\}$ for $1 \leq i \leq k-1$ (any homomorphism $\mathbb{F}_2^{k-1} \to \mathbb{F}_2$ is of the form $(x_1, x_2, \ldots, x_{k-1}) \to \sum_{i=1}^{k-1} \epsilon_i x_i$). Thus, if we put $\epsilon_k = 1$, we have

$$K = \{(\sigma_1, \sigma_2, \ldots, \sigma_k) \in S_n^k : \prod_{i=1}^{k} \mathrm{sgn}(\sigma_i)^{\epsilon_i} = 1\}.$$

On the other hand, since P_I is surjective for all $I \subsetneq \{1, 2, \ldots, k\}$ we must have $\epsilon_i = 1$ for $1 \leq i \leq k$.

As for the case $k = 2$, we recall that the only nontrivial normal subgroup of S_n is A_n, except when $n = 4$ in which case H is also a normal subgroup. Since N_1 and N_2 are both normal in S_n, and $S_n/N_1 \cong S_n/N_2$, we must have $N_1 = N_2$, and the result follows.

$\square$

In order to show that $\mathrm{Gal}(E/\mathbb{F}_p(t))$ contains an element with odd sign, we will need the following:

Lemma 16. *Let $H, S \subset \mathbb{F}_p$. If $p > 4^{|S|+|H|} + 1$ then there exists $t \in \mathbb{F}_p$ such that the number of $h \in H$ with $t \in S - h$ is odd.*

Proof. Since

$$|\{h \in H : t \in S - h\}| = |\{h \in \alpha H : \alpha t \in \alpha S - h\}|$$

for $\alpha \in \mathbb{F}_p^\times$, we may replace S and H by αS and αH where $\alpha \in \mathbb{F}_p^\times$ is chosen freely; similarly we may also replace S and H by $S + \beta$ and $H + \beta'$ for any $\beta, \beta' \in \mathbb{F}_p$. Now, given $\vec{v} \in \mathbb{F}_p^{|S|+|H|}$ we may partition $\mathbb{F}_p^{|S|+|H|}$ into $4^{|S|+|H|}$ boxes with sides at most $p/4$. If $4^{|S|+|H|} < p-1$, the Dirichlet box principle gives that there exists α', α'' such that all components of $\alpha'\vec{v}$ and $\alpha''\vec{v}$ differ by at most $p/4$. Thus, with $\alpha = \alpha' - \alpha''$ we may choose β such that $\alpha\vec{v} + \beta(1, 1, 1, \ldots, 1) \equiv (x_1, x_2, \ldots, x_{|S|+|H|})$ mod p where $0 \leq x_i < p/2$ for $1 \leq i \leq |S| + |H|$. We may thus assume that integer representatives for all elements of S can be chosen in $[0, p/2)$ and, by replacing H by $H + \beta'$ for an appropriate β', we may also assume that integer representatives for all elements in H may be chosen in the interval $(p/2, p]$.

Thus, if we define $h(T), s(T) \in \mathbb{F}_2[T]/(T^p - 1)$ by $h(T) = \sum_{h \in H} T^{p-h}$ and $s(T) = \sum_{s \in S} T^s$ we find that the degrees of $h(T)$ and $s(T)$ are less than $p/2$. Now, if the number of $h \in H$ with $t \in S - h$ is even for all t, then

$$h(T)s(T) \equiv 0 \mod T^p - 1.$$

However, this cannot happen since the degree of $h(T)s(T)$ is less than p. $\square$

Remark 4. The conclusion of the Lemma does not hold for $p = 7$, $S = \{0, 1, 2, 4\}$ and $H = \{0, 4, 6\}$, so it is necessary to make some assumption on the size of p.

We can now show that the Galois group is maximal:

Proposition 17. *If $p \gg_{k,|R|} 1$ and $h_0 = 0, h_1, h_2, \dots h_{k-1}$ are distinct modulo p, then*
$$\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong S_n^k.$$

Proof. Since
$$\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t)) \lhd \mathrm{Gal}(E/\mathbb{F}_p(t)) < S_n^k$$
it is enough to show that $\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t)) = S_n^k$, i.e., we may assume that the field of constants is algebraically closed. We also note that this implies that the constant field of E is $\mathbb{F}_p$, i.e.,
$$E \cap \overline{\mathbb{F}_p} = \mathbb{F}_p. \tag{23}$$

We may regard $\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t))$ as a subgroup of $S_n^{k-1} \times S_n$. By induction we may assume that the assumptions in Lemma 15 are satisfied. Hence $\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t))$ is either isomorphic to S_n^k, or to $\{\sigma \in S_n^k : \mathrm{sgn}(\sigma) = 1\}$. To show that the second case cannot occur it is enough to prove that the Galois group contains an element with odd sign.

We will now show that there exists a prime ideal $\mathfrak{m} \subset \mathbb{F}_p[t]$ such that the number of h_i for which $\mathfrak{m}$ ramifies in K_{h_i} is *odd*. We begin by noting that ramification of the ideal $(t - \alpha)$ in K_{h_j} is equivalent to $\alpha + h_j \in R$. Choose an arbitrary $r_0 \in R$. We can then find $z \in \mathbb{F}_p$ such that $\mathfrak{m} = (t - (r_0 + z))$ ramifies in K_{h_j} for an *odd* number of j (for $0 \le j \le k - 1$) in the following way: With
$$R' := R \cap (r_0 + \mathbb{F}_p)$$
we find that $(t - (r_0 + z))$ ramifies in K_{h_j} if and only if $r_0 + z + h_j \in R'$. Putting $R'' = R' - r_0$, we see that the number of j for which $r_0 + z + h_j \in R'$ equals the number of j for which $z + h_j \in R''$, which in turn equals the number of j such that $z \in R'' - h_j$. By Lemma 16, applied with $S = R''$ and $H = \{0, h_1, \dots, h_{k-1}\}$, it is possible to choose z so that this happens for an odd number of j.

If $\mathfrak{M}$ is a prime in E lying above $\mathfrak{m}$, then the decomposition group $\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t))_{\mathfrak{M}} \cong \mathrm{Gal}(E_{\mathfrak{M}}/\overline{\mathbb{F}_p}(t)_{\mathfrak{m}})$. After a linear change of variables we may assume the following: $\mathfrak{m} = (t)$, the roots of $F_{h_i}(x_i, t)$ are distinct modulo (t) for those h_i for which $\mathfrak{m}$ does not ramify in K_{k_i}, and for those h_i for which $\mathfrak{m}$ does ramify in K_{k_i}, we have
$$F_{h_i}(x_i, t) = f(x_i) - h_i - t = x_i^2 g_i(x_i) - t$$

where the roots of g_i are distinct modulo (t) and $g_i(0) \neq 0$. Using Hensel's Lemma it readily follows that $E_{\mathfrak{M}} = \overline{\mathbb{F}_p}((\sqrt{t}))$, i.e., a totally ramified quadratic extension of $\overline{\mathbb{F}_p}(t)$. Thus $\mathrm{Gal}(E_{\mathfrak{M}}/\overline{\mathbb{F}_p}(t)_{\mathfrak{m}})$ is group of order two, and is generated by an element σ that maps $\sqrt{t}$ to $-\sqrt{t}$. Now, for all h_i, σ acts trivially on the unramified roots of $F_{h_i}(x_i, t)$, and by transposing pairs of roots that are congruent modulo (t). Thus, when regarded as an element of S_n^k, σ is a product of an odd number of transposition, and hence $\mathrm{Gal}(E/\overline{\mathbb{F}_p}(t))$ must equal S_n^k. □

Since $E \cap \overline{\mathbb{F}_p} = \mathbb{F}_p$, we note that

$$|\{\mathfrak{m} \in \mathbb{F}_p[t] : \mathfrak{M}|\mathfrak{m} \text{ for some degree one prime } \mathfrak{M} \in \mathbb{F}_p[X_{k,\mathbf{h}}]\ \}|$$

equals (taking into account $O_{k,n}(1)$ ramified primes)

$$|\{\mathfrak{m} \in \mathbb{F}_p[t] : \deg(\mathfrak{m}) = 1,\ \mathfrak{M}|\mathfrak{m} \in \mathbb{F}_p[Y_{k,\mathbf{h}}] \text{ and } \mathrm{Frob}(\mathfrak{M}|\mathfrak{m}) \in \mathrm{Fix}_{k,\mathbf{h}}\}| + O_{k,n}(1)$$

where $\mathrm{Fix}_{k,\mathbf{h}} \subset \mathrm{Gal}(E/\mathbb{F}_p(t))$ is the conjugacy class

$$\mathrm{Fix}_{k,\mathbf{h}} := \{\sigma \in \mathrm{Gal}(E/\mathbb{F}_p(t)) \text{ such that } \sigma \text{ fixes at least one root of } F_{h_i} \text{ for } i = 0, 1, \dots, k-1\}$$

Thus (recall Eq. 22)

$$\begin{aligned} (24)\quad & N_k((h_1, h_2, \dots, h_{k-1}), p) \\ &= |\{\mathfrak{m} \in \mathbb{F}_p[t] : \deg(\mathfrak{m}) = 1,\ \mathfrak{M}|\mathfrak{m} \in \mathbb{F}_p[Y_{k,\mathbf{h}}] \text{ and } \mathrm{Frob}(\mathfrak{M}|\mathfrak{m}) \in \mathrm{Fix}_{k,\mathbf{h}}\}| \\ &\qquad + O_{k,n}(1) \end{aligned}$$

The Chebotarev density theorem (see [5], Proposition 5.16) gives

$$N_k((h_1, h_2, \dots, h_{k-1}), p) = \frac{|\,\mathrm{Fix}_{k,\mathbf{h}}\,|}{|\,\mathrm{Gal}(E/\mathbb{F}_p(t))|} \cdot p + O_{k,n}(\sqrt{p}).$$

We conclude by determining $\frac{|\,\mathrm{Fix}_{k,\mathbf{h}}\,|}{|\,\mathrm{Gal}(E/\mathbb{F}_p(t))|}$:

Lemma 18. *If* $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong S_n^k$ *then*

$$\frac{|\,\mathrm{Fix}_{k,\mathbf{h}}\,|}{|\,\mathrm{Gal}(E/\mathbb{F}_p(t))|} = r_p^k + O_{n,k}(p^{-1/2}).$$

Proof. Since $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong S_n^k$ we have $|\,\mathrm{Gal}(E/\mathbb{F}_p(t))| = |S_n|^k$ and $\mathrm{Fix}_{k,\mathbf{h}}$, regarded as a subgroup of S_n^k, equals

$$\{(\sigma_1, \sigma_2, \dots, \sigma_k) \in S_n^k : \sigma_i \text{ has at least one fixed point for } 1 \leq i \leq k\}.$$

Thus

$$|\,\mathrm{Fix}_{k,\mathbf{h}}\,| = |\{\sigma \in S_n : \sigma \text{ has at least one fixed point}\}|^k$$

and hence

$$\frac{|\operatorname{Fix}_{k,\mathbf{h}}|}{|\operatorname{Gal}(E/\mathbb{F}_p(t))|} = \left(\frac{|\{\sigma \in S_n : \sigma \text{ has at least one fixed point}\}|}{|S_n|}\right)^k$$

Finally, again by the Riemann hypothesis for curves, we note that

$$\begin{aligned} r_p &= |\Omega_p|/p \\ &= \frac{|\{t \in \mathbb{F}_p \text{ for which there exits } x \in \mathbb{F}_p \text{ such that } f(x) = t\}|}{p} \\ &= \frac{|\{\sigma \in S_n : \sigma \text{ has at least one fixed point}\}|}{|S_n|} + O_{n,k}(p^{-1/2}). \end{aligned}$$

and thus

$$\frac{|\operatorname{Fix}_{k,\mathbf{h}}|}{|\operatorname{Gal}(E/\mathbb{F}_p(t))|} = r_p^k + O_{n,k}(p^{-1/2}).$$

□

4.2. **Theorem 14 does not hold for all polynomials.** We return to the example $f(x) = x^4 - 2x^2$. The critical values of f are $0, -1$, and for p large, the Galois group of the polynomial $f(x) - t$ over $\overline{\mathbb{F}_p}(t)$ is isomorphic to the dihedral group D_4. In fact, regarded as a subgroup of S_4, it is generated by the elements $(12)(34)$ and (23), corresponding to the ramification at $t = -1$ respectively $t = 0$. However, the Galois group H of the compositum of the extensions generated by $f(x)-t$ and $f(y) - (t+1)$ is not isomorphic to $D_4 \times D_4$; as a subgroup of $S_4 \times S_4$ it is generated by the elements $(12)(34)$, $(23)(56)(78)$ and (67). This group has order 32, and $\operatorname{Fix}_{2,1}$, i.e., the elements of H that fixes at least one root of $f(x)-t$, and at least on root of $f(y)-(t+1)$, consists of $(), (58), (67)$. Thus, for primes p for which the Galois group of the polynomials $f(x)-t$ and $f(y)-(t+1)$ over $\mathbb{F}_p(t)$ equals the geometric Galois group[8], the following happens: The elements of D_4 that fixes at least one root of $f(x) - t$ are $1, (14), (23)$, hence $r_p = 3/8 + O(p^{-1/2})$. We would thus expect that

$$N_2(1,p) = r_p^2 \cdot p + O(\sqrt{p}) = 9/64 \cdot p + O(\sqrt{p}).$$

However, since $|G'| = 32$ and $|\operatorname{Fix}_{2,1}| = 3$ we have

$$N_2(1,p) = 3/32 \cdot p + O(\sqrt{p}).$$

To determine for which primes p splits in the field of constants (in $\overline{\mathbf{Q}}$), and to determine what happens when p does not split, we "lift" the setup to $\mathbf{Q}$: Let L_0' respectively L_1' be the splitting fields, over $\mathbf{Q}(t)$,

[8]More precisely, all sufficiently large primes that split completely in a certain finite extension of $\mathbf{Q}$, namely the field of constants of the Galois extension generated by adjoining the roots of $f(x) - t$ and $f(y) - (t+1)$ to $\mathbf{Q}(t)$.

of the polynomials $f(x)-t$ respectively $f(y)-(t+1)$. Let E' be the compositum of L_0' and L_1', and let $l' = E \cap \overline{\mathbf{Q}}$. Then $\mathrm{Gal}(E'/l'(t)) \cong H$.

As before, $\mathrm{Gal}(L_0'/(L_0' \cap \overline{\mathbf{Q}})(t)) \cong D_4$ and since it must be a normal subgroup of S_4, we find that $L_0' \cap \overline{\mathbf{Q}} = \mathbf{Q}$ and that $\mathrm{Gal}(L_0'/\mathbf{Q}(t)) \cong D_4$. Similarly $\mathrm{Gal}(L_1'/\mathbf{Q}(t)) \cong D_4$, and thus $\mathrm{Gal}(E'/\mathbf{Q}(t))$ embeds into $D_4 \times D_4$, contains H as a normal subgroup, hence $\mathrm{Gal}(E'/\mathbf{Q}(t))$ is either isomorphic to $D_4 \times D_4$ or H. We note that the first case is equivalent to l' being a quadratic extension of $\mathbf{Q}$, whereas the second is equivalent to $l' = \mathbf{Q}$. On the other hand, $y_1 = \sqrt{1+\sqrt{t+2}}$ and $y_2 = \sqrt{1-\sqrt{t+2}}$ are roots of $f(y)-(t+1)$, and since $\sqrt{1+t} \in L_0'$ we find that $i \in L_0'L_1'$ since $(y_1 y_2/\sqrt{1+t})^2 = (1-(t+2))/(1+t) = -1$. Thus $l' = \mathbf{Q}(i)$ and $\mathrm{Gal}(E'/\mathbf{Q}(t)) \cong D_4 \times D_4$.

Let E be the splitting field of the polynomials $f(x)-t$ and $f(y)-(t+1)$ over $\mathbb{F}_p$. Since the geometric Galois group over $\mathbf{Q}$ is the same as the geometric Galois group over $\mathbb{F}_p$ (for large p), reduction modulo p gives that $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong D_4 \times D_4$ if $p \equiv 3 \mod 4$, and $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong H$ if $p \equiv 1 \mod 4$ (and p is sufficiently large). Thus, as we already have seen, $N_2(1,p) = 3/32 \cdot p + O(\sqrt{p})$ if $p \equiv 1 \mod 4$.

If $p \equiv 3 \mod 4$, we have $l = E \cap \overline{\mathbb{F}_p} = \mathbb{F}_p(i) = \mathbb{F}_{p^2}$, and hence the Frobenius automorphism must act nontrivially on l, i.e., Frobenius takes values in

$$\mathrm{Gal}(E/\mathbb{F}_p(t))^* = \{\sigma \in \mathrm{Gal}(E/\mathbb{F}_p(t)) : \sigma|_l \neq 1\}.$$

Given a subset X of $\mathrm{Gal}(E/\mathbb{F}_p(t))$, let

$$\begin{aligned}\mathrm{Fix}(X) = \{\sigma \in X :\ & \sigma \text{ fixes at least one root of } f(x)=t,\\ & \text{and at least one root of } f(y)=t+1.\}\end{aligned}$$

The Riemann hypothesis for curves then gives that

$$N_2(1,p) = \frac{|\,\mathrm{Fix}(\mathrm{Gal}(E/\mathbb{F}_p(t))^*)|}{|\,\mathrm{Gal}(E/\mathbb{F}_p(t))^*|} \cdot p + O(\sqrt{p})$$

Noting that $\mathrm{Gal}(E/\mathbb{F}_{p^2}(t)) \cong H$, we conclude that

$$|\,\mathrm{Fix}(\mathrm{Gal}(E/\mathbb{F}_p(t))^*)| = |\,\mathrm{Fix}(\mathrm{Gal}(E/\mathbb{F}_p(t)))| - |\,\mathrm{Fix}(H)|$$

and since $\mathrm{Gal}(E/\mathbb{F}_p(t) \cong D_4 \times D_4$, we find that $|\,\mathrm{Fix}(\mathrm{Gal}(E/\mathbb{F}_p(t)))| = 9$. We already know that $|\,\mathrm{Fix}(H)| = 3$, hence $|\,\mathrm{Fix}(\mathrm{Gal}(E/\mathbb{F}_p(t))^*)| = 6$. Moreover, since $\mathrm{Gal}(E/\mathbb{F}_p(t))^* = \mathrm{Gal}(E/\mathbb{F}_p(t)) \setminus H$, we have

$$|\,\mathrm{Gal}(E/\mathbb{F}_p(t))^*| = |D_4 \times D_4| - |H| = 64 - 32 = 32,$$

and thus

$$N_2(1,p) = 3/16 \cdot p + O(\sqrt{p}).$$

In fact, this can be seen without Galois theory as follows: Let S_p be the numbers of the form $(x^2-1)^2 \mod p$. The squares modulo p are $b^2, 0 \le b < p/2$, and b^2 is in S_p iff either $(1+b)$ or $(1-b)$ is a square modulo p. Thus the number of elements of S_p is (where $\left(\frac{a}{p}\right)$ is the Legendre symbol)

$$\frac{1}{2}\sum_{b \mod p}\left(1-\frac{1}{4}\left(1+\left(\frac{1+b}{p}\right)\right)\left(1+\left(\frac{1-b}{p}\right)\right)\right)+O(1)=\frac{3p}{8}+O(1)$$

Now, if a and $a+1$ are in S_p, let $b^2=a, c^2=a+1$ so that $(c-b)(c+b)=1$. With $c+b=r$ we have $c=(1/2)(r+1/r)$ and $b=(1/2)(r-1/r)$ for some value of $r \mod p$. Now $b^2 \in S_p$ iff either $(1/2)(2+r-1/r)$ or $(1/2)(2-r+1/r)$ is a square modulo p, and $c^2 \in S_p$ iff either $(1/2)(2+r+1/r)=(1/2r)(r+1)^2$ or $(1/2)(2-r-1/r)=(-1/2r)(r-1)^2$ is a square modulo p.

On the other hand, given r such that $(1/2)(2+r-1/r)$ or $(1/2)(2-r+1/r)$ is a square modulo p, and $2r$ or $-2r$ is a square modulo p then we can construct a. (Note that $r, -r, 1/r$, and $-1/r$ lead to the same value of a.) Therefore, the number of a such that a and $a+1$ are in S_p is

$$\begin{aligned}(25)\quad &\frac{1}{4}\sum_{r \mod p}\left(1-\frac{1}{4}\left(1+\left(\frac{2r}{p}\right)\right)\left(1+\left(\frac{-2r}{p}\right)\right)\right)\cdot\\ &\cdot\left(1-\frac{1}{4}\left(1+\left(\frac{2r(r^2+2r-1)}{p}\right)\right)\left(1+\left(\frac{-2r(r^2-2r-1)}{p}\right)\right)\right)\\ &\qquad=\frac{1}{64}\sum_{r \mod p}\left(9-3\left(\frac{-1}{p}\right)+\sum_i c_i\left(\frac{f_i(r)}{p}\right)\right)\end{aligned}$$

where the $f_i(r)$ are all non-constant polynomials without repeated roots of degree ≤ 5, and the c_i are constants. By the Riemann hypothesis for curves, we get that (25) equals

$$\frac{1}{64}\left(9-3\left(\frac{-1}{p}\right)\right)p+O(p^{1/2}).$$

Thus, if $p\equiv 1 \mod 4$ we get $N_2(1,p)=3/32\cdot p+O(p^{1/2})$ and if $p\equiv 3 \mod 4$ we get $N_2(1,p)=3/16\cdot p+O(p^{1/2})$.

5. Chinese Remainder Theorem for q_1 and q_2

By (2) we know that the spacings of elements in Ω_q become Poisson with parameter θ_q (as $s_q \to \infty$) if, for any $k \geq 2$ and $X \in \mathbb{B}_k$, we have

$$\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_q) = o\left(\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} 1 \right),$$

where $H = \theta_q s_q X$. We shall say that the spacings are *strongly Poisson* with parameter θ_q if

$$\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_q)^2 = o_k\left(\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} 1 \right)$$

for the same H. Note that such spacings are Poisson with parameter θ_q as may be seen by an immediate application of the Cauchy-Schwarz inequality.

Theorem 19. *Suppose that we are given an infinite sequences of sets $\Omega_{q_1} \subset \mathbf{Z}/q_1\mathbf{Z}$ and $\Omega_{q_2} \subset \mathbf{Z}/q_2\mathbf{Z}$ for $q_1 = q_{1,n}$ and $q_2 = q_{2,n}$ for all $n \geq 3$ where $(q_1, q_2) = 1$. Let $q = q_n = q_{1,n}q_{2,n}$. Suppose that the spacings of elements in Ω_{q_1} become strongly Poisson with parameter s_{q_2} (as $n \to \infty$); and that*

$$\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_{q_2})^2 = O_k\left(\sum_{\mathbf{h} \in H \cap \mathbf{Z}^{k-1}} 1 \right)$$

uniformly for $H \in s_q\mathbb{B}_k$. Then the spacing of elements in Ω_q become Poisson as $n \to \infty$ if and only if the spacing of elements in Ω_{q_2} become Poisson with parameter s_{q_1} as $n \to \infty$

Proof. By the Chinese Remainder Theorem,

$$\begin{aligned} &\varepsilon_k(\mathbf{h}, \Omega_q) + 1 \\ &\qquad = \frac{N_k(\mathbf{h}, \Omega_{q_1})}{q_1 r_{q_1}^k} \frac{N_k(\mathbf{h}, \Omega_{q_2})}{q_2 r_{q_2}^k} = \left(\varepsilon_k(\mathbf{h}, \Omega_{q_1}) + 1\right)\left(\varepsilon_k(\mathbf{h}, \Omega_{q_2}) + 1\right), \end{aligned}$$

so that

$$\varepsilon_k(\mathbf{h}, \Omega_q) = \varepsilon_k(\mathbf{h}, \Omega_{q_1})\varepsilon_k(\mathbf{h}, \Omega_{q_2}) + \varepsilon_k(\mathbf{h}, \Omega_{q_1}) + \varepsilon_k(\mathbf{h}, \Omega_{q_2}).$$

Now, by the Cauchy-Schwarz inequality,

$$\left| \sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_1})\varepsilon_k(\mathbf{h},\Omega_{q_2}) \right|^2 \leq \left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_1})^2 \right) \left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_2})^2 \right) = o_k\left(\left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} 1 \right)^2 \right),$$

and so

$$\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_q) = \sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_2}) + o\left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} 1 \right)$$

by hypothesis, which gives our theorem. □

A simple calculation reveals that if Ω_q ranges over random subsets of $\mathbf{Z}/q\mathbf{Z}$, where the probability measure on the subsets of $\mathbf{Z}/q\mathbf{Z}$ is defined using independent Bernoulli random variables with parameter $1/\sigma$ (see section 2.1), then the set Ω_q is strongly Poisson with parameter $\theta_q > 0$, with probability 1, if and only if $\sigma = q^{o(1)}$; and thus we can apply the above result. In fact in this case we can weaken the hypothesis in the Theorem above:

Theorem 20. *Suppose that we are given an infinite sequences of integers $q_1 = q_{1,n}$ and $q_2 = q_{2,n}$, and positive real numbers $\sigma_1 = \sigma_{q_{1,n}}, s_2 = s_{q_{2,n}}$ which are both $q_1^{o(1)}$; and let $q = q_n = q_{1,n}q_{2,n}$. We shall assume that $\sigma_1 \to \infty$ as $n \to \infty$, but not necessarily s_2. Suppose Ω_{q_2} are given subsets of $\mathbf{Z}/q_2\mathbf{Z}$ with $|\Omega_{q_2}| = q_2/s_2$. If Ω_{q_1} ranges over random subsets of $\mathbf{Z}/q_1\mathbf{Z}$, where the probability measure on the subsets of $\mathbf{Z}/q_1\mathbf{Z}$ is defined using independent Bernoulli random variables with parameter $1/\sigma_1$ then, with probability 1, the spacing of elements in Ω_q become Poisson as $n \to \infty$ if and only if the spacing of elements in Ω_{q_2} become Poisson with parameter σ_1 as $n \to \infty$.*

Proof. The only difference from the proof above is in the bounds we find for

$$\left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_1})^2 \right) \left(\sum_{\mathbf{h}\in H\cap \mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h},\Omega_{q_2})^2 \right).$$

Now, trivially, $N_k(\mathbf{h},\Omega_{q_2}) \leq N_1(0,\Omega_{q_2}) = |\Omega_{q_2}| = q_2/s_2$, and therefore $|\varepsilon_k(\mathbf{h},\Omega_{q_2})| \leq s_2^{k-1}$.

If $\{z_t : 1 \le t \le q_1\}$ are each independent Bernoulli random variables with parameter $1/\sigma_1$ then

$$\mathbb{E}((N_k(\mathbf{h},\Omega_{q_1}) - q_1/\sigma_1^k)^2) = \mathbb{E}\left(\sum_{t \mod q_1}\left(\prod_{i=0}^{k-1} z_{t+h_i} - \sigma_1^{-k}\right)\right)^2$$
$$= \mathbb{E}\left(\sum_{t,u \mod q_1}\prod_{i=0}^{k-1} z_{t+h_i}z_{u+h_i}\right) - q_1^2\sigma_1^{-2k}$$

Let $\eta(a)$ be the number of pairs $0 \le i, j < k$ for which $h_j - h_i \equiv a \mod q_1$. Then $\mathbb{E}\left(\sum_{t \mod q_1}\prod_{i=0}^{k-1} z_{t+h_i}z_{t+a+h_i}\right) = q_1\sigma_1^{\eta(a)-2k}$, so that the above equals

$$q_1\sigma_1^{-2k}\left(\sum_{a \mod q_1}(\sigma_1^{\eta(a)} - 1)\right).$$

Evidently $\eta(a) \le k$ for all a, and there are no more than k^2 values of a for which $\eta(k) > 0$. Thus the above is $\ll_k q_1\sigma_1^{-2k}(\sigma_1^k - 1)$; and thus for any $\mathbf{h} \in H$ we have $\mathbb{E}(\varepsilon_k(\mathbf{h},\Omega_{q_1})^2) \ll_k \sigma_1^{k+1}/q_1$ with probability 1. The result therefore follows since $s_2^{k-1}\sigma_1^{k+1}/q_1 = o(1)$ by hypothesis. □

6. Counterexamples

Despite the negative aspects of Theorem 19, one might still hope that one can often take the Chinese Remainder theorem of two fairly arbitrary sets and obtain something that has Poisson spacings. Here we give several examples to indicate when we cannot expect some kind of "Central limit theorem" for the Chinese remainder theorem!

6.1. Counterexample 1.

In this case we select a vanishing proportion of the residues mod q_1 randomly, together with half the residues mod q_2 picked with care. Thus, in Theorem 20 we fix $s_2 = 2$ and take $q_2 = 2\sigma_1$ with $\Omega_{q_2} = \{1, 2, \ldots, \sigma_1\}$. Evidently Ω_{q_2} is not Poisson with parameter σ_1, so Ω_q is not Poisson.

6.2. Counterexample 2.

In this case we select a vanishing proportion of the residues mod q_1 and mod q_2 randomly, but strongly correlated. In fact, let $u_1, u_2, \ldots, u_{q_1}$ are independent Bernoulli random variables with probability $1/\sigma_1 = q_1^{-1/2}$. Let $S = \{i : \ u_i = 1\}$, and then take $q_2 = q_1 + 1$ with $\Omega_{q_1} = \Omega_{q_2} = S$.

It will be convenient to let $y_i = z_i = u_i$ for $1 \le i \le q_1$, with $z_0 = 0$, and then have $y_{j+q_1} = y_j$ and $z_{j+q_2} = z_j$ for all j. Note that

$N_2(h,\Omega_{q_1}) = \sum_{j=1}^{q_1} y_j y_{j+h}$ and $N_2(h,\Omega_{q_2}) = \sum_{j=1}^{q_2} z_j z_{j+h}$ only differ by $O(h)$ terms. (Note that $s_2 = s_1 + o(1) = \sigma_1 + o(1)$.)

Let $q = q_1 q_2$ and define $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ from Ω_{q_1} and Ω_{q_2} using the Chinese remainder theorem, so that $j \in \Omega_q$ if and only if $x_j = 1$ where $x_j = y_j z_j$.

Lemma 21. *Let $I = (0,t) \subset (0,1/3)$ be an interval, and let $\Omega_{q_1}, \Omega_{q_2}$ be as above. Then $\mathbb{E}(R_2(I,q)) = 2t - t^2/2 + o(1)$.*

Proof. Recall that

$$\mathbb{E}(R_2(I,q)) \;=\; \sum_{h\in s_q I} \sum_{r\geq 2}^{q} \frac{1}{r} \mathbb{E}\left(N_2(h,q) : |\Omega_q| = r\right) \cdot \text{Prob}(|\Omega_q| \;=\; r)$$

Since $|\Omega_{q_2}| = |\Omega_{q_1}|$ we have $|\Omega_q| = |\Omega_{q_1}|^2$ and thus

$$\begin{aligned}&\mathbb{E}(R_2(I,q))\\ &\qquad = \sum_{h\in s_q I} \sum_{r_1=1}^{q_1} \frac{1}{r_1^2} \mathbb{E}\left(\sum_{i=1}^{q} x_i x_{i+h} : |\Omega_{q_1}| = r_1 \right) \cdot \text{Prob}(|\Omega_{q_1}| = r_1)\end{aligned}$$

Now, $\text{Prob}(|\Omega_{q_1}| = r_1) = (1/\sigma_1)^{r_1}(1-1/\sigma_1)^{q_1-r_1}\binom{q_1}{r_1}$. Using the Chinese Remainder theorem and the linearity of expectations we obtain

$$\begin{aligned}\mathbb{E}\left(\sum_{i=1}^{q} x_i x_{i+h} : |\Omega_{q_1}| = r_1 \right) &= \sum_{i_1=1}^{q_1} \sum_{i_2=1}^{q_2} \mathbb{E}\left(y_{i_1} y_{i_1+h} z_{i_2} z_{i_2+h} : |\Omega_{q_1}| = r_1\right)\\ &= \sum_{i_1=1}^{q_1} \sum_{i_2=1}^{q_2} \binom{q_1 - L}{r_1 - L} \Big/ \binom{q_1}{r_1}\end{aligned}$$

where $L = L(i_1, i_2, h)$ denotes the number of distinct integers amongst i_1, i_2, the least positive residue of $i_1 + h \bmod q_1$, and the least positive residue of $i_2 + h \bmod q_2$. Therefore

$$\mathbb{E}(R_2(I,q)) = \sum_{h\in s_q I} \sum_{i_1=1}^{q_1} \sum_{i_2=1}^{q_2} \sum_{r_1=1}^{q_1} \frac{1}{r_1^2} \binom{q_1 - L}{r_1 - L} (1/\sigma_1)^{r_1}(1-1/\sigma_1)^{q_1-r_1}.$$

Now using, as in the proof of Lemma 4, that

$$\begin{aligned}\frac{1}{r_1^2} = &\frac{1}{(r_1 - L + 1)(r_1 - L + 2)} +\\ &\qquad + O_L\left(\frac{1}{(r_1 - L + 1)(r_1 - L + 2)(r_1 - L + 3)} \right)\end{aligned}$$

we obtain

$$\sum_{r_1=1}^{q_1} \frac{1}{r_1^2}\binom{q_1-L}{r_1-L}(1/\sigma_1)^{r_1}(1-1/\sigma_1)^{q_1-r_1} = \frac{1}{q_1\sigma_1^L}\left(1+O\left(\frac{1}{\sigma_1}\right)\right).$$

Moreover for each h the number of i_1, i_2 with $L(i_1, i_2, h) = 4$ is $q_1^2 + O(q_1)$, the number with $L = 3$ is $O(q_1)$, and the number with $L = 2$ (which is when $i_2 = i_1$) is $q_1 - h + O(1)$. Thus

$$\begin{aligned}\mathbb{E}(R_2(I,q)) &= \sum_{h\in s_q I}\left\{\frac{q_1^2}{q_1\sigma_1^4} + \frac{O(q_1)}{q_1\sigma_1^3} + \frac{q_1-h}{q_1\sigma_1^2}\right\}\left(1+O\left(\frac{1}{\sigma_1}\right)\right)\\ &= 2t - t^2/2 + O\left(\frac{1}{\sigma_1}\right).\end{aligned}$$

□

6.3. **Counterexample 3.** In this example the sets are independently random but nonetheless, highly correlated. We assume m divides every element of Ω_1, a set of residues modulo q_1, and every element of Ω_2, a set of residues modulo q_2, where $m < \sigma_1, \sigma_2$ and σ_1, σ_2 to be $o(\min(q_1^{1/4}, q_2^{1/4}))$.

Select x_j's randomly from the q_i/m integers divisible by m, in the range $1 \le x_j \le q_i$, each selected with probability $m/\sigma_i \quad (= o(1)$, say). Since $N_2(h, q_i) = O(h/m) \quad$ if $m \nmid h$, and $N_2(h, q_i) \sim |\Omega_i| m/\sigma_i + O(h/m) \quad$ if $m \mid h$, we have $1 + \varepsilon_2(h, q_i) = o(1) \quad$ if $m \nmid h$, and $1 + \varepsilon_2(h, q_i) \sim m \quad$ if $m \mid h$. Therefore $1 + \varepsilon_2(h, q) = \prod_{i=1}^2 (1 + \varepsilon_2(h, q_i)) = o(1)$ unless m divides h, in which case it is $\sim m^2$. In intervals (for h) of length m this averages to $\sim \frac{1}{m}(m^2 + o(m)) = m + o(1)$ and so

$$R_2(X,q) = 1/\sigma_q \sum_{h\in\sigma_q X\cap\mathbf{Z}} (1+\varepsilon_2(h,q)) \sim \frac{m}{\sigma_q}\operatorname{vol}(\sigma_q X) \sim m \operatorname{vol}\ X,$$

which is non-trivial for $m \ge 2$.

If m_i divides the elements of Ω_i, and with the elements chosen as above then, by an analogous calculation to that above,

$$R_2(X,q) \sim \frac{m_1 m_2}{\operatorname{lcm}(m_1,m_2)}\operatorname{vol}(X) = \gcd(m_1,m_2)\operatorname{vol}(X).$$

References

[1] *P. Billingsley*, Probability and measure. John Wiley & Sons, New York-Chichester-Brisbane, 1979, Wiley Series in Probability and Mathematical Statistics.

[2] *B. J. Birch and H. P. F. Swinnerton-Dyer*, Note on a problem of Chowla. Acta Arith. **5** (1959), 417–423 (1959).

[3] *C. Cobeli and A. Zaharescu*, On the distribution of primitive roots mod p. Acta Arith. **83** (1998), no. 2, 143–153.

[4] *H. Davenport*, On the distribution of quadratic residues (mod p). Jour. London Math. Soc. **6** (1931), 49–54.

[5] *M. D. Fried and M. Jarden*, Field arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 11, Springer-Verlag, Berlin, 1986.

[6] *D. Hilbert*, Ueber die irreducibilität ganzer rationaler functionen mit ganzzahligen coefficienten. J. für Math. **CX** (1892), 104–129.

[7] *C. Hooley*, On the difference between consecutive numbers prime to n. II. Publ. Math. Debrecen **12** (1965), 39–49.

[8] ———, On the difference between consecutive numbers prime to n. III. Math. Z. **90** (1965), 355–364.

[9] *P. Kurlberg*, The distribution of spacings between quadratic residues. II. Israel J. Math. **120** (2000), no. A, 205–224.

[10] *P. Kurlberg and Z. Rudnick*, The distribution of spacings between quadratic residues. Duke Math. J. **100** (1999), no. 2, 211–242.

[11] *S. Lang*, Algebra. third ed., Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1993.

[12] *J.-P. Serre*, Topics in Galois theory. Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992.

Département de Mathématiques et statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal QC H3C 3J7, Canada

E-mail address: `andrew@DMS.UMontreal.CA`

Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden

E-mail address: `kurlberg@math.kth.se`