Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Advances in Mathematics ••• (••••) •••–•••
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

Poisson statistics via the Chinese Remainder Theorem

Andrew Granville [a,1], Pär Kurlberg [b,*,2]

[a] *Département de Mathématiques et Statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal QC H3C 3J7, Canada*
[b] *Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden*

Received 8 December 2006; accepted 10 April 2008

Communicated by Michael J. Hopkins

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 has 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.

MSC: primary 11N69; secondary 11K36

Keywords: ???

* Corresponding author.
E-mail addresses: andrew@dms.umontreal.ca (A. Granville), kurlberg@math.kth.se (P. Kurlberg).
[1] A.G. has been supported in part by the National Science Foundation and by NSERC (Canada) during the preparation of this paper.
[2] P.K. supported in part by the National Science Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council.

0001-8708/$ – see front matter © 2008 Published by Elsevier Inc.
doi:10.1016/j.aim.2008.04.001

1. Introduction

Let $1 = x_1 < x_2 < \cdots < x_m < q$ be the set of squares[3] modulo a large integer q. If $q = p$ is an odd 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 $x_i \bmod p$, 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 [5] 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 proportion of $x \in S$ such that the next smallest element of S is $x + d$ is $\sim 1/2^d$ with probability 1.)

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 $1, 2, \ldots, q-1$, 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 [10,12] proved that this is true for the squares mod q.

To a number theorist this is reminiscent of Hooley's 1965 result [8,9] 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.[4]

In both of these examples the sets of integers $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ are obtained from sets of integers $\Omega_{p^e} \subset \mathbf{Z}/p^e\mathbf{Z}$ (for each prime power $p^e \parallel q$) by the Chinese Remainder Theorem (that is $a \in \Omega_q$ if and only if $a \in \Omega_{p^e}$ for all $p^e \parallel q$). We thus ask whether, in general, sets $\Omega_q \subset \mathbf{Z}/q\mathbf{Z}$ created from sets $\Omega_{p^e} \subset \mathbf{Z}/p^e\mathbf{Z}$ (for each prime power $p^e \parallel q$) 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 $1 \leqslant j \leqslant m-1$. For any given real numbers $t_1, t_2, \ldots, t_k \geqslant 0$ define $\mathrm{Prob}_q(t_1, \ldots, t_k)$ to be the proportion of these integers j for which $\Delta_{j+i} > t_i$ for each $i = 1, 2, \ldots, k$.[5]

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

[4] Under a similar assumption, namely that $s_p = (p-1)/\phi(p-1)$ tends to infinity, Cobeli and Zaharescu [4] have shown that the spacings between primitive roots modulo p becomes Poissonian as p tends to infinity along primes.

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

Suppose that Q is an infinite set of squarefree, positive integers that 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 $t_1, t_2, \dots, t_m \geqslant 0$,

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

For a given vector of integers $\mathbf{h} = (h_1, h_2, \dots, h_{k-1})$, let $h_0 = 0$ and define the counting function[6] for k-tuples mod q by

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

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*

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

provided that $0, h_1, h_2, \dots, h_{k-1}$ 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 13 in Section 4 actually gives something a little more explicit and stronger.

Remark 2. When q is not squarefree we suspect that analogous results will follow in most cases. In particular, in the following two cases:

1. The case of q being a product of prime powers p^{e_p} (where for each prime p the exponent e_p is fixed) and the assumptions of Theorem 1 hold when p, Ω_p, s_p, r_p, and $N_k(\mathbf{h}, \Omega_p)$ are replaced by p^{e_p}, $\Omega_{p^{e_p}}$, $s_{p^{e_p}} = p^{e_p}/|\Omega_{p^{e_p}}|$, $r_{p^{e_p}} = 1/s_{p^{e_p}}$, and $N_k(\mathbf{h}, \Omega_{p^{e_p}})$, respectively.
2. The case when for each prime power p^{e_p}, the set $\Omega_{p^{e_p}} \subset \mathbf{Z}/p^{e_p}\mathbf{Z}$ is essentially defined modulo p in the following sense: with $\bar{x} \in \mathbf{Z}/p\mathbf{Z}$ denoting the reduction modulo p of an element $x \in \mathbf{Z}/p^{e_p}\mathbf{Z}$, there exists $\Omega_p \subset \mathbf{Z}/p\mathbf{Z}$ such that $x \in \Omega_{p^{e_p}}$ if and only $\bar{x} \in \Omega_p$, except for $O(1)$ values of $\bar{x}$. In particular, $N_k(\mathbf{h}, \Omega_{p^{e_p}}) = p^{e_p-1}(N_k(\mathbf{h}, \Omega_p) + O(1))$ for all $\mathbf{h}$. E.g., by Hensel's Lemma, this is the case when $\Omega_{p^{e_p}}$ is the image of a polynomial modulo p^{e_p}.

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

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

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

Further, we easily obtain a generalization of Kurlberg–Rudnick's result by 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 dth 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 $\{x \bmod q\colon$ there exists $y \bmod q$ such that $y^2 \equiv x^3 + ax + b \pmod q\}$, for any given integers a, b; and indeed to co-ordinates of any given non-singular hyperelliptic curve. Thus we may deduce the analogy to Corollary 2 in these cases.

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*[7] (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., $\Omega_q := \{x \bmod q\colon$ there exists $y \bmod q$ 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 3. Theorem 3 is true for all non-constant polynomials, but the proof of this is considerably more complicated and will appear in a separate paper [11]. In fact, there are polynomials for which (1) does not hold,[8] see Remark 6 and Section 4.2 for more details. We also note that if f has $n-1$ distinct critical values, Birch and Swinnerton-Dyer [2] have proved that

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

where

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

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.

Remark 4. In [3], Cobeli, Vâjâitu, and Zaharescu considered a similar problem, namely the spacing distribution of elements in the set $\{x \bmod q\colon x \in I_q,\ x^{-1} \in J_q\}$ where $I_q, J_q \subset [1, q]$

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

[8] In particular, the distribution of spacings between elements in Ω_p is *not consistent* with the spacings of a random subset (having size $|\Omega_p|$) of $\mathbf{Z}/p\mathbf{Z}$!

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

are large intervals. They showed that spacings are Poisson distributed provided that q is taken along a subsequence of integers such that $q/\phi(q) \to \infty$, and $|I_q| > q^{1-(2/9(\log\log q)^{1/2})}$, $|J_q| > q^{1-1/(\log\log q)^2}$. As for spacings of polynomial images of incomplete sets of residues modulo q, it is also worth mentioning that Rudnick, Sarnak and Zaharescu [14] have shown that the k-level correlation of elements in the set $\{bn^2 \bmod q\}_{n=1}^{N_q}$ (where $(b,q)=1$) is consistent with Poisson spacings provided $N_q \in [q^{1-\frac{1}{2k}+\delta}, q/\log q]$ for some $\delta > 0$ and q tending to infinity along the primes.

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 sets 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

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

where the sum is over all $\mathbf{h}$ for which $0, h_1, h_2, \ldots, h_{k-1}$ 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 are very weak. So perhaps in our problem we do not need to make an assumption that 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 $\Omega_{q_2} = \{a\colon 1 \leqslant a \leqslant q_2/2\}$.
- $\Omega_{q_2} = \Omega_{q_1}$ is a random subset of $\{1, 2, \ldots, q_1\}$ where $q_2 = q_1 + 1$.
- Each Ω_{q_i} is a random subset of $\{a\colon 1 \leqslant a \leqslant q_i,\ m \mid a\}$ for $i = 1, 2$, with integer $m \geqslant 2$.

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 $0 < x_1 < x_2 < \cdots$ are the positive integers belonging to Ω_q, then define $\Delta_j = (x_{j+1} - x_j)/s_q$ for all $j \geqslant 1$. 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

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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 $k \geqslant 0$, 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 that is relatively easy to work with: The *k-level correlation* for a compact set $X \subset \{\mathbf{x} \in \mathbf{R}^{k-1}\colon\ 0 < x_1 < x_2 < \cdots < x_{k-1}\}$ 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 require that $0 < h_1 < \cdots < h_{k-1}$, else $N_k(\mathbf{h}, \Omega_q) = N_\ell(\mathbf{h}', \Omega_q)$, where $0 < h'_1 < \cdots < h'_{\ell-1}$ 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

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

where we let $x_0 = 0$. Let $\mathbb{B}_k$ be the set of such (not necessarily rectangular) boxes. We then have the following criteria for Poisson spacings in terms of the correlations (cf. Appendix A of [12]):

Lemma 4. *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 the spacings of the elements in Ω_{q_n} become Poisson as $n \to \infty$ if and only if for each integer $k \geqslant 2$ and box $X \in \mathbb{B}_k$,*

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

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 $k \geqslant 2$ and box $X \in \mathbb{B}_k$,

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

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

$$\mathbb{E}\bigl(R_k(X, q)\bigr) = \operatorname{vol}(X) + O_{k,X}(1/\sigma + \sigma/q)$$

and

$$\mathbb{E}\big(\big(R_k(X,q)-\mathrm{vol}(X)\big)^2\big) \ll_{k,X} 1/\sigma + \sigma/q.$$

Proof. Using conditional expectations, we write

$$\begin{aligned}\mathbb{E}\big(R_k(X,q)\big) &= \sum_{r=k}^{q} \mathrm{Prob}\big(|\Omega_q|=r\big)\,\mathbb{E}\big(R_k(X,q) : |\Omega_q|=r\big)\\ &= \sum_{\mathbf{h}\in\sigma X\cap\mathbf{Z}^{k-1}} \sum_{r=k}^{q} \frac{\mathrm{Prob}(|\Omega_q|=r)}{r} \sum_{i=1}^{q} \mathbb{E}\big(x_i x_{i+h_1}\dots x_{i+h_{k-1}} : |\Omega_q|=r\big).\end{aligned}$$

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,

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

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

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

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

$$\begin{aligned}\mathbb{E}\big(R_k(X,q)\big) &= \big|\sigma X\cap\mathbf{Z}^{k-1}\big| \sum_{r=k}^{q} \frac{1}{r}\,\sigma^{-r}(1-1/\sigma)^{q-r} q\cdot\binom{q-k}{r-k}\\ &= q\sigma^{-k}\big(\sigma^{k-1}\ \mathrm{vol}(X)+O\big(\sigma^{k-2}\big)\big)\cdot\sum_{r=k}^{q}\frac{\sigma^{k-r}}{r}\,(1-1/\sigma)^{(q-k)-(r-k)}\binom{q-k}{r-k}\\ &= (q/\sigma)\big(\mathrm{vol}(X)+O(1/\sigma)\big)\cdot\sum_{R=0}^{Q}\frac{1}{R+k}\,(1/\sigma)^R(1-1/\sigma)^{Q-R}\binom{Q}{R},\end{aligned}$$

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

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

so the last sum is

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

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

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

For the variance, note that

$$\begin{aligned}\mathbb{E}\big(R_k(X,q)^2\big) &= \sum_{r=k}^{q} \mathrm{Prob}\big(|\Omega_q| = r\big)\mathbb{E}\big(R_k(X,q)^2 : |\Omega_q| = r\big)\\ &= \sum_{r=k}^{q} \sum_{\mathbf{h},\mathbf{H}\in\sigma X\cap\mathbf{Z}^{k-1}} \sum_{i,j=1}^{q} \binom{q}{r} \frac{\sigma^{-r}(1-1/\sigma)^{q-r}}{r^2}\\ &\quad \times \mathbb{E}\big(x_i x_{i+h_1} x_{i+h_2} \dots x_{i+h_{k-1}} x_j x_{j+H_1} \dots x_{j+H_{k-1}} : |\Omega_q| = r\big).\end{aligned}$$

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

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

Given $\alpha, \beta, \mathbf{h}$ and $\mathbf{H}$, 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

$$\big(q^2 + O_k(q)\big)\binom{q-2k}{r-2k}\bigg/\binom{q}{r}.$$

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[9]

$$\begin{aligned}&\mathbb{E}\big(R_k(X,q)^2\big)\\ &\quad= \sum_{r=k}^{q} \frac{\sigma^{-r}(1-1/\sigma)^{q-r}}{r^2}\\ &\qquad \times \left(\big|\sigma X \cap \mathbf{Z}^{k-1}\big|^2 \binom{q-2k}{r-2k}\big(q^2 + O(q)\big) + O\left(\sum_{m=1}^{k} \binom{q-2k+m}{r-2k+m} q\sigma^{2k-1-m}\right)\right)\\ &\quad= \big(q^2 + O(q)\big)\big(\sigma^{k-1}\,\mathrm{vol}(X) + O_X\big(\sigma^{k-2}\big)\big)^2 \sum_{r=2k}^{q} \binom{q-2k}{r-2k}\frac{1}{r^2}\,\sigma^{-r}(1-1/\sigma)^{q-r}\end{aligned}$$

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

JID:YAIMA AID:3039 /FLA [m1+; v 1.91; Prn:18/04/2008; 14:09] P.9 (1-30)

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

Now, for $k \leqslant \ell \leqslant 2k$ 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

$$\begin{aligned}\sum_{r=\ell}^{q} \binom{q-\ell}{r-\ell} \frac{1}{r^2}\, \sigma^{-r}(1-1/\sigma)^{q-r} &= \sigma^{-\ell} \sum_{R=0}^{Q} \binom{Q}{R} \frac{1}{(R+\ell)^2}\, (1/\sigma)^R (1-1/\sigma)^{Q-R} \\ &\quad \times \left(\frac{\sigma^2}{(Q+1)(Q+2)} + O_k\left(\frac{\sigma^3}{q^3}\right)\right) \\ &= \frac{\sigma^{2+2k-\ell}}{\sigma^{2k} q^2}\left(1 + O_k\left(\frac{\sigma}{q}\right)\right).\end{aligned}$$

Substituting this in the above formula for $\mathbb{E}(R_k(X,q)^2)$ gives that

$$\mathbb{E}\big(R_k(X,q)^2\big) = \operatorname{vol}(X)^2 + O_{X,k}(1/\sigma + \sigma/q),$$

and hence

$$\mathbb{E}\Big(\big(R_k(X,q) - \operatorname{vol}(X)\big)^2\Big) = \mathbb{E}\Big(\big(R_k(X,q)\big)^2\Big) - \operatorname{vol}(X)^2 = O_{X,k}(1/\sigma + \sigma/q). \qquad \square$$

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

3. Correlations via the Chinese Remainder Theorem

3.1. Counting solutions to congruences

Suppose that $\Gamma = \{\gamma_{i,j}\colon\ 0 \leqslant i \neq j \leqslant k-1 \text{ with } \gamma_{i,j} = \gamma_{j,i}\}$ is a given set of positive squarefree integers for which

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

Define

$$\gamma_j := \operatorname*{LCM}_{0 \leqslant i \leqslant j-1} \gamma_{i,j}$$

and let

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

We now show that $\gamma(\Gamma)$ is invariant under reordering of the indices.

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

Lemma 6. *If σ is a permutation of $\{1,\dots,k-1\}$ and $\sigma(0)=0$, define $\gamma_{i,j}^{(\sigma)} := \gamma_{\sigma(i),\sigma(j)}$ and $\gamma^{(\sigma)}(\Gamma) := \gamma_{\sigma(1)}\dots\gamma_{\sigma(k-1)}$. Then $\gamma^{(\sigma)}(\Gamma)=\gamma(\Gamma)$.*

Proof. Given a prime p, it is enough to show that $\gamma(\Gamma)$ and $\gamma^{\sigma}(\Gamma)$ are divisible by the same power of p. Thus, given p, partition $\{0,1,\dots,k-1\}$ by letting i,j belong to the same partition if and only if p divides $\gamma_{i,j}$. (This is well defined since (3) can be viewed as a transitivity property.) Let $\{C_l\}_l$ denote the partitions, where each $C_l \subset \{0,1,\dots,k-1\}$, and let $e=\sum_l(|C_l|-1)$ where $|C_l|$ denotes the cardinality of C_l. Noting that $p \mid \gamma_i$ if and only if the partition containing j also contains an element smaller than j, we find that $p^e \parallel \gamma(\Gamma)$. Since e does not depend on the labeling, the lemma follows. □

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

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

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

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

$$M_\Gamma(H) := \#\bigl\{(h_0=0,h_1,\dots,h_{k-1}) \in \mathbb{Z}^k\colon\ h_i \neq h_j \text{ for } i \neq j,\ 0 \leqslant h_i \leqslant H \\ \text{for all } 0 \leqslant i \leqslant k-1 \text{ and } \Gamma(\mathbf{h})=\Gamma\bigr\}. \tag{4}$$

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

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

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 $H < \gamma_{i,j} \leqslant |h_i-h_j| \leqslant H$. Thus if $\gamma > H^{\binom{k}{2}}$, then $M_\gamma(H)=0$, else $\max \gamma_{i,j} \geqslant \gamma^{1/\binom{k}{2}} > H$.

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 $S(k,k-e) \leqslant \binom{k}{2}^e$.

Lemma 7. $\#\{\Gamma\colon\ \gamma(\Gamma)=\gamma\} \leqslant \prod_{p^e \parallel \gamma} S(k,k-e) \leqslant \binom{k}{2}^{\#\{p^e\colon\ p^e|\gamma\}}$.

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 $p \mid \gamma_{i,j}$ (by (3) this is consistent). The bound follows. □

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

Proposition 8. *We have*

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

Proof. Certainly we may rearrange the order, using σ, without changing the question; so relabel $\sigma(i)$ as i. Now by induction on $k \geqslant 1$, 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 $0 \leqslant i \leqslant k-1$, that if $(h_1, \dots, h_{k-1}) \in M_\Gamma(H)$, then $h_{k-1} \equiv h_i \pmod{\gamma_{i,k-1}}$ for each i, $0 \leqslant i \leqslant k-2$ and so h_{k-1} is determined modulo γ_{k-1}. Thus the number of possibilities for h_{k-1} is $\leqslant H/\gamma_{k-1}+1$, and the result follows. $\square$

Corollary 9. *We have*

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

In particular,

$$M_\Gamma(H) \leqslant \begin{cases} 2^{k-1}H^{k-1}/\gamma(\Gamma) & \text{if each } \gamma_i \leqslant H; \\ 2^{k-1}H^{k-2} & \text{if some } \gamma_j \geqslant H. \end{cases} \tag{6}$$

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 $M_\Gamma(H) \leqslant 4H/T$ 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 $\mathrm{LCM}(\gamma_{\sigma(2),1}, \gamma_{\sigma(2),0})$. Proceeding like this, we obtain

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

Note that

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

Now, in our general construction, let $I = \{i \in [1, \dots, k-1]\colon \gamma_i \leqslant H\}$ and write $D(\Gamma) = \prod_{i=1}^{k-1}\min(\gamma_i, H)$ so that $M_\Gamma(H) \leqslant (2H)^{k-1}/D(\Gamma)$, 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 $\gamma_{r+1} \leqslant H\gamma_r$, and thus

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

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

and

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

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

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

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

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

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

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

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

and thus

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

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 $k-2 \geqslant \mu \geqslant \tau-1$. With this notation, (10) is equivalent to

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

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

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

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

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

so that

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

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

Corollary 10. *Let τ be an integer $1 \leqslant \tau \leqslant k$, and define $w(\tau) = \frac{1}{2}(\tau-\frac{1}{2})^2 + k - \frac{9}{8}$. If $H^{w(\tau-1)} < \gamma(\Gamma) \leqslant H^{w(\tau)}$, 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 7 and Corollary 9 gives that

$$\begin{aligned} M_\gamma(H) &\ll_k \prod_{p^e \| \gamma} S(k, k-e) \\ &\quad \times \begin{cases} H^{k-1}/\gamma & \text{for } \gamma \leqslant H; \\ H^{k-2} & \text{for } H < \gamma \leqslant H^{w(0)}; \\ H^{k+1/2-\sqrt{2k+1/4}} & \text{for } H^{w(0)} < \gamma \leqslant H^{w(\tau_1)}; \\ H^{k-\tau} & \text{for } H^{w(\tau-1)} < \gamma \leqslant H^{w(\tau)},\ \tau_1+1 \leqslant \tau \leqslant k-1. \end{cases} \end{aligned}$$

3.2. Proof of Theorem 1

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

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

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

$$\left|\varepsilon_k(\mathbf{h}, p)\right| \leqslant A_{p,k}$$

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 $\ell \geqslant 1$ 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.[10]

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

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

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

so that

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

Remark 5. In what follows, d is always a divisor of q, hence d will always be squarefree.

With this notation

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

where

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

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

$$r_q^{k-1} \sum_{\mathbf{h}\in s_q X\cap \mathbf{Z}^{k-1}} 1 = r_q^{k-1}\bigl(\operatorname{vol}(s_q X) + O\bigl(s_q^{k-2}\bigr)\bigr) = \operatorname{vol}(X) + O_X(1/s_q).$$

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 11. *If $d > 1$ and d is square free, 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

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

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. □

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 $\tau_1 + 1 \leqslant \tau \leqslant k - 1$ and $w(\tau) = k - 9/8 + (\tau - 1/2)^2/2$.

Proposition 12. *Suppose that we are given $R \in [0, 1]$, as well as $\alpha_0, \alpha_1, \beta_1, \alpha(\tau) > 0$, and $\beta(\tau) \geqslant 0$, for $\tau_1 \leqslant \tau \leqslant k - 1$. Assume that $|\Omega_p| \gg p^{1-\alpha(\tau)}$ for all τ and all primes p (so that $s_p \ll p^{\alpha(\tau)}$). Then*

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

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

Small d: We first consider $d \leqslant s_q^R$. 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

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

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 11, the sum over the d-interior points is zero, and hence

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

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

$$\begin{aligned}&\ll_X r_q^{k-1} \sum_{\substack{d|q\\ 1<d\leqslant s_q^R}} (s_q/d)^{k-2} \sum_{\mathbf{h}\in(\mathbf{Z}/d\mathbf{Z})^{k-1}} \bigl|e_k(\mathbf{h}, d)\bigr|\\ &= \frac{1}{s_q} \sum_{\substack{d|q\\ 1<d\leqslant s_q^R}} \frac{1}{d^{k-2}} \sum_{\mathbf{h}\in(\mathbf{Z}/d\mathbf{Z})^{k-1}} \bigl|e_k(\mathbf{h}, d)\bigr|.\end{aligned} \tag{14}$$

Further,

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

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

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

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

Now $s_p/p \leqslant 1/2$ 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

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

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

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

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),

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

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

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

Now

$$\sum_{\substack{\mathbf{h}\in s_q X\cap\mathbf{Z}^{k-1}\\ \gamma(\mathbf{h})=\gamma}} 1 \leqslant M_\gamma(H)$$

as defined earlier, where $H = O_X(s_q)$. Using Corollary 10, we bound this in various ranges. For $\gamma \leqslant H$ we obtain

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

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

$$\leqslant \sum_{\substack{\gamma\geqslant 1\\ c|\gamma|c^{k-1}}} \left(\frac{H}{\gamma}\right)^{\alpha_1} \frac{1}{\gamma} \prod_{p^e\|\gamma} \bigl(S(k,k-e)\bigl(s_p^e - 1 + s_p^e A_{p,k}\bigr)\bigr)$$

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

and substituting this above gives that (17) is

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

as d is square free. The other ranges for γ take the form $\gamma \leqslant H^{w(\tau)}$ (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 $\alpha(\tau) > 0$,

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

where $\tau = 0$, τ_1 or $\tau_1 + 1 \leqslant \tau \leqslant k-1$. We need to bound $r_q^{k-1} \sum_{d|q,\, d>s_q^R} \rho(d)$ with $\rho(d)$ as in (18) or (19). Clearly this is

$$\leqslant r_q^{k-1} \sum_{\substack{d|q\\ d\geqslant 1}} \rho(d) \bigl(d/s_q^R\bigr)^\beta$$

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

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

and

$$\ll_{X,k} s_q^{v(\tau)+\alpha(\tau)w(\tau)-(k-1)-\beta(\tau)R} \prod_{p|q} \left(1 + p^{\beta(\tau)} \left(A_{p,k} + O_k\left(\frac{s_p - 1 + s_p A_{p,k}}{p^{\alpha(\tau)}} \right) \right) \right) \tag{21}$$

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

Define $\lambda_k := \min_\tau (k-1-v(\tau))/w(\tau)$ so that $\lambda_2 = (\sqrt{17}-3)/2 = 0.56155\ldots$, $\lambda_3 = 1/3$, and $\lambda_k = \frac{1}{k-1}$ for all $k \geqslant 4$.

We will deduce the following theorem from Proposition 12, which implies Theorem 1 after the discussion in Section 2.

Theorem 13. *Fix $\epsilon > 0$ and an 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 $k \leqslant K$ provided that*

$0, h_1, h_2, \ldots, h_{k-1}$ are distinct mod p. Then, for $X \subset \{\mathbf{x} \in \mathbf{R}^{k-1}\colon\ 0 < x_1 < x_2 < \cdots < x_{k-1}\}$, the k-level correlation function satisfies

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

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

This follows immediately from Proposition 12 and the following lemma.

Lemma 14. *Fix $\epsilon > 0$ and assume that*

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

Then there exists $\delta = \delta_\epsilon > 0$ such that[11] Error $\ll s_q^{-\delta}$.

Proof. Taking $\alpha_0 = 1$, $\alpha_1 \leqslant R\beta_1 - 2\delta$, where $0 < \beta_1 < \epsilon/2$, $\beta(\tau) = 0$ and $\alpha(\tau) = \lambda_k - \epsilon$ (so that $s_p \ll_k p^{\alpha(\tau)-\epsilon}$) in Proposition 12, we find that the pth factor in each Euler product is $\leqslant 1 + O((1 - r_p)/p^{\epsilon/2})$. Now if $1 \leqslant s_p \leqslant 2$, then this is $\leqslant 1 + O((s_p - 1)/p^{\epsilon/2}) = s_p^{O(1/p^{\epsilon/2})} = s_p^{o(1)}$, 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

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

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

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

also has $n - 1$ elements.

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

Theorem 15. *Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree $n < p$, let Ω_p denote the image of f modulo p, i.e.,*

$$\Omega_p := \{x \in \mathbb{F}_p\colon \textit{ there exists } y \in \mathbb{F}_p \textit{ such that } f(y) = x\},$$

and let

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

[11] Recall that Error is defined in (12).

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

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

Remark 6. Theorem 15 is not true for all polynomials. For example, if we take $f(x) = x^4 - 2x^2$, then the critical values of f are $0, -1$ (for if $f'(\xi) = 0$ then $\xi = -1, 0$ or 1, so that $f(\xi) = -1$ or 0), and for certain primes p, $N_2(1, \Omega_p) = 3/32 \cdot p + O(\sqrt{p})$, 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 15

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

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

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

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

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

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

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

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

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

Hilbert [7] has shown (e.g., see Serre [15, 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

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

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 16. *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*

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

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

$$K = \big\{\sigma \in S_n^k\colon \mathrm{sgn}(\sigma) = 1\big\}.$$

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

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

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

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

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 Chapter 1 in [13]), K may be described as follows (were we have identified S_n^k with $S_n^{k-1} \times S_n$):

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

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

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

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 $f_2(\sigma) = \mathrm{sgn}(\sigma)$ and that f_1 must be of the form

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

for some choice of $\epsilon_i \in \{0,1\}$ for $1 \leqslant i \leqslant k-1$ (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

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

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

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. □

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

Lemma 17. *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

$$\bigl|\{h \in H \colon t \in S - h\}\bigr| = \bigl|\{h \in \alpha H \colon \alpha t \in \alpha S - h\}\bigr|$$

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 $\alpha\vec{v} + \beta(1, 1, 1, \ldots, 1) \equiv (x_1, x_2, \ldots, x_{|S|+|H|}) \pmod p$, where $0 \leqslant x_i < p/2$ for $1 \leqslant i \leqslant |S| + |H|$. 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

$$h(T)s(T) \equiv 0 \pmod{T^p - 1}.$$

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

Remark 7. 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 18. *If $p \gg_{k,|R|} 1$ and $h_0 = 0, h_1, h_2, \ldots, h_{k-1}$ are distinct modulo p, then*

$$\mathrm{Gal}\bigl(E/\mathbb{F}_p(t)\bigr) \cong S_n^k.$$

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

JID:YAIMA AID:3039 /FLA [m1+; v 1.91; Prn:18/04/2008; 14:09] P.22 (1-30)

Proof. Since

$$\mathrm{Gal}\big(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t)\big) \lhd \mathrm{Gal}\big(E/\mathbb{F}_p(t)\big) < S_n^k,$$

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 16 are satisfied. Hence $\mathrm{Gal}(E\overline{\mathbb{F}_p}/\overline{\mathbb{F}_p}(t))$ is either isomorphic to S_n^k, or to $\{\sigma \in S_n^k\colon \mathrm{sgn}(\sigma) = 1\}$. 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 $0 \leqslant j \leqslant k-1$) 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 17, applied with $S = R''$ and $H = \{0, h_1, \ldots, h_{k-1}\}$, 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

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

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

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

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

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

Thus (recall Eq. (22))

$$\begin{aligned} &N_k\bigl((h_1, h_2, \ldots, h_{k-1}), \Omega_p\bigr) \\ &\quad = \bigl|\bigl\{\mathfrak{m} \in \mathbb{F}_p[t]\colon \deg(\mathfrak{m}) = 1, \mathfrak{M} \mid \mathfrak{m} \in \mathbb{F}_p[Y_{k,\mathbf{h}}] \text{ and } \mathrm{Frob}(\mathfrak{M} \mid \mathfrak{m}) \in \mathrm{Fix}_{k,\mathbf{h}}\bigr\}\bigr| + O_{k,n}(1). \end{aligned} \tag{24}$$

The Chebotarev density theorem (see [6], Proposition 5.16) gives

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

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

Lemma 19. *If* $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong S_n^k$, *then*

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

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

$$\bigl\{(\sigma_1, \sigma_2, \ldots, \sigma_k) \in S_n^k\colon \sigma_i \text{ has at least one fixed point for } 1 \leqslant i \leqslant k\bigr\}.$$

Thus

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

and hence

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

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

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

and thus

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

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

4.2. Theorem 15 does not hold for all polynomials

We return to the example $f(x) = x^4 - 2x^2$ mentioned in Remark 6. 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 $\mathrm{Fix}_{2,1}$, i.e., the elements of H that fix 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,[12] 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

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

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

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

To determine what are the primes p that split 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 $\mathbf{Q}(t)$, 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 $p \equiv 3 \pmod 4$, and $\mathrm{Gal}(E/\mathbb{F}_p(t)) \cong H$ if $p \equiv 1 \pmod 4$ (and p is sufficiently large). Thus, as we already have seen, $N_2(1, \Omega_p) = 3/32 \cdot p + O(\sqrt{p})$ if $p \equiv 1 \pmod 4$.

If $p \equiv 3 \pmod 4$, 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

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

[12] 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 $\mathbf{Q}(t)$.

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

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

The Riemann hypothesis for curves then gives that

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

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

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

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

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

and thus

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

In fact, this can be seen without Galois theory. Namely, let S_p be the numbers of the form $(x^2 - 1)^2 \bmod p$. The squares modulo p are $b^2, 0 \leqslant b < p/2$, 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 $(\frac{a}{p})$ is the Legendre symbol)

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

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 $r \bmod p$. 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

$$\frac{1}{4}\sum_{r \bmod p}\left(1 - \frac{1}{4}\left(1 + \left(\frac{2r}{p}\right)\right)\left(1 + \left(\frac{-2r}{p}\right)\right)\right)\left(1 - \frac{1}{4}\left(1 + \left(\frac{2r(r^2+2r-1)}{p}\right)\right)\right.$$
$$\left.\times\left(1 + \left(\frac{-2r(r^2-2r-1)}{p}\right)\right)\right)$$

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

$$= \frac{1}{64} \sum_{r \bmod p} \left(9 - 3\left(\frac{-1}{p}\right) + \sum_i c_i \left(\frac{f_i(r)}{p}\right)\right), \tag{25}$$

where the $f_i(r)$ are all non-constant polynomials without repeated roots of degree $\leqslant 5$, and the c_i are constants. By the Riemann hypothesis for curves, the right-hand side of (25) equals

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

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

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 $k \geqslant 2$ 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, for the same H,

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

Note that such spacings are Poisson with parameter θ_q, as may be seen by an immediate application of the Cauchy–Schwarz inequality.

Theorem 20. *Suppose that we are given an infinite sequence 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 $n \geqslant 3$ 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 $n \to \infty$.

Remark 8. The assumption that q is squarefree (and hence implicitly that q_1 and q_2 are squarefree) is not needed provided that $(q_1, q_2) = 1$.

Proof. By the Chinese Remainder Theorem,

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

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,

$$\begin{aligned}\Bigg|\sum_{\mathbf{h}\in H\cap\mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_{q_1})\varepsilon_k(\mathbf{h}, \Omega_{q_2})\Bigg|^2 &\leqslant \Bigg(\sum_{\mathbf{h}\in H\cap\mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_{q_1})^2\Bigg)\Bigg(\sum_{\mathbf{h}\in H\cap\mathbf{Z}^{k-1}} \varepsilon_k(\mathbf{h}, \Omega_{q_2})^2\Bigg)\\ &= o_k\Bigg(\Bigg(\sum_{\mathbf{h}\in H\cap\mathbf{Z}^{k-1}} 1\Bigg)^2\Bigg),\end{aligned}$$

and so

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

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 21. *Suppose that we are given an infinite sequence of integers $q_1 = q_{1,n}$ and $q_2 = q_{2,n}$, and positive real numbers $\sigma_1 = \sigma_{q_{1,n}}$, $s_2 = s_{q_{2,n}}$ that 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

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

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

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

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

$$= \mathbb{E}\left(\sum_{t,u \bmod q_1} \prod_{i=0}^{k-1} z_{t+h_i} z_{u+h_i} \right) - q_1^2 \sigma_1^{-2k}.$$

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

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

Evidently $\eta(a) \leqslant k$ 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 20, 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 21 we fix $s_2 = 2$ and take $q_2 = 2\sigma_1$ with $\Omega_{q_2} = \{1, 2, \dots, \sigma_1\}$. 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 $u_1, u_2, \dots, u_{q_1}$ be independent Bernoulli random variables with probability $1/\sigma_1 = q_1^{-1/2}$. Let $S = \{i\colon u_i = 1\}$, 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 $1 \leqslant i \leqslant q_1$, 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 22. *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

$$\mathbb{E}\bigl(R_2(I, q)\bigr) = \sum_{h \in s_q I} \sum_{r \geqslant 2}^{q} \frac{1}{r} \mathbb{E}\bigl(N_2(h, q) : |\Omega_q| = r\bigr) \cdot \operatorname{Prob}\bigl(|\Omega_q| = r\bigr).$$

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001

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

$$\mathbb{E}\big(R_2(I,q)\big) = \sum_{h \in s_q I} \sum_{r_1=1}^{q_1} \frac{1}{r_1^2} \mathbb{E}\left(\sum_{i=1}^{q} x_i x_{i+h} : |\Omega_{q_1}| = r_1\right) \cdot \mathrm{Prob}\big(|\Omega_{q_1}| = r_1\big).$$

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

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

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

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

Now using, as in the proof of Lemma 5, the fact that

$$\frac{1}{r_1^2} = \frac{1}{(r_1 - L + 1)(r_1 - L + 2)} + O_L\left(\frac{1}{(r_1 - L + 1)(r_1 - L + 2)(r_1 - L + 3)}\right),$$

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

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

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 are $o(\min(q_1^{1/4}, q_2^{1/4}))$.

Select x_j's randomly from the q_i/m integers divisible by m, in the range $1 \leqslant x_j \leqslant q_i$, each selected with probability m/σ_i $(= o(1)$, say). Since $N_2(h, q_i) = O(h/m)$ if $m \nmid h$, and $N_2(h, q_i) \sim |\Omega_i| m/\sigma_i + O(h/m)$ if $m \mid h$, we have $1 + \varepsilon_2(h, q_i) = o(1)$ if $m \nmid h$, and $1 + \varepsilon_2(h, q_i) \sim m$ 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

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

which is nontrivial for $m \geqslant 2$.

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

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

Acknowledgments

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

References

[1] P. Billingsley, Probability and Measure, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, New York/Chichester/Brisbane, 1979.
[2] B.J. Birch, H.P.F. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith. 5 (1959) 417–423.
[3] C. Cobeli, M. Vâjâitu, A. Zaharescu, Distribution of gaps between the inverses mod q, Proc. Edinb. Math. Soc. (2) 46 (1) (2003) 185–203.
[4] C. Cobeli, A. Zaharescu, On the distribution of primitive roots mod p, Acta Arith. 83 (2) (1998) 143–153.
[5] H. Davenport, On the distribution of quadratic residues (mod p), J. London Math. Soc. 6 (1931) 49–54.
[6] M.D. Fried, M. Jarden, Field Arithmetic, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 11, Springer-Verlag, Berlin, 1986.
[7] D. Hilbert, Über die irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten, J. Reine Angew. Math. CX (1892) 104–129.
[8] C. Hooley, On the difference between consecutive numbers prime to n. II, Publ. Math. Debrecen 12 (1965) 39–49.
[9] C. Hooley, On the difference between consecutive numbers prime to n. III, Math. Z. 90 (1965) 355–364.
[10] P. Kurlberg, The distribution of spacings between quadratic residues. II, Israel J. Math. 120 (A) (2000) 205–224.
[11] P. Kurlberg, Poisson spacing statistics for value sets of polynomials, Int. J. Number Theory, in press.
[12] P. Kurlberg, Z. Rudnick, The distribution of spacings between quadratic residues, Duke Math. J. 100 (2) (1999) 211–242.
[13] S. Lang, Algebra, third ed., Addison–Wesley Publishing Company Advanced Book Program, Reading, MA, 1993.
[14] Z. Rudnick, P. Sarnak, A. Zaharescu, The distribution of spacings between the fractional parts of $n^2\alpha$, Invent. Math. 145 (1) (2001) 37–57.
[15] J.-P. Serre, Topics in Galois Theory, Res. Notes Math., vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992.

Please cite this article in press as: A. Granville, P. Kurlberg, Poisson statistics via the Chinese Remainder Theorem, Adv. Math. (2008), doi:10.1016/j.aim.2008.04.001