The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$

Manjul Bhargava, John Cremona, Tom Fisher, and Stevan Gajović

January 26, 2021

Abstract

We determine the probability that a random polynomial of degree n over $\mathbb{Z}_p$ has exactly r roots in $\mathbb{Q}_p$, and show that it is given by a rational function of p that is invariant under replacing p by $1/p$.

1 Introduction

Let $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$ be a random polynomial having coefficients $c_0, c_1, \ldots, c_n \in \mathbb{Z}_p$. In this paper, we determine the probability that f has a root in $\mathbb{Q}_p$, and more generally the probability that f has exactly r roots in $\mathbb{Q}_p$. More precisely, we normalise the additive p-adic Haar measure μ on the set of coefficients $\mathbb{Z}_p^{n+1}$ such that $\mu(\mathbb{Z}_p^{n+1}) = 1$, and determine the density $\mu(S_r)$ of the set S_r of degree n polynomials in $\mathbb{Z}_p[x]$ having exactly r roots in $\mathbb{Q}_p$. We prove that this density $\mu(S_r)$ is given by a rational function $\rho^*(n, r; p)$ of p, which satisfies the remarkable identity

$$\rho^*(n, r; p) = \rho^*(n, r; 1/p)$$

for all n, r and p. We also prove that if $X_n(p)$ is the random variable giving the number of $\mathbb{Q}_p$-roots of a random polynomial $f \in \mathbb{Z}_p[x]$ of degree n, then the d-th moment of $X_n(p)$ is independent of n provided that $n \geq 2d - 1$.

Let us now more formally define the probabilities, expectations and generating functions required to state our main results. Fix a prime p and, for $0 \leq r \leq n$, let $\rho^*(n, r) := \rho^*(n, r; p)$ denote the density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$. This is also the probability that a binary form of degree n over $\mathbb{Z}_p$ has exactly r roots in $\mathbb{P}^1(\mathbb{Q}_p)$. For $0 \leq d \leq n$, set

$$\rho(n, d) = \sum_{r=0}^{n} \binom{r}{d} \rho^*(n, r). \tag{1}$$

Thus $\rho(n, d)$ is the expected number of d-sets[1] of $\mathbb{Q}_p$-roots. For fixed n, determining $\rho(n, d)$ for all d is equivalent to determining $\rho^*(n, r)$ for all r, via the inversion formula

$$\rho^*(n, r) = \sum_{d=0}^{n} (-1)^{d-r} \binom{d}{r} \rho(n, d). \tag{2}$$

[1] We find it convenient to refer to a set of size d as a "d-set".

Equations (1) and (2) are equivalent to the standard observation that a probability distribution is determined by its moments; the formulation in terms of d-sets is most convenient for our purposes.

Analogous to $\rho(n,d)$, let $\alpha(n,d)$ (resp. $\beta(n,d)$) denote the expected number of d-sets of $\mathbb{Q}_p$-roots of *monic* polynomials of degree n over $\mathbb{Z}_p$ (resp. monic polynomials of degree n over $\mathbb{Z}_p$ that reduce to x^n modulo p). Define the generating functions:

$$\mathcal{A}_d(t) = (1-t)\sum_{n=0}^{\infty}\alpha(n,d)t^n;$$

$$\mathcal{B}_d(t) = (1-t)\sum_{n=0}^{\infty}\beta(n,d)t^n;$$

$$\mathcal{R}_d(t) = (1-t)(1-pt)\sum_{n=0}^{\infty}(p^n+p^{n-1}+\cdots+1)\rho(n,d)t^n.$$

Then we prove the following theorem.

Theorem 1. *Let p be a prime number and n, d any integers such that $0 \le d \le n$. Then:*

(a) *For fixed n and d, the expectations $\alpha(n,d;p)$, $\beta(n,d;p)$ and $\rho(n,d;p)$ are rational functions of p, which satisfy the identities:*

$$\rho(n,d;p) = \rho(n,d;1/p); \tag{3}$$

$$\alpha(n,d;p) = \beta(n,d;1/p). \tag{4}$$

(b) *We have the following power series identities in two variables t and u:*

$$\sum_{d=0}^{\infty}\mathcal{A}_d(pt)u^d = \left(\sum_{d=0}^{\infty}\mathcal{B}_d(t)u^d\right)^p; \tag{5}$$

$$\sum_{d=0}^{\infty}\mathcal{R}_d(t)u^d = \left(\sum_{d=0}^{\infty}\mathcal{A}_d(pt)u^d\right)\left(\sum_{d=0}^{\infty}\mathcal{B}_d(t)u^d\right) = \left(\sum_{d=0}^{\infty}\mathcal{B}_d(t)u^d\right)^{p+1}; \tag{6}$$

$$\mathcal{B}_d(t) - t\mathcal{B}_d(t/p) = \Phi\left(\mathcal{A}_d(t) - t\mathcal{A}_d(pt)\right), \tag{7}$$

where Φ is the operator on power series that multiplies the coefficient of t^n by $p^{-\binom{n}{2}}$.

(c) *The power series $\mathcal{A}_d$, $\mathcal{B}_d$ and $\mathcal{R}_d$ are in fact polynomials of degree at most $2d$. Moreover, we have $\alpha(n,d) = \mathcal{A}_d(1)$ and $\beta(n,d) = \mathcal{B}_d(1)$ for $n \ge 2d$, and $\rho(n,d) = \mathcal{R}_d(1)$ for $n \ge 2d-1$. Thus the expectations $\alpha(n,d)$, $\beta(n,d)$, and $\rho(n,d)$ are independent of n provided that n is sufficiently large relative to d.*

We observe that $\mathcal{A}_d$ and $\mathcal{B}_d$ (for $d = 0, 1, 2, \ldots$) are the unique power series satisfying the relations (5) and (7) together with the requirements that $\mathcal{A}_d$ and $\mathcal{B}_d$ are $O(t^d)$, $\mathcal{A}_0 = \mathcal{B}_0 = 1$ and $\mathcal{A}_1$ and $\mathcal{B}_1$ are $t + O(t^2)$. This last requirement is needed, since otherwise we could replace $\mathcal{A}_d$ and $\mathcal{B}_d$ by $\lambda^d\mathcal{A}_d$ and $\lambda^d\mathcal{B}_d$ where λ is a constant. This uniqueness statement is easily proved by induction on d and n. The power series $\mathcal{R}_d$ are then uniquely determined by (6).

While we have stated all our results above in terms of the ring $\mathbb{Z}_p$, the generalisation to any complete discrete valuation ring with finite residue field (as considered in [2]) is immediate.

1.1 Examples and relation to previous work

Theorem 1, together with the uniqueness statement that follows it, enables us to explicitly compute $\rho^*(n,r)$, $\rho(n,d)$, $\alpha(n,d)$, and $\beta(n,d)$ for any given values of n, r, and d. We may similarly compute the analogues $\alpha^*(n,r)$ and $\beta^*(n,r)$ of $\rho^*(n,r)$, i.e., $\alpha^*(n,r)$ (resp. $\beta^*(n,r)$) denotes the probability that a random *monic* polynomial of degree n (resp. monic polynomial reducing to x^n modulo p) has exactly r roots over $\mathbb{Q}_p$. Indeed, the formulas (1) and (2) continue to hold when the symbol ρ is replaced by α (resp. β). Moreover, it follows from (2) that $\rho^*(n,r)$, $\alpha^*(n,r)$, and $\beta^*(n,r)$ then satisfy the same symmetry properties (3) and (4) as their unstarred counterparts.

We also thus recover all previously known values of ρ^*, α^*, β^*, ρ, α, and β, including that $\rho(n,1) = 1$ for all n (a result of Caruso [3]), that $\alpha(n,1) = p/(p+1)$ (a result of Shmueli [6]), and the values of $\rho^*(n,n)$ for all n (as determined by Buhler, Goldstein, Moews, and Rosenberg [2]).

We illustrate some particularly interesting cases of Theorem 1 below.

1.1.1 The expected number of roots of a random p-adic polynomial

By definition, the quantities $\rho(n,1)$, $\alpha(n,1)$, and $\beta(n,1)$ represent the expected number of roots over $\mathbb{Q}_p$ of a random polynomial over $\mathbb{Z}_p$ of degree n, a random monic polynomial over $\mathbb{Z}_p$ of degree n, and a random monic polynomial over $\mathbb{Z}_p$ of degree n reducing to $x^n \pmod p$, respectively.

Setting $d = 1$, we compute

$$\mathcal{A}_1(t) = t - \frac{1}{p+1}t^2, \quad \mathcal{B}_1(t) = t - \frac{p}{p+1}t^2, \quad \mathcal{R}_1(t) = (p+1)t - pt^2.$$

Therefore,

$$\alpha(n,1) = \begin{cases} 1 & \text{if } n = 1, \\ \dfrac{p}{p+1} & \text{if } n \geq 2, \end{cases} \qquad \beta(n,1) = \begin{cases} 1 & \text{if } n = 1, \\ \dfrac{1}{p+1} & \text{if } n \geq 2, \end{cases}$$

and

$$\rho(n,1) = 1 \text{ for all } n \geq 1,$$

This recovers, in particular, the aforementioned results of Caruso [3] and Shmueli [6] on the values of $\rho(n,1)$ and $\alpha(n,1)$, respectively, who obtained them via quite different methods.

1.1.2 The second moment of the number of $\mathbb{Q}_p$-roots of a random p-adic polynomial

Next, we determine the expected number of 2-sets (i.e., unordered pairs) of $\mathbb{Q}_p$-roots of a polynomial over $\mathbb{Z}_p$ of degree n. Setting $d = 2$, we compute

$$\begin{aligned} 2\mathcal{A}_2(t) &= (p/(p+1))t^2 - p(p+1)(2p^3+p+1)\eta t^3 + p^4\eta t^4, \\ 2\mathcal{B}_2(t) &= (1/(p+1))t^2 - p(p+1)(p^3+p^2+2)\eta t^3 + p^2\eta t^4, \\ 2\mathcal{R}_2(t) &= (p^2+p+1)t^2 - p(p+1)^3(2p^4+3p^2+2)\eta t^3 + p^2(p+1)^2(p^4+p^2+1)\eta t^4, \end{aligned}$$

where $\eta = 1/((p+1)^2(p^4+p^3+p^2+p+1))$. Therefore,

$$2\alpha(n,2) = \begin{cases} p/(p+1) & \text{if } n = 2, \\ p^3(p^3+1)\eta & \text{if } n = 3, \\ p^3(p^3+p+1)\eta & \text{if } n \geq 4, \end{cases} \qquad 2\beta(n,2) = \begin{cases} 1/(p+1) & \text{if } n = 2, \\ (p^3+1)\eta & \text{if } n = 3, \\ (p^3+p^2+1)\eta & \text{if } n \geq 4, \end{cases}$$

and

$$\rho(2,2) = 1/2, \quad 2\rho(n,2) = (p^2+1)^2/(p^4+p^3+p^2+p+1) \text{ for all } n \geq 3.$$

There is no difficulty in extending these calculations to larger values of d.

1.1.3 The density of p-adic polynomials of degree n having r roots

Once we have computed the expectations $\rho(n,d)$, $\alpha(n,d)$, and $\beta(n,d)$, we may use (2) and its analogues for α and β to compute the probabilities $\rho^*(n,r)$, $\alpha^*(n,r)$, and $\beta^*(n,r)$. Since the probability of a repeated root is zero, we always have $\rho^*(n,n-1) = \alpha^*(n,n-1) = \beta^*(n,n-1) = 0$.

For $n = 2$ and 3, the probabilities $\rho^*(n,r)$ can already be deduced from results in [1], [2] and [3]. Namely, we have

$$\rho^*(2,0) = \rho^*(2,2) = 1/2,$$

and

$$\rho^*(3,0) = 2\gamma, \;\; \rho^*(3,1) = 1-3\gamma, \;\; \rho^*(3,3) = \gamma,$$

where

$$\gamma = \frac{(p^2+1)^2}{6(p^4+p^3+p^2+p+1)}.$$

For quartic polynomials in $\mathbb{Z}_p[x]$, the probability of having $0, 1, 2$ or 4 roots in $\mathbb{Q}_p$ is given by

$$\rho^*(4,0) = \frac{\delta}{8}(3p^{12}+5p^{11}+8p^{10}+12p^9+13p^8+12p^7+17p^6+12p^5+13p^4+12p^3+8p^2+5p+3),$$

$$\rho^*(4,1) = \frac{\delta}{3}(p^{12}+2p^{11}+4p^{10}+3p^9+6p^8+7p^7+2p^6+7p^5+6p^4+3p^3+4p^2+2p+1),$$

$$\rho^*(4,2) = \frac{\delta}{4}(p^{12}+3p^{11}+2p^{10}+6p^9+5p^8+4p^7+9p^6+4p^5+5p^4+6p^3+2p^2+3p+1),$$

$$\rho^*(4,4) = \frac{\delta}{24}(p^{12}-p^{11}+4p^{10}+3p^8+4p^7-p^6+4p^5+3p^4+4p^2-p+1),$$

where

$$\delta = \frac{(p-1)^2}{(p^5-1)(p^9-1)}.$$

The last of these probabilities, $\rho^*(4,4)$, was determined in [2], where it is denoted r_4^{nm}. As predicted by Theorem 1(a), the sequence of coefficients in each numerator and in each denominator is palindromic. Again, there is no difficulty in computing $\rho^*(n,r)$ for larger values of n.

For $n = 2$ and 3, the probabilities $\alpha^*(n,r)$ were computed by Limmer [5, p27] and Weiss [7, Theorem 5.3], who only considered primes $p > n$. Our work shows that the same formulas hold for all primes p. Namely, we have

$$\alpha^*(2,0) = \frac{1}{2}\,\frac{p+2}{p+1}, \qquad \alpha^*(2,2) = \frac{1}{2}\,\frac{p}{p+1};$$

$$\alpha^*(3,0) = \frac{1}{3}\,\frac{p^4+p^3+3p^2+3}{p^4+p^3+p^2+p+1},$$

$$\alpha^*(3,1) = \frac{1}{2}\,\frac{p^5+3p^4+p^3+2p^2+2p}{(p+1)(p^4+p^3+p^2+p+1)},$$

$$\alpha^*(3,3) = \frac{1}{6}\,\frac{p^5-p^4+p^3}{(p+1)(p^4+p^3+p^2+p+1)}.$$

For monic quartic polynomials in $\mathbb{Z}_p[x]$, the probability of having 0, 1, 2 or 4 roots in $\mathbb{Z}_p$ is given by

$$\alpha^*(4,0) = \frac{1}{8}\,\frac{3p^{11}+8p^{10}+6p^9+2p^8-3p^6+4p^5-4p^3-8p-8}{(p+1)^2(p^9-1)},$$
$$\alpha^*(4,1) = \frac{1}{3}\,\frac{p^{14}+2p^{12}-6p^{11}+9p^{10}-9p^9+2p^8+3p^7-2p^6-3p^5+3p^4-3p^2+3p}{(p^5-1)(p^9-1)},$$
$$\alpha^*(4,2) = \frac{1}{4}\,\frac{p^{16}+2p^{15}-4p^{14}+2p^{13}+2p^{12}-6p^{11}+4p^{10}+2p^9-6p^8+2p^7+p^6-2p^5+2p^3}{(p+1)^2(p^5-1)(p^9-1)},$$
$$\alpha^*(4,4) = \frac{1}{24}\,\frac{p^{16}-4p^{15}+6p^{14}-2p^{13}-4p^{12}+6p^{11}-4p^{10}-2p^9+6p^8-4p^7+p^6}{(p+1)^2(p^5-1)(p^9-1)}.$$

By the analogue of (4) for α^* and β^*, we may obtain the values of β^* from those of α^* by substituting $1/p$ for p.

1.1.4 The density of p-adic polynomials that split completely

The quantities $\rho(n,n)$ and $\alpha(n,n)$ represent the probabilities that a (general or monic) polynomial of degree n over $\mathbb{Z}_p$ splits completely over $\mathbb{Q}_p$. These probabilities were previously computed by Buhler, Goldstein, Moews, and Rosenberg [2]. We may recover these probabilities from Theorem 1 as follows. If we replace $\mathcal{A}_d$, $\mathcal{B}_d$, and $\mathcal{R}_d$ by their coefficients of t^d (these being the terms of lowest degree in t), then Theorem 1(b) reduces to

$$\sum_{n=0}^{\infty}\alpha(n,n)(pt)^n = \left(\sum_{n=0}^{\infty}\beta(n,n)t^n\right)^p \tag{8}$$
$$\sum_{n=0}^{\infty}(p^n+p^{n-1}+\cdots+1)\rho(n,n)t^n = \left(\sum_{n=0}^{\infty}\beta(n,n)t^n\right)^{p+1} \tag{9}$$
$$\beta(n,n) = p^{-\binom{n}{2}}\alpha(n,n), \tag{10}$$

from which one can inductively compute $\rho(n,n)$, $\alpha(n,n)$, and $\beta(n,n)$ for all n. In [2], Buhler *et al.* write r_n^{nm}, r_n, and $p^n s_n$ for $\rho(n,n)$, $\alpha(n,n)$, and $\beta(n,n)$, respectively. Our equations (8) and (9) appear as Equations (1-2) and (3-1) in their paper; and their Lemma 4.1(iv), which states that $r_n(q) = r_n(1/q)q^{\binom{n}{2}}$, follows by combining our general Equation (4) with (10). The explicit values of $\rho(n,n) = \rho^*(n,n)$, $\alpha(n,n) = \alpha^*(n,n)$, and $\beta(n,n) = \beta^*(n,n)$ for $n \le 4$ were recorded in §1.1.3.

1.1.5 The density of p-adic polynomials with a root

We may also compute $1-\rho^*(n,0)$, the probability that a polynomial of degree n over $\mathbb{Z}_p$ has at least one root over $\mathbb{Q}_p$. Indeed, as a special case of (2), we have $\rho^*(n,0) = \sum_{d=0}^{n}(-1)^d\rho(n,d)$, and likewise for the α's and β's. In terms of generating functions, we have

$$\mathcal{A}^*(t) := (1-t)\sum_{n=0}^{\infty}\alpha^*(n,0)t^n = \sum_{d=0}^{\infty}(-1)^d\mathcal{A}_d(t)$$

$$\mathcal{B}^*(t) := (1-t)\sum_{n=0}^{\infty}\beta^*(n,0)t^n = \sum_{d=0}^{\infty}(-1)^d\mathcal{B}_d(t)$$

and

$$\mathcal{R}^*(t) := (1-t)(1-pt)\sum_{n=0}^{\infty}(p^n+p^{n-1}+\cdots+1)\rho^*(n,0)t^n = \sum_{d=0}^{\infty}(-1)^d\mathcal{R}_d(t).$$

Specialising Theorem 1(b) by setting $u=-1$ gives

$$\mathcal{A}^*(pt) = \mathcal{B}^*(t)^p \tag{11}$$
$$\mathcal{R}^*(t) = \mathcal{A}^*(pt)\mathcal{B}^*(t) = \mathcal{B}^*(t)^{p+1} \tag{12}$$
$$\mathcal{B}^*(t) - t\mathcal{B}^*(t/p) = \Phi(\mathcal{A}^*(t) - t\mathcal{B}^*(pt)) \tag{13}$$

where Φ is as before.

We may therefore use (11) and (13) to recursively solve for $\alpha^*(n,0)$ and $\beta^*(n,0)$, and then compute $\rho^*(n,0)$ using (12). The explicit values of $\alpha^*(n,0)$, $\beta^*(n,0)$, and $\rho^*(n,0)$ for $n \le 4$ were recorded in §1.1.3.

1.1.6 Large p limits

We note that $\alpha(n,d)$, $\rho(n,d)$, $\alpha^*(n,r)$, and $\rho^*(n,r)$ are rational functions in p whose numerators and denominators have the same degree. Hence, for fixed n, d, and r, we may compute the limits of these functions as p tends to infinity. Meanwhile, $\beta(n,d)$ and $\beta^*(n,r)$ are rational functions in p whose denominator has higher degree than the numerator in most cases. Thus, a correction factor of a power of p is needed to make the limit finite and nonzero. We have the following proposition.

Proposition 1.1.

(a) *Let $0 \le d \le n$ be integers, and let $k = \min(d+1, n)$. Then*

$$\lim_{p\to\infty}\alpha(n,d) = \lim_{p\to\infty}\rho(n,d) = \lim_{p\to\infty}p^{\binom{k}{2}}\beta(n,d) = \frac{1}{d!}.$$

(b) *Let $0 \le r \le n$ be integers. Then*

$$\lim_{p\to\infty}\rho^*(n,r) = \lim_{p\to\infty}\alpha^*(n,r) = \sum_{d=0}^{n}(-1)^{d-r}\binom{d}{r}\frac{1}{d!} = \frac{1}{r!}\sum_{d=0}^{n-r}(-1)^d\frac{1}{d!}.$$

Hence, if we also let $n\to\infty$, we obtain

$$\lim_{n\to\infty}\lim_{p\to\infty}\rho^*(n,r) = \lim_{n\to\infty}\lim_{p\to\infty}\alpha^*(n,r) = \frac{1}{r!}e^{-1}.$$

(c) *Finally, let $0 \le r \le n$ be integers, and let $k = \min(r+1, n)$. If $r \ne n-1$ then*

$$\lim_{p\to\infty}p^{\binom{k}{2}}\beta^*(n,r) = \frac{1}{r!}.$$

We prove these claims in Section 4.

1.2 A general conjecture

Theorem 1(a) naturally leads us to formulate a much more general conjecture. Namely, we conjecture that the density of polynomials of degree n over $\mathbb{Z}_p$ cutting out étale extensions of $\mathbb{Q}_p$ of degree n in which p has *any* given splitting type is a rational function of p satisfying the identities (3) and (4).

Recall that a *splitting type of degree* n is a tuple $\sigma = (d_1^{e_1}\, d_2^{e_2}\, \cdots\, d_t^{e_t})$, where the d_j and e_j are positive integers satisfying $\sum d_j e_j = n$. We allow repeats in the list of symbols $d_j^{e_j}$, but the order in which they appear does not matter. To make it clear when two splitting types are the same, we could for example order the pairs (d_j, e_j) lexicographically. Exponents $e_j = 1$ may be omitted.

For an étale extension $K/\mathbb{Q}_p$ of degree n, we define the symbol (K, p) to be the splitting type $\sigma = (d_1^{e_1}\, d_2^{e_2}\, \cdots\, d_t^{e_t})$ if p factors in K as $P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$, where $P_1, P_2, \ldots, P_t$ are primes in K having residue field degrees $d_1, d_2, \ldots, d_t$, respectively. We say that p *has splitting type* σ *in* K if $(K, p) = \sigma$.

We then make the following conjecture.

Conjecture 1.2. *Let σ be any splitting type of degree n, and set*

$$\begin{aligned}
\rho(n, \sigma; p) &:= \text{density of polynomials } f \in \mathbb{Z}_p[x] \text{ of degree } n \\
&\qquad \text{such that } K := \mathbb{Q}_p[x]/f(x) \text{ is étale over } \mathbb{Q}_p \text{ and } (K, p) = \sigma, \\
\alpha(n, \sigma; p) &:= \text{density of monic polynomials } f \in \mathbb{Z}_p[x] \text{ of degree } n \\
&\qquad \text{such that } K := \mathbb{Q}_p[x]/f(x) \text{ is étale over } \mathbb{Q}_p \text{ and } (K, p) = \sigma, \\
\beta(n, \sigma; p) &:= \text{density of monic polynomials } f \in \mathbb{Z}_p[x] \text{ of degree } n \text{ with } f(x) \equiv x^n \pmod{p} \\
&\qquad \text{such that } K := \mathbb{Q}_p[x]/f(x) \text{ is étale over } \mathbb{Q}_p \text{ and } (K, p) = \sigma.
\end{aligned}$$

Then $\rho(n, \sigma; p)$, $\alpha(n, \sigma; p)$, and $\beta(n, \sigma; p)$ are rational functions of p and satisfy the identities:

$$\rho(n, \sigma; p) = \rho(n, \sigma; 1/p); \tag{14}$$
$$\alpha(n, \sigma; p) = \beta(n, \sigma; 1/p). \tag{15}$$

We have proven that Conjecture 1.2 holds in the quadratic and cubic cases. For example,

$$\begin{aligned}
\rho(2, (11); p) &= 1/2 \\
\rho(2, (2); p) &= 1/2 - p/(p^2 + p + 1) \\
\rho(2, (1^2); p) &= p/(p^2 + p + 1) \\
\rho(3, (111); p) &= (1/6)(p^4 + 2p^2 + 1)/(p^4 + p^3 + p^2 + p + 1) \\
\rho(3, (12); p) &= (1/2)(p^4 + 1)/(p^4 + p^3 + p^2 + p + 1) \\
\rho(3, (3); p) &= (1/3)(p^4 - p^2 + 1)/(p^4 + p^3 + p^2 + p + 1) \\
\rho(3, (1^2 1); p) &= (p^3 + p)/(p^4 + p^3 + p^2 + p + 1) \\
\rho(3, (1^3); p) &= p^2/(p^4 + p^3 + p^2 + p + 1).
\end{aligned}$$

Note again that the numerators and denominators are all palindromic, and thus these expressions satisfy (14). Analogous formulas hold for the α's and β's that satisfy (15). In particular, these formulas hold for all p, including $p = 2$ and $p = 3$.

Theorem 1(a) may also be viewed as a special case of Conjecture 1.2, since the density $\rho^*(n,r;p)$ of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots over $\mathbb{Q}_p$ is simply the sum of the densities $\rho(n,\sigma;p)$ over all splitting types σ having exactly r 1's (and similarly for the α's and β's); thus if the equalities (14) and (15) hold for all $\rho(n,\sigma;p)$, then they will also hold for $\rho^*(n,r)$ and $\rho(n,d)$ (and similarly for the α's and β's), implying Theorem 1(a).

1.3 Methods and organization of the paper

In Section 2, we explain some preliminaries needed for the proof of Theorem 1, regarding counts of polynomials in $\mathbb{F}_p[x]$ having given factorization types, power series identities involving these counts, resultants of polynomials over $\mathbb{Z}_p$, and explicit forms of Hensel's lemma for polynomial factorization.

In Section 3, we then turn to the proof of Theorem 1. We first explain how Theorem 1(b) easily implies Theorem 1(a). To prove Theorem 1(b), we begin by writing the $\alpha(n,d)$ in terms of the $\beta(n',d')$ for $n' \le n$ and $d' \le d$. This involves considering how a monic polynomial over $\mathbb{Z}_p$ factors mod p and showing that the random variables given by the number of $\mathbb{Z}_p$-roots above each $\mathbb{F}_p$-root are independent. The answers may be expressed in terms of the generating functions $\mathcal{A}_d$ and $\mathcal{B}_d$ as

$$\begin{aligned}
\mathcal{A}_1(pt) &= p\mathcal{B}_1(t)\\
\mathcal{A}_2(pt) &= p\mathcal{B}_2(t) + \frac{1}{2}p(p-1)\mathcal{B}_1(t)^2\\
\mathcal{A}_3(pt) &= p\mathcal{B}_3(t) + p(p-1)\mathcal{B}_1(t)\mathcal{B}_2(t) + \frac{1}{6}p(p-1)(p-2)\mathcal{B}_1(t)^3\\
&\vdots
\end{aligned} \tag{16}$$

which may be expressed more succinctly in the form (5). We then explain how to write the $\beta(n,d)$ in terms of the $\alpha(n',d)$ for $n' \le n$. This is proved by making substitutions of the form $x \leftarrow px$, and analysing the valuations of the resulting coefficients; the relation we obtain is expressed succinctly in the form (7). These two types of relations allow us then to recursively solve for the α's and β's. We then write the ρ's in terms of the α's and β's, using another related independence result, and the relations we thereby obtain are expressed succinctly in the form (6), completing the proof of Theorem 1(b).

As previously noted, Theorem 1(b) gives a way to compute the power series $\mathcal{A}_d$, $\mathcal{B}_d$ and $\mathcal{R}_d$ for each d. However, it does not seem to give any way of showing that these are in fact polynomials for all d. In establishing Theorem 1(c), we thus use a different technique to prove the stabilisation result for the α's, or equivalently, that $\mathcal{A}_d$ is a polynomial of degree at most $2d$. We could also give a similar proof of the corresponding result for the β's, but there is no need, since it follows from that for the α's, using either (4) or (16).

Once we have shown that $\mathcal{A}_d$ and $\mathcal{B}_d$ are polynomials of degree at most $2d$, the same result for $\mathcal{R}_d$ then follows by (6). This is not sufficient to prove the stabilisation result for the ρ's, since the definition of $\mathcal{R}_d$ involves additional factors. However, a variant of the ideas used to show that $\mathcal{A}_d$ is a polynomial also show that $\mathcal{A}_d(1) = \mathcal{A}_d(p)$, and from this we deduce the stabilisation result for the ρ's.

Finally, in Section 4, we prove the asymptotic results contained in §1.1.6.

2 Preliminaries

2.1 Basic notation

For a ring R, let $R[x]$ denote the ring of univariate polynomials over R, and for $n \geq 0$, let $R[x]_n$ denote the subset of polynomials of degree n, and $R[x]_n^1$ the subset of monic polynomials of degree n.

In the case $R = \mathbb{Z}_p$, we identify $\mathbb{Z}_p[x]_n^1$ with $\mathbb{Z}_p^n$ via

$$x^n + \sum_{i=0}^{n-1} a_i x^i \leftrightarrow (a_0, a_1, \ldots, a_{n-1}),$$

and thereby use the usual p-adic measure on subsets of $\mathbb{Z}_p[x]_n^1$ inherited via this identification.

For $f \in \mathbb{Z}_p[x]$, we denote by $\overline{f}$ its image under reduction modulo p in $\mathbb{F}_p[x]$. A polynomial with coefficients in $\mathbb{Z}_p$ is *primitive* if not all its coefficients are divisible by p, that is, if $\overline{f} \neq 0$. For a primitive polynomial $f \in \mathbb{Z}_p[x]$, we define the *reduced degree* of f to be $\deg(\overline{f})$. Hence $\deg(\overline{f}) \leq \deg(f)$, with equality if and only if the leading coefficient of f is a unit.

2.2 Counts involving splitting types of polynomials over $\mathbb{F}_p$

We will require expressions for the number of monic polynomials in $\mathbb{F}_p[x]$ that factor as a product of irreducible polynomials with given degrees and multiplicities. These counts, and the corresponding probabilities for a random polynomial to have given factorization types, are collected in this subsection.

To this end, let $\mathcal{S}(n)$ denote the set of all splitting types of degree n. Thus, for example, $\mathcal{S}(2) = \{(1\,1), (1^2), (2)\}$ has three elements, $\mathcal{S}(3)$ has five elements, and $\mathcal{S}(4)$ has 11.

We say that a monic polynomial f in $\mathbb{F}_p[x]$ of degree n has *splitting type* $(d_1^{e_1}\, d_2^{e_2} \cdots d_t^{e_t}) \in \mathcal{S}(n)$ if it factors as $f(x) = \prod_{j=1}^{t} f_j(x)^{e_j}$, where the f_j are distinct irreducible monic polynomials over $\mathbb{F}_p$ with $\deg(f_j) = d_j$. We write $\sigma(f)$ for the splitting type of f, and N_σ for the number of monic polynomials in $\mathbb{F}_p[x]$ with splitting type σ.

If $\sigma = (d)$, then we simply write N_d for N_σ. That is, N_d is the number of degree d irreducible monic polynomials in $\mathbb{F}_p[x]$. Writing μ for the Möbius function, it is well known that

$$N_d = \frac{1}{d} \sum_{k|d} \mu(k) p^{d/k}.$$

In general, for $\sigma = (d_1^{e_1}\, d_2^{e_2} \cdots d_t^{e_t}) \in \mathcal{S}(n)$, we have

$$N_\sigma = \prod_{d=1}^{n} \binom{N_d}{m_d} \binom{m_d}{m_{d1}\ m_{d2}\ \cdots\ m_{dn}}, \tag{17}$$

where

$$m_{de} = m_{de}(\sigma) := \#\{s : d_s^{e_s} = d^e\},$$

and

$$m_d = m_d(\sigma) := \#\{s : d_s = d\} = \sum_{e=1}^{n} m_{de}.$$

Since there are p^n monic polynomials of degree n in $\mathbb{F}_p[x]$, the probability that a degree n monic polynomial $f \in \mathbb{F}_p[x]$ has splitting type σ, for $\sigma \in \mathcal{S}(n)$, is N_σ / p^n. This is evidently a rational function of p.

2.3 Power series identities involving N_σ

We now establish some power series identities involving the counts N_σ defined in the last section.

Let x_{de} for $d, e \geq 1$ be indeterminates. For a splitting type $\sigma \in \mathcal{S}(n)$ of degree n, let

$$x_\sigma = \prod_{d^e \in \sigma} x_{de}.$$

Polynomials in the x_{de} will be weighted by setting $\mathrm{wt}(x_{de}) = de$. We set $y_0 = 1$, and for $n \geq 1$ define

$$y_n = \sum_{\sigma \in \mathcal{S}(n)} N_\sigma x_\sigma,$$

so that every monomial in y_n has weight n. We set $x_{d0} = 1$ for all $d \geq 1$.

Proposition 2.1. *We have the following identity in* $\mathbb{Z}[\{x_{de}\}_{d,e\geq 1}][[t]]$*:*

$$\sum_{n=0}^{\infty} y_n t^n = \prod_{d=1}^{\infty} \left(\sum_{e=0}^{\infty} x_{de} t^{de} \right)^{N_d}. \tag{18}$$

Proof. We must show that when the right hand side is multiplied out, the coefficient of t^n is y_n. The coefficient of t^n is a sum of monomials in the x_{de} of weight n. Each such product has the form x_σ for some $\sigma \in \mathcal{S}(n)$, and the number of times each monomial occurs is N_σ. □

By specializing the x_{de}, we obtain the following corollary.

Corollary 2.2. *We have the following identity in* $\mathbb{Z}[[t]]$*:*

$$(1 - pt)^{-1} = \prod_{d=1}^{\infty} (1 - t^d)^{-N_d}. \tag{19}$$

Proof. In (18), set $x_{de} = 1$ for all d, e. Then $x_\sigma = 1$, so $y_n = p^n$, and (19) follows. □

Corollary 2.3. *Let* x_e *for* $e \geq 1$ *be indeterminates, and set* $x_0 = 1$*. Then, in* $\mathbb{Z}[x_1, x_2, \ldots][[t]]$*, we have:*

$$\sum_{n=0}^{\infty} \sum_{\sigma \in \mathcal{S}(n)} N_\sigma \left(\prod_{1^e \in \sigma} x_e \right) t^n = \left(\sum_{n=0}^{\infty} x_n t^n \right)^p (1 - t)^p (1 - pt)^{-1}. \tag{20}$$

Proof. In (18), set $x_{1e} = x_e$, and set $x_{de} = 1$ for all $d \geq 2$. Then, by Corollary 2.2, we have

$$\prod_{d=2}^{\infty} (1 - t^d)^{-N_d} = (1 - t)^p (1 - pt)^{-1},$$

yielding (20). □

2.4 Resultants, coprime factorizations, and independence

2.4.1 Resultants

We begin with an observation about resultants of polynomials in $\mathbb{Z}_p[x]$ and their behavior upon reduction modulo p.

Lemma 2.4. *Let $f, g \in \mathbb{Z}_p[x]$ have degrees m and n respectively.*

1. *If the leading coefficients of f and g are both units, then $\overline{\mathrm{Res}(f,g)} = \mathrm{Res}(\overline{f}, \overline{g})$.*
2. *If the leading coefficient a_m of f is a unit and $d = \deg(\overline{g}) < n$, then $\overline{\mathrm{Res}(f,g)} = \overline{a_m}^{n-d} \mathrm{Res}(\overline{f}, \overline{g})$.*
3. *If the leading coefficients of f and g are both non-units, then $\overline{\mathrm{Res}(f,g)} = 0$.*

Proof. These are standard properties of resultants and may be seen by examination of the definition of $\mathrm{Res}(f,g)$ as the value of the $(m+n) \times (m+n)$ Sylvester determinant. □

Corollary 2.5. *Let $f, g \in \mathbb{Z}_p[x]$ have degrees m and n respectively. Then $\mathrm{Res}(f,g)$ is a unit if and only if at least one of the leading coefficients of f, g is a unit, and the reductions $\overline{f}, \overline{g}$ are coprime.*

Our reason to consider resultants is the following.

Lemma 2.6. *Let R be a ring. For any $d \geq 1$, we identify $R[x]_d^1 \cong R^d$ and $R[x]_d \cong R^{d+1}$ as R-modules.*

(a) *The multiplication map $R[x]_m^1 \times R[x]_n^1 \to R[x]_{m+n}^1$ has Jacobian given by $\mathrm{Res}(f,g)$.*

(b) *The multiplication map $R[x]_m^1 \times R[x]_n \to R[x]_{m+n}$ has Jacobian given by $\mathrm{Res}(f,g)$.*

Proof. We first consider case (a), when both polynomials are monic. Let $f(x) = x^m + \sum_{i=0}^{m-1} a_i x^i$, $g(x) = x^n + \sum_{j=0}^{n-1} b_j x^j$, and $h(x) = x^{m+n} + \sum_{k=0}^{m+n-1} c_k x^k$ be monic polynomials in $R[x]$ having degrees m, n, and $m+n$ respectively. If $h(x) = f(x)g(x)$, then $c_k = \sum_{i+j=k} a_i b_j$, and the matrix of partial derivatives of the c_k with respect to the a_i and b_j is precisely the Sylvester matrix whose determinant is $\mathrm{Res}(f,g)$.

We next consider case (b), and assume that $f(x) = x^m + \sum_{i=0}^{m-1} a_i x^i \in R[x]_m^1$ is monic while $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x]_n$ is not necessarily so. Let $f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k$, and let M be the $(m+n+1) \times (m+n+1)$ matrix of partial derivatives of the c_k with respect to the a_i and b_j. Since $c_{m+n} = b_n$, the last row consists of 0's except for the final entry which is 1. Expanding the determinant by the last row, we again obtain $\mathrm{Res}(f,g)$. □

Corollary 2.7. *Let $A \subset \mathbb{Z}_p[x]_m^1$, $B \subset \mathbb{Z}_p[x]_n^1$ (resp. $B \subset \mathbb{Z}_p[x]_n$), and $AB \subset \mathbb{Z}_p[x]_{m+n}^1$ (resp. $AB \subset \mathbb{Z}_p[x]_{m+n}$) be measurable subsets such that multiplication induces a bijection*

$$A \times B \to AB = \{ab \mid a \in A,\ b \in B\}.$$

If $\mathrm{Res}(a,b) \in \mathbb{Z}_p^*$ for all $a \in A$ and $b \in B$, then this bijection is measure-preserving.

2.4.2 Coprime factorizations and Hensel lifting

We next recall Hensel's lemma for polynomial factorizations in certain quantitative forms. The first is standard, and is stated as Lemma 2.3 in [2], while the variant is mentioned in [2, p. 24].

For $f \in \mathbb{F}_p[x]^1_d$, we denote by P_f the set of polynomials in $\mathbb{Z}_p[x]^1_d$ that reduce to f modulo p; and for $n \geq d$, we denote by P_f^n the set of polynomials in $\mathbb{Z}_p[x]_n$ that reduce to f modulo p.

Lemma 2.8. *Suppose that $g, h \in \mathbb{F}_p[x]$ are monic and coprime. Then the multiplication map*

$$P_g \times P_h \to P_{gh} \tag{21}$$

is a measure-preserving bijection.

Proof. Let $f \in \mathbb{Z}_p[x]^1_n$ be such that $\overline{f}$ factors in $\mathbb{F}_p[x]$ as $\overline{f} = gh$. Then by Hensel's lemma f factors uniquely in $\mathbb{Z}_p[x]$ as $f = \tilde{g}\tilde{h}$, where $\tilde{g} \in P_g$ and $\tilde{h} \in P_h$. Therefore (21) is a bijection. The measure-preserving property holds by Corollaries 2.5 and 2.7. □

The following variant will be used to handle polynomials $f \in \mathbb{Z}_p[x]$ whose leading coefficient is not a unit.

Lemma 2.9. *For $n \geq m$, the multiplication map*

$$\mathbb{Z}_p[x]^1_m \times P_1^{n-m} \to \{f \in \mathbb{Z}_p[x]_n : \overline{f} \in \mathbb{F}_p[x]^1_m\} \tag{22}$$

is a measure-preserving bijection.

Proof. Let $f \in \mathbb{Z}_p[x]_n$ be such that $\overline{f}$ is monic of degree m. Then homogenising, applying Hensel's lemma, and dehomogenising, shows that f factors uniquely in $\mathbb{Z}_p[x]$ as $f = f_1 f_2$ where $f_1 \in \mathbb{Z}_p[x]^1_m$ and $f_2 \in P_1^{n-m}$. Therefore, (22) is a bijection. The measure-preserving property again holds by Corollaries 2.5 and 2.7, since f_1 is monic. □

2.4.3 Independence lemmas

Finally, we may phrase Lemmas 2.8 and 2.9 as statements regarding the independence of suitable random variables.

Corollary 2.10. *Let $g, h \in \mathbb{F}_p[x]$ be coprime monic polynomials. For $f \in P_{gh}$, let π_1 and π_2 denote the projections of P_{gh} onto P_g and P_h, respectively, under the bijection $P_{gh} \to P_g \times P_h$. Then the number of $\mathbb{Q}_p$-roots of $f \in P_{gh}$ is $X + Y$, where $X, Y : P_{gh} \to \{0, 1, 2, \ldots\}$ are independent random variables distributed on $f \in P_{gh}$ as the number of $\mathbb{Q}_p$-roots of $\pi_1(f) \in P_g$ and $\pi_2(f) \in P_h$, respectively.*

Corollary 2.11. *Let $m \leq n$, and let*

$$B_{m,n} := \{f \in \mathbb{Z}_p[x]_n : \overline{f} \in \mathbb{F}_p[x]^1_m\}.$$

For $f \in B_{m,n}$, let ψ_1 and ψ_2 denote the projections of $B_{m,n}$ onto $\mathbb{Z}_p[x]^1_m$ and P_1^{n-m}, respectively, under the bijection $B_{m,n} \to \mathbb{Z}_p[x]^1_m \times P_1^{n-m}$. Let $X, Y : B_{m,n} \to \{0, 1, 2, \ldots\}$ be the random variables giving the numbers of roots of $f \in B_{m,n}$ in $\mathbb{Z}_p$ and in $\mathbb{Q}_p \setminus \mathbb{Z}_p$, respectively. Then X and Y are independent random variables distributed on $f \in B_{m,n}$ as the number of $\mathbb{Q}_p$-roots of $\psi_1(f)(x) \in \mathbb{Z}_p[x]^1_m$ and of $\psi_2(f)^{\mathrm{rev}}(x) := x^{n-m}\psi_2(f)(1/x) \in P_{x^{n-m}}$, respectively.

3 Proof of Theorem 1

3.1 Theorem 1(b) implies Theorem 1(a)

Theorem 1(b) allows us to compute $\alpha(n,d)$, $\beta(n,d)$, and $\rho(n,d)$ for any n and d. Indeed we use (5) and (7) to solve for the α's and β's, and then (6) to compute the ρ's. The answers obtained are rational functions of p. The relation (5) is invariant under replacing $t \to t/p$ and switching $p \leftrightarrow 1/p$ and $\mathcal{A}_d \leftrightarrow \mathcal{B}_d$, while the relation (7) is invariant under switching $p \leftrightarrow 1/p$ and $\mathcal{A}_d \leftrightarrow \mathcal{B}_d$. The symmetry (4) then follows by induction on n and d, while (3) follows from (6). □

3.2 Proof of Theorem 1(b)

3.2.1 Conditional expectations

The expectations $\alpha(n,d)$ and $\beta(n,d)$ were defined in the introduction. To help evaluate them, we make the following additional definitions.

Definition 3.1.

(i) For $f \in \mathbb{F}_p[x]_n^1$, let $\alpha(n,d \mid f)$ denote the expected number of d-sets of $\mathbb{Q}_p$-roots of a polynomial in $P_f \subset \mathbb{Z}_p[x]_n^1$. Since P_f has relative density p^{-n} in $\mathbb{Z}_p[x]_n^1$, we have

$$\alpha(n,d) = p^{-n} \sum_{f \in \mathbb{F}_p[x]_n^1} \alpha(n,d \mid f). \tag{23}$$

Also, $\beta(n,d) = \alpha(n,d \mid x^n)$.

(ii) For σ in $\mathcal{S}(n)$, let $\alpha(n,d \mid \sigma)$ be the expected number of d-sets of $\mathbb{Q}_p$-roots of a polynomial in $\mathbb{Z}_p[x]_n^1$ whose mod p splitting type is σ. Thus

$$\alpha(n,d) = p^{-n} \sum_{\sigma \in \mathcal{S}(n)} N_\sigma \, \alpha(n,d \mid \sigma), \tag{24}$$

and

$$\alpha(n,d \mid \sigma) = N_\sigma^{-1} \sum_{f \in \mathbb{F}_p[x]_n^1 \colon \sigma(f) = \sigma} \alpha(n,d \mid f), \tag{25}$$

where $\sigma(f)$ denotes the splitting type of f.

3.2.2 Writing the α's in terms of the β's

The aim of this subsection is to prove (5), the first part of Theorem 1(b).

Lemma 3.2. *Let $g, h \in \mathbb{F}_p[x]$ be monic and coprime. Then*

$$\alpha(\deg(gh), d \mid gh) = \sum_{d_1 + d_2 = d} \alpha(\deg(g), d_1 \mid g) \cdot \alpha(\deg(h), d_2 \mid h), \tag{26}$$

where the sum is over all pairs (d_1, d_2) of nonnegative integers summing to d.

If, additionally, h has no roots in $\mathbb{F}_p$, then

$$\alpha(\deg(gh), d \mid gh) = \alpha(\deg(g), d \mid g).$$

Proof. The lemma follows from Corollary 2.10 and the observation that if X and Y are independent random variables taking values in $\{0, 1, 2, \ldots\}$ then

$$\mathbb{E}\binom{X+Y}{d} = \sum_{d_1+d_2=d} \mathbb{E}\binom{X}{d_1}\mathbb{E}\binom{Y}{d_2}. \tag{27}$$

□

Recall that $\beta(n,d) = \alpha(n,d \mid x^n)$ is the expected number of d-sets of roots of a monic polynomial of degree n which reduces to x^n modulo p. Using Lemma 3.2, we can express $\alpha(n,d \mid f)$ for monic $f \in \mathbb{F}_p[x]_n$ in terms of $\beta(n',d')$ for appropriate n', d'.

Lemma 3.3. *Let $\sigma = (1^{n_1} \cdots 1^{n_k} \cdots) \in \mathcal{S}(n)$ be a splitting type with exactly $k = m_1(\sigma)$ powers of 1. Then*

$$\alpha(n,d \mid \sigma) = \sum_{d_1+\cdots+d_k=d} \prod_{i=1}^{k} \beta(n_i,d_i). \tag{28}$$

Proof. Let $f \in \mathbb{F}_p[x]_n^1$ have splitting type σ. To evaluate $\alpha(n,d \mid f)$, we may ignore the factors of f of degree greater than 1, since if $f = f_1 f_2$ where $\sigma(f_1) = (1^{n_1} \cdots 1^{n_k})$ and f_2 has no linear factors, then $\alpha(n,d \mid f) = \alpha(\deg(f_1), d \mid f_1)$ by the last part of Lemma 3.2.

Now let $f = \prod_{i=1}^{k} \ell_i^{n_i}$, where the ℓ_i are distinct, monic, and of degree 1. Using Lemma 3.2 repeatedly gives

$$\alpha(n,d \mid f) = \sum_{d_1+\cdots+d_k=d} \prod_{i=1}^{k} \alpha(n_i,d_i \mid \ell_i^{n_i}).$$

Finally, $\alpha(n_i,d_i \mid \ell_i^{n_i}) = \alpha(n_i,d_i \mid x^{n_i}) = \beta(n_i,d_i)$, since for fixed $c \in \mathbb{Z}_p$ the map $g(x) \mapsto g(x+c)$ is measure-preserving on monic polynomials in $\mathbb{Z}_p[x]$ of a given degree. Thus

$$\alpha(n,d \mid f) = \sum_{d_1+\cdots+d_k=d} \prod_{i=1}^{k} \beta(n_i,d_i), \tag{29}$$

and (28) now follows from (25) and (29). □

Proof of Theorem 1(b), Equation (5). Let $\sigma = (1^{n_1} \cdots 1^{n_k} \cdots) \in \mathcal{S}(n)$ be as in Lemma 3.3. Then, by (24) and Lemma 3.3, we have

$$\alpha(n,d) = p^{-n} \sum_{\sigma \in \mathcal{S}(n)} N_\sigma \, \alpha(n,d \mid \sigma) = p^{-n} \sum_{\sigma \in \mathcal{S}(n)} N_\sigma \sum_{d_1+\cdots+d_k=d} \prod_{i=1}^{k} \beta(n_i,d_i). \tag{30}$$

Multiplying by u^d and summing over d gives

$$\sum_{d=0}^{n} \alpha(n,d) u^d = p^{-n} \sum_{\sigma \in \mathcal{S}(n)} N_\sigma \prod_{1^e \in \sigma} \left(\sum_{d=0}^{e} \beta(e,d) u^d \right).$$

Multiplying by $(pt)^n$, summing over n, and using Corollary 2.3, we obtain

$$\sum_{d=0}^{\infty} \left(\sum_{n=0}^{\infty} \alpha(n,d)(pt)^n \right) u^d = \left(\sum_{d=0}^{\infty} \left(\sum_{n=0}^{\infty} \beta(n,d) t^n \right) u^d \right)^p (1-t)^p (1-pt)^{-1}.$$

Finally, multiplying both sides by $1-pt$ yields (5). □

3.2.3 Writing the ρ's in terms of the α's and β's

The aim of this section is to prove (6), the second part of Theorem 1(b).

Recall that $\rho(n,d)$ is the expected number of d-sets of $\mathbb{Q}_p$-roots of polynomials $f \in \mathbb{Z}_p[x]$ of degree n. It is evident that this does not change if we restrict to primitive polynomials.

Let $f \in \mathbb{Z}_p[x]$ be a primitive polynomial of degree n. Let $m = \deg(\overline{f})$ be the reduced degree of f. For fixed m with $0 \le m \le n$, the density of primitive polynomials $f \in \mathbb{Z}_p[x]_n$ with reduced degree m is $\frac{p-1}{p^{n+1}-1}p^m$. Therefore, conditioning on the value of m, we have

$$\rho(n,d) = \frac{p-1}{p^{n+1}-1}\sum_{m=0}^{n} p^m \rho(n,d,m), \tag{31}$$

where $\rho(n,d,m)$ is the expected number of d-sets of $\mathbb{Q}_p$-roots of f as $f \in \mathbb{Z}_p[x]_n$ runs over polynomials of degree n with reduced degree m. This expectation does not change if we restrict to f whose reduction mod p is monic.

Equation (6) now follows from (31) and the following lemma.

Lemma 3.4. *We have*

$$\rho(n,d,m) = \sum_{d_1+d_2=d} \alpha(m,d_1)\cdot\beta(n-m,d_2). \tag{32}$$

Proof. This follows from Corollary 2.11 and (27). □

3.2.4 Writing the β's in terms of the α's

The aim of this section is to prove (7), the third and last part of Theorem 1(b).

Fixing d, we put $\alpha_n := \alpha(n,d)$ and $\beta_n := \beta(n,d)$. In the following lemma, we express β_n in terms of α_s for $s \le n$.

Lemma 3.5. *We have*

$$\beta_n = p^{-\binom{n}{2}}\alpha_n + (p-1)\sum_{0\le s<r<n} p^{-\binom{r+1}{2}}p^s\alpha_s. \tag{33}$$

Proof. Recall that β_n is the expected value of the random variable X distributed as the number of d-sets of $\mathbb{Z}_p$-roots of $f \in P_{x^n}$. All such roots must lie in $p\mathbb{Z}_p$, and thus correspond to $\mathbb{Z}_p$-roots of $f(px)$. To each $f \in P_{x^n}$, we associate a pair of integers (r,s) with $0 \le s \le r \le n$ as follows. Consider $f(px)$, and let r be the largest integer such that $p^r \mid f(px)$, so that $1 \le r \le n$. Let s be the reduced degree of $p^{-r}f(px)$. Then either $0 \le s < r < n$, or $s = r = n$.

The relative density of the subset of $f \in P_{x^n}$ such that $p^r \mid f$ is $p^{-\binom{r}{2}}$, since for $0 \le i \le r-2$ we require the coefficient of x^i in f to be divisible by p^{r-i} and not just by p. Given $r < n$, the condition that $p^{-r}f(px)$ has reduced degree at least s imposes $r-s-1$ additional divisibility conditions, so the relative density of those f such that the reduced degree is exactly s is $p^{-(r-s-1)}(1-1/p) = p^{s-r}(p-1)$. Thus the relative density of $f \in P_{x^n}$ with parameters (r,s) is given by $p^{-\binom{r}{2}}p^{s-r}(p-1) = p^{-\binom{r+1}{2}}p^s(p-1)$ for $0 \le s < r < n$. If $r = n$, then $s = r$, and therefore the density of f with parameters (n,n) is $p^{-\binom{n}{2}}$.

Given the values of r and s, the conditional expected value of X is α_s, independent of r, by Corollary 2.11. Hence $\beta_n = p^{-\binom{n}{2}}\alpha_n + \sum_{0\le s<r<n} p^{-\binom{r+1}{2}}p^s(p-1)\alpha_s$. □

Proof of (7). Taking Equation (33) for n and $n-1$ and subtracting gives

$$p^{\binom{n}{2}}(\beta_n - \beta_{n-1}) = (\alpha_n - p^{n-1}\alpha_{n-1}) + (p-1)\sum_{s=0}^{n-2} p^s \alpha_s. \tag{34}$$

Now taking Equation (34) for n and $n-1$ and again subtracting yields

$$p^{\binom{n}{2}}[(\beta_n - \beta_{n-1}) - p^{1-n}(\beta_{n-1} - \beta_{n-2})] = (\alpha_n - \alpha_{n-1}) - p^{n-1}(\alpha_{n-1} - \alpha_{n-2}),$$

and this indeed asserts the equality of the coefficient of t^n on both sides of (7). □

We have completed the proof of Theorem 1(b).

Remark 3.6. Equations (30), (31), (32) and (33) are sufficient to compute the α's, β's and ρ's. We were motivated to find the neater formulation in Theorem 1(b) by the desire to prove the $p \leftrightarrow 1/p$ symmetries.

3.3 Proof of Theorem 1(c)

Consider a random polynomial of degree n in $\mathbb{Z}_p[x]$. Let $\widetilde{\alpha}(n,d)$ be the expected number of d-sets of roots in $\mathbb{Z}_p$. Conditioning on the reduced degree and applying Corollary 2.11 shows that

$$\widetilde{\alpha}(n,d) = \sum_{m=0}^{n} \left(1 - \frac{1}{p}\right) \frac{1}{p^m} \alpha(n-m,d) + \frac{1}{p^{n+1}} \widetilde{\alpha}(n,d).$$

This rearranges to give

$$\widetilde{\alpha}(n,d) = \sum_{m=0}^{n} (1-p) p^m \alpha(m,d) + p^{n+1} \widetilde{\alpha}(n,d). \tag{35}$$

In other words, $\widetilde{\alpha}(n,d)$ is a weighted average of the $\alpha(m,d)$ for $m \le n$.

We now show that $\alpha(n,d)$ and $\widetilde{\alpha}(n,d)$ are equal and independent of n, provided that $n \ge 2d$.

Let $A_n = \mathbb{Z}_p[X]_n^1$ denote the set of monic polynomials over $\mathbb{Z}_p$ of degree n, and B_n the set of all polynomials of degree less than n. Then we have $A_n = \{X^n + h : h \in B_n\}$, and both A_n and B_n may be identified with $\mathbb{Z}_p^n$ and have measure 1. Let A_n^{split} be the subset of those f in A_n that split completely. The measure of A_n^{split} is $\alpha(n,n)$.

Now consider the multiplication map $A_d^{\text{split}} \times \mathbb{Z}_p[x]_{n-d} \to \mathbb{Z}_p[x]_n$, whose image is the set of $f \in \mathbb{Z}_p[x]_n$ with at least d roots in $\mathbb{Z}_p$; in general, the number of preimages of f in $\mathbb{Z}_p[x]_n$ is equal to the number of d-sets of roots of f in $\mathbb{Z}_p$. This implies that $\widetilde{\alpha}(n,d)$ is the p-adic measure of the image of the multiplication map, viewed as a multiset. The change of variables from $A_d^{\text{split}} \times \mathbb{Z}_p[x]_{n-d}$ to $\mathbb{Z}_p[x]_n$ introduces a Jacobian factor which, by Lemma 2.6, is just the resultant. Therefore,

$$\widetilde{\alpha}(n,d) = \int_{g \in A_d^{\text{split}}} \int_{h \in \mathbb{Z}_p[x]_{n-d}} |\operatorname{Res}(g,h)| \, dh \, dg. \tag{36}$$

Similarly, we have

$$\alpha(n,d) = \int_{g \in A_d^{\text{split}}} \int_{h \in A_{n-d}} |\operatorname{Res}(g,h)| \, dh \, dg. \tag{37}$$

The following lemma now proves the first part of Theorem 1(c), namely, that $\mathcal{A}_d(t)$ is a polynomial of degree at most $2d$.

Lemma 3.7. *The expectations $\alpha(n,d)$ and $\widetilde{\alpha}(n,d)$ are equal and independent of n for $n \geq 2d$.*

Proof. By (36) and (37) it suffices to show that for each fixed g in A_d^{split}, the values of the inner integrals $\int_{h\in\mathbb{Z}_p[x]_{n-d}} |\operatorname{Res}(g,h)|\ dh$ and $\int_{h\in A_{n-d}} |\operatorname{Res}(g,h)| dh$ are equal and independent of n for $n \geq 2d$. Our argument is quite general, in that we only use that g is monic, not that it is split.

We assume that $n \geq 2d$, and write each $h \in \mathbb{Z}_p[x]_{n-d}$ uniquely as $h = qg+r$ with $q \in \mathbb{Z}_p[x]_{n-2d}$ and $r \in B_d$. This sets up a bijection $(q,r) \mapsto h = qg + r$ from $\mathbb{Z}_p[x]_{n-2d} \times B_d$ to $\mathbb{Z}_p[x]_{n-d}$ (using here that $n - d \geq d$). Now using $\operatorname{Res}(g,h) = \operatorname{Res}(g,r)$, and the fact that our bijection has trivial Jacobian (the change of basis matrix is triangular with 1's on the diagonal since g is monic), we deduce that

$$\int_{h\in\mathbb{Z}_p[x]_{n-d}} |\operatorname{Res}(g,h)|dh = \int_{q\in\mathbb{Z}_p[x]_{n-2d}} \int_{r\in B_d} |\operatorname{Res}(g,r)|drdq = \int_{r\in B_d} |\operatorname{Res}(g,r)|dr,$$

since the integral over $q \in \mathbb{Z}_p[x]_{n-2d}$ is just the measure of $\mathbb{Z}_p[x]_{n-2d}$ which is 1. In an identical manner, we have

$$\int_{h\in A_{n-d}} |\operatorname{Res}(g,h)|dh = \int_{q\in A_{n-2d}} \int_{r\in B_d} |\operatorname{Res}(g,r)|drdq = \int_{r\in B_d} |\operatorname{Res}(g,r)|dr.$$

Hence

$$\widetilde{\alpha}(n,d) = \alpha(n,d) = \int_{g\in A_d^{\mathrm{split}}} \int_{r\in B_d} |\operatorname{Res}(g,r)|\ dr\ dg$$

for $n \geq 2d$. The inner integral above clearly depends on g and d, but not on n. □

We now turn to proving the remaining parts of Theorem 1(c). By Lemma 3.7, we have that $\mathcal{A}_d(t)$ is a polynomial of degree at most $2d$. Thus, fixing any $n \geq 2d$, we may write

$$\mathcal{A}_d(t) = (1-t)\sum_{m=0}^{n} \alpha(m,d)t^m + \alpha(n,d)t^{n+1}. \tag{38}$$

Lemma 3.7 allows us to replace $\widetilde{\alpha}(n,d)$ by $\alpha(n,d)$ in (35). Taking $t = 1$ in (38) shows that the left hand side of (35) is $\mathcal{A}_d(1)$. Taking $t = p$ in (38) shows that the right hand side of (35) is $\mathcal{A}_d(p)$. Therefore, $\mathcal{A}_d(1) = \mathcal{A}_d(p)$.

Since $\mathcal{A}_d$ is a polynomial of degree at most $2d$, it follows by (5), or equally (4), that $\mathcal{B}_d$ is a polynomial of degree at most $2d$. Directly from the definitions of $\mathcal{A}_d$ and $\mathcal{B}_d$, these results are equivalent to the statements that $\alpha(n,d) = \mathcal{A}_d(1)$ and $\beta(n,d) = \mathcal{B}_d(1)$ for all $n \geq 2d$.

It follows by (6) that $\mathcal{R}_d$ is a polynomial of degree at most $2d$. To prove the stabilisation result for the $\rho(n,d)$, we use the fact we just proved that $\mathcal{A}_d(1) = \mathcal{A}_d(p)$. It follows by (5), or equally (4), that $\mathcal{B}_d(1) = \mathcal{B}_d(1/p)$. By (6), we then have $\mathcal{R}_d(1) = \mathcal{R}_d(1/p)$. We may therefore write $\mathcal{R}_d(t) = \mathcal{R}_d(1) + (1-t)(1-pt)F(t)$ where F has degree at most $2d-2$. Finally, from the definition of $\mathcal{R}_d$, we have $\rho(n,d) = \mathcal{R}_d(1)$ for all $n > \deg(F)$.

This completes the proof of Theorem 1(c).

4 Asymptotic results

In this section, we prove Proposition 1.1. The proof is essentially independent of our earlier results, although for convenience we will reference some of our earlier formulas. We begin with a well-known lemma (see, e.g., [4, p. 256] for a proof).

Lemma 4.1. *Let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree n, and $C \subset S_n$ a conjugacy class (i.e., a cycle type) corresponding to the partition $d_1 + \cdots + d_t = n$. Let $\lambda(C,p)$ be the probability that f factors into irreducible polynomials of degrees $d_1, \ldots, d_t$, respectively. Then $\lambda(C,p) \to |C|/n!$ as $p \to \infty$.*

If $\sigma = (d_1^{e_1}\, d_2^{e_2} \cdots d_t^{e_t}) \in \mathcal{S}(n)$ is a splitting type of degree n, then by (17), we have that N_σ is a polynomial in p of degree $\sum_{i=1}^t d_i$. Therefore, if $e_i > 1$ for at least one $i \in \{1, 2, \ldots, t\}$, then

$$\lim_{p\to\infty} \frac{N_\sigma}{p^n} = 0.$$

By (24), to compute $\lim_{p\to\infty} \alpha(n,d)$, it thus suffices to consider only $\sigma \in \mathcal{S}(n)$ that correspond to factorizations without multiple factors, i.e., to partitions $d_1 + \cdots + d_t = n$ of n. It is sufficient to consider only those squarefree polynomials modulo p that have $r \geq d$ distinct roots (since all of these roots lift by Hensel's lemma), where each such polynomial is weighted by $\binom{r}{d}$. By Lemma 4.1, we wish to count all permutations in S_n with r fixed points, where each such permutation is weighted by $\binom{r}{d}$. The total weighted number of such permutations is $\binom{n}{d}(n-d)! = \frac{n!}{d!}$, because we can choose d fixed points in $\{1, 2, \ldots, n\}$, and then randomly permute the other $n-d$ numbers. It follows that

$$\lim_{p\to\infty} \alpha(n,d) = \frac{1}{n!}\frac{n!}{d!} = \frac{1}{d!}. \tag{39}$$

By (31), we have $\lim_{p\to\infty} \rho(n,d) = \lim_{p\to\infty} \rho(n,d,n)$. Either directly from the definitions, or as a special case of (32), we have $\rho(n,d,n) = \alpha(n,d)$. Therefore,

$$\lim_{p\to\infty} \rho(n,d) = \lim_{p\to\infty} \alpha(n,d) = \frac{1}{d!},$$

proving Proposition 1.1(a) for ρ and α.

Using (2), and its analogue for α^*, we then have

$$\lim_{p\to\infty} \rho^*(n,r) = \lim_{p\to\infty} \alpha^*(n,r) = \sum_{d=0}^{n} (-1)^{d-r} \binom{d}{r} \frac{1}{d!} = \frac{1}{r!} \sum_{d=0}^{n-r} (-1)^d \frac{1}{d!},$$

proving Proposition 1.1(b).

To prove the large p limits involving β, we note that if $d = n-1$ or $d = n$, then (33) is just

$$\beta(n,d) = p^{-\binom{n}{2}} \alpha(n,d),$$

while if $d < n-1$, then Equation (33) takes the shape

$$\beta(n,d) = p^{-\binom{d+1}{2}} \alpha(d,d) + O(p^{-\binom{d+1}{2}-1}).$$

From the previous two equations and (39), we see that

$$\lim_{p\to\infty} p^{\binom{n}{2}} \beta(n,n) = \frac{1}{n!} \quad \text{and} \quad \lim_{p\to\infty} p^{\binom{d+1}{2}} \beta(n,d) = \frac{1}{d!} \text{ for } d < n,$$

proving Proposition 1.1(a) for β.

The analogue of (2) for β^* shows that for $r \leq n-2$, we have

$$\lim_{p\to\infty} p^{\binom{r+1}{2}}\beta^*(n,r) = \frac{1}{r!}.$$

Since $\beta^*(n,n) = \beta(n,n)$, this completes the proof of Proposition 1.1(c). Note that $\beta^*(n,n-1) = 0$, so there is no need to compute the limits in this case.

If we take $r = 0$ in Proposition 1.1, we see that

$$\lim_{p\to\infty} \rho^*(n,0) = \sum_{d=0}^{n}(-1)^d/d!.$$

The reader may recognise this as the answer to the derangements problem, i.e., the probability that a random permutation on n letters has no fixed point. This is the case because, by Lemma 4.1, monic polynomials without $\mathbb{Q}_p$-roots correspond, in the large p limit, to permutations without fixed points. Similarly, the limit $\lim_{p\to\infty}\rho^*(n,r) = (1/r!)\sum_{d=0}^{n-r}(-1)^d/d!$ is equal to the probability that a random permutation on n letters has exactly r fixed points.

Acknowledgments

We thank the CMI-HIMR Summer School in Computational Number Theory held at the University of Bristol in June 2019, where this work began. We also thank Xavier Caruso for kindly sharing with us his unpublished lecture notes [3], and Hendrik Lenstra, Steffen Müller, Lazar Radičević, Arul Shankar, and Jaap Top for many helpful conversations.

The first author was supported by a Simons Investigator Grant and NSF grant DMS-1001828. The second author was supported by the Heilbronn Institute for Mathematical Research. The fourth author was supported in parts by DFG-Grant MU 4110/1-1 and NWO grant VI.Vidi.192.106.

References

[1] M. Bhargava, J. E. Cremona, T. A. Fisher, N. G. Jones, and J. P. Keating, What is the probability that a random integral quadratic form in n variables has an integral zero?, *Int. Math. Res. Not.* **2016**, Issue 12 (2016), 3828–3848. https://doi.org/10.1093/imrn/rnv251.

[2] J. Buhler, D. Goldstein, D. Moews, and J. Rosenberg, The probability that a random monic p-adic polynomial splits, *Exper. Math.* **15:1** (2006), 21–32.

[3] X. Caruso, Where are the zeroes of a random p-adic polynomial?. Unpublished notes. Available at http://xavier.toonywood.org/papers/publis/randompoly-talk.pdf.

[4] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271.

[5] D. J. Limmer, *Measure-equivalence of quadratic forms*, Ph.D. Thesis, Oregon State University, 1999.

[6] R. Shmueli, The expected number of roots over the field of p-adic numbers, arXiv:2101.03561v1 , Jan. 2021.

[7] B. L. Weiss, Probabilistic Galois theory over p-adic fields, *J. Number Theory* **133:5** (2013), 1537–1563.