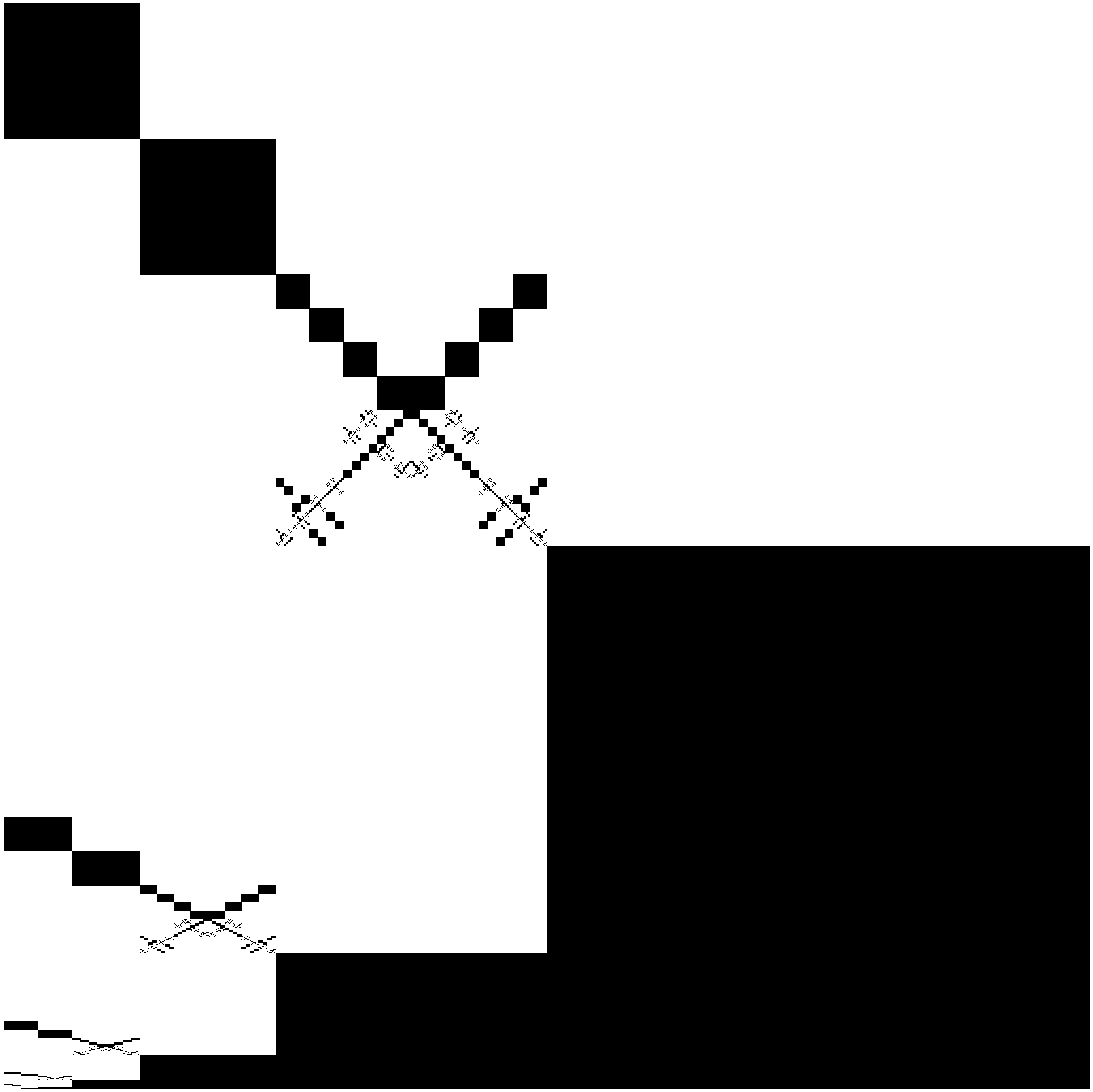
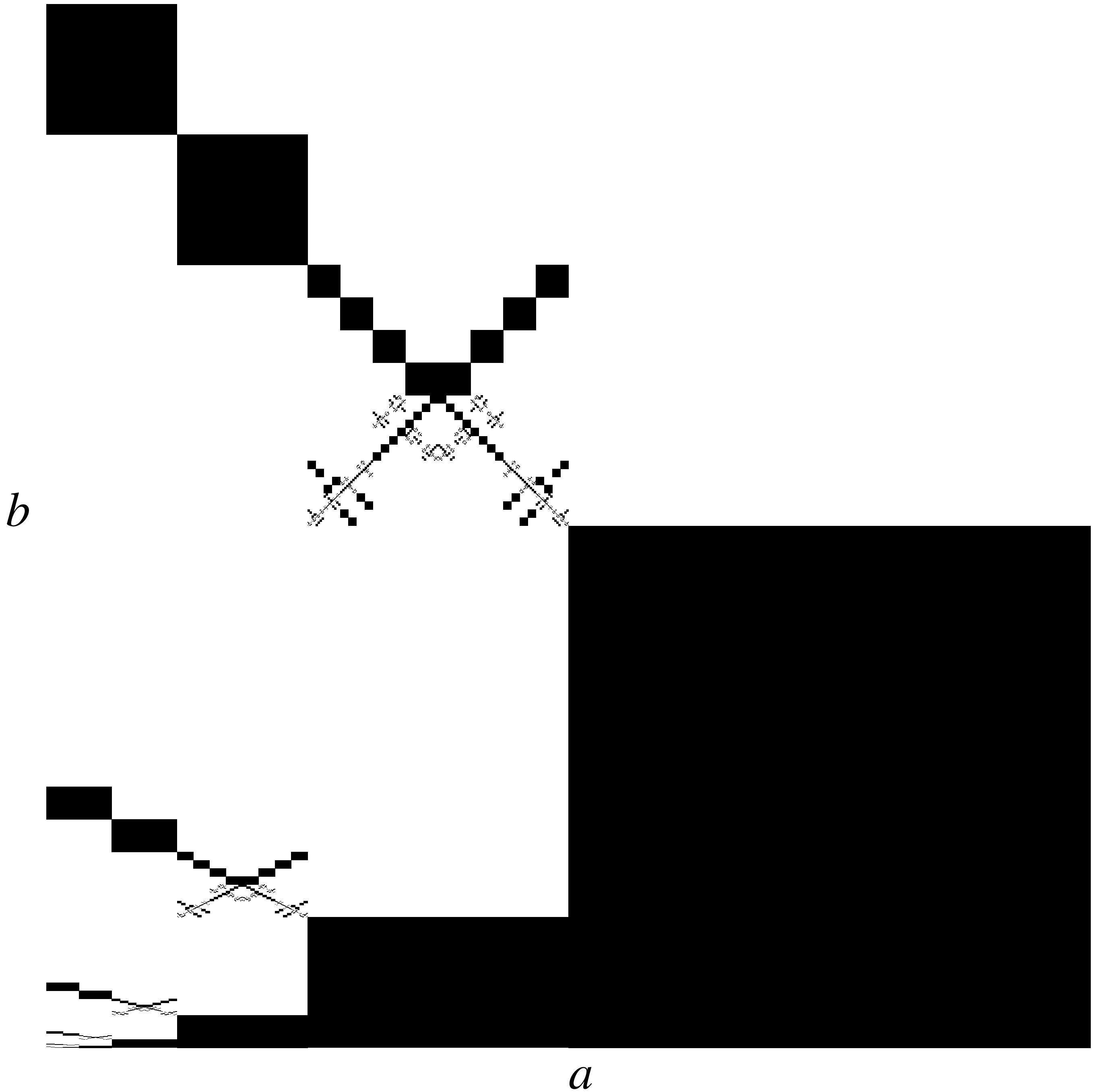


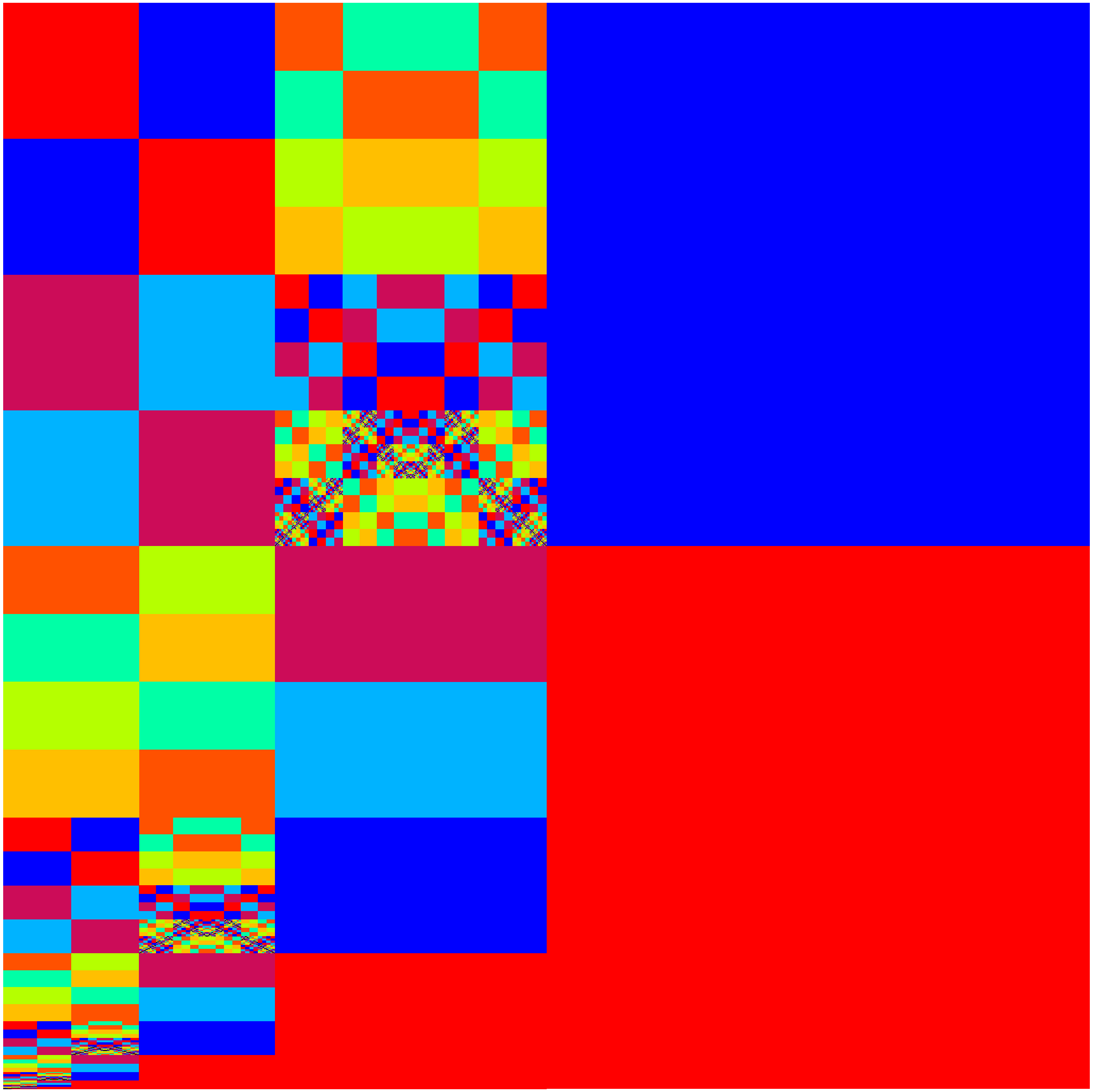
The probability that a p-adic polynomial splits.

Asher Auel, University of Pennsylvania

Joint work with:
Joe P. Buhler, CCR Labs



x^2+ax+b splits? a,b in $\mathbf{Z}_2$



The p-adic integers

The ring $\mathbf{Z}_p$ is a local ring, with unique maximal ideal $p\mathbf{Z}_p$ and units

$$\mathbf{Z}_p^* = \mathbf{Z}_p \backslash z\mathbf{Z}_p = \{a_0 + a_1\,p + \cdots \in \mathbf{Z}_p : a_0 \neq 0\}.$$

If $a \in \mathbf{Z}_p$ is not a unit, then

$$\begin{aligned} a &= a_k\,p^k + a_{k+1}\,p^{k+1} + \cdots \\ &= p^k(a_k + a_{k+1}\,p + \cdots) \\ &= p^k\,u, \quad \text{for some } u \in \mathbf{Z}_p^*, \end{aligned}$$

so there's a disjoint union

$$\mathbf{Z}_p \backslash \{0\} = \bigcup_{k=0}^{\infty} p^k \mathbf{Z}_p^*.$$

Absolute Value (Norm)

Definition 1.

$$|a|_p = \begin{cases} p^{-v_p(a)} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases},$$

where

$$v_p(a) = \begin{cases} \min(a_v : a_v \neq 0) & \text{if } a \neq 0 \\ \infty & \text{if } a = 0 \end{cases},$$

is called the valuation of $a = a_0 + a_1 p + a_2 p^2 + \cdots$.

The p-adic absolute value has all the properties any absolute value should and more,

$$|ab|_p = |a|_p \, |b|_p \, ,$$

$$|a + b|_p \leq \max(|a|_p \, , |b|_p).$$

The ring $\mathbf{Z}_p$ with $|\cdot|_p$ is a compact metric space, in fact, a compact topological group.

Integration

Theorem. Let G be a compact topological group, then there exists a unique *Haar measure (integral)* on G, i.e. a map

$$\int_G : C(G, \mathbf{R}) \to \mathbf{R},$$

such that

- it's normalized :$\int_G \mathbf{1} = 1$
- positive: $f > 0 \Rightarrow \int_G f > 0$
- continuous in the sup-norm topology of $C(G, \mathbf{R})$
- linear
- translation invariant: $\int_G f(x + a) = \int_G f(x)$.

Example. We will integrate the continuous function $x \mapsto |x|_p : \mathbf{Z}_p \to \mathbf{R}$. First, by the decomposition of the p-adic integers,

$$\int_{\mathbf{Z}_p} |x|_p = \sum_{k=0}^{\infty} \int_{p^k \mathbf{Z}_p^*} |x|_p = \sum_{k=0}^{\infty} \int_{p^k \mathbf{Z}_p^*} \left|p^k u\right|_p = \sum_{k=0}^{\infty} \frac{1}{p^k} \int_{p^k \mathbf{Z}_p^*} \mathbf{1}.$$

Now note that we have the disjoint union

$$\mathbf{Z}_p = \bigcup_{r=0}^{p-1} (r + p\mathbf{Z}_p),$$

of sets which are all translates, so they all have the same volume, namely $1/p$, thus we have

$$\int_{\mathbf{Z}_p^*} \mathbf{1} = \frac{p-1}{p},$$

and by similar arguments,

$$\int_{p^k \mathbf{Z}_p^*} \mathbf{1} = \frac{1}{p^k} \frac{p-1}{p}.$$

Continuing on, we have

$$\int_{\mathbf{Z}_p} |x|_p = \sum_{k=0}^{\infty} \frac{1}{p^k} \int_{p^k \mathbf{Z}_p^*} \mathbf{1} = \sum_{k=0}^{\infty} \frac{1}{p^k} \frac{1}{p^k} \frac{p-1}{p} = \frac{p-1}{p} \frac{1}{1 - \frac{1}{p^2}} = \frac{p}{p+1}.$$

The quadratic case

Consider the map parametrizing the split quadratic polynomials,

$$\begin{aligned} \varphi : \mathbf{Z}_p^2 &\rightarrow \mathsf{Split}_p(2) \subset \mathbf{Z}_p[x] \\ (a,b) &\mapsto (x-a)(x-b) = x^2 - (a+b)x + ab. \end{aligned}$$

It's a surjective (almost everywhere) 2-to-1 map. We have an isomorphism of topological groups

$$\begin{aligned} \mathbf{Z}_p[x]_2 &\stackrel{\sim}{\rightarrow} \mathbf{Z}_p^2 \\ x^2 - cx + d &\mapsto (c,d), \end{aligned}$$

and so the composition

$$\begin{aligned} \tilde{\varphi} : \mathbf{Z}_p^2 &\rightarrow \mathbf{Z}_p^2 \\ (a,b) &\mapsto (a+b, ab). \end{aligned}$$

So now we just need to compute the integral,

$$s_p(2) = \int_{\mathsf{Split}_p(2)} \mathbf{1} = \int_{\varphi(\mathbf{Z}_p^2)} \mathbf{1} = \frac{1}{2} \int_{\mathbf{Z}_p^2} |\mathsf{det}(J\tilde{\varphi})|_p \, .$$

$$
\begin{aligned}
s_p(2) &= \frac{1}{2}\int_{\mathbf{Z}_p^2} |a-b|_p \; da\, db \\
&= \frac{1}{2}\int_{b\in\mathbf{Z}_p} \left(\int_{a\in\mathbf{Z}_p} |a-b|_p \; da\right) db \\
&= \frac{1}{2}\int_{\mathbf{Z}_p} |a|_p \; da \\
&= \frac{1}{2}\frac{p}{p+1}.
\end{aligned}
$$

So in particular

$$s_2(2) = \frac{1}{3}.$$

Also note that

$$\lim_{p\to\infty} s_p(2) = \frac{1}{2}.$$

The general split case

Now define a map

$$\begin{aligned} \varphi_n : \mathbf{Z}_p^n &\rightarrow \mathrm{Split}_p(n) \subset \mathbf{Z}_p[x] \\ a = (a_1, \ldots, a_n) &\mapsto \prod_{j=1}^{n} (x - a_j) \end{aligned}$$

Then φ_n is a (almost everywhere) $n!$-to-1 mapping Again, by the standard isomorphism of topological groups,

$$\begin{aligned} \tilde{\varphi}_n : \mathbf{Z}_p^n \rightarrow \mathbf{Z}_p[x] &\stackrel{\sim}{\rightarrow} \mathbf{Z}_p^n \\ (a_1, \ldots, a_n) &\mapsto (a_1 + \cdots + a_n, \ldots, a_1 \cdots a_n). \end{aligned}$$

So we have to compute

$$\begin{aligned} s_p(n) &= \mathrm{vol}(\mathrm{Split}_p(n) = \tilde{\varphi}_n(\mathbf{Z}_p))1 = \frac{1}{n!} \int_{\mathbf{Z}_p^n} |\det(J\tilde{\varphi}_n)|_p \\ &= \frac{1}{n!} \int_{\mathbf{Z}_p^n} \prod_{i<j} \left| a_i - a_j \right|_p da. \end{aligned}$$

Theorem. Let p be a prime. Denote by $s_p(n)$ the probability that a monic polynomial of degree n with p-adic integer coefficients will split completely, then we have the following recursion

$$s_p(n) = \sum_{\lambda} \prod_{k=0}^{p-1} p^{-\binom{\lambda_k+1}{2}} I_{\lambda_k},$$

where the sum is taken over all $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{p-1}) \in \mathbf{N}^p$ such that $\lambda_0 + \cdots + \lambda_{p-1} = n$. I define $I_0 = 1$, and $I_1 = 1$ is obvious.

Corollary. With the above notation,

$$\lim_{p \to \infty} s_p(n) = \frac{1}{n!}.$$

For $p = 2$ the recursion is

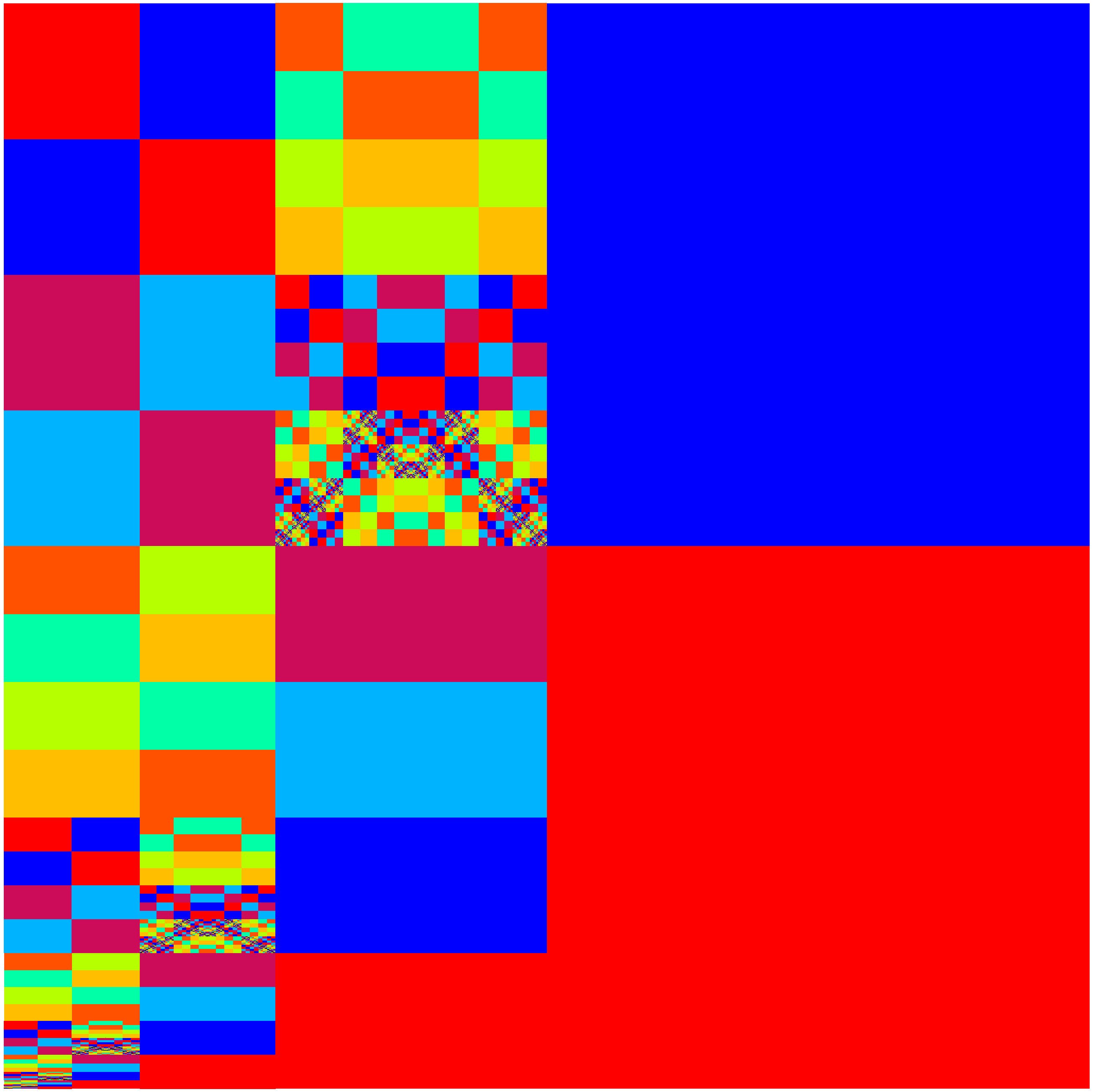
$$s_2(n) = \sum_{r+s=n} 2^{-\binom{r+1}{2}-\binom{s+1}{2}} s_2(r) s_2(s),$$

where the sum is taken over all non-negative integers r and s with $r+s = n$. Setting

$$r_n := 2^{-\binom{n+1}{2}} s_2(n),$$

we can write this recursion as

$$2^{\binom{n+1}{2}} r_n = \sum_{i=0}^{n} r_i r_{r-i}.$$



Extension to Extensions

The p-adic integers $\mathbf{Z}_p$ are the ring of integers of the field of p-adic numbers $\mathbf{Q}_p$. One extension of this problem is to ask

"What is the probability that a polynomial will have roots in a given algebraic extension of $\mathbf{Q}_p$?"

There are in fact only a finite number of extensions of a given degree over $\mathbf{Q}_p$. For example, over $\mathbf{Q}_2$, there are 7 different quadratic extensions. Below I give a list of these extensions and the probability that a monic irreducible quadratic polynomial has roots in that extension:

$\mathbf{Q}_2(\zeta_3)$	$\mathbf{Q}_2(\sqrt{3})$	$\mathbf{Q}_2(\sqrt{7})$	$\mathbf{Q}_2(\sqrt{2})$	$\mathbf{Q}_2(\sqrt{6})$	$\mathbf{Q}_2(\sqrt{10})$	$\mathbf{Q}_2(\sqrt{14})$
$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$

As we computed, the completely splitting polynomials have probability 1/3, as these are the only ways that the polynomials can factor, the sum of these probabilities is

$$\frac{1}{3}+\frac{1}{3}+\frac{1}{12}+\frac{1}{12}+\frac{1}{24}+\frac{1}{24}+\frac{1}{24}+\frac{1}{24}=1.$$