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? \quad a, b \text{ in } \mathbb{Z}_2$
The \( p \)-adic integers

The ring \( \mathbb{Z}_p \) is a local ring, with unique maximal ideal \( p\mathbb{Z}_p \) and units

\[
\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{ a_0 + a_1 p + \cdots \in \mathbb{Z}_p : a_0 \neq 0 \}.
\]

If \( a \in \mathbb{Z}_p \) is not a unit, then

\[
a = a_k p^k + a_{k+1} p^{k+1} + \cdots = p^k (a_k + a_{k+1} p + \cdots) = p^k u, \quad \text{for some } u \in \mathbb{Z}_p^*,
\]

so there's a disjoint union

\[
\mathbb{Z}_p \setminus \{0\} = \bigcup_{k=0}^{\infty} p^k \mathbb{Z}_p^*.
\]
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 \( \mathbb{Z}_p \) 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

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

such that

- it's normalized: $\int_G 1 = 1$
- positive: $f > 0 \Rightarrow \int_G f > 0$
- continuous in the sup-norm topology of $C(G, \mathbb{R})$
- linear
- translation invariant: $\int_G f(x + a) = \int_G f(x)$.
Example. We will integrate the continuous function $x \mapsto |x|_p : \mathbb{Z}_p \to \mathbb{R}$. First, by the decomposition of the $p$-adic integers,

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

Now note that we have the disjoint union

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

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

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

and by similar arguments,

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

Continuing on, we have

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

Consider the map parametrizing the split quadratic polynomials,

\[ \varphi : \mathbb{Z}_p^2 \to \text{Split}_p(2) \subset \mathbb{Z}_p[x] \]

\[ (a, b) \mapsto (x - a)(x - b) = x^2 - (a + b)x + ab. \]

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

\[ \mathbb{Z}_p[x]_2 \sim \mathbb{Z}_p^2 \]

\[ x^2 - cx + d \mapsto (c, d), \]

and so the composition

\[ \tilde{\varphi} : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2 \]

\[ (a, b) \mapsto (a + b, ab). \]

So now we just need to compute the integral,

\[ s_p(2) = \int_{\text{Split}_p(2)} 1 = \int_{\varphi(\mathbb{Z}_p^2)} 1 = \frac{1}{2} \int_{\mathbb{Z}_p^2} |\det(J\tilde{\varphi})|_p. \]
\[ s_p(2) = \frac{1}{2} \int_{\mathbb{Z}_p^2} |a - b|_p \, da \, db \]

\[ = \frac{1}{2} \int_{b \in \mathbb{Z}_p} \left( \int_{a \in \mathbb{Z}_p} |a - b|_p \, da \right) \, db \]

\[ = \frac{1}{2} \int_{\mathbb{Z}_p} |a|_p \, da \]

\[ = \frac{1}{2p + 1} \cdot \frac{1}{p} \cdot \frac{1}{2p + 1}. \]

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

\[ \varphi_n : \mathbb{Z}_p^n \to \text{Split}_p(n) \subset \mathbb{Z}_p[x] \]

\[ a = (a_1, \ldots, a_n) \mapsto \prod_{j=1}^n (x - a_j) \]

Then \( \varphi_n \) is a (almost everywhere) \( n! \)-to-1 mapping

Again, by the standard isomorphism of topological groups,

\[ \tilde{\varphi}_n : \mathbb{Z}_p^n \to \mathbb{Z}_p[x] \sim \mathbb{Z}_p^n \]

\[ (a_1, \ldots, a_n) \mapsto (a_1 + \cdots + a_n, \ldots, a_1 \cdots a_n). \]

So we have to compute

\[ s_p(n) = \text{vol}(\text{Split}_p(n) = \tilde{\varphi}_n(\mathbb{Z}_p))1 = \frac{1}{n!} \int_{\mathbb{Z}_p^n} |\det(J \tilde{\varphi}_n)|_p \]

\[ = \frac{1}{n!} \int_{\mathbb{Z}_p^n} \prod_{i<j} |a_i - a_j|_p \, da. \]
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

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

where the sum is taken over all $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{p-1}) \in \mathbb{N}^p$ 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

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

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

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

we can write this recursion as

$$2^{(n+1)/2} r_n = \sum_{i=0}^{n} r_ir_{r-i}.$$
Extension to Extensions

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

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

There are in fact only a finite number of extensions of a given degree over $\mathbb{Q}_p$. For example, over $\mathbb{Q}_2$, 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:

\[
\begin{array}{cccccccc}
\mathbb{Q}_2(\zeta_3) & \mathbb{Q}_2(\sqrt{3}) & \mathbb{Q}_2(\sqrt{7}) & \mathbb{Q}_2(\sqrt{2}) & \mathbb{Q}_2(\sqrt{6}) & \mathbb{Q}_2(\sqrt{10}) & \mathbb{Q}_2(\sqrt{14}) \\
\frac{1}{3} & \frac{1}{12} & \frac{1}{12} & \frac{1}{24} & \frac{1}{24} & \frac{1}{24} & \frac{1}{24}
\end{array}
\]

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

\[
\frac{1}{3} + \frac{1}{3} + \frac{1}{12} + \frac{1}{12} + \frac{1}{24} + \frac{1}{24} + \frac{1}{24} + \frac{1}{24} = 1.
\]