# Burda on Folding Polynomials and Cutting Cakes

June-28-12
3:11 PM

What polynomials $Q \in \mathbb{Z}[x]$ have the property that $Q : \mathbb{Z}/p \to \mathbb{Z}/p$ is invertible for $\infty$-many primes $p$. "Q is exceptional"

---

Question. Does

$$f(x,y) = \frac{Q(x)-Q(y)}{x-y} = 0$$

have zeros in $(\mathbb{Z}/p)^2$?

(Probabilistically, expect $p$ solutions)

---

Thm (Weil) If $f(x,y)$ is irred over $\mathbb{C}$,

$$\left|\#[f(x,y)=0] - p\right| \leq C\sqrt{p}$$

... So $\frac{Q(x)-Q(y)}{x-y} = 0$ must have several components.

$\iff$

$$\begin{array}{c} \{(x,y) : Q(x)=Q(y),\ x \neq y\} \\ \big\downarrow Q \\ \mathbb{CP}^1 \end{array}$$

We want the monodromy group of $Q$ to not be 2-transitive.

⋮

The only exceptional polynomials are $z^n$ & Chebyshev polynomials:

$$T_n(\cos x) = \cos(nx)$$

or

$$T_n\left(\frac{z+z^{-1}}{2}\right) = \frac{z^n+z^{-n}}{2} \qquad (n \neq 2)$$