

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

Question. Does

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

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

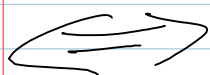
(Probabilistically,
expect p
solutions)

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

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

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

several components.



$$\{(x, y): Q(x) = Q(y), x \neq y\}$$

$$\downarrow Q$$

$$\mathbb{C}P^1$$

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

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