Burda: Arithmetic properties of Chebyshev polynomials

December-10-12
2:10 PM

$z \mapsto z^n$ as $\mathbb{F}_p \to \mathbb{F}_p$ is a multiplicative homomorphism. $|\text{Image}| \mid p-1$; if $(n, p-1) = 1$, $|\text{Image}| = p-1$.

Yet for a generic $q(x) \in \mathbb{Z}(x)$, then

$$q : \mathbb{F}_p \to \mathbb{F}_p$$

For $p \gg n$, $\frac{|\text{Image}|}{p-1} \sim 63\%$

Schur's Question. Are there other polynomials q in $\mathbb{Q}[x]$ s.t. $q : \mathbb{F}_p \to \mathbb{F}_p$ is surjective for infinitely many primes.

Ans. Yes, only compositions of

$z \mapsto z^n$ $\quad n > 2$

$z \mapsto T_n(z)$, Chebychev poly for $n > 3$

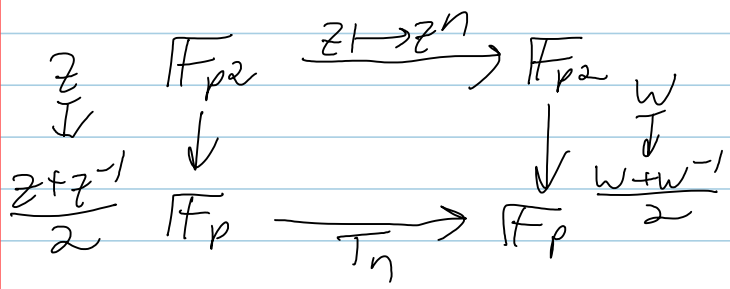
& $z \mapsto az + b$

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

More algebraically:

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

$\frac{(n-1)(p^2-1)}{2}$



So if $(n, p^2-1) = 1$

then

$|\text{Image}(T_n)| = p$