Young Mathematicians Conference 2018

The Ohio State University, August 10-12

A Formula for the Number of Monic Degree m Polynomials in $F_q[x]$ with Discriminant d

Michael J Seaman (mseaman@caltech.edu)

Caltech [Mentor:Zavosh Amir-Khosravi]

Abstract of Report Talk: We show a formula for the distribution of discriminants of monic polynomials over a finite field. For an odd prime power q, integer $m \geq 2$, and $d \in \mathbb{F}_q$, let $|V_d^m(\mathbb{F}_q)|$ be the number of monic polynomials in $\mathbb{F}_q[x]$ of degree m with discriminant d. We express $|V_d^m(\mathbb{F}_q)|$ as a discrete Fourier transform of Gauss sums, computable in polynomial time.

For $d \neq 0$, we show

$$|V_d^m(\mathbb{F}_q)| = \sum_{c=1}^{q-1} \frac{G_\psi(c)^m \tau(-1)^{\frac{cm(m-1)}{2}} \tau(d)^{c+\frac{q-1}{2}}}{G_\psi(cm)} (B(c, m-1) - q^{-1} B(c, m))$$

where τ is a multiplicative character of order $q-1$, ψ a nontrivial additive character, $G_\psi(c)$ is the Gauss sum $G(\tau^c, \psi)$, and

$$B(c, m) = \begin{cases} q^{\frac{m \gcd(c, q-1)}{q-1}}, & \text{if } (q-1) | cm \\ 0, & \text{otherwise} \end{cases}$$

Among other corollaries, we show previously known asymptotic equidistribution of discriminants is actually exact equidistribution, that is $|V_d^m(\mathbb{F}_q)| = q^{m-1}$ for all $d \in \mathbb{F}_q$, if and only if $\gcd(q-1, m(m-1)) = 2$

Received: July 20, 2018