Polynomial point counts for curves over finite fields

Bogdan Grechuk • 23 Apr 2026

In (Canning et al. 2024), recently accepted for publication in *Acta Mathematica*, Canning, Larson, Payne, and Willwacher proved a striking result: the number of genus-g curves over a finite field $\mathbb{F}_q$, counted up to geometric isomorphism, is given by a polynomial in q if and only if $g \leq 8$.

Arithmetic algebraic geometry studies polynomial equations over arbitrary fields, with finite fields playing a particularly important role. If $q = p^r$ is a prime power, then, up to isomorphism, there is a unique finite field with q elements, denoted $\mathbb{F}_q$. An *algebraic closure* of $\mathbb{F}_q$ is an algebraically closed field $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$ such that every element of $\overline{\mathbb{F}}_q$ is a root of some nonzero polynomial with coefficients in $\mathbb{F}_q$.

For any field K, the projective space $\mathbb{P}^n(K)$ is the set of nonzero vectors in K^{n+1} modulo multiplication by nonzero scalars. We write the class of $(x_0, \ldots, x_n)$ as $(x_0 : \cdots : x_n)$. If K is algebraically closed and $F_1, \ldots, F_r$ are homogeneous polynomials over K, their common zero set in $\mathbb{P}^n(K)$ is called a *projective algebraic set*. If $X \subseteq \mathbb{P}^n(K)$ is a projective algebraic set, a *closed algebraic subset* of X is a subset of the form $X \cap Y$, where $Y \subseteq \mathbb{P}^n(K)$ is a projective algebraic set. A subset of X is called *open* if its complement is closed. The set X is *irreducible* if it cannot be written as the union of two proper closed algebraic subsets.

A *projective curve* over K is an irreducible projective algebraic set of dimension 1, meaning that it is not a point and that all of its proper irreducible closed algebraic subsets are points.

Let $C \subseteq \mathbb{P}^n(K)$ be a projective curve, and let $P \in C$. We say that C is nonsingular at P if, in some affine chart U containing P, there is an open neighborhood $V \subseteq U$ of P and polynomials $f_1, \ldots, f_m$ on U such that $C \cap V$ is the common zero set of $f_1, \ldots, f_m$ on V, and the Jacobian matrix $\big(\partial f_a / \partial u_j\big)(P)$ has rank $n - 1$. The curve is called *smooth* if it is nonsingular at every point.

Let $X \subseteq \mathbb{P}^n(K)$ and $Y \subseteq \mathbb{P}^m(K)$ be projective algebraic sets. A map $\phi : X \to Y$ is *regular* if for every point $P \in X$ there is an open subset $U \subseteq X$ containing P and homogeneous polynomials $G_0, \ldots, G_m \in K[x_0, \ldots, x_n]$ of the same degree such that for every point $Q = (a_0 : \cdots : a_n) \in U$, the values $G_j(a_0, \ldots, a_n)$, $j = 0, \ldots, m$, are not all zero, and

$$\phi(Q) = \big(G_0(a_0, \ldots, a_n) : \cdots : G_m(a_0, \ldots, a_n)\big).$$

A bijection $\phi : X \to Y$ is an *isomorphism* if both ϕ and ϕ^{-1} are regular.

A smooth projective curve $C \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ is said to be *defined over* $\mathbb{F}_q$ if it can be cut out by homogeneous equations with coefficients in $\mathbb{F}_q$. Two smooth projective curves defined over $\mathbb{F}_q$ are *geometrically isomorphic* if they are isomorphic over $\overline{\mathbb{F}}_q$.

Now let C be a smooth projective curve defined over $\mathbb{F}_q$. For each integer $n \geq 1$, let $\mathbb{F}_{q^n}$ denote the field with q^n elements, and let $N_n(C)$ be the number of points of C whose homogeneous coordinates may be chosen in $\mathbb{F}_{q^n}$. The *zeta function* of C is the formal power series

$$Z(C, T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n(C)}{n} T^n\right).$$

Weil proved that there is a unique polynomial $P_C(T) \in \mathbb{Z}[T]$ such that

$$Z(C, T) = \frac{P_C(T)}{(1 - T)(1 - qT)}.$$

The degree of $P_C(T)$ is even, and the *genus* of C is defined by

$$g(C) := \frac{1}{2} \deg P_C(T).$$

For a fixed integer $g \geq 0$, let $N_g(q)$ denote the number of geometric isomorphism classes of smooth projective curves C defined over $\mathbb{F}_q$ with $g(C) = g$. It is known that

$$N_0(q) = 1, \qquad N_1(q) = q, \qquad N_2(q) = q^3,$$

$$N_3(q) = q^6 + q^5 + 1, \qquad N_4(q) = q^9 + q^8 + q^7 - q^6.$$

These examples suggest a natural question: for which genera is $N_g(q)$ always given by a polynomial in q? We say that N_g is *polynomial* if there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that

$$N_g(q) = f(q)$$

for every prime power q.

In 2024, Canning, Larson, Payne, and Willwacher posted the preprint (Canning et al. 2024), proving the following theorem.

Theorem 1 *For every integer $g \geq 0$, the function N_g is polynomial if and only if $g \leq 8$.*

Thus $g = 8$ is precisely the largest genus for which the number of smooth projective curves over $\mathbb{F}_q$, up to geometric isomorphism, is given by a single polynomial in q for all finite fields.

References

Canning, Samir, Hannah Larson, Sam Payne, and Thomas Willwacher. 2024. "Moduli Spaces of Curves with Polynomial Point Counts." *arXiv Preprint arXiv:2410.19913*.