Thinking Positive: Arithmetic Geometry in Characteristic p

Renee Bell, Julia Hartmann, Valentijn Karemaker, Padmavathi Srinivasan, and Isabel Vogt

Arithmetic geometry arose as a beautiful and powerful theory unifying geometry and number theory, formalizing striking analogies between them in a way that allowed tools, results, and intuition of each to be transported to the other—a notable example of this is the proof of the centuries-old problem, Fermat's Last Theorem. This theory provides a geometric viewpoint of objects over fields of prime characteristic p, like finite fields. Decades after these ideas were formalized, characteristic p arithmetic geometry is rapidly expanding to include work in the vibrant young fields of arithmetic dynamics and derived algebraic geometry.

Fields of positive characteristic p have a fundamentally distinct flavor from the classical setting of fields of characteristic 0. In addition, having to let go of the archimedean framework requires a radically different geometric intuition. Working in characteristic p therefore comes with additional challenges, but there are also additional tools and structure that can be exploited, which have led to remarkable results. In some instances these results even carry over to solve open problems in characteristic 0.

Historical overview. While number theorists had been studying the rational numbers and other number fields using the Riemann and Dedekind zeta functions, E. Artin in his 1921 thesis [1] first proposed an analogous theory of zeta functions for curves over finite fields. Hasse extended this to prove the Riemann hypothesis for elliptic curves over finite fields. Their work further sparked the development of the theory of function fields, as well as the theory of algebraic varieties, by several mathematicians, including Weil. In the 1940's, Weil published a book [11] on the foundations of algebraic geometry in characteristic p, and subsequently proved the Riemann hypothesis for function fields over finite fields [12]. Moreover, in 1949, Weil proposed conjectures on the behavior of zeta functions of varieties over finite fields—including the Riemann hypothesis—which came to be known as the Weil conjectures [13]. The breakthrough which enabled Grothendieck,

Renee Bell is a Hans Rademacher Instructor at the University of Pennsylvania. Her email address is rhbell@math.upenn.edu.

Julia Hartmann is a professor at the University of Pennsylvania. Her email address is hartmann@math.upenn.edu.

Valentijn Karemaker is a postdoctoral research fellow at the University of Pennsylvania. Her email address is vkarem@math.upenn.edu.

Padmavathi Srinivasan is a Hale Visiting Assistant Professor at the Georgia Institute of Technology. Her email address is padmavathi.srinivasan @math.gatech.edu.

Isabel Vogt is a Massachusetts Institute of Technology graduate student currently visiting Stanford University. Her email address is ivogt@mit.edu.

M. Artin, and Verdier to prove all but one of the Weil conjectures in 1964 [5] was their development of ℓ-adic cohomology. Building on this, the Riemann hypothesis was eventually proven in two different ways by Deligne ([3, 1974], [4, 1980]). For more historical details, see e.g. [8].

Weil conjectures and counting points. The zeta function $Z_X(T)$ of an algebraic variety X over $\mathbb{F}_q$ encompasses information about point counts over all finite extensions of $\mathbb{F}_q$:

$$Z_X(T) = \exp\left(\sum_{n\geq 0} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right).$$

The Weil conjectures predict that the power series $Z_X(T)$ is a rational function, whose zeros and poles can be described in terms of natural group actions on the associated étale cohomology groups. For example, when $X = \mathbb{P}^1_{\mathbb{F}_q}$, direct calculation gives $\#\mathbb{P}^1(\mathbb{F}_{q^n}) = q^n + 1$, and

$$Z_{\mathbb{P}^1}(T) = \frac{1}{(1 - qT)(1 - T)}.$$

In 1954 Lang and Weil [7] proved a weaker version of the Weil Conjectures: if X has d irreducible components of maximal dimension r, then

$$\#X(\mathbb{F}_{q^n}) \sim d(q^n)^r + O(q^{r-1/2}),$$

as n goes to infinity. These Lang–Weil estimates are useful in both directions: information either about point counts or about the parameters r and d can be traded for the other. This technique is particularly striking in combination with the technique of spreading out from characteristic 0 to characteristic p: counting points on a specialization to characteristic p can give information about dimension and irreducibility in characteristic 0!

This idea was used in recent work of Browning–Vishe [2], building on an idea of Ellenberg–Venkatesh, to show that certain spaces parameterizing rational curves on hypersurfaces over $\mathbb{C}$ are irreducible of the expected dimension. This is a beautiful illustration of the synergy between characteristic 0 and characteristic p algebraic geometry.

Characteristic p phenomena.

Example 1: Elliptic curves of unbounded rank. Another notable application of these modern tools is an explicit example, due to Ulmer [10], of a family of elliptic curves of unbounded rank defined over a function field over a finite field. The construction makes clever use of the known cases of the Tate conjecture [9] over finite fields. The existence of such a family of elliptic curves over number fields is a topic of heated debate amongst number theorists today! Numerous heuristics have been developed about the behavior of ranks and other fundamental invariants of elliptic curves.

Example 2: Automorphisms. A broad theme in mathematics is that one should study the symmetries (i.e. automorphisms) of an object alongside the object itself. In the simplest case of an algebraic curve over $\mathbb{C}$, the automorphism group varies by the topological type: it is infinite for curves of genus $g = 0$ or 1, but once $g \geq 2$, Hurwitz famously proved that its order is at most $84(g - 1)$. In characteristic p, an algebraic curve could have additional symmetries! For example, the projective plane curve $x^{p+1} + yz^p + zy^p$ over $\mathbb{F}_{p^2}$ has genus $p(p - 1)/2$, but $O(p^8)$ symmetries. These symmetries arise in analogy with the fact that the unitary group $\text{PGU}_3(\mathbb{C})$ preserves the Hermitian form $Q(x, y, z) = x\bar{x} + y\bar{z} + z\bar{y}$, and so acts on $Q = 0$. Replacing complex conjugation with the Frobenius involution $x \mapsto \bar{x} = x^p$ (special to characteristic p) of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$ gives rise to an action of $\text{PGU}_3(\mathbb{F}_{p^2})$ on this curve.

Example 3: Fundamental groups. An important objective of mathematics is to classify spaces; a natural approach to this is introducing and comparing algebraic invariants associated to a space. One important example of such an invariant is the fundamental group, which captures information about the geometry of a space and its maps to other spaces. For a variety X over $\mathbb{C}$, the topological fundamental group $\pi_1(X)$ has a description in terms of loops on X. In particular, the line $\mathbb{A}^1_{\mathbb{C}}$ has trivial π_1, since it's contractible. Using an equivalent description of π_1, this says that $\mathbb{A}^1_{\mathbb{C}}$ has no nontrivial unramified covers. The same is true when we replace $\mathbb{C}$ with any other characteristic 0 field. In characteristic p, the theory of étale covers gives a direct analog $\pi_1^{\text{ét}}$ of the topological fundamental group. Grothendieck proved that the prime-to-p part of $\pi_1^{\text{ét}}$ is the same as that of π_1 of an analogous curve over $\mathbb{C}$ [6]. However, the p-part of $\pi_1^{\text{ét}}$ detects that the theory of covers is much richer in this setting. For example, over a characteristic p ground field, $\pi_1^{\text{ét}}(\mathbb{A}^1)$ is far from trivial; in fact, its cardinality is huge and depends on the ground field. It is even conjectured that $\pi_1^{\text{ét}}(\mathbb{A}^1_k)$ determines the ground field when k is algebraically closed.

Mathematics research communities. Arithmetic geometry in characteristic p lends itself to a rich and varied collection of accessible problems, in topics such as isogeny classes of abelian varieties over finite fields, Galois covers of curves and lifting problems, and arithmetic dynamics. Many of these problems are existential, and can be attacked by an explicit or computational approach. Significant progress in this setting has been made in the last year alone, due to both recent theoretical technical innovations

and to recent computational advances that have aided experimentation. Relatedly, there are new approaches to explicitly constructing examples exhibiting certain phenomena.

We invite early-career mathematicians from a wide range of backgrounds to continue this story at our upcoming MRC, "Explicit Methods in Arithmetic Geometry in Characteristic p."

Renee Bell

Julia Hartmann

References

[1] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I, II. *Math. Z.*, 19(1):153–246, 1924.

[2] Tim Browning and Pankaj Vishe. Rational curves on smooth hypersurfaces of low degree. *Algebra Number Theory*, 11(7):1657–1675, 2017.

[3] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[4] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[5] Alexander Grothendieck. Formule de Lefschetz et rationalité des fonctions L. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris, 1995.

[6] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. I, II*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[7] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[8] Peter Roquette. The Riemann Hypothesis in Characteristic p in Historical Perspective. *available at* `https://www.mathi.uni-heidelberg.de/~roquette/2017rv_with_pictures.pdf`, 2018.

[9] John Tate. Conjectures on algebraic cycles in l-adic cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 71–83. Amer. Math. Soc., Providence, RI, 1994.

[10] Douglas Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002.

[11] André Weil. *Foundations of Algebraic Geometry*. American Mathematical Society Colloquium Publications, vol. 29. American Mathematical Society, New York, 1946.

[12] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.

[13] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

Valentijn Karemaker Padmavathi Srinivasan

Isabel Vogt

Credits