The Mathematical Contributions of Serge Lang

Jay Jorgenson and Steven G. Krantz

This article is the second in a two-part series in memory of Serge Lang, who passed away on September 12, 2005. In the first article, which appeared in the May 2006 issue of the *Notices*, we invited contributions from a number of individuals who knew Serge on a somewhat personal level. For this part, we sought expositions which would describe, with certain technical details as necessary, aspects of Serge's contribution to mathematical research.

To begin understanding the breadth and depth of Serge's research endeavors, we refer to Volume I of his *Collected Papers*,[1] where he outlined his mathematical career in a number of periods. We list here Lang's own description of his research, using only a slight paraphrasing of what he wrote (see table at top of next page). For this article, the editors choose to use this list as a guide, though it should be obvious that we cannot address all facets of Lang's mathematical research.

In addition to research, Lang's contribution to mathematics includes, as we all know, a large number of books. How many books did Lang write? We (the editors) are not sure how to answer that question. Should we count political monographs such as *Challenges*? How do we count multiple editions and revisions? For example, he wrote two books, entitled *Cyclotomic Fields I* and *Cyclotomic Fields II*, which were later revised and published in a single volume, yet his text *Algebra: Revised Third Edition* has grown to more than 900 pages and is vastly different from the original version. In an attempt to determine how many books he wrote, we consulted the bibliography from Lang's *Collected Papers*, where he highlighted the entries which he considered to be a book or lecture note. According to that list, Lang wrote an astonishing number of books and lecture notes—namely sixty—as of 1999. Furthermore, he published several items after 1999, there are more books in production at this time, and a few unfinished manuscripts exist. In 1999, when Lang received the Leroy P. Steele Prize for Mathematical Exposition, the citation stated that "perhaps no other author has done as much for mathematical exposition at the graduate and research levels, both through timely expositions of developing research topics ... and through texts with an excellent selection of topics." We will leave it to others to assess the impact of Serge Lang's books on the education of mathematics students and mathematicians throughout the world; this topic seems to be a point of discussion properly addressed by historians as well as by history itself.

On February 17, 2006, a memorial event was held at Yale University in honor of Serge Lang. At that time, Anthony and Cynthia Petrello, friends of Serge since the early 1970s, announced their intention to create a fund for the purpose of financing mathematical activities in memory of Lang. As mathematicians, we the editors express our sincere thanks to Anthony and Cynthia Petrello for

Jay Jorgenson is a professor of mathematics at City College of New York and the Graduate Center. His email address is jjorgenson@mindspring.com.

Steven G. Krantz is deputy director of the American Institute of Mathematics. His email address is skrantz@aimath.org.

Based on mathematical contributions from: Alexandru Buium, Jay Jorgenson, Minhyong Kim, David E. Rohrlich, John Tate, Paul Vojta, and Michel Waldschmidt.

[1] Serge Lang: Collected Papers. Vols. I–V, *Springer-Verlag, New York, 2000.*

1.	1951–1954	Thesis on quasi-algebraic closure and related matters
2.	1954–1962	Algebraic geometry and abelian (or group) varieties; geometric class field theory
3.	1963–1975	Transcendental numbers and Diophantine approximation on algebraic groups
4.	1970	First paper on analytic number theory
5.	1975	$SL_2(\mathbf{R})$
6.	1972–1977	Frobenius distributions
7.	1973–1981	Modular curves, modular units
8.	1974, 1982–1991	Diophantine geometry, complex hyperbolic spaces, and Nevanlinna theory
9.	1985, 1988	Riemann-Roch and Arakelov theory
10.	1992–2000+	Analytic number theory and connections with spectral analysis, heat kernel, differential geometry, Lie groups, and symmetric spaces

Chronological description of Serge Lang's mathematics career.

their generous support of mathematical research. As teachers, we see the story of Serge, Anthony, and Cynthia as a wonderful example of the type of lifelong friendship that can develop between instructors and students. As editors of the two articles on Lang, we are in awe at being shown yet another way in which Serge has influenced the people he encountered. We look forward to seeing the results from the development of the "Lang Fund" and its impact on the mathematical community.

Serge Lang's Early Years

John Tate

These remarks are taken from my talk at the Lang Memorial at Yale on Lang and his work in the early years, roughly 1950–1960. Lang's papers from this period fill less than one half of the first of the five volumes of his collected works. His productivity was remarkably constant for more than fifty years, but my interaction with him was mostly early on. We were together at Princeton as graduate students and postdocs from 1947 to 1953 and in Paris during 1957–58.

In the forward of his *Collected Papers*, Lang takes the opportunity to "express once more" his appreciation for having been Emil Artin's student, saying "I could not have had a better start in my mathematical life." His Ph.D. thesis was on quasi-algebraic closure and its generalizations. He called a field k a C_i field if for every integer $d > 0$, every homogeneous polynomial of degree d in more than d^i variables with coefficients in k has a nontrivial zero in k. A field is C_0 if and only if it is algebraically closed. Artin's realization that Tsen's proof (1933) that the Brauer group of a function field in one variable over an algebraically closed constant field is trivial was achieved by showing that such a field is C_1, and he called that property quasi-algebraic closure. In analogy with Tsen's theorem, he conjectured that the field of all roots of unity is C_1. This is still an open question. In his thesis Lang proved various properties of C_i fields and showed that a function field in j variables over a C_i field is C_{i+j}. He also proved that the maximal unramified extension of a local field with perfect residue field is C_1. Artin had also conjectured that a local field with finite residue field is C_2. Lang could prove this for power series fields, but not for p-adic fields. In 1966 it became clear why he failed. G. Terjanian produced an example of a quartic form in 18 variables over the field $\mathbf{Q}_2$ of 2-adic numbers with no zero. Terjanian found his example a few months after giving a talk in the Bourbaki Seminar (November 1965) on a remarkable theorem of Ax and Kochen. Call a field $C_i(d)$ if the defining property of C_i above holds for forms of degree d. Using ultrafilters to relate $\prod_p \mathbf{Q}_p$ to $\prod_p \mathbf{F}_p((t))$, they showed that for each prime p, $\mathbf{Q}_p$ has property $C_2(d)$ for all but a finite set of d. In that sense, Artin was almost right.

Lang got his Ph.D. in 1951. After that he was a postdoc at Princeton for a year and then spent a year at the Institute for Advanced Study before going to Chicago, where he was mentored by Weil—if anyone could mentor Serge after his Ph.D. He and Weil wrote a joint paper generalizing Weil's theorem on the number of points on a curve over a finite field. They show that the number N of rational points on a projective variety in $\mathbb{P}^n$ of dimension r and degree d defined over a finite field satisfies

$$|N - q^r| \le (d-1)(d-2)q^{r-\frac{1}{2}} + Aq^{r-1},$$

where q is the number of elements in the finite field and A is a constant depending only on n, d, and r. (Here and in the following, "variety defined over k" means essentially the same thing as a geometrically irreducible k-variety.) From this result

John Tate is a professor of mathematics at the University of Texas at Austin. His email address is `tate@math.utexas.edu`.

they derive corollaries for arbitrary abstract varieties. They show, for example, that a variety over a finite field has a rational zero-cycle of degree 1. The paper is a very small step towards Weil's conjectures on the number of points of varieties over finite fields which were proved by Deligne.

Lang proved for abelian varieties in 1955 and soon after for arbitrary group varieties that over a finite field k a homogeneous space for such a variety has a k-rational point. A consequence is that for a variety V over k, a "canonical map" $\alpha : V \to \mathrm{Alb}(V)$ of V into its Albanese variety can be defined over k and is then unique up to translation by a k-rational point on $\mathrm{Alb}(V)$.

In 1955 Lang dedicated to Artin a paper in which he generalized Artin's reciprocity law to most unramified abelian extensions (those "of Albanese type") of a function field K of arbitrary dimension over a finite constant field k. Let V/k be a projective normal model for K/k. For each finite separable extension L/K, let V_L be the normalization of V in L; and let Z_L denote the group of 0-cycles on V_L rational over the constant field k_L of L, Z_L^0 those of degree 0, and Z_L^a the kernel of the canonical map of Z_L^0 into $A_L(k_L)$, the group of k_L-rational points on the Albanese variety A_L of V_L. Let $C_L := Z_L/Z_L^a$ denote the group of classes of 0-cycles on V_L defined over k_L. Lang calls L/K "of Albanese type" if its "geometric part" $L\bar{k}/K\bar{k}$ is obtained by pullback, via a canonical map $\alpha : V = V_K \to A_K$, from a separable isogeny $B \to A_K$ defined over the algebraic closure $\bar{k}$ of k. Such an extension is abelian if the isogeny and α are defined over k and the kernel of the isogeny consists of k-rational points. If the Neron-Severi group of V is torsion free, then every finite abelian extension of degree prime to the characteristic is of Albanese type. Lang shows that the map which associates to an extension L/K its trace group $S_K^L C_L$ gives a one-one correspondence between the set of abelian extensions L/K of Albanese type and the set of subgroups of finite index in C_K. He also shows, in exact analogy with Artin's reciprocity law, that the homomorphism $Z_K \to \mathrm{Gal}(L/K)$ which takes each prime rational 0-cycle P to its associated Frobenius automorphism $(P, L/K)$ vanishes on the Albanese kernel Z_K^a and induces an isomorphism $C_K/S_K^L C_L \approx \mathrm{Gal}(L/K)$. Moreover, from Lang's geometric point of view, this reciprocity law becomes transparent and quite easy to prove.

A year later, in his first paper written in French, Lang defined the analogue of Artin's nonabelian L-functions for Galois coverings $f : W \to V$ and proved with them the analogue of Tchebotarov's density theorem. He also generalized his reciprocity law for abelian coverings $W \to V$ of Albanese type described above to any covering obtained by pullback of a separable isogeny $B \to A$ of commutative group varieties, via a map $\alpha : V \to A$ defined outside a divisor. These coverings, which he calls "de type (α, A)" can be highly ramified, and Lang notes that in the case where V is a curve, taking Rosenlicht's generalized Jacobians for A and throwing in constant field extensions, one gets all abelian coverings, so that his theory recovers the classical class field theory over global function fields.

These papers were the beginning of higher-dimensional class field theory and earned Lang a Cole Prize in 1959. In his acceptance remarks, he acknowledges his indebtedness to others. In his paper on unramified class field theory, he expresses his great and sincere appreciation to Chow, Matsusaka, and Weil for discussions on the algebraic aspects of the Picard and Albanese varieties and for proving the theorems he needed for the work. (In the L-series paper he also thanks Serre, writing "Je ne voudrais pas terminer cette introduction sans exprimer ma reconnaissance à J.-P. Serre, qui a bien voulu se charger de la corection des phautes d'orthografe." I too thank Serre here for pointing out an error in my first description of these results of Lang.)

During the next couple of years Lang collaborated with many people. In a paper "Sur les revêtements non ramifiés" he and Serre proved that coverings in characteristic p behave more or less as in characteristic 0, provided the variety is projective, and applied this to abelian varieties in order to show that every covering is given by an isogeny. After a paper with Chow on the birational invariance of good reduction, Lang collaborated with me on a study of the Galois cohomology of abelian varieties. We were able to show, for each positive integer m, the existence of a curve of genus 1 over a suitable algebraic number field K, the degrees of whose divisors defined over K are exactly the multiples of m. Over a p-adic field F we essentially proved the prime-to-p part of the duality theorem

$$\mathrm{Hom}(H^1(\mathrm{Gal}(\bar{F}/F), A(\bar{F})), \mathbf{Q}/\mathbf{Z}) = \hat{A}(F)$$

for dual abelian varieties A and $\hat{A}$ without stating it that way.

Then, after a paper with Kolchin applying the theory of torsors for algebraic groups to the Galois theory of differential fields, Lang published with Néron a definitive account of the "theorem of the base": the finite generation of the Néron-Severi group of divisors modulo algebraic equivalence on a variety. Néron had proved this earlier, but here the proof is made more transparent. Using a criterion of Weil, they show that the theorem follows from the Mordell-Weil theorem for abelian varieties over function fields, which they prove in the usual way.

I view this as the end of Lang's first period of research, in which he applied Weil's algebraic geometry to class field theory and to questions of rational points on varieties with great success. At this time (around 1960) he began to consider questions of integral points on curves and varieties and function field analogues of the Thue-Siegel-Roth theorem on Diophantine approximations, a new direction in which his ideas of generalization and unification of classical results had great influence.

In addition to doing outstanding research, Lang has had a tremendous influence as a communicator, teacher, and writer, as everyone knows. In closing I would like to mention a few examples of these things from the period I am writing about. Wonderful as it was, our graduate training with Artin was almost totally one-dimensional and nongeometric: number fields and function fields in one variable. In the following years Serge helped me become comfortable with higher-dimensional things such as the Jacobian, Picard and Albanese varieties over arbitrary ground fields and also with "reduction mod $\mathfrak{p}$", which was not such a simple matter working with Weil's *Foundations* in those days before schemes. Serre tells me it was Lang who made him appreciate the importance of the Frobenius automorphism. In general, Serge, who travelled regularly to Paris, Bonn, Moscow, and Berkeley, was an excellent source of information about what was happening in the world of mathematics. He was an energetic communicator who seemed driven to publish. The Artin-Tate book on class field theory is a good example. Lang took the original notes of the seminar, typed them, continued for years to urge their publication (over my perfectionist and unrealistic objections), and finally arranged for their publication by Addison-Wesley. His name should be on the cover.

Serge Lang's Early Work on Diophantine and Algebraic Geometry

Alexandru Buium

In this article we review some of Serge Lang's early work on Diophantine equations and algebraic geometry. We are mainly concerned here with papers written before the 1970s (roughly the first volume of his *Collected Papers* [44]).

Diophantine equations are polynomial equations $f(x_1, ..., x_n) = 0$ with rational coefficients or, more generally, with coefficients in fields K that have an "arithmetic flavor" (e.g., number fields, function fields, local fields, finite fields, etc.). The main problem is to determine whether such an equation has solutions with coordinates in K and, more generally, to "count" or "construct" all such solutions. Morally, one expects "many" solutions if the degree d of f is "small" with respect to the number n of variables, and one expects "few" solutions if d is "big" with respect to n. In the language of algebraic geometry, systems of polynomial equations correspond to varieties (or schemes) V over K, and solutions correspond to K-points $P \in V(K)$ of our varieties. According to conjectures made by Lang in the 1980s, the above conditions on d and n, controlling the size of the set of solutions to $f = 0$, should be replaced by precise algebro-geometric and complex analytic properties of the varieties in question.

Most of Lang's early work stems from his interest in Diophantine equations. In his thesis [22] Lang obtained remarkable new results on polynomial equations of low degree over local fields and function fields. Diophantine equations naturally led Lang [23] to the study of algebraic groups and their homogeneous spaces. Closely related to these are Lang's class field theory of function fields of characteristic p [24] and his work with Néron [29] on the Mordell-Weil theorem over function fields of any characteristic. From the latter Lang passed to his investigation, in the line of Mordell and Siegel, of finiteness of integral points [30] and division points [31] on curves. In [30] [31], he formulated his celebrated conjecture on *subvarieties of semiabelian varieties*. (Later [41], [42], [43] Lang came back to this circle of ideas by formulating his Diophantine conjectures for *arbitrary varieties*; we will not review this aspect of Lang's later work here.) Problems on integral points are intertwined with problems in the theory of Diophantine approximation, while the latter shares its spirit and methods with transcendence theory; in both these theories Lang made important contributions [32], [33], [34], [38], [39], [40], [5].

These are but a few of the themes that Lang pursued in his early work. Lang's impact on these themes was substantial. Not only did he contribute fundamental results, but, at the same time, he reorganized and systematized each of these subjects by attempting to clearly define their scope, formulate their basic problems, and make sweeping conjectures. In what follows we will review these themes in some detail.

Equations of Small Degree over Local Fields

E. Artin defined quasi-algebraically closed fields (in Lang's terminology, C_1 fields [22]) as fields K such that any form of degree d in n variables with $n > d$ and coefficients in K has a nontrivial

Alexandru Buium is a professor of mathematics at the University of New Mexico. His email address is buium@math.unm.edu.

zero in K. He noted that a method of Tsen [60] implies that function fields of one variable over an algebraically closed field are C_1 and conjectured that finite fields are C_1; this was proved by Chevalley [9]. Artin also conjectured that certain "local fields", such as $\mathbf{Q}_p^{ur}$ (the maximum unramified extension of the p-adic field), are C_1. This conjecture was proved by Lang in his thesis [22]; here is his strategy. Lang first uses Witt coordinates to transform the equation $f = 0$ with coefficients in $K = \mathbf{Q}_p^{ur}$ into an infinite system of equations $f_0 = f_1 = f_2 = \cdots = 0$ in infinitely many variables with coefficients in the algebraic closure k of the prime field $\mathbf{F}_p$. He is able to solve this infinite system in an algebraically closed extension k_1 of k by purely algebro-geometric considerations; here the hypothesis on the degree d is used to control the dimensions of the algebraic sets defined by various truncations of the infinite system. From the solution of the system in k_1 he gets a solution of $f = 0$ in K_1, a complete field with residue field k_1. Next he specializes this solution to a solution in $\hat{K}$, the completion of K. Finally, from a solution in $\hat{K}$ he gets solutions in K itself via a beautiful argument involving a variant of "Newton approximation". The proof outlined above contained a number of fruitful new ideas that provided starting points for further developments by other mathematicians. The step involving "Newton approximation" is one of the origins of M. Artin's work on approximating formal solutions to algebraic equations [4], which was crucial in his work on moduli. The viewpoint whereby equations over $\hat{K}$ can be transformed into infinite systems of equations over k was put into a general context by M. Greenberg [19] and has been intensely used ever since; in particular, it plays a role in Raynaud's work [54], [55] on Lang's conjecture [31] on division points; cf. the discussion below.

Points on Homogeneous Spaces over Finite Fields

In [23] Lang proves his celebrated theorem that if $\mathbf{F}_q$ is a finite field, then any homogeneous space $H/\mathbf{F}_q$ for an algebraic group $G/\mathbf{F}_q$ has an $\mathbf{F}_q$-point. The proof is beautifully simple and runs as follows: Let $G(k) \to G(k)$, $x \mapsto x^{(q)}$ be the q-power Frobenius map on k-points where k is the algebraic closure of $\mathbf{F}_q$. Then Lang proves that the map $G(k) \to G(k)$, $x \mapsto x^{-1}x^{(q)}$ is surjective. He then takes any point $y_0 \in H(k)$. By transitivity of the G-action there is a point $x_0 \in G(k)$ such that $x_0 y_0^{(q)} = y_0$. By surjectivity of $x \mapsto x^{-1}x^{(q)}$ there is a point $x_1 \in G(k)$ such that $x_0 = x_1^{-1}x_1^{(q)}$. Then $x_1^{-1}x_1^{(q)}y_0^{(q)} = y_0$; hence $(x_1 y_0)^{(q)} = x_1 y_0$, so one finds the desired point $x_1 y_0 \in H(\mathbf{F}_q)$. Lang's theorem generalizes a result of F. K. Schmidt about elliptic curves and also generalizes a result of Châtelet, who had proved that if a variety over $\mathbf{F}_q$ becomes isomorphic over the algebraic closure of $\mathbf{F}_q$ to a projective space $\mathbf{P}^n$, then the variety is already isomorphic over $\mathbf{F}_q$ to $\mathbf{P}^n$.

In [24], [25], [23] Lang uses the map $x \mapsto x^{-1}x^{(q)}$ as a key ingredient in his class field theory for function fields over finite fields (equivalently for coverings of varieties over finite fields). He shows that abelian coverings are essentially induced by appropriate isogenies of commutative algebraic groups (of which $x \mapsto x^{-1}x^{(q)}$ is a basic example), and he introduces his reciprocity mapping, which turns out to have the expected properties. It is interesting to note that this function field theory was developed (long) after E. Artin's work in the 1920s [3] on its number field prototype; usually, in the history of number theory, the number field theorems are being proved *after* their function field analogues. (Cf. the discussion of the Mordell conjecture below.) In the case at hand, the function field analogue had to wait until the necessary algebro-geometric tools (especially the algebraic theory of abelian varieties) became available.

Finite Generation of Points of Abelian Varieties over Function Fields

Lang was actively involved [26], [27], [28] in establishing the foundations of the algebraic theory of abelian varieties, following the pioneering work of Weil, Chow, and Matsusaka. With this theory at hand, Lang and Néron [29] were able to provide elegant proofs for some basic finiteness theorems in algebraic geometry. Néron had proved [50] the "Néron-Severi" theorem of the base stating that the group $D(V)$ of divisors on a variety V (over an algebraically closed field k) modulo the group $D_a(V)$ of divisors algebraically equivalent to 0 is finitely generated. In [29] Lang and Néron show how to reduce the proof of the finite generation of $D(V)/D_a(V)$ to proving the finite generation of a group of the form $A(K)/\tau B(k)$, where A is an abelian variety over a function field K over k and (B, τ) is the K/k-trace of A. Then they prove the finite generation of $A(K)/\tau B(k)$, which is the "Mordell-Weil" theorem in the function field context. Recall that the number field version of the Mordell-Weil theorem asserts that for any abelian variety A over a number field K, the group $A(K)$ is finitely generated. The latter was conjectured by Poincaré and proved by Mordell [48] in case $\dim A = 1$, $K = \mathbf{Q}$, and by Weil [66] in general. Here again, the number field theorem preceded the function field theorem.

Integral Points, Rational Points, and Division Points

Lang became interested in questions related to the Mordell conjecture around 1960; this conjecture and the impact of Lang's insights into it have a long history. We briefly sketch the evolution of this circle of ideas below; our discussion is inherently incomplete and is meant to give only a hint as to the role of some of Lang's early ideas on the subject. Mordell [48] had conjectured that a nonsingular projective curve V of genus $g \geq 2$ over a number field K has only finitely many points in K. In particular, an equation $f = 0$ where f is a nonsingular homogeneous polynomial of degree ≥ 4 in 3 variables with $\mathbf{Q}$-coefficients should have, up to scaling, only finitely many solutions in $\mathbf{Q}$. Siegel [58] proved, using Diophantine approximations, that if V is an affine curve over a number field K, of genus $g \geq 1$, then V has only finitely many integral points (i.e. points with coordinates in the ring of integers of K). Mahler [45] conjectured that the same holds for S-integral points (S a finite set of places), and he proved this for $g = 1$ and $K = \mathbf{Q}$. In [30] Lang proves Mahler's conjecture by revisiting the arguments of Siegel and Mahler in the light of the new developments in Diophantine approximations (Roth's Theorem) and abelian varieties (especially the Lang-Néron paper [29]). Lang also makes, in [30], a conjecture which later, in [31], he strengthens to what came to be known as the *Lang conjecture* (on subvarieties of semiabelian varieties):

(*) *Let G be a semiabelian variety over an algebraically closed field F of characteristic 0, let $V \subset G$ be a subvariety, and let $\Gamma \subset G$ be a finite rank subgroup. Then V contains finitely many translates X_i of algebraic subgroups of G such that $V(F) \cap \Gamma \subset \cup_i X_i(F)$.*

Here, by Γ of finite rank, one understands that $\dim_{\mathbf{Q}} \Gamma \otimes \mathbf{Q} < \infty$. The weaker version of Conjecture (*) stated in [30] only assumes Γ is finitely generated; this is a reformulation and generalization of a conjecture of Chabauty [8]. A proof in case V is a curve, G is a linear torus, and Γ is finitely generated is given by Lang in [36] using Diophantine approximations. Lang remarks in [30] that Conjecture (*) (for Γ finitely generated) implies the Mordell conjecture; indeed if V is a curve of genus ≥ 2 defined over a number field K, then one lets F be the algebraic closure of K, embeds V into its Jacobian A, and notes that $V(K) = A(K) \cap V(F)$. But $A(K)$ is finitely generated by the Mordell-Weil Theorem, so $V(K)$ is finite and the Mordell conjecture follows. In a similar vein, Lang conjectures in [30] that if V is a nonsingular projective curve over a function field K of characteristic zero such that $V(K)$ is infinite, then V can be defined over the constants of K; this is the *Mordell conjecture over function fields of characteristic zero.* Lang proves in [30] that a curve as in the latter conjecture cannot have infinitely many points of bounded height; this implies an analogue of Siegel's Theorem [58] for curves over function fields of characteristic zero. In the same paper [30] Lang conjectures that

(**) *If V is an affine open set of an abelian variety over a number field K and S is a finite set of places of K, then the set of S-integral places of V is finite.*

The Mordell conjecture for curves over function fields of characteristic zero was proved by Manin [46]. Subsequently other proofs and new insights were provided [18], [56], [51], [2], [59], [12], etc. In Manin's work the question arose whether a curve, embedded into its Jacobian, contains only finitely many torsion points. This was independently asked by Mumford and came to be known as the *Manin-Mumford conjecture.* In [31] Lang stated Conjecture (*) so as to make the Mordell conjecture and the Manin-Mumford conjecture special cases of one and the same conjecture. The Manin-Mumford conjecture was proved by Raynaud [54], and in the same year Faltings [13] proved the original Mordell conjecture. Faltings's proof did not involve Diophantine approximations; later Vojta [61] provided a completely different proof of the Mordell conjecture involving Diophantine approximations. This led to another breakthrough by Faltings [14] in the higher-dimensional case, followed by more work of Vojta [62]. The full Lang conjecture (*) was subsequently proved by McQuillan [47], based partly on ideas of Hindry [20] and Raynaud about how to reduce the case "Γ of finite rank" to the case "Γ finitely generated". For curves over function fields in characteristic p, a remarkably short proof of a variant of the Lang conjecture (*) was given by Voloch [63]; cf. also [1]. Conjecture (**) was proved by Faltings [14]; function field analogues of Conjecture (**) were proved in [52], [7], [64].

We would like to close this discussion by noting that the Lang conjecture (*) is a purely algebro-geometric statement, i.e., a statement about varieties over an algebraically closed field F, and one could expect a purely algebro-geometric proof of this conjecture (in which the arithmetic of a global field of definition contained in F doesn't play any role). Implicit in Lang's viewpoint was that the Mordell conjecture could be attacked via the Lang conjecture (*); the whole arithmetic in the proof could then be concentrated into the Mordell-Weil Theorem. The decisive breakthroughs in the subject (by Manin and Faltings) went the other way around: the Mordell conjecture was proved directly (and then the Lang conjecture (*) followed by work of Raynaud, Hindry, McQuillan). A proof along Lang's original plan of attack was given by the author in [6], where the Lang conjecture (*), in the case A has no quotient defined over a number field and V is nonsingular, was proved "without global field arithmetic"; no such proof is known for A defined over a number field. The proof in [6] had a key complex analytic ingredient; Hrushovski [21] saw how to replace this ingredient by an argument from mathematical logic (model theory) which also applied to function fields in characteristic p. In characteristic zero, Hrushovski's model theoretic argument can be rephrased, in its turn, as an entirely algebro-geometric argument [53].

Diophantine Approximations and Transcendence

A surprising discovery of Lang's [32] was that if β is a quadratic real irrational number and $c \geq 1$, then the number of integers q with $|q| \leq B$ such that $0 < q\beta - p < c|q|^{-1}$ for some integer p is a multiple of $\log B + O(1)$. This was in sharp contrast with the known fact that for c sufficiently small the inequality $|q\beta - p| < c/q$ has only finitely many solutions. Lang further explored asymptotic approximations in [33], [35], [34]. As already mentioned, Diophantine approximations are closely related to Lang's conjecture on intersections of subvarieties of algebraic groups with finitely generated subgroups. Partially motivated by this circle of ideas, Lang conjectured [37] strong inequalities for heights of points in algebraic groups; these conjectures roughly replaced heights in inequalities following from work of Mahler, Siegel, and Roth by logarithmic heights. The subject of Diophantine approximations evolved spectacularly after the 1970s, mainly due to breakthroughs by Baker, Bertrand, Bombieri, Brownawell, Faltings, Feldman, Lang, Masser, Nesterenko, Philippon, Roy, Schmidt, Vojta, Waldschmidt, Wüstholz, and many others. In particular, the following conjecture of Lang was recently proven by David and Hirata-Kohno [11], [10] (following work of Ably and followed by a generalization by Gaudron [16]): if E is an elliptic curve over a number field K and ϕ is a rational function on E/K, then there is a constant $c > 0$ such that for any point $P \in E(K)$ which is not a pole of ϕ, one has

$$|\phi(P)| \geq (\hat{h}(P) + 2)^{-c},$$

where $\hat{h}$ is the Néron-Tate height. Lang's original form of this conjecture [37] actually makes the constant c more explicit in terms of E/K and ϕ; in this more precise form the conjecture is still open. We refer to [11] for a history of work on this conjecture of Lang. For an in-depth presentation of Diophantine approximations on linear groups up to the year 2000, we refer to [65]. For more on Diophantine approximations on abelian varieties, we refer to [4], [43], [49].

In [38] Lang proved a conjecture of Cartier stating that if G is an algebraic group over a number field K and $\alpha \in (\mathrm{Lie}\, G)(K)$ is such that $t \mapsto \exp_G(t\alpha)$ is not an algebraic function, then $\exp(\alpha)$ is transcendental over K. For G a linear group this reduces to the classical result about the exponential function. The novelty comes from the nonlinear case; in case G is an abelian variety, Lang's result is a transcendence result for values of theta functions. Lang derived the above theorem from his transcendence criterion generalizing the method of Gelfond [17] and Schneider [57]. His criterion says the following: Let K be a number field and let $g_1, \dots, g_n$ be meromorphic functions on $\mathbf{C}$ of finite order ρ such that the field $K(g_1, \dots, g_n)$ has transcendence degree ≥ 2 over K. Assume d/dt sends $K[g_1, \dots, g_n]$ into itself. Let $w_1, \dots, w_m \in \mathbf{C}$ be distinct complex numbers such that $g_i(w_j) \in K$. Then $m \leq 10\rho[K : \mathbf{Q}]$. Using ideas of Schneider, Lang extended his transcendence criterion to meromorphic functions of several variables in [39], [40]. In particular, in [40] he derives the celebrated "Theorem on the 6 exponentials": if $\beta_1, \beta_2 \in \mathbf{C}$ are $\mathbf{Q}$-linearly independent and $z_1, z_2, z_3 \in \mathbf{C}$ are $\mathbf{Q}$-linearly independent, then not all 6 numbers $e^{\beta_i z_j}$ are algebraic. (Apparently this had been known to Siegel; Lang rediscovered the result, and his proof was the first published proof.) In the same vein, Lang proves that if A is an abelian variety over a number field K and $\Gamma \subset A(K)$ is a subgroup of rank ≥ 7 contained in a 1-parameter subgroup of A, then this 1-parameter subgroup is algebraic, i.e., an elliptic curve. Later, using deep analytic arguments, Bombieri and Lang [5] extended this theory to s-parameter subgroups. For a comprehensive survey of transcendence up to the year 1997, we refer to [15].

References

[1] D. Abramovich and J. F. Voloch, Toward a proof of the Mordell-Lang conjecture in characteristic p, *International Math. Res. Notices* **5** (1992), 103–115.

[2] S. J. Arakelov, Families of algebraic curves with fixed degeneracies, *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 1269–1293.

[3] E. Artin, Beweis des Reziprozitätsgesetzes, *Abh. Math. Sem. Hamburg* **5** (1927), 353–363.

[4] M. Artin, On the solutions of analytic equations, *Invent. Math.* **5** (1968), 277–291.

[5] E. Bombieri and S. Lang, Analytic subgroups of group varieties, *Invent. Math.* **11** (1970), 1–14.

[6] A. Buium, Intersections in jet spaces and a conjecture of S. Lang, *Ann. of Math. (2)* **136** (1992), 557–567.

[7] A. Buium and F. J. Voloch, Integral points on abelian varieties over function fields, *Math. Ann.* **297** (1993), 303–307.

[8] C. Chabauty, Sur les équations Diophantiennes liées aux unités d'un corps de nombres algébriques fini, *Ann. of Math.* **17** (1938), 127–168.

[9] C. Chevalley, Démonstration d'une hypothèse de M. Artin, *Abh. Math. Sem. Hansischen Univ.* **11** (1935), 73.

[10] S. David and N. Hirata-Kohno, Linear forms in elliptic logarithms, *Crelle J.*, to appear.

[11] ———, Recent progress on linear forms in elliptic logarithms, *A Panorama of Number Theory or the*

View from Baker's Garden, Cambridge Univ. Press, Cambridge, 2002, pp. 26–37.

[12] H. Esnault and E. Viehweg, Effective bounds for semipositive sheaves and the height of points on curves over complex function fields, *Compositio Math.* **76** (1990), 69–85.

[13] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[14] ———, Diophantine approximation on abelian varieties, *Ann. of Math. (2)* **133** (1991), 549–567.

[15] N. I. Feldman and Yu. V. Nesterenko, *Number Theory IV: Transcendental Numbers*, Springer, 1998.

[16] E. Gaudron, Mesures d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif, *Invent. Math.* **162**, no. 1 (2005).

[17] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.

[18] H. Grauert, Mordell's Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörpern, *Publ. Math. IHES* **25** (1965), 131–149.

[19] M. Greenberg, Schemata over local rings I, II, *Ann. of Math. (2)* **73** (1961), 624–648; **78** (1963), 256–266.

[20] M. Hindry, Autour d'une conjecture de Serge Lang, *Invent. Math.* **94** (1988), 575–603.

[21] E. Hrushovski, The Mordell-Lang conjecture over function fields, *J. Amer. Math. Soc.* **9** (1996), 667–690.

[22] S. Lang, On quasi algebraic closure, *Ann. of Math. (2)* **55** (1952), 373–390.

[23] ———, Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.

[24] ———, Unramified class field theory over function fields in several variables, *Ann. of Math. (2)* **64** (1956), 285–325.

[25] ———, Sur les séries L d'une variété algébrique, *Bull. Soc. Math. France* **84** (1956), 385–407.

[26] ———, Divisors and endomorphisms on an abelian variety, *Amer. J. Math.* **79**, no. 4 (1957), 761–777.

[27] ———, Reciprocity and correspondences, *Amer. J. Math.* **80**, no. 2 (1957), 431–440.

[28] ———, *Abelian Varieties*, Wiley-Interscience, 1959.

[29] S. Lang and A. Néron, Rational points of abelian varieties over function fields, *Amer. J. Math.* **81**, no. 1 (1959), 95–118.

[30] S. Lang, Integral points on curves, *Publ. Math. IHES* **6** (1960), 27–43.

[31] ———, Division points on curves, *Ann. Mat. Pura Appl.*, Serie IV, **70** (1965), 177–192.

[32] ———, Asymptotic approximations to quadratic irrationalities, I, *Amer. J. Math.* **2** (1965), 481–487.

[33] ———, Asymptotic approximations to quadratic irrationalities, II, *Amer. J. Math.* **2** (1965), 488–496.

[34] ———, Asymptotic Diophantine approximations, *Proc. Nat. Acad. Sci.* **55** (1966), 31–34.

[35] ———, Report on Diophantine approximations, *Bull. Soc. Math. France* **93** (1965), 177–192.

[36] ———, *Diophantine Geometry*, Interscience Publ., New York, 1962.

[37] ———, Diophantine approximations on toruses, *Amer. J. Math.* **3** (1964), 521–533.

[38] ———, Transcendental points on group varieties, *Topology* **1** (1962), 313–318.

[39] ———, Algebraic values of meromorphic functions, *Topology* **3** (1965), 183–191.

[40] ———, Algebraic values of meromorphic functions, II, *Topology* **5** (1966), 363–370.

[41] ———, Higher dimensional Diophantine problems, *Bull. Amer. Math. Soc.* **80**, no. 5 (1974), 779–787.

[42] ———, Hyperbolic and Diophantine analysis, *Bull. Amer. Math. Soc. N.S.* **14**, no. 2 (1986), 159–205.

[43] ———, *Number Theory III: Diophantine Geometry*, Springer, 1991.

[44] ———, *Collected Papers, Vol. I*, Springer, 2000.

[45] K. Mahler, Über die rationalen Punkte auf Kurven vom Geschlecht Eins, *J. Reine Angew. Math.* **170** (1934), 168–178.

[46] Yu. I. Manin, Rational points of algebraic curves over function fields, *Izv. Akad. Nauk SSSR Ser. Mat.* **27** (1963), 1395–1440.

[47] M. McQuillan, Division points on semi-abelian varieties, *Invent. Math.* **120** (1995), 143–159.

[48] L. J. Mordell, On the rational solutions of the indeterminate equation of the third and fourth degrees, *Math. Proc. Cambridge Philos. Soc.* **21** (1922), 179–192.

[49] M. Nakamaye, Diophantine approximation on algebraic varieties, *J. Théor. Nombres Bordeaux* **11** (1999), 439–502.

[50] A. Néron, Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique sur un corps, *Bull. Soc. Math. France* **80** (1952), 101–166.

[51] A. N. Parshin, Algebraic curves over function fields, *Math. USSR Izv.* **2** (1968), 1145–1170.

[52] ———, Finiteness theorems for hyperbolic manifolds, *The Grothendieck Festschrift*, Birkhäuser Boston, 1990, pp. 163–178.

[53] A. Pillay, Mordell-Lang conjecture for functions fields in characteristic zero, revisited, *Compositio Math.* **140** (2004), 64–68.

[54] M. Raynaud, Courbes sur une variété abélienne et points de torsion, *Invent. Math.* **71** (1983), 207–233.

[55] ———, Around the Mordell conjecture for function fields and a conjecture of S. Lang, Lecture Notes in Math., vol. 1016, Springer, Berlin, 1983, pp. 1–20.

[56] P. Samuel, Compléments à un article de Hans Grauert sur la conjecture de Mordell, *Publ. Math. IHES* **29** (1966), 55–62.

[57] T. Schneider, *Einführung in die transcendenten Zahlen*, Springer, Berlin, 1957.

[58] C. L. Siegel, Über einige Anwendungen Diophantischer Approximationen, *Abh. Preussischen Akad. Wiss. Phys. Math. Kl.* (1929), 41–69.

[59] L. Szpiro, Séminaire sur les pinceaux de courbes de genre au moins deux, *Astérisque* **86** (1981).

[60] C. Tsen, Divisionalgebren über Funktionenkörper, *Nachr. Ges. Wiss. Göttingen* (1933), 335.

[61] P. Vojta, Siegel's theorem in the compact case, *Ann. of Math. (2)* **33** (1991), 509–548.

[62] ———, Integral points on subvarieties of semiabelian varieties, *Invent. Math.* **126** (1996), 133–181.

[63] F. J. Voloch, On the conjectures of Mordell and Lang in positive characteristic, *Invent. Math.* **104** (1991), 643–646.

[64] ———, *Diophantine approximation on abelian varieties in characteristic p*, *Amer. J. Math.* **117**, no. 4 (1995), 1089–1095.

[65] M. Waldschmidt, Diophantine Approximations on Linear Algebraic Groups, Grundlehren, vol. 326, Springer, 2000.

[66] A. WEIL, L'arithmétique des courbes algébriques, *Acta Math.* **52** (1928), 281–315.

Serge Lang's Contributions to the Theory of Transcendental Numbers[2]

Michel Waldschmidt

When Serge Lang started to work on transcendental number theory in the early 1960s, the subject was not fashionable. It became fashionable only a few years later, thanks to the work of S. Lang certainly, but also to the contributions of A. Baker. At that time the subject was considered as very technical, not part of the main stream, and only a few specialists were dealing with it. The proofs were somewhat mysterious: why was it possible to prove some results while other conjectures resisted?

With his outstanding insight and his remarkable pedagogical gifts, Lang comes into the picture and contributes to the subject in at least two very different ways: on the one hand, he simplifies the arguments (sometimes excessively) and produces the first very clear proofs which can be taught easily; on the other hand, he introduces new tools, like group varieties, which put the topic closer to the interests of many a mathematician.

His proof of the Six Exponentials Theorem is a good illustration of the simplicity he introduced in the subject. His arguments are clear; one understands for instance why the construction of an auxiliary function is such a useful tool. Probably nobody knows so far why the arguments do not lead to a proof of the four exponentials conjecture, but this is something which will be clarified only later. Several mathematicians knew the Six Exponentials Theorem; Lang was the first to publish its proof (a few years later, K. Ramachandra rediscovered it).

Another nice example is the so-called Schneider-Lang criterion. Schneider had produced a general statement on the algebraic values of meromorphic functions in 1949. This statement of Schneider is powerful; it includes a number of transcendence results, and it was the first result containing at the same time the Hermite–Lindemann Theorem on the transcendence of $\log \alpha$, the Gel'fond–Schneider solution of Hilbert's seventh problem on the transcendence of α^{β}, and the Six Exponentials Theorem. However, Schneider's criterion was quite complicated; the statement itself included a number of technical hypotheses. Later, in 1957 (in his book on transcendental number theory), Schneider produced a simplified version dealing with functions satisfying differential equations (at the cost of losing the Six Exponentials Theorem from the corollaries, but Schneider did not state this theorem explicitly anyway). S. Lang found nice hypotheses which enabled him to produce a simple and elegant result.

Lang also extended this Schneider-Lang criterion to several variables, again using ideas of Schneider (which he introduced in 1941 for proving the transcendence of the values $B(a, b)$ of Euler's Beta function at rational points). Lang's extension to several variables involves Cartesian products. M. Nagata suggested a stronger statement involving algebraic hypersurfaces. This conjecture was settled by E. Bombieri in 1970 using a generalization in several variables of Schwarz's Lemma, which was obtained by Bombieri and Lang using also some deep L^2 estimates from Hörmander. It is ironic that Bombieri's Theorem is not required but that the statement with Cartesian product suffices for the very surprising proof of Baker's Theorem (and its extension to elliptic curves) found by D. Bertrand and D. W. Masser in 1980.

The introduction by S. Lang of group varieties in transcendental number theory followed a conjecture of Cartier, who asked him whether it would be possible to extend the Hermite-Lindemann Theorem from the multiplicative group to a commutative algebraic group over the field of algebraic numbers. This is the result that Lang proved in 1962. At that time there were a few transcendence results (by Siegel and Schneider) on elliptic functions and even Abelian functions. But Lang's introduction of algebraic groups in this context was the start of a number of important developments in the subject.

Among the contributions of Lang to transcendental number theory (also to Diophantine approximation and Diophantine geometry), the least are not his many conjectures which shed a new light on the subject. On the contrary, he had a way of considering what the situation should be, which was impressive. Indeed, he succeeded in getting rid of the limits from the existing results and methods. He made very few errors in his predictions, especially if we compare them with the large number of conjectures he proposed. His description of the subject will be a guideline for a very long time.

---

[2] *Editor's note: An expanded version of Waldschmidt's contribution is published in: "Les contributions de Serge Lang à la théorie des nombres transcendants",* Gaz. Math. **108** (2006), 35–46.

Michel Waldschmidt is a professor at the Université P. et M. Curie (Paris VI). His email address is `miw@math.jussieu.fr`.

Lang's Work on Modular Units and on Frobenius Distributions[3]

David E. Rohrlich

In 1972 Lang joined the Department of Mathematics of Yale University, where he remained a faculty member until his retirement. The move to Yale coincided with a change of direction in Lang's research, a change which reflected a broader trend in number theory as a whole: Whereas the theory of automorphic forms had previously been the exclusive domain of specialists, by the early seventies modular forms and the Langlands program were playing a central role in the thinking of number theorists of a variety of stripes. In Lang's case these influences were particularly apparent in the work with Kubert on modular units and in the work with Trotter on Frobenius distributions.

Modular Units

Two brief notes on automorphisms of the modular function field (articles [1971c] and [1973] in the *Collected Papers*) signaled Lang's developing interest in modular functions, but his primary contribution in this domain was the joint work with Kubert on modular units, expounded in a long series of papers from 1975 to 1979 and subsequently compiled in their book *Modular Units*, published in 1981. The work has two distinct components: the function theory of modular units on the one hand and the application to elliptic units on the other.

The Function-Theoretic Component

In principle the problem considered by Kubert and Lang can be formulated for any compact Riemann surface X and any finite nonempty set S of points on X. Let C_S be the subgroup of the divisor class group of X consisting of the classes of divisors of degree 0 which are supported on S. If one prefers, one can think of C_S as the subgroup of the Jacobian of X generated by the image of S under an Albanese embedding. In any case, the problem is to determine if C_S is finite, and when it is finite to compute its order.

In practice this problem is rarely of interest: if the genus of X is ≥ 1, then for most choices of S we can expect that C_S will be the free abelian group of rank $|S|-1$, and there is nothing further to say. However, in the work of Kubert and Lang X is a modular curve and S its set of cusps. In this case Manin [18] and Drinfeld [9] had already proved the finiteness of C_S, but their proof rested on a clever use of the Hecke operators and gave no information about the order of C_S. Kubert and Lang found an altogether different proof of the Manin-Drinfeld theorem in which the whole point was to exhibit a large family of functions on X with divisorial support on S. (These functions, by the way, are the "modular units". If R_S is the subring of the function field of X consisting of functions holomorphic outside S, then the modular units are indeed the elements of the unit group $R_S^\times$ of R_S.) In optimal cases, in particular when X is the modular curve usually denoted $X(N)$ and N is a power of a prime $p \geq 5$, Kubert and Lang were able to deduce an explicit formula for $|C_S|$ in terms of certain "Bernoulli-Cartan numbers" closely related to the generalized Bernoulli numbers $b_{2,\chi}$ which appear in formulas for the value of a Dirichlet L-function $L(s,\chi)$ at $s=-1$.

This work found immediate application in the proof by Mazur and Wiles [19] of the main conjecture of classical Iwasawa theory, and since then it has found many other applications as well. But quite apart from its usefulness, the work can be appreciated as a counterpoint to the "Manin-Mumford conjecture", enunciated by Lang in an earlier phase of his career (see [1965b]) in response to questions posed by the eponymous authors. The conjecture asserts that the image of a curve X of genus ≥ 2 under an Albanese embedding intersects the torsion subgroup of the Jacobian of X in only finitely many points. A strong form of the conjecture was proved by Raynaud in 1983 [23], and the subject was subsequently enriched by Coleman's theory of "torsion packets" [5]: a torsion packet on X is an equivalence class for the equivalence relation

$$P \equiv Q \Leftrightarrow n(P-Q) \text{ principal for some } n \geq 1$$

on the points of X. Of particular relevance here is the proof by Baker [1] of a conjecture of Coleman, Kaskel, and Ribet, from which it follows that for most values of N (including in particular $N = p^n$ with p outside a small finite set) the cuspidal torsion packet on $X(N)$ consists precisely of the cusps. Thus the results of Kubert and Lang provide one of the relatively rare examples of a curve for which the order of the subgroup of the Jacobian generated by the image under an Albanese embedding of a nontrivial torsion packet on the curve has been calculated explicitly.

Elliptic Units

Let us now view modular functions f as functions on the complex upper half-plane $\mathfrak{H}$ rather than on the modular curves. Given an imaginary quadratic field K, we can then embed K in $\mathbf{C}$ and evaluate f at points $\tau \in K \cap \mathfrak{H}$. It has been known since the time of Kronecker and Weber that for

[3]*Editor's note: In addition to contributions to both* Notices *articles about Lang, David Rohrlich has also written the following piece: "Serge Lang", Gaz. Math.* **108** *(2006), 33–34.*

David E. Rohrlich is professor of mathematics at Boston University. His email address is rohrlich@math.bu.edu.

appropriate choices of f and τ the values $f(\tau)$ generate ray class fields L of K, and if f is in addition a modular unit, then $f(\tau)$ is a unit of L. Roughly speaking, the group of *elliptic units* of L is the group of units obtained in this way, and a major theme of the theory is that the index of the group of elliptic units in the group of all units of L should be closely related to the class number of L. Achieving an optimal statement of this sort has proved to be an incremental process. Kubert and Lang built on the work of Siegel [28], Ramachandra [22], and especially Robert [24], and they also drew inspiration from Sinnott [29], who had solved the analogous problem which arises when the base field K is replaced by $\mathbf{Q}$ (the role of the elliptic units is then played by the cyclotomic units). In the end it was Lang's doctoral student Kersey who obtained some of the definitive results of the theory, for example the determination of a group of roots of elliptic units in the Hilbert class field H of K such that the index of this group in the group of all units of H is precisely the class number of H. Kersey was in effect a third author of the part of *Modular Units* having to do with class number formulas.

In recent years the theory of elliptic units has to some extent been subsumed in and overshadowed by broader developments in Iwasawa theory, notably Rubin's proof [25] of the one-variable and two-variable main conjectures in the Iwasawa theory of imaginary quadratic fields. But the need for explicit formulas at finite level never really ends. The very recent work of Á. Lozano-Robledo [17] and A. L. Folsom [12] attests to the ongoing vitality of the problems considered more than a quarter of a century ago by Robert and Kubert-Lang.

Frobenius Distributions

The circle of ideas known as the "Lang-Trotter conjectures" comprises two distinct themes that are developed respectively in the book *Frobenius Distributions in* GL_2*-Extensions* (reproduced in its entirety as article [1976d] of the *Collected Papers*) and the paper "Primitive points on elliptic curves" [1977b]. What these two works have in common, besides their joint authorship with Trotter, is that both are concerned with Frobenius distributions arising from elliptic curves. Here the term "Frobenius distribution" is used broadly to include any function $p \mapsto a(p)$ from prime numbers to integers which arises naturally in algebraic number theory or Diophantine geometry. Henceforth E denotes an elliptic curve over $\mathbf{Q}$ and Δ its minimal discriminant.

Frobenius Distributions in GL_2-Extensions

In this subsection we assume that E does not have complex multiplication. For $p \nmid \Delta$ put

$$a(p) = 1 + p - |\tilde{E}(\mathbf{F}_p)|,$$

where $\tilde{E}$ is the reduction of E modulo p. Given an integer t and an imaginary quadratic field K, Lang and Trotter consider the counting functions $N_t(x)$ and $N_K(x)$ corresponding to what they call the "fixed trace" and "imaginary quadratic" distributions of the map $p \mapsto a(p)$. By definition, $N_t(x)$ is the number of primes $p \le x$ ($p \nmid \Delta$) such that $a(p) = t$, and $N_K(x)$ is the number of primes $p \le x$ ($p \nmid \Delta$) such that the polynomial $X^2 - a(p)X + p$ factors into linear factors in K. Of course this polynomial is just the characteristic polynomial of a Frobenius element $\sigma_p \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acting on the ℓ-adic Tate modules of E ($\ell \neq p$), and the "trace" in "fixed trace distribution" is an allusion to this interpretation of $a(p)$. In fact Lang and Trotter define $N_t(x)$ and $N_K(x)$ for any strictly compatible family of ℓ-adic representations $\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}(2, \mathbf{Z}_\ell)$ such that the image of the product representation into $\mathrm{GL}(2, \hat{\mathbf{Z}})$ is an open subgroup of $\mathrm{GL}(2, \hat{\mathbf{Z}})$ and such that the characteristic polynomial of $\rho_\ell(\sigma_p)$ has the form $X^2 - a(p)X + p$ with $a(p) \in \mathbf{Z}$ and $|a(p)| \le 2\sqrt{p}$. The authors ask by the way whether any such families exist besides the ones coming from elliptic curves, and to my knowledge their question has not been explicitly addressed in the literature. In any case, given this framework Lang and Trotter define certain constants $c_t \ge 0$ and $c_K > 0$ (depending on the compatible family $\{\rho_\ell\}$ as well as on t and K) and conjecture that

$$N_t(x) \sim c_t\sqrt{x}/\log x$$

and

$$N_K(x) \sim c_K\sqrt{x}/\log x$$

for $x \to \infty$. Here we are following the convention of Lang-Trotter that if $c_t = 0$, then the relation $N_t(x) \sim c_t\sqrt{x}/\log x$ means that $N_t(x)$ is constant for large x (in other words the underlying set of primes is finite).

Let us refer to this conjecture as the *first Lang-Trotter conjecture*; the conjecture on primitive points discussed below is then the *second Lang-Trotter conjecture*. An important aspect of the first conjecture is the precise definition of the constants c_t and c_K, which is based on a probabilistic model. This feature distinguishes the conjecture from, say, Tuskina's earlier attempt [30] to study the asymptotics of supersingular primes (the case $t = 0$) without a probabilistic model and without any prediction about the value of c_0. A similar comment pertains to V. K. Murty's paper [21], which is in other respects a vast generalization of the Lang-Trotter conjecture. On the other hand, in their study of the asymptotics of supersingular primes for modular abelian varieties, Bayer and González [2] do consider a probabilistic model generalizing that of Lang and Trotter.

What is immediately striking about the first Lang-Trotter conjecture is its apparent utter inaccessibility. As Lang once remarked, the conjecture is contained "in the error term of the Riemann hypothesis." Nonetheless, there are a few results (referring for the most part to an elliptic curve E rather than to an abstract compatible family $\{\rho_\ell\}$ satisfying the Lang-Trotter axioms) that have some bearing on the conjecture. To begin with, the theorem of Elkies [10] that an elliptic curve over $\mathbf{Q}$ has infinitely many supersingular primes is at least consistent with the conjecture, because Lang and Trotter show that $c_0 > 0$ in this case. Also consistent are a number of "little oh" results about $N_t(x)$ and $N_K(x)$, starting with Serre's observation that these functions are $o(x/\log x)$ (i.e., the underlying sets of primes have density 0) and even $o(x/(\log x)^\gamma)$ with $\gamma > 1$ (see [26], [27]). Further improvements in the bound for $N_t(x)$ were made by Wan [31] and V. K. Murty [20], and in the case of supersingular primes the bound $N_0(x) = O(x^{3/4})$ was obtained by Elkies, Kaneko, and M. R. Murty [11]. There are also results giving the conjectured growth rate "on average" for $N_0(x)$ (Fouvry-Murty [13]) and more generally for $N_t(x)$ (David-Pappalardi [8]), the average being taken over a natural two-parameter family of elliptic curves. As for $N_K(x)$, the best upper bound to date is in the recent paper of Cocojaru, Fouvry, and M. R. Murty [4], who also give estimates under the generalized Riemann hypothesis. Finally, and in an altogether different direction, analogous problems for Drinfeld modules have been investigated by Brown [3] and David [6], [7].

Primitive Points on Elliptic Curves

The first Lang-Trotter conjecture can be viewed as an analogue of the Chebotarev density theorem in which finite Galois extensions of $\mathbf{Q}$ are replaced by the infinite Galois extensions generated by division points on elliptic curves. The second Lang-Trotter conjecture also has a classical antecedent, but it is Artin's primitive root conjecture, which predicts the density of the set of primes p such that a given nonzero integer a is a primitive root modulo p. In particular, if $a \neq -1$ and a is not a square, then this density is conjectured to be positive. The analogue proposed by Lang and Trotter involves an elliptic curve E over $\mathbf{Q}$ of positive rank and a given point $P \in E(\mathbf{Q})$ of infinite order. There is no longer any need to assume that E is without complex multiplication. Consider the set of primes $p \nmid \Delta$ such that $\tilde{E}(\mathbf{F}_p)$ is generated by the reduction of P modulo p (and is therefore in particular cyclic). Lang and Trotter conjecture that this set has a density, and they explain how to compute the conjectured density using reasoning analogous to Artin's. More generally, Lang and Trotter consider an arbitrary free abelian subgroup Γ of $E(\mathbf{Q})$. If we let $N_\Gamma(x)$ denote the number of primes $p \le x$ ($p \nmid \Delta$) such that $\tilde{E}(\mathbf{F}_p)$ coincides with the reduction of Γ modulo p, then the general form of the conjecture is that

$$N_\Gamma(x) \sim c_\Gamma x/\log x$$

for some constant c_Γ.

Just as Hooley [16] was able to prove Artin's primitive root conjecture by assuming the generalized Riemann hypothesis, R. Gupta and M. R. Murty [14] were able to prove a conditional result in the Lang-Trotter setting: Under the generalized Riemann hypothesis we have $N_\Gamma(x) \sim c_\Gamma x/\log x$ whenever the rank of Γ is ≥ 18. In fact in the case of elliptic curves with complex multiplication, Gupta and Murty obtain an asymptotic relation of this sort even when the rank of Γ is one, but for a slightly different counting function, say $N'_\Gamma(x)$, which differs from $N_\Gamma(x)$ in that we count only primes which split in the field of complex multiplication. Unconditionally, Gupta and Murty prove that if the rank of Γ is ≥ 6, then $N'_\Gamma(x) \gg x/(\log x)^2$.

An analogue of the second Lang-Trotter conjecture can also be formulated for an elliptic curve over a global field of positive characteristic, and in very recent work Hall and Voloch [15] have proved the analogue whenever the rank of Γ is ≥ 6.

References

[1] M. BAKER, Torsion points on modular curves, *Invent. Math.* **140** (2000), 487–509.

[2] P. BAYER and J. GONZÁLEZ, On the Hasse-Witt invariants of curves, *Experiment. Math.* (1997), 57–76.

[3] M. BROWN, Singular moduli amd supersingular moduli of Drinfeld modules, *Invent. Math.* **110** (1992), 419–439.

[4] A. C. COJOCARU, E. FOUVRY, and M. R. MURTY, The square sieve and the Lang-Trotter conjecture, *Canad. J. Math.* **57** (1995), 1155–1177.

[5] R. F. COLEMAN, Torsion points on curves and p-adic Abelian integrals, *Ann. Math.* **121** (1985), 111–168.

[6] C. DAVID, Average distributions of supersingular Drinfeld modules, *J. Number Theory* **56** (1996), 366–380.

[7] ———, Frobenius distributions of Drinfeld modules of any rank, *J. Number Theory* **90** (2001), 329–340.

[8] C. DAVID and F. PAPPALARDI, Average Frobenius distributions of elliptic curves, *Internat. Math. Res. Notices* **4** (1999), 165–183.

[9] V. DRINFELD, Two theorems on modular curves, *Func. Anal. Appl.* **7** (1973), 155–156.

[10] N. ELKIES, The existence of infinitely many supersingular primes for every elliptic curve over **Q**, *Invent. Math.* **89** (1987), 561–567.

[11] ———, Distribution of supersingular primes, in: Journées Arithmétiques (Luminy 1989), *Astérisque* (1992), 127–132.

[12] A. L. FOLSOM, UCLA doctoral thesis (2006).
[13] E. FOUVRY and M. R. MURTY, On the distribution of supersingular primes, *Canad. J. Math.* **48** (1996), 81–204.
[14] R. GUPTA and M. R. MURTY, Primitive points on elliptic curves, *Compos. Math.* **58** (1986), 13–44.
[15] C. HALL and J. F. VOLOCH, Towards Lang-Trotter for elliptic curves over functions fields, to appear.
[16] C. HOOLEY, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
[17] Á. LOZANO-ROBLEDO, On elliptic units and p-adic Galois representations attached to elliptic curves, *J. Number Theory* **117** (2006).
[18] J. MANIN, Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk. SSSR Ser. Math.* **36** (1972), 19–66.
[19] B. MAZUR and A. WILES, Class fields of abelian extensions of **Q**, *Invent. Math.* **76** (1984), 179–330.
[20] V. K. MURTY, Modular forms and the Chebotarev density theorem, II, *Analytic Number Theory*, edited by Y. Motohashi, London Math. Soc. Lecture Notes, vol. 247, Cambridge Univ. Press, 1997, pp. 287–308.
[21] ———, Frobenius distributions and Galois representations, in: *Automorphic Forms, Automorphic Representations, and Arithmetic*, edited by R. Doran, Z.-L. Dou, and G. Gilbert, Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999.
[22] K. RAMACHANDRA, Some applications of Kronecker's limit formula, *Ann. Math.* **80** (1964), 104–148.
[23] M. RAYNAUD, Courbes sur une variété Abélienne et points de torsion, *Invent. Math.* **71** (1983), 207–233.
[24] G. ROBERT, Unités elliptiques, *Bull. Soc. Math. France Supplément* **36** (1973).
[25] K. RUBIN, On the main conjecture of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **93** (1988), 701–713.
[26] J-P. SERRE, Groupes de Lie l-adiques attachés aux courbes elliptiques, *Colloque CNRS* **143** (1966), 239–256.
[27] ———, Quelques applications du théorème de densité de Chebotarev, *Pub. Math. IHES* **54** (1981), 123–201.
[28] C. L. SIEGEL, *Lectures on Advanced Analytic Number Theory*, Tata Institute of Fundamental Research, Bombay, 1965.
[29] W. SINNOTT, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math. (2)* **108** (1978), 107–134.
[30] T. A. TUSKINA, A numerical experiment on the calculation of the Hasse invariant for certain curves, *Izv. Akad. Nauk. SSSR Ser. Math.* **29** (1965), 1203–1204.
[31] D. WAN, On the Lang-Trotter conjecture, *J. Number Theory* **35** (1990), 247–268.

Serge Lang's Work in Diophantine Geometry

Paul Vojta

I first knew of Serge Lang through his books: *Algebra, Algebraic Number Theory*, and *Elliptic Functions.* Later, as I was finishing my degree and getting ready to join him at Yale, he was finishing his book *Fundamentals of Diophantine Geometry*, a substantial rewrite of his earlier *Diophantine Geometry*. In Serge's world view, the way you choose to look at a theorem is often more important than the theorem itself. As the title suggests, Serge's outlook on number theory was decidedly geometric. While others at the time shared this viewpoint (e.g., Weil, Tate, Serre), it is easy to forget that others did not, as Mordell's review of the earlier *Diophantine Geometry* attests.

A few years later Serge wrote *Introduction to Arakelov Theory*, which, together with Cornell-Silverman and Soulé-Abramovich-Burnol-Kramer, forms the short list of key introductory books in this area.

Beyond books, Serge's influence on number theory derives more from his conjectures than from his theorems, although he had quite a few of those, too. His earliest major conjecture in this area was that a projective variety over a number field embedded in **C** is *Mordellic* (i.e., had only finitely many points rational over any given number field containing the field of definition of the variety) if and only if the corresponding complex projective variety is Kobayashi hyperbolic. Recall that the *Kobayashi semidistance* on a complex space X is the largest semidistance satisfying the property that all holomorphic maps from **D** to X are distance nonincreasing, where **D** is the unit disk in **C** with the Poincaré metric. A complex space is then *Kobayashi hyperbolic* if its Kobayashi semidistance is actually a distance. For example, a compact Riemann surface of genus g is Kobayashi hyperbolic if and only if $g \geq 2$, exactly the condition of Mordell's conjecture. Later Serge extended this conjecture to include subfields of **C** finitely generated over **Q**.

In 1978 Brody showed that a compact complex space X is Kobayashi hyperbolic if and only if there are no nonconstant holomorphic maps from **C** to X, thus simplifying the above conjecture to the assertion that X is Mordellic if and only if there are no nonconstant holomorphic maps $\mathbf{C} \to X$. In general, this conjecture is still open, although it has been proved for curves and more generally for closed subvarieties of abelian

Paul Vojta is a professor of mathematics at the University of California, Berkeley. His email address is vojta@math.berkeley.edu.

varieties. It is also closely related to conjectures and theorems in Nevanlinna theory.

The above special case came as a consequence of a proof of another of Lang's conjectures. Let A be a semiabelian variety over $\mathbf{C}$, let X be a closed subvariety of A, and let Γ be a subgroup of $A(\mathbf{C})$ such that $\dim_{\mathbf{Q}} \Gamma \otimes_{\mathbf{Z}} \mathbf{Q}$ is finite. Then $\Gamma \cap X(\mathbf{C})$ is contained in a finite union of translated semiabelian subvarieties of A contained in X. This was proved by Faltings, Vojta, and McQuillan (who stated it over the algebraic closure $\mathbf{Q}^a$ of $\mathbf{Q}$, but the general case follows by the function field variant of the same theorem). This gives finiteness statements for $X(k)$ in the abelian case by letting $\Gamma = A(k)$ and correctly anticipated the fact that working with rational points (or integral points in the semiabelian case) really boils down to finite rank of Γ. The conjecture was also proved for function fields of characteristic $p > 0$ by Hrushovsky (suitably restated). Returning to the case over $\mathbf{Q}^a$, this conjecture of Lang has been combined with Bogomolov's conjecture on points in $X(\mathbf{Q}^a)$ of small height to give an elegant result conjectured by Poonen and proved by Rémond.

Another conjecture of Lang that has received a lot of attention is his conjecture (originally posed as a question by Bombieri) that if X is a pseudo-canonical projective variety defined over a subfield of $\mathbf{C}$ finitely generated over $\mathbf{Q}$, then X is pseudo-Mordellic. Here a variety is *pseudo-canonical* if it is of general type. This follows Griffiths's definition that a variety is *canonical* if its canonical bundle is ample; in Lang's terminology, *pseudo* means outside of a proper Zariski-closed subset, so pseudo-ample means big and therefore pseudo-canonical means general type.[4] Likewise pseudo-Mordellic means that the rational points over any given subfield of $\mathbf{C}$ finitely generated over $\mathbf{Q}$ and containing the field of definition of the variety are not Zariski dense. This is sometimes called the "weak Lang conjecture"; the strong version asserts that there is a proper Zariski-closed subset Z of X such that $X(k) \setminus Z(k)$ is finite for all fields k as above.

A number of consequences of these conjectures have been proved over the years. For example, Caporaso, Harris, and Mazur showed that if the weak Lang conjecture holds, then for all integers $g \geq 2$ and for all number fields k there is a bound $B(g,k) \in \mathbf{Z}$ such that $\#C(k) \leq B(g,k)$ for all curves C of genus g over k. If the strong Lang conjecture is true, they showed in addition that for all $g \geq 2$ there is a bound $N(g) \in \mathbf{Z}$ such that for all k there are only finitely many smooth projective curves of genus g over k (up to isomorphism) with $\#C(k) > N(g)$. It should be noted that some people (e.g., Bogomolov) believe this conjecture to be false.

Serge never let controversy stop him, though, and he formulated additional conjectures regarding the proper Zariski-closed subset in the strong form of his conjecture. Let X be a projective variety over a field $k \subseteq \mathbf{C}$. We define the *algebraic special set* to be the Zariski closure of the union of the images of all nonconstant rational maps of group varieties over k^a into $X \times_k k^a$. He then conjectured that X is pseudo-canonical if and only if its special set is not all of X. He further conjectured that if X is pseudo-canonical, then the proper Zariski-closed subset in his strong conjecture can be taken to be the special set and also (assuming $k = \mathbf{C}$) that all nonconstant holomorphic maps $\mathbf{C} \to X$ lie in the special set (pseudo-Brody hyperbolic). This last conjecture thus generalizes his conjecture on Kobayashi hyperbolicity. A recurring theme in these conjectures is that one has algebraic criteria for analytic conditions of hyperbolicity.

In recent years Serge set aside these conjectures in favor of working on the heat kernel, but he returned to an aspect of them during his last few years. Recall that Roth's theorem (in its simplest form) states that if α is an algebraic number and $\epsilon > 0$, then there are only finitely many $p/q \in \mathbf{Q}$ (with p and q relatively prime integers and $q > 0$) such that $-\log|\alpha - p/q| > (2+\epsilon)\log q$. In the 1960s Lang conjectured that this could be improved to $2\log q + c\log\log q$ for some constant c, possibly $1 + \epsilon$, and subsequent computations with Trotter backed this up. Furthermore, based on a theorem of Khinchin, he conjectured that the error term $\epsilon \log q$ in Roth could be improved to $\log \psi(q)$ for any given increasing function ψ for which the sum $\sum (q \log \psi(q))^{-1}$ converges. His philosophy was that Khinchin's theorem applied to almost all real numbers, in a measure theoretic sense, and that algebraic numbers should behave likewise.

When the conjecture with Nevanlinna theory came on the scene, he posed the corresponding question in that context. It was proved by P.-M. Wong and Lang, and subsequent refinements have been obtained by Hinkkanen, Ye, and others. The original question on Diophantine approximation still remains open though.

In the last two years, Lang and van Frankenhuijsen started work on the question of what the best error term should be for the abc conjecture. For some time it has been well known that a Khinchin-type error term is too strong. Instead, they suggest $O(\sqrt{h/\log h})$, where h is the logarithmic height of the point $[a : b : c]$. Sadly, van Frankenhuijsen will have to continue work on this on his own.

[4] *As Serge would say, "The notation is functorial with respect to the ideas."*

Diophantine Geometry As Galois Theory in the Mathematics of Serge Lang

Minhyong Kim

Lang's conception of Diophantine geometry is rather compactly represented by the following celebrated conjecture [4]:

> Let V be a subvariety of a semi-abelian variety A, $G \subset A$ a finitely generated subgroup, and $\mathrm{Div}(G)$ the subgroup of A consisting of the division points of G. Then $V \cap \mathrm{Div}(G)$ is contained in a finite union of subvarieties of V of the form $B_i + x_i$, where each B_i is a semi-abelian subvariety of A and $x_i \in A$.

There is a wealth of literature at this point surveying the various ideas and techniques employed in its resolution, making it unnecessary to review them here in any detail [10], [39]. However, it is still worth taking note of the valuable *generality* of the formulation, evidently arising from a profound instinct for the plausible structures of mathematics. To this end, we remark merely that it was exactly this generality that made possible the astounding interaction with geometric model theory in the1990s [3]. That is to say, analogies to model-theoretic conjectures and structure theorems would have been far harder to detect if attention were restricted, for example, to situations where the intersection is expected to be finite. Nevertheless, in view of the sparse subset of the complex net of ideas surrounding this conjecture that we wish to highlight in the present article, our intention is to focus exactly on the case where A is compact and V does *not* contain any translate of a connected nontrivial subgroup. The motivating example, of course, is a compact hyperbolic curve embedded in its Jacobian. Compare then the two simple cases of the conjecture that are amalgamated into the general formulation:

(1) $V \cap A[\infty]$, the intersection between V and the torsion points of A, is finite.

(2) $V \cap G$ is finite.

Lang expected conjecture (1) to be resolved using Galois theory alone. This insight was based upon work of Ihara, Serre, and Tate ([28], VIII.6) dealing with the analogous problem for a torus and comes down to the conjecture, still unresolved, that the image of the Galois representation in $\mathrm{Aut}(A[\infty]) \simeq \mathrm{GL}_{2g}(\hat{\mathbf{Z}})$ contains an open subgroup of the homotheties $\hat{\mathbf{Z}}^*$. Even while assertion (1) is already a theorem of Raynaud [44], significant progress along the lines originally envisioned by Lang was made in [2] by replacing $A[\infty]$ with $A[p^\infty]$, the points of p-power torsion, and making crucial use of p-adic Hodge theory.

It is perhaps useful to reflect briefly on the overall context of Galois-theoretic methods in Diophantine geometry, of course without attempting to do justice to the full range of interactions and implications. Initially, that Galois theory is relevant to the study of Diophantine problems should surprise no one. After all, if we are interested in $X(F)$, the set of rational points of a variety X over a number field F, what is more natural than to observe that $X(F)$ is merely the fixed point set of $\Gamma := \mathrm{Gal}(\bar{F}/F)$ acting on $X(\bar{F})$? Since the latter is an object of classical geometry, such an expression might be expected to nicely circumscribe the subset $X(F)$ of interest. This view is of course very naive, and the action of Γ on $X(\bar{F})$ is notoriously difficult to use in any direct fashion. The action on *torsion points* of commutative group varieties on the other hand, while still difficult, is considerably more tractable, partly because a finite abelian subgroup behaves relatively well under specialization. Such an arithmetic variation exerts tight control on the fields generated by the torsion points, shaping Galois theory into a powerful tool for investigations surrounding (1).

On the other hand, for conjecture (2), where the points to be studied are not torsion, it is not at all clear that Galois theory can be as useful. In fact, my impression is that Lang expected *analytic geometry* of some sort to be the main input to conjectures of type (2). This is indicated, for example, by the absence of any reference to arithmetic in the formulation. We might even say that implicit in the conjecture is an important idea that we will refer to as the *analytic strategy*:

> (a) Replace the difficult Diophantine set $V(F)$ by the geometric intersection $V \cap G$.
>
> (b) Try to prove this intersection finite by analytic means.

In this form, the strategy appears to have been extraordinarily efficient over function fields, as in the work of Buium [4]. Even Hrushovski's [15] proof can be interpreted in a similar light where passage to the completion of suitable theories is analogous to the move from algebra to analysis (since the theory of fields is not good enough). These examples should already suffice to convince us that it is best left open as to what kind of analytic means are most appropriate in a given situation. The proof over number fields by Faltings [9], as well as the curve case by Vojta [47], utilizes rather heavy Archimedean analytic geometry. Naturally, the work of Vojta and Faltings draws us away from the realm of traditional Galois theory. However, in Chabauty's theorem [5], where V is a curve and the rank of G is strictly

Minhyong Kim is a professor of mathematics at Purdue University. His email address is `kimm@math.purdue.edu`.

less than the dimension of A, it is elementary non-Archimedean analysis, more specifically p-adic abelian integrals, that completes the proof. Lang makes clear in several different places ([28], [28], notes to Chapter 8; [36], I.6) that Chabauty's theorem was a definite factor in the formulation of his conjecture. This then invites a return to our main theme, as we remind ourselves that non-Archimedean analysis has come to be viewed profitably over the last several decades as a projection of *analysis on Galois groups*, a perspective of which Lang was well aware ([33], Chapter 4). As such, it has something quite substantial to say about nontorsion points, at least on elliptic curves ([18], for example). Hodge theory is again a key ingredient, this time as the medium in which to realize such a projection [43].

It is by now known even to the general public that a careful study of Galois actions underlies the theorem of Wiles [49] and roughly one-half of the difficulties in the theorem of Faltings [8]. There, Galois representations must be studied in conjunction with an array of intricate auxiliary constructions. However, the most basic step in the Galois-theoretic description of nontorsion points, remarkable in its simplicity, goes through the Kummer exact sequence

$$0 \to A[m](F) \to A(F) \to A(F) \xrightarrow{\delta} H^1(\Gamma, A[m]) \to H^1(\Gamma, A) \to \dots.$$

In this case, an easy study of specialization allows us to locate the image of δ inside a subgroup $H^1(\Gamma_S, A[m])$ of cohomology classes with restricted ramification which then form a finite group. We deduce thereby the finiteness of $A(F)/mA(F)$, the weak Mordell-Weil theorem. Apparently, a streamlined presentation of this proof, systematically emphasizing the role of Galois cohomology, first appears in Lang's paper with Tate [38]. There they also emphasize the interpretation of Galois cohomology groups as classifying spaces for *torsors*, in this case, for A and $A[m]$. (We recall that a torsor for a group U in some category is an object corresponding to a set with simply transitive U-action, where the extra structure of the category, such as Galois actions, prevents them from being trivial. See, for example, [40], III.4.) This construction has been generalized in one direction to study nontorsion algebraic cycles by associating to them extensions of motives [7]. More pertinent to the present discussion, however, is a version of the Kummer map that avoids any attempt to abelianize, taking values in fact in *nonabelian* cohomology classes.

In the course of preparing this article, I looked into Lang's *magnum opus* [28] for the first time in many years and was a bit surprised to find a section entitled "Non-abelian Kummer theory". What is nonabelian there is the Galois group that needs to be considered if one does not assume a priori that the torsion points of the group variety are rational over the ground field. The field of m-division points of the rational points will then have a Galois group H of the form

$$0 \to A[m] \to H \to M \to 0$$

where $M \subset GL_{2g}(\mathbf{Z}/m)$. Thus, "non-abelian" in this context is used in the same sense as in the reference to nonabelian Iwasawa theory. But what is necessary for hyperbolic curves is yet another layer of noncommutativity, this time in the coefficients of the action. Given a variety X with a rational point b, we can certainly consider the étale fundamental group $\hat{\pi}_1(\bar{X}, b)$ classifying finite étale covers of $\bar{X}$. But the same category associates to any other point $x \in X(F)$ the set of étale paths

$$\hat{\pi}_1(\bar{X}; b, x)$$

from b to x which is naturally a torsor for $\hat{\pi}_1(\bar{X}, b)$. All these live inside the category of pro-finite sets with Galois action. There is then a nonabelian continuous cohomology set $H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$ that classifies torsors and a nonabelian Kummer map

$$\delta^{na} : X(F) \to H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

sending a point x to the class of the torsor $\hat{\pi}_1(\bar{X}; b, x)$. This is obviously a basic construction whose importance, however, has begun to emerge only in the last twenty or so years. It relies very much on the flexible use of varying base points in Grothendieck's theory of the fundamental group, and it appears to have taken some time after the inception of the arithmetic π_1 theory [45] for the importance of such a variation to be properly appreciated [12], [6], [16]. In fact, the impetus for taking it seriously came also for the most part from Hodge theory [13], [14]. As far as Diophantine problems are concerned, in a letter to Faltings [12] written shortly after the proof of the Mordell conjecture, Grothendieck proposed the remarkable conjecture that δ^{na} should be a bijection for compact hyperbolic curves. He expected such a statement to be directly relevant to the Mordell problem and probably its variants like conjecture (2). This expectation appears still to be rather reasonable. For one thing, it is evident that the conjecture is a hyperbolic analogue of the finiteness conjecture for Tate-Shafarevich groups. And then profound progress is represented by the work of Nakamura, Tamagawa, and Mochizuki [42], [46], [41], where a statement of this sort is proved when points in the number field are replaced by dominant maps from other varieties. Some marginal insight might also be gleaned from [22] and [23], where a unipotent analogue of the Kummer map is related to Diophantine finiteness theorems. There, the ambient space inside which the analysis takes place is a classifying variety

$H^1_f(\Gamma_v, U_n^{et})$ of torsors for the local unipotent étale fundamental group (rather than the Jacobian), while the finitely generated group G is replaced by the image of a map

$$H^1_f(\Gamma_S, U_n^{et}) \to H^1_f(\Gamma_v, U_n^{et})$$

coming from a space of global torsors. Thereby, one obtains a new manifestation of the analytic strategy proving $X \cap \mathrm{Im}[H^1_f(\Gamma_S, U_n^{et})]$ to be finite in some very special circumstances and in general for a hyperbolic curve over $\mathbf{Q}$ if one admits standard conjectures from the theory of mixed motives (for example, the Fontaine-Mazur conjecture on geometric Galois representations). Fortunately, Chabauty's original method fits naturally into this setting as the technical foundation of the analytic part now becomes nonabelian p-adic Hodge theory and iterated integrals. Incidentally, some sense of the Diophantine content of these ideas can already be gained by deriving the *injectivity* of δ^{na} from the Mordell-Weil theorem.

It should be clear at this point that the Galois theory of the title refers in general to the theory of the fundamental group. Serge Lang was profoundly concerned with the fundamental group for a good part of his mathematical life. A rather haphazard list of evidence might be comprised of:

—his foundational work on unramified class field theory for varieties over finite fields, where he proves the surjectivity of the reciprocity map among many other things [25], [26];

—his study of the ubiquitous "Lang torsor" [27];

—his work with Serre on fundamental groups of proper varieties in arbitrary characteristic [37];

—his extensive study with Kubert of the modular function field [24];

—his work with Katz [21] on finiteness theorems for relative π_1's that made possible the subsequent proof by Bloch [1] and then Kato and Saito [19], [20] of the finiteness of CH_0 for arithmetic schemes.

Besides these influential papers, the reader is referred to his beautiful AMS colloquium lectures [31] for a global perspective on the role of covering spaces in arithmetic.

Even towards the end of his life when his published work went in an increasingly analytic direction, he had a keen interest both in fundamental groups and in the analogy between hyperbolic manifolds and number fields wherein fundamental groups play a central role. In my last year of graduate school, he strongly urged me to study the work of Kato and Saito (and apply it to Arakelov theory!) even though it had been years since he had himself been involved with such questions. From the spring of 2004 I recall a characteristically animated exchange in the course of which he explained to me a theorem of Geyer [11] stating that abelian subgroups of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ are pro-cyclic. It was clear that he perceived this fact to fit nicely into his vivid ideas about the heat kernel [17], but in a manner that I failed (and still fail) to comprehend properly. (He was unfortunately secretive with his deeper reflections on the arithmetic significance of his later work, allowing only informal glimpses here and there. It is tempting but probably premature to speculate about a Galois theory that encompasses even Archimedean analysis.) The preoccupation with hyperbolic geometry that was evident even from the 1970s ([30], [34], [35], and [36], Chapters 8 and 9) could rather generally be construed as reflecting a persistent intuition about the relevance of fundamental groups to Diophantine problems. (An intuition that was shared by Grothendieck [12] and even Weil [48].)

As for the direct application of nonabelian fundamental groups to Diophantine geometry that we have outlined here, one can convincingly place it into the general framework of Lang's inquiries. He is discussing the theorem of Siegel in the following paragraph from the notes to Chapter 8 of [28]:

> The general version used here was presented in [28] following Siegel's (and Mahler's) method. The Jacobian replaces the theta function, as usual, and the mechanism of the covering already used by Siegel appears here in its full formal clarity. It is striking to observe that in [25], I used the Jacobian in a formally analogous way to deal with the class field theory in function fields. In that case, Artin's reciprocity law was reduced to a formal computation in the isogeny $u \mapsto u^{(q)} - u$ of the Jacobian. In the present case, the heart of the proof is reduced to a formal computation of heights in the isogeny $u \mapsto mu + a$.

We have emphasized above the importance of the Kummer map

$$x \mapsto [\hat{\pi}_1(\bar{X}; b, x)] \in H^1(\Gamma, \hat{\pi}_1(\bar{X}; b)).$$

When X is defined over a finite field $\mathbf{F}_q$ and we replace $\hat{\pi}_1(\bar{X}, b)$ by its abelian quotient $H_1(\bar{X}, \hat{\mathbf{Z}})$, the map takes values in

$$\begin{aligned} &H^1(\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q), H_1(\bar{X}, \hat{\mathbf{Z}})) \\ &\qquad = H_1(\bar{X}, \hat{\mathbf{Z}})/[(\mathrm{Fr} - 1)H_1(\bar{X}, \hat{\mathbf{Z}})], \end{aligned}$$

$\mathrm{Fr} \in \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ being the Frobenius element. But this last group is nothing but the kernel

$$\hat{\pi}_1^{ab}(X)^0$$

of the structure map

$$\hat{\pi}_1^{ab}(X) \to \hat{\pi}_1(\mathrm{Spec}(\mathbf{F}_q)).$$

Thus the abelian quotient of the Kummer map becomes identified with the *reciprocity* map [19]

$$\mathrm{CH}_0(X)^0 \to \hat{\pi}_1^{ab}(X)^0$$

of unramified class field theory evaluated on the cycle $(x)-(b)$. In other words, the reciprocity map is merely an "abelianized" Kummer map in this situation. There is no choice but to interprete the reciprocity law [19], [20] as an "abelianized Grothendieck conjecture" over finite fields.

Of course it is hard to imagine exactly what Lang himself found striking in the analogy when he wrote the lines quoted above. What is not hard to imagine is that he would have been very much at home with the ideas surrounding Grothendieck's conjecture and the nonabelian Kummer map.

References

[1] SPENCER BLOCH, Algebraic K-theory and classfield theory for arithmetic surfaces, *Ann. of Math. (2)* **114** (1981), no. 2, 229–265.

[2] FEDOR ALEKSEIVICH BOGOMOLOV, Sur l'algébricité des représentations l-adiques, *C. R. Acad. Sci. Paris Sér. A-B* **290** (1980), no. 15, A701–A703.

[3] *Model Theory and Algebraic Geometry. An Introduction to E. Hrushovski's Proof of the Geometric Mordell-Lang Conjecture*, edited by Elisabeth Bouscaren, Lecture Notes in Mathematics, vol. 1696, Springer-Verlag, Berlin, 1998, xvi+211 pp.

[4] A. BUIUM, Intersections in jet spaces and a conjecture of S. Lang, *Ann. of Math. (2)* **136** (1992), no. 3, 557–567.

[5] CLAUDE CHABAUTY, Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, *C. R. Acad. Sci. Paris* **212**, (1941), 1022–1024.

[6] P. DELIGNE, Le groupe fondamental de la droite projective moins trois points, *Galois Groups over Q* (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 79–297.

[7] CHRISTOPHER DENINGER and ANTHONY J. SCHOLL, *The Beilinson Conjectures. L-functions and Arithmetic* (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, 173–209.

[8] G. FALTINGS, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349–366.

[9] GERD FALTINGS, Diophantine approximation on abelian varieties, *Ann. of Math. (2)* **133** (1991), no. 3, 549–576.

[10] ______, The general case of S. Lang's conjecture. *Barsotti Symposium in Algebraic Geometry* (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182.

[11] WULF-DIETER GEYER, The automorphism group of the field of all algebraic numbers, *Proceedings of the 5th School of Algebra* (Rio de Janeiro, 1978), Soc. Brasil. Mat., Rio de Janeiro, 1978, pp. 167–199.

[12] ALEXANDER GROTHENDIECK, Brief an G. Faltings. London Math. Soc. Lecture Note Ser., vol. 242, *Geometric Galois Actions*, vol. 1, Cambridge Univ. Press, Cambridge, 1997, pp. 49–58.

[13] RICHARD M. HAIN, The geometry of the mixed Hodge structure on the fundamental group. *Algebraic Geometry*, Bowdoin, 1985 (Brunswick, Maine, 1985), pp. 247–282, Proc. Sympos. Pure Math., vol. 46, Part 2, Amer. Math. Soc., Providence, RI, 1987.

[14] RICHARD M. HAIN and STEVEN ZUCKER, Unipotent variations of mixed Hodge structure. *Invent. Math.* **88** (1987), no. 1, 83–124.

[15] EHUD HRUSHOVSKI, The Mordell-Lang conjecture for function fields. *J. Amer. Math. Soc.* **9** (1996), no. 3, 667–690.

[16] IHARA YASUTAKA, Braids, Galois groups, and some arithmetic functions. Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), pp. 99–120, Math. Soc. Japan, Tokyo, 1991.

[17] JAY JORGENSON and SERGE LANG, The ubiquitous heat kernel. *Mathematics Unlimited—2001 and Beyond*, pp. 655–683, Springer, Berlin, 2001.

[18] KAZUYA KATO, p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III. *Astérisque* No. 295 (2004), ix, 117–290.

[19] KAZUYA KATO and SHUJI SAITO, Unramified class field theory of arithmetical surfaces. *Ann. of Math. (2)* **118** (1983), no. 2, 241–275.

[20] ______, Global class field theory of arithmetic schemes. Applications of algebraic K-theory to algebraic geometry and number theory. Parts I, II (Boulder, CO, 1983), pp. 255–331, Contemp. Math., 55, Amer. Math. Soc., Providence, RI, 1986.

[21] NICHOLAS M. KATZ and SERGE LANG, Finiteness theorems in geometric classfield theory. With an appendix by Kenneth A. Ribet. *Enseign. Math. (2)* **27** (1981), no. 3–4, 285–319 (1982).

[22] MINHYONG KIM, The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, *Invent. Math.* **161** (2005), no. 3, 629–656.

[23] ______, The unipotent Albanese map and Selmer varieties for curves. Arxiv math.NT/0510441.

[24] DANIEL S. KUBERT and SERGE LANG, *Modular Units*, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer-Verlag, New York-Berlin, 1981, xiii+358 pp.

[25] SERGE LANG, Unramified class field theory over function fields in several variables, *Ann. of Math. (2)* **64** (1956), 285–325.

[26] ______, Sur les séries L d'une variété algébrique, *Bull. Soc. Math. France* **84** (1956), 385–407.

[27] ______, Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.

[28] ______, Integral points on curves, *Inst. Hautes Etudes Sci. Publ. Math.*, No. 6 (1960), 27–43.

[29] ______, Division points on curves, *Ann. Mat. Pura Appl.* (4) **70** (1965), 229–234.

[30] ______, Higher dimensional diophantine problems, *Bull. Amer. Math. Soc.* **80** (1974), 779–787.

[31] ______, Units and class groups in number theory and algebraic geometry, *Bull. Amer. Math. Soc. (N.S.)* **6** (1982), no. 3, 253–316.

[32] ______, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983, xviii+370 pp.

[33] ______, *Cyclotomic Fields I and II.* Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, xviii+433 pp.

[34] ———, Hyperbolic and Diophantine analysis, *Bull. Amer. Math. Soc. (N.S.)* **14** (1986), no. 2, 159–205.
[35] ———, *Introduction to Complex Hyperbolic Spaces*, Springer-Verlag, New York, 1987, viii+271 pp.
[36] ———, *Number Theory. III. Diophantine Geometry*. Encyclopaedia of Mathematical Sciences, vol. 60, Springer-Verlag, Berlin, 1991, xiv+296 pp.
[37] SERGE LANG and JEAN-PIERRE SERRE, Sur les revêtements non ramifiés des variétés algébriques, *Amer. J. Math.* **79** (1957), 319–330.
[38] SERGE LANG and JOHN TATE, Principal homogeneous spaces over abelian varieties, *Amer. J. Math.* **80** (1958), 659–684.
[39] MICHAEL MCQUILLAN, Division points on semi-abelian varieties, *Invent. Math.* **120** (1995), no. 1, 143–159.
[40] JAMES S. MILNE, *Étale Cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, NJ, 1980, xiii + 323 pp.
[41] SHINICHI MOCHIZUKI, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, *J. Math. Sci. Univ. Tokyo* **3** (1996), no. 3, 571–627.
[42] HIROAKI NAKAMURA, Galois rigidity of the étale fundamental groups of punctured projective lines, *J. Reine Angew. Math.* **411** (1990), 205–216.
[43] BERNADETTE PERRIN-RIOU, Fonctions L p-adiques. Proceedings of the International Congress of Mathematicians, Vols. 1, 2 (Zürich, 1994), pp. 400–410, Birkhäuser, Basel, 1995.
[44] M. RAYNAUD, Sous-variétés d'une variété abélienne et points de torsion, *Arithmetic and Geometry*, Vol. I, pp. 327–352, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983.
[45] Revêtements étales et groupe fondamental. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1). Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud. Lecture Notes in Mathematics, vol. 224, Springer-Verlag, Berlin-New York, 1971, xxii+447 pp.
[46] AKIO TAMAGAWA, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), no. 2, 135–194
[47] PAUL VOJTA, Siegel's theorem in the compact case, *Ann. of Math. (2)* **133** (1991), no. 3, 509–548.
[48] ANDRÉ WEIL, Généralisations des fonctions abéliennes, *J. Math. Pures Appl.* 9 **17**, 47–87.
[49] ANDREW WILES, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

Serge Lang and the Heat Kernel

Jay Jorgenson

Beginning in the early 1990s, Serge Lang viewed the heat kernel and heat kernel techniques as a potentially unlimited source of mathematics which would touch many fields of study. In [19] we presented an argument supporting the term "the ubiquitous heat kernel" by citing numerous results where the heat kernel played a prominent role. In Lang's own writing, one can see the incorporation of the heat kernel in several places, including: The Weierstrass approximation theorem and Poisson summation formula in [26], the explicit formulas for number theory in [25], the Gamma function in [27], and the background for the entire development in [28]. Lang's fascination with the heat kernel was so thorough that, according to Peter Jones, Serge began referring to himself as "an analyst" when asked to describe his research interests.

From the early 1990s until his death in 2005, Serge's own research activities can be described as addressing two points: Analytic aspects of regularized products and harmonic series, and geometric constructions of zeta functions. Both endeavors included heat kernels and heat kernel analysis, and the projects together focused on the long-term goal of developing a theory of "ladders" of zeta functions. I had the unique honor of working with Serge on these and other projects for nearly fifteen years, and I will now describe a portion of the mathematics Serge and I had in mind.

Regularized Products and Harmonic Series

Children learn how to multiply numbers, developing the ability to compute the product of a finite set of numbers. The astute student will realize they actually can evaluate the product of a countably infinite set of numbers provided that all but a finite number of terms in the product are equal to one. In undergraduate analysis courses, students study a slight perturbation of the elementary setting, namely when the terms in the countably infinite sequence approach one sufficiently fast. The convergence result established also demonstrates that when evaluating the infinite product, one can simply multiply a sufficiently large number of terms in the sequence and obtain an answer quite close to the theoretical result which exists for the infinite product. This connection with the elementary situation is intuitively consistent with that which is learned in childhood.

In another direction, one can seek other mathematical means by which one can determine the product of a finite sequence and then study the situations when the definition extends. For example, let $A = \{a_k\}$ with $k = 1, \ldots, n$ be a finite sequence of real, positive numbers, and let

$$(1) \qquad \zeta_A(s) = \sum_{k=1}^{n} a_k^{-s},$$

which we consider as a function of a complex variable s. Elementary calculus applies to show that

$$(2) \qquad \prod_{k=1}^{n} a_k = \exp(-\zeta_A'(0)).$$

Jay Jorgenson is a professor of mathematics at City College of New York and the Graduate Center. His email address is `jjorgenson@mindspring.com`.

In words, a special value of the zeta function (1) can be used to realize a product of the elements of the finite set of numbers A.

To generalize (2), we seek to describe the countably infinite sets of numbers for which (2) makes sense. Perhaps the first example to consider is $A = \mathbf{Z}_{>0}$, the set of natural integers, so then $\zeta_A(s)$ is the Riemann zeta function. Classically, it is known that the Riemann zeta function admits a meromorphic continuation to all $s \in \mathbf{C}$ and is holomorphic at $s = 0$. Furthermore, it can be easily shown (using the functional equation of the Riemann zeta function) that $-\zeta'_{\mathbf{Z}_{>0}}(0) = \log(\sqrt{2\pi})$, which leads to the remark "infinity factorial is equal to $\sqrt{2\pi}$". Of course, such a comment needs to be understood in the sense of (2) and meromorphic continuation.

More generally, we define a countably infinite sequence $A = \{a_k\}$ to have a *zeta regularized product*, or *regularized product*, if the zeta function

$$\zeta_A(s) = \sum_{k=1}^{\infty} a_k^{-s}$$

converges for $s \in \mathbf{C}$ with $\mathrm{Re}(s)$ sufficiently large, admits a meromorphic continuation at $s = 0$, and is holomorphic at $s = 0$. With these conditions, the regularized product of the elements of A is defined by the special value of the zeta function as in (2). The problem which naturally arises is to determine the conditions on the sequence A for which a regularized product exists. For this, we rewrite the zeta function ζ_A as

$$\zeta_A(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \theta_A(t) t^s \frac{dt}{t} \tag{3}$$

where

$$\theta_A(t) = \sum_{k=1}^{\infty} e^{-a_k t} \tag{4}$$

and $\Gamma(s)$ is the Gamma function. As further background, we refer to the articles [1] and [29], which discuss some of the important roles played by the zeta regularized products.

The first part of my work with Lang appeared in [14] and [15]. The paper [14] establishes general conditions for theta functions which will lead to regularized products as well as to regularized harmonic series. As an example of the type of general computations in [14], a connection is made relating zeta regularized products with Weierstrass products from complex analysis, which we call the Lerch formula, thus establishing a relation with the elementary notion of infinite products of numbers which approach one sufficiently fast.

Further analysis in [15] and [17] leaned toward a type of formal analytic number theory associated with regularized products. Functional equations of zeta functions were shown to be equivalent to inversion formulas for the associated theta functions, so then one is drawn to study theta functions rather than zeta functions in this context. In the development of the explicit formulas, the Weil functional comes from evaluating a complex integral involving the multiplicative factors in the functional equations of zeta functions. If the multiplicative factors are assumed to be expressed in terms of regularized products, then in [15] it is shown that the Weil functional can be evaluated in terms of a Parseval-type formula, so again one is seeking theta functions with certain properties, this time for the factors in the functional equations.

Quite naturally, the problem which arises is to characterize sequences from which one can obtain regularized products. From (3), this problem amounts to determining sequences whose associated theta function admits certain asymptotic behaviors as t approaches zero and infinity. From Riemannian geometry, theta functions naturally appear as the trace of heat kernels associated to certain differential and pseuo-differential operators. The asymptotic conditions defined in [14] were established with the heat kernel in mind.

From analytic number theory, where one does not know if an appropriate operator exists, an obvious sequence to study is given by the nontrivial zeros of a zeta function. In [2] Cramér studied the theta function

$$\theta_{\mathbf{Q}}(z) = \sum_{\rho} e^{\rho z}, \tag{5}$$

where the sum is over the zeros of the Riemann zeta function with positive imaginary part, which we denote by $A^+(\mathbf{Q})$, and with $z \in \mathbf{C}$, again having positive imaginary part. Cramér's results in [2] consisted of two main parts: The theta function (5) admits a branched meromorphic continuation to all $z \in \mathbf{C}$, and the singularities of the continuation of (5) are at points of the form $\pm i \log p^n$ for a positive integer n and a prime number p; and if we set $z = it$ for $t \in \mathbf{R}_{>0}$, then (5) satisfies the asymptotic conditions required of a theta function (4) in order to form a regularized product from the sequence $A^+(\mathbf{Q})$. Cramér's theorem forms a key component in Deninger's program [3], which has the goal of developing a cohomological approach to analytic number theory (see also [29] and [31]).

In [16] and [18] Lang and I extended Cramér's theorem to a wide range of zeta functions which satisfy very general conditions. In addition, in [20] we extended Guinand's results from [7], [8], and [9] which proved, among other theorems, several functional relations for Cramér's function. The point of view taken in [16], [18] and [20] is to "load an induction", as Lang would say, by placing various hypotheses on the factors in the functional equation; specifically, it was assumed that the factors in the functional equations could be expressed as regularized products. With this hypothesis and other general assumptions such as the existence of an Euler product, or Bessel sum, expansion, it was proved that the original zeta function could be expressed as regularized products. As an example, since the Gamma function can be expressed as a regularized product, which comes from the first example mentioned above, we concluded that the Riemann zeta function is also expressible as regularized products. A similar argument applies to virtually all zeta functions from number theory.

Turning to geometry, one can define a (Selberg) zeta function associated to any finite volume hyperbolic Riemann surface (see [10] and references therein for a complete development of the Selberg zeta function in this context). In the case when the surface is compact, the known functional equation and Euler product expansions allow one to apply the results from [16] to conclude that the Selberg zeta function can be expressed as regularized products, re-proving a known result from [4] and [30]. For noncompact yet finite volume surfaces, attempts were made to express the Selberg zeta function as a regularized product, but the successful results required the surface to be arithmetic. Using the results from [16], we were able to conclude that the Selberg zeta function in general is a regularized product through the induction we defined. The most interesting example for us was the Selberg zeta function associated to the discrete group $\mathrm{PSL}(2, \mathbf{Z})$, since the functional equation involves the Riemann zeta function, thus producing the following finite "ladder" of functions: the Gamma function, the Riemann zeta function, and the Selberg zeta function for $\mathrm{PSL}(2, \mathbf{Z})$. As stated, a direct calculation shows that the Gamma function is a regularized product, and the induction hypothesis from [16] implies that the Riemann zeta function and then the Selberg zeta function for $\mathrm{PSL}(2, \mathbf{Z})$ are expressible as regularized products.

Constructions from Geometry

What is the next step in the "ladder" of zeta functions? Lang and I believed that one can construct zeta functions using heat kernel analysis on symmetric spaces, resulting in an infinite "ladder" of zeta functions with functional equations involving zeta functions on the lower levels. Consider a general setting involving a symmetric space X and discrete group Γ with finite volume and noncompact quotient $\Gamma\backslash X$. As described in [23], the procedure we propose is the following: Start with a heat kernel on X, periodize with respect to Γ, evaluate a regularized trace of the heat kernel, and then compute a certain integral transform (the Gauss transform, which is the Laplace transform with a quadratic change of variables) of the regularized trace of the heat kernel. The resulting object is our proposed zeta function associated to $\Gamma\backslash X$. In the work we were undertaking, Lang and I were focusing our attention on the symmetric spaces associated to $\mathrm{SL}(n, \mathbf{C})$, though one certainly could consider the spaces associated to $\mathrm{SL}(n, \mathbf{R})$. By taking $\Gamma = \mathrm{SL}(n, \mathbf{Z})$ and $G = \mathrm{SL}(n, \mathbf{R})$, we felt that one could obtain an infinite "ladder" of zeta-type functions for each $n \geq 2$, with the case $n = 2$ yielding the Selberg zeta function. Furthermore, we believe that the functional equation for the zeta function at level n will involve all zeta functions from lower levels, as demonstrated by the case $n = 2$.

In [21], [22], and [23], Lang and I initiated our program of study, which I plan to continue. In particular, in [22] we defined Eisenstein series obtained by "twisting with heat kernels rather than automorphic forms," as Lang would say, and we proposed what can be viewed as a repackaging of spectral decompositions in terms of heat Eisenstein series. At this stage, we felt that one could already see new relations involving zeta functions, namely that the constant term of Fourier expansions of heat Eisenstein series should involve the Selberg zeta function of lower levels. One implication of such a result would be an identity involving L-functions and zeta functions which would follow by comparing the Fourier coefficients in the heat Eisenstein series with the sum of Fourier coefficients of Eisenstein series attached to automorphic forms, which are known to be expressible in terms of L-functions (see [6] and references therein).

Recent Developments

Throughout our time together Lang remained optimistic that our proposed "ladder" of zeta functions would provide new ideas in analytic number theory. Admittedly, many of our concepts have yet to be fully tested; only future endeavors will determine if Lang's belief in our program of study was well founded.

Beyond our own work, there have been many developments in mathematics which Lang would have pointed to as providing further support for his faith in the heat kernel. Certainly, the successful completion of the Poincaré conjecture is one instance where heat kernel ideas have played a role. In [5] the author states the need for a "second independent proof of the Moonshine conjectures" and states that the heat kernel could provide one possibility. Lang would have been thrilled by this statement. Serge was very taken by the article [24], where the authors consider spectral theory and spectral expansions on the spaces $n\mathbf{Z}\backslash\mathbf{Z}$, showing that even in the case when $n = 1$ the results are nontrivial. In my own work with Kramer, we have used the heat kernel associated to the hyperbolic metric to obtain new expressions for the analytic invariants of the Arakelov theory of algebraic curves; see [11] and [12]. In recent developments, we have shown that by taking the Rankin-Selberg integral of an identity from [11], one obtains theta-function type expressions involving certain L-functions attached to nonholomorphic Maass forms, ultimately obtaining an identity in terms of the certain L-function attached to an orthonormal basis of holomorphic weight two forms; the full development of this identity is presented in [13]. In some ways, the work in [13] relates to one of the first steps envisioned by Lang and me, namely the uncovering of new relations, possibly regularized in some sense, involving known and new zeta functions.

Soon after Lang and I completed the article [19], we discussed at length the ideas and hopes we had for the results one could obtain from "ladders". At one point he said to me, "I wish I were thirty years old again so I could concentrate on the heat kernel." Given the way Serge devoted his life to mathematics, let us take that statement as summarizing his sincere and profound belief in the strength of the heat kernel and heat kernel analysis.

References

[1] P. CARTIER and A. VOROS, Une nouvelle interprétation de la formule des traces de Selberg. In: *The Grothendieck Festschrift*, Vol. II, pp. 1–67, Progr. Math., **87** (1990), Birkhäuser Boston, Boston, MA.

[2] H. CRAMÉR, Studien über die Nullstellen der Riemannschen Zetafunktion. *Math. Zeit* **4** (1919), 104–130.

[3] C. DENINGER, Local L-factors of motives and regularized determinants. *Invent. Math.* **107** (1992), 135–150.

[4] E. D'HOKER and D. H. PHONG, On determinants of Laplacians on Riemann surfaces. *Comm. Math. Phys.* **104** (1986), 537–545.

[5] T. GANNON, Monstrous Moonshine—The first twenty-five years. *Bull. London Math. Soc.* **38** (2006), 1–33.

[6] D. GOLDFELD, *Automorphic Forms and L-Functions for the Group* $GL(n, \mathbf{R})$). Cambridge Studies in Advanced Mathematics, vol. 99, Cambridge University Press, Cambridge, UK, 2006.

[7] A. GUINAND, A class of self-reciprocal functions connected with summation formulae, *Proc. London Math. Soc (2)* **43** (1937), 439–448.

[8] ———, A summation formula in the theory of prime numbers, *Proc. London Math. Soc (2)* **50** (1949), 107–119.

[9] ———, Fourier reciprocities and the Riemann zeta function, *Proc. London Math. Soc (2)* **51** (1950), 401–414.

[10] D. HEJHAL, *The Selberg trace formula for* $\mathrm{PSL}_n(\mathbf{R})$, *Vol. 2*, Lecture Notes in Mathematics, vol. 1001, Springer-Verlag, New York, 1983, xii+806 pp.

[11] J. JORGENSON and J. KRAMER, Expressing Arakelov invariants using hyperbolic heat kernels, in: *The Ubiquitous Heat Kernel*, ed. J. Jorgenson and L. Walling, Contemp. Math., vol. 398, Amer. Math. Soc., Providence, RI, 2006, pp. 295–309.

[12] ———, Bounds on Faltings's delta function through covers, to appear in *Ann. of Math.*

[13] ———, A summation formula relation Fourier coefficients of Maass formulas and Fourier coefficients of holomorphic weight two forms, in preparation.

[14] J. JORGENSON and S. LANG, Complex analytic properties of regularized products and series. In *Basic Analysis of Regularized Products and Series*, Springer Lecture Notes in Mathematics, vol. 1564, 1993, pp. 1–88.

[15] ———, A Parseval formula for functions with a singular asymptotic expansion at the origin. In *Basic Analysis of Regularized Products and Series*, Springer Lecture Notes in Mathematics, vol. 1564, 1993, pp. 89–122.

[16] ———, On Cramér's theorem for general Euler products with functional equation, *Math. Ann.* **297** (1993), 383–416.

[17] ———, Explicit formulas for regularized products and series. In *Explicit Formulas*, Springer Lecture Notes in Mathematics, vol. 1593, 1994, pp. 1–134.

[18] ———, Extension of analytic number theory and the theory of regularized harmonic series from Dirichlet series to Bessel series, *Math. Ann.* **306** (1996), 75–124.

[19] ———, The ubiquitous heat kernel. *Mathematics Unlimited—2001 and Beyond*, pp. 655–683, Springer, Berlin, 2001.

[20] ———, Guinand's theorem and functional equations for the Cramér function, *J. Number Theory* **86** (2001), 351–367.

[21] ———, The heat kernel and theta inversion on $\mathrm{SL}_2(\mathbf{C})$, Springer-Verlag, New York, to appear.

[22] ———, Heat Eisenstein series on $\mathrm{SL}_n(\mathbf{C})$, *Memoirs AMS*, to appear.

[23] ———, The heat kernel, theta inversion and zetas on $\Gamma\backslash G/K$, to appear.

[24] ANDERS KARLSSON and MARKUS NEUHAUSER, Heat kernels, theta identities, and zeta functions on cyclic groups, in: *Topological and Asymptotic Aspects of Group Theory*, ed. R. Grigorchuk, M. Mihalik, M. Sapir, and Z. Sunik, Contemp. Math., vol. 394, 2006, pp. 177–189.

[25] S. LANG, *Algebraic Number Theory*, second edition. Springer-Verlag, New York, 1994, xiii + 357 pp.

[26] ———, *Undergraduate Analysis*, second edition. Springer-Verlag, New York, 1997, xvi + 642 pp.

[27] ———, *Complex Analysis*, fourth edition. Springer-Verlag, New York, 1999, xiv + 485 pp.

[28] ———, *Fundamentals of Differential Geometry*. Springer-Verlag, New York, 1999, xvii + 535 pp.

[29] Y. MANIN, Lectures on zeta functions and motives (according to Deninger and Kurokawa). In: *Columbia University Number Theory Seminar*, Astérisque **228** (1995), 12-1-164.

[30] P. SARNAK, Determinants of Laplacians, *Comm. Math. Phys.* **110** (1987), 113–120.

[31] M. SCHROETER and C. SOULÉ, *On a result of Deninger concerning Riemann's zeta function*, Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, vol. 55, 1994, pp. 745–747.