Curr. Dev. Math. (1997) 199 - 203

Open Problems in Number Theory

Barry Mazur

Department of Mathematics
Harvard University

Number Theory has a rich assortment of ancient and modern problems, many of which have been extensively formulated and discussed in the literature. Four problems in Number Theory were contributed (to the Number Theory portion of **"Open Problems"**), each of which is either new, or else is a new suggestion regarding one of our more well known ones.

1. On Newforms, central values, and Siegel zeroes.

Let N be a larger prime, and let $H_2^+(N)$ be set of newforms of weight two for $\Gamma_0(N)$ whose L-functions have even functional equation. We (Iwaniec-Sarnak) have recently proven that as $N \to \infty$ at least 50% of the central values of $L(_{s,f})$ for f in $H_2^+(N)$ are larger than $(log\mathrm{N})^{-2}$.

Problem A. Show that more than 50% of these central values are nonzero.

Problem B. Better still, show that more than 50% of the central values are larger than $(log\mathrm{N})^{-A}$ for some positive constant A.

One of the consequences of our recent work, is that a solution to **Problem B** implies that there are no Siegel zeros! Of course, in view of the connection via the Birch-Swinnerton Conjectures and what is known

about them, one can formulate these problems in terms of the ranks of $J_0(N)/\mathbf{Q}$ and their quotients.

(Submitted by Henry Iwaniec and Peter Sarnak.)

2. Intelligent counting of rational points.

Let (V, L) be a projective manifold over a number field k endowed with a metrized ample sheaf allowing one to construct the height function $h_L : V(k) \to \mathbb{R}$. The naive problem of finding asymptotics for the number of k–points of bounded height has the refined version: to understand the analytic properties of the height zeta–function $Z(V, L; s) = \sum_x h_L(x)^{-s}$.

Unfortunately, it seems that if V is not homogeneous or something like that, $Z(V, L; s)$ does not have good analytic properties, unlike the more traditional Hasse–Weil–Serre– ... L–functions.

The problem I want to draw attention to is:

Find a class of good generating series counting $V(k)$.

The model I have in mind is that of Gromov–Witten invariants and quantum cohomology which provide absolutely remarkable functions counting rational curves instead of rational points.

The geometric framework for this counting is highly non–trivial and involves drastic redefinition of the naive prescription, even if one speaks about rational curves on three–dimensional quintics. The redefinition achieves the goal of moving the problem to general position in a quite sophisticated way.

An arithmetical version of this theory, if it can be built, would require a deformation theory of embedded arithmetic curves. It would be a test of maturity of Arakelov geometry, applicable to the case of manifolds with many rational points where precise analytic results are expected, as opposed to manifolds with finite number of points where qualitative results already make us happy.
(Submitted by Yuri Manin.)

References

Yu. Manin. Problems on rational points and rational curves on algebraic varieties. *Surveys in Differential Geometry, vol. 2 (1995), Int. Press, 214–245.*

M. Kontsevich, Yu. Manin. Gromov–Witten classes, quantum cohomology, and enumerative geometry. *Comm. Math. Phys., 164:3 (1994), 525–562.*

K. Behrend. Gromov–Witten invariants in algebraic geometry. *Inv. Math., 127 (1997), 601–617.*

3. Finiteness Questions

a) Concerning the Galois group of $\mathbb{Q}$

Let K be a number field contained in $\mathbb{C}$ and S a finite set of places of $\mathbb{Q}$ (possibly including archimedean places). Let $G_{K,S}$ be the Galois group of the maximal algebraic subfield of $\mathbb{C}$ which is unramified outside of S. It has been an open question for over three decades (e.g., as raised in articles of Shafarevich in *Algebraic Number Fields*, Proc. Intl. Cong. Math. Stokholm 1962) to determine whether or not $G_{K,S}$ is topologically finitely generated. It is, however, long well known that the topological group $G_{K,S}$ does have the property that the abelianization H^{ab} of any open subgroup $H \subset G_{K,S}$ of finite index is topologically finitely generated. Using the fundamental isomorphism of Class Field Theory one can even find an explicit finite system of topological generators for H^{ab}. Moreover, Leopoldt's conjecture (still, in general, outstanding) would allow us to give a simple formula for the minimal number of elements needed to generate a subgroup of H^{ab} of finite index.

In particular, in the cases where $G_{K,S}$ itself is abelian, $G_{K,S}$ *is* topologically finitely generated, although there only finitely many such examples known and in these known cases S is contained in the set of infinite places.

Problem: Can one find instances where $G_{\mathbb{Q},S}$ is abelian when S contains at least one finite prime?

Note that if S contains the prime at infinity, and at least one finite prime p, then $G_{\mathbb{Q},S}$ is non-abelian since all p-adic Galois representations attached to cuspidal newforms of level a power of p factor through $G_{\mathbb{Q},S}$.

Is $G_{\mathbb{Q},S}$ abelian for $S = \{2\}$ or $S = \{3\}$ or $S = \{5\}$? As Lenstra pointed out, one can use the reflection principle to show, it is not abelian when $S = \{37\}$.

b) Concerning points on curves

Suppose X is a curve over a field of characteristic 0 and $\pi\colon A \to X$ is an abelian scheme over X. Let Γ be a group of sections of π and suppose there is no element of Γ which factors through a subfamily of group varieties of relative dimension one. For $P \in X(\bar{K})$, let Γ_P be the fiber of Γ above P. Then show for all but finitely many P.

$$rank(\Gamma_P) = rank(\Gamma).$$

This statement implies both the Manin-Mumford conjecture (Raynaud's theorem) and the Mordell conjecture (Faltings' theorem). Indeed, suppose X is complete. Let J be its Jacobian, and $a\colon X \to J$

be an Albanese morphism, $A = X \times J$, and π the first projection. Let $M \subset J(K)$ be a subgroup of finite rank. Finally, let Γ be the group generated by the sections of $A \to X$, $\{x \mapsto (x, m) : m \in M\}$ and $x \mapsto (x, a(x))\}$. Then the rank of Γ_P is less than $rank(M) + 1$ only when $a(P)$ is a point in the smallest divisible subgroup of $J(K)$ group containing M. When K is a number field and M is the Mordell-Weil group $(*)$ is Mordell's conjecture and when K is algebraically closed and $M = 0$, $(*)$ is the Manin-Mumford conjecture.

c) Concerning Endomorphism Rings

Let K be a number field and g a positive integer. Then show that the number of distinct endomorphism rings of abelian varieties of dimension g defined over K is finite. This is known when $g = 1$. When $g = 2$ it implies theorems (qualitatively) of Mazur and Merel. Indeed, if E and E' are two non-CM elliptic curve there is a cyclic N-isogeny between them then the endomorphism ring of $E \times E'$ is isomorphic to $\Gamma_0(N)$. If they are not isogenous but there exists a Galois isomorphism ϕ: $E[N] \to E'[N]$, then the endomorphism ring of the quotient of $E \times E'$ by the graph of ϕ has endomorphism ring $\{(a, b : a, b \in \mathbb{Z}, a \equiv b modulo N\}$.

(Submitted by Robert Coleman.)

4. On the S-unit equation and polylogarithms.

If S is a finite set of rational primes, let $X(S)$ denote the set of rational numbers $x \in \mathbb{Q}$ such that both x and $1 - x$ are S-units, and denote by $N(s)$ the maximum of the cardinalities $|X(S)|$ as S ranges through all finite sets of primes with $|S| = s$. By results of Evertse, one has that $N(s) \leq 1000 \cdot 50^s$, and by results of Erdös-Stewart-Tijdeman one has that $N(s)$ is bounded from below by $\exp\left((2 - o(1))\sqrt{\frac{s}{\log s}}\right)$ for large s. One expects $N(s) = \exp(s^{\frac{2}{3}+o(1)})$. For general number fields the analogue of Evertse's result still holds (with an appropriately modified bound) but the situation for the lower bound is less clear.

The functionfield analogue of these problems has direct applications to the existence of nontrivial functional equations for polylogarithms, and deserves to be studied.

Specifically let $S = \{P_1, \ldots, P_s\}$ be a finite set of irreducible polynomials in $\mathbb{Z}[t]$ and let $X(S)$ denote the set of $x \in \mathbb{Z}[t][1/P_1, \ldots, 1/P_s]$ such that both x and $1 - x$ are units. This is a finite set $[L]$.

Problem: Is there a lower bound for $|X(S)|$ (or for the maximum of the cardinalities $|X(S)|$ ranging over sets S with $|S| = s$) which grows more than polynomially in s?

Aproof of this would imply the existence of non-trivial functional equations for polyligarithms at any level, by the result of [Z], §7. Specifically, an element of the m -th Bloch group for $\mathbb{Q}(t)$ is a functional equation for $Li_m(z)$, and the number of conditions required to make an element $\sum n_i[x_i] \in \mathbb{Q}[X(S)]$ belong to the m-th Bloch group grows like s^m.

[L] S.Lang: Integral points on curves, Publ. Math. IHES **6** 1960 27-43.

[Z] D.Zagier: Polylogarithms, Dedekind zeta functions, and the algebraic K - theory of fields, in *Arithmetics Algebraic Geometry* (eds. G. van der Geer, F. Oort, J. Steenbrink), Prog. in Math. **89**, Birkhäuser, Boston 1991, 391-430.

(Submitted by Don Zagier.)