AI and Number Theory

May 2026

Notes by Jane Shi, with assistance from the workshop participants

This problem list is an outcome of the workshop "AI and Number Theory" held at the American Institute of Mathematics in the Merkin Center for Pure and Applied Mathematics on the campus of Caltech in Pasadena, CA. The workshop was sponsored by AIM, Harmonic, AWS Automated Reasoning, and the NSF.

The ordering within each section is for organizational purposes, and *distinctly not* an ordering of perceived importance or difficulty.

1 Big problems

These problems are generally viewed to be out of reach of current methods and likely will require new ideas in order to be resolved. Many of the questions in this section serve as motivation for current research.

Problem 1. Prove that $n^2 + 1$ is prime infinitely often.

Problem 2. Legendre's conjecture. Prove that for every $n \geq 1$ there is a prime between n^2 and $(n+1)^2$.

Problem 3. Prove Goldbach's conjecture. Every even number exceeding 2 is the sum of two prime numbers.

Problem 4. Prove that there exist infinitely many twin primes.

Problem 5. Prove that $L(s, \chi) > 0$ for $0 < s < 1$ and any quadratic character χ.

Problem 6. The Birch and Swinnerton-Dyer conjecture.

Or progress toward BSD in the form: an inequality between the rank of the elliptic curve and the order of vanishing of the L-function.

Problem 7. The Lindelöf Hypothesis.

Or progress toward LH in the form: $\zeta\left(\frac{1}{2} + it\right) \ll t^{\frac{1}{8}}$

Problem 8. (Gauss) Prove there are infinitely many fundamental discriminants $d > 0$ such that $\mathbb{Q}(\sqrt{d})$ has unique factorization.

Problem 9. The error term in the Dirichlet divisor problem is $O(x^{\frac{1}{4}+\varepsilon})$.

Problem 10. Ranks of elliptic curves $E/\mathbb{Q}$ are bounded.

Note: if ranks are unbounded, it is possible that AI could discover a construction which creates such examples.

Problem 11. Waring's problem: let $G(k)$ denote the smallest number s such that all large natural numbers n are the sum of s positive integral k-th powers. Prove that for all natural numbers k one has $G(k) \leq 4k$, and that provided that congruence conditions are met, then $k + 1$ variables suffice.

Or progress of the form $G(k) = O(k)$ for large k.

Problem 12. A polynomial time factoring algorithm.

Or progress in the form of an $L(\delta)$ algorithm for some $\delta < \frac{1}{10}$.

Problem 13. Find a deterministic polynomial-time algorithm for primitive roots mod$p$, for p prime, without assuming GRH?

Problem 14. Show the Euler–Mascheroni constant γ is irrational.

Problem 15. Show that all the non-trivial zeros of the Riemann zeta function are simple.

Problem 16. The zeros of the Riemann zeta-function are linearly independent over the rationals.

Problem 17. The Riemann hypothesis.
Or progress toward RH in the form: there are no zeros to the right of 0.99999.
Or progress in the form: prove that 100 percent of the zeros of $\zeta(s)$ lie on the 1/2 line.

Problem 18. The uniform boundedness conjecture in arithmetic dynamics.

- Uniform bounds for rational preperiodic points of unicritical (univariate) polynomials.
- (even more specialized) Uniform bounds for rational preperiodic points of quadratic (univariate) polynomials.

Problem 19. The inverse Galois problem.

- AI possibly could help solve it for specific groups, like M_{23}, but not in general.

Problem 20. (Erdős) Can one walk to infinity on Gaussian primes taking only steps of bounded size?

Problem 21. Prove that

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^6\ dt \sim 42 \prod_p \left(1+\frac{4}{p}+\frac{1}{p^2}\right)\left(1-\frac{1}{p}\right)^4 \frac{\log^9 T}{9!}$$

A lower bound with 42 replaced by 34.1 is known. It is known that there is an upper bound with 42 replaced by a large number, conditional on RH, but a specific bound has not been calculated. Prove, unconditionally, that for any $\epsilon > 0$, a lower bound with 42 replaced by $42 - \epsilon$ is true.

Asked by Brian Conrey

2 Problems where AI might be helpful

It is possible, maybe even likely, that AI can be of assistance in attacking the following problems. The problems are categorized according to the expected nature of the assistance.

2.1 AI might help with computation/manipulation

(As in human guidance + AI-performed computations can be helpful)

Problem 22. Let $f(s)$ be the Riemann–Siegel function. Prove that most of the zeros of $f(s)$ lie to the left of the 1/2-line.

Asked by Brian Conrey

Problem 23. Prove the exact value of the rank of the Elkies–Klagsbrun elliptic curve (which has rank ≥ 29.
This is a specialization of the more general problem of making an algorithm to determine the rank of any elliptic curve.

Problem 24. (Gauss' circle problem.) Prove that the number of lattice points inside a circle of radius r is

$$\pi r^2 + O(r^{1/2+\epsilon}).$$

Problem 25. Prove that for any $\epsilon > 0$ there is a number $C_\epsilon > 0$ such that the number of solutions of

$$n = xyz + x + y + z$$

is

$$\leq C_\epsilon n^\epsilon.$$

Asked by Brian Conrey

Problem 26. What is a lower bound for $\log \|\Delta(P(x))\|/d \log d$? (With Littlewood polys)

Problem 27. Assume RH. Let $0 < \gamma_1 < \gamma_2 < \dots$ denote the ordinates of zeros of $\zeta(s)$. Find good values of $c > 0$ such that

$$\gamma_{n+1} - \gamma_n < c\frac{2\pi}{\log n}$$

holds for infinitely many n. The best value of such a c that is currently known is $c = 0.515396$. A value of $c < 1/2$ would have implications for Landau-Siegel zeros. Can one get to $c = 1/2 + \epsilon$ for any $\epsilon > 0$?

Asked by Brian Conrey

Problem 28. Improve/study the Stoll bounds on $\#X(\mathbb{Q})$ for X a hyperelliptic curve of genus 3 or more and and $\operatorname{rk} \operatorname{Jac}(X)(\mathbb{Q}) \leq g - 3$.

Problem 29. Use Selberg's method for $\zeta(s)$ in the case of modular form L-function and get explicit constants.

Asked by Micah Milinovich

Problem 30. In the moduli space of curves of genus 4: what is the dimension of the supersingular locus? How many components does it have?

Asked by Rachel Pries

2.2 AI might have useful suggestions

Problem 31. Prove that 100 percent of zeros of $\zeta(s)$ are simple.

Problem 32. Prove that a primitive degree 2 L-function has $\gg T^{1-\epsilon}$ simple zeros up to a height T.

Asked by Brian Conrey

Problem 33. Suppose

$$s(t) = \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{a_n}{n} \sin(2\pi n t),$$

with $a_n \in \{\pm 1\}$ completely multiplicative. Must we have

$$\sup_t |s(t)| \geq \frac{1}{2} \quad ?$$

Computationally, $\sup_t |s(t)| \geq 0.43$.

Asked by Jonathan Bober

Problem 34. Show that the Dirichlet series associated to any half-integral weight modular Hecke eigencuspform has at least one zero off the critical line.

Asked by David Lowry-Duda

Problem 35. Erdős–Ingham conjecture: Prove that $1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{5^s}$ has no zeros on the 1-line.

Problem 36. Are there infinitely many long intervals with no twin primes?
i.e. no twin primes in $(n, n + f(n)\log(n)^2)$ for infinitely many n, where $f(n) \to \infty$.

Asked by Mayank Pandey

Problem 37. Generalize known methods for Fano varieties to count points on stacks.

Asked by Brandon Alberts

Problem 38. Prove that there exists a primitive degree 3 L-function (in the Selberg class) with infinitely many zeros on the 1/2-line.

Problem 39. Prove that

$$2^k \left\{ \frac{3}{2} \right\}^k + \left\lfloor \frac{3}{2} \right\rfloor^k \leq 2^k$$

for all k. Implications for the value of $g(k)$ in Waring's problem.

This has been numerically verified for k up to $471,600,000$.

Asked by Trevor Wooley

Problem 40. Show that all sufficiently large numbers are sums of 4 positive cubes.

Is 1290740 the largest number that is not a sum of 5 positive cubes?

Asked by Kevin McCurley

Problem 41. Improve the bound of multiplicities of nontrivial zeroes of $\zeta(s)$.

Problem 42. Show there there are no elements in the Selberg class of L-functions with degree $2 < d < 3$.

2.3 AI might be able to generate useful examples

Problem 43. Determine which Salem numbers appear as the dynamic degree of an automorphic algebraic surface.

Problem 44. Tightly biased prime races? Skewes numbers?

Asked by Andrew Pearce-Crump

Problem 45. Find an elliptic curve with rank 30.

Asked by Brian Conrey

Problem 46. Prove that you can pack, without overlapping,

$$x^2 + O(x^{1/2+\epsilon})$$

unit squares inside a (big) square of side-length x.

Asked by Brian Conrey

Problem 47. Find regions or points on the half-line where $|\zeta\left(\frac{1}{2} + it\right)|$ is likely to be large.

Asked by Ghaith Hiary

Problem 48. Find regions on the half line where the zeta function (i.e. $|\zeta(\frac{1}{2} + it)|$) stays small over the span of several zeros.

Asked by David Farmer

Problem 49. Lehmer's question: Is there a polynomial with integer coefficients with Mahler measure between 1 and 1.17?

There is a polynomial of degree 10 with Mahler measure of 1.17 - it is self-reciprocal and it has coefficients in $\{-1, 0, 1\}$.

Two more questions about Mahler measure:

Problem 50. Lehmer's quesiton with the rational integers replaced by $\mathbb{F}_q[t]$?

Asked by Alexandra Florea

Problem 51. Are there polynomials with coefficients in $\{-1, 1\}$ of degree d such that $\frac{M(P)}{\sqrt{d}} \to 1$.

Asked by Jonathan Bober

Problem 52. A special case of a theorem of Stoll: genus 3 hyperelliptic curve (Jacobian rank 0) has at most 67 rational points. (In general, there is a bound for hyperelliptic curves of Jacobian rank $r \leq g-3$.)

So far we have one with 12 rational points $C : y^2 = (x^2-1)(x^2-4)(x^2-9)(x^2-36)$, but we would like curves with more rational points. Can we find one with more than 12?

Or prove the 67 upper bound. What is the actual max number?

If it's not hyperelliptic, but the Jacobian rank $r \leq g-3$, then by work of Katz, Rabinoff, Zureick-Brown there is an upper bound that is quadratic in g.

Asked by Jennifer Balakrishnan

Problem 53. Vandiver's conjecture: does p divide the size of the class group of the maximal real subfield of $\mathbb{Q}(\zeta_p)$?

Problem 54. Is the K-group $K_{12}(\mathbb{Z})$ trivial? (related to Vandiver's conjecture)

2.4 Unsurprising if AI can do in near future

Problem 55. Formalize a proof that the second Euclid-Mullin sequence omits infinitely many primes in LEAN.

Asked by Alyson Deines

Problem 56. Find the explicit constant in Dobrowoski's theorem ("Is GRH useful?")

Problem 57. Can we find elliptic curves with rank greater than or equal to 8 with conductor smaller then currently known?

Problem 58. Determine which finite abelian groups can occur as Jacobians of genus 2 or 3 curves over finite fields?

We know exactly what they are for elliptic curves, we have information for genus 2, but genus 3 is open.

Asked by Jane Shi

Problem 59. Suppose

$$s(t) = \sum_{n=1}^{\infty} \frac{a_n}{t^2+n^2},$$

with $a_n \in \{\pm 1\}$. Show that the number of zeros of $s(t)$ with $|t| < X$ is $o(X)$.

Asked by Jonathan Bober

Problem 60. Find the value of $a < 10^{20}$ such that the least value of $x > 0$ for which $x^{12} + a$ is prime is as large as possible.

Asked by Brian Conrey

For example, $x^{12} + 488669$ is composite for $1 \leq x \leq 616979$ and then prime. No choice of $a < 10^6$ produces a larger "first prime."

Problem 61. : Let

$$s_2(t) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^2} \sin(2\pi n t).$$

It is known that if $s_2(t) \geq 0$, for $t \in (0, \frac{1}{4})$, then RH is true.

Show the converse, i.e. that RH implies $s_2(t) \geq 0$ for for $t \in (0, \frac{1}{4})$.

Asked by Brian Conrey

3 Algorithms

3.1 Congruences and Discrete Logarithms

3.1.1 The DLP in $(\mathbb{Z}/p\mathbb{Z})^*$

- Can one beat, heuristically, the Number Field Sieve bound $L_p[1/3, \sqrt[3]{64/9}]$ for computing discrete logarithms in $\mathbb{F}_p^*$?

- NFS-DL (prime-field DLP) achieves the *same* heuristic complexity as the NFS, $L[1/3, \sqrt[3]{64/9}]$. Find an algorithm for the DLP in $(\mathbb{Z}/p\mathbb{Z})^*$ that improves on this.
- Find a polynomial-time classical algorithm for the DLP in $\mathbb{F}_p^*$ (or prove none exists).

3.2 Shortest Vector Problem and Integer Relations

- The exact SVP is NP-hard. Is there a polynomial-time algorithm that achieves a *polynomial* approximation factor, rather than exponential?
- Find a polynomial-factor approximation for SVP in quantum polynomial time.

3.3 Elliptic Curves

3.3.1 Arithmetic

- Is the rank of elliptic curves over $\mathbb{Q}$ bounded or unbounded?
- Find an elliptic curve of rank 30 or higher.
- Find infinitely many elliptic curve of rank 30 or higher.

3.3.2 The Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Is there a subexponential algorithm for the ECDLP over a prime field $E(\mathbb{F}_p)$?

3.4 Riemann zeta function

- Develop an algorithm that can evaluate $\zeta(1/2 + it)$ in polynomial time.
- Develop an algorithm that can evaluate $\zeta(1/2 + it)$ in quantum polynomial time.

4 Other problems

These problems are open, but it is not clear if AI could be useful in their solution.

Problem 62. Prove that $\zeta(3)$ is transcendental and $\zeta(5)$ is irrational.

Problem 63. Prove the ratios conjecture for the family of quadratic L-functions over function fields.

Asked by Brian Conrey

Problem 64. Use Levinson's method to give a proof of RH over function fields.

Asked by Brian Conrey

Problem 65. Find a conjecture with power savings for

$$\int_0^T |\zeta(1/2 + it)| \, dt.$$

Problem 66. Let χ_q be a real, primitive Dirichlet character, and $L(s, \chi_q)$ its L-function. Define

$$c = \limsup_{q \to \infty} \frac{e^{-\gamma} L(1, \chi_q)}{\log \log q}.$$

Littlewood proved, assuming GRH, that $1 \leq c \leq 2$.
Narrow the range of possible values of c.

Asked by Brian Conrey

Problem 67. Let t_n be the (unique) n-digit number all of whose (base 10) digits are 1's and 2's and which is divisible by 2^n.
For example, $t_1 = 2$, $t_2 = 12$, $T_3 = 112$, $t_4 = 2112$, $t_5 = 22112$, $t_6 = 122112$.
Prove or disprove that for large n, t_n has $\frac{n}{2} + o(n)$ ones in its decimal representation.

Asked by Brian Conrey

Problem 68. (A conjecture of Gauss) Prove that there is $\delta > 0$ such that there are infinitely many fundamental discriminants d such that the class number of $Q(\sqrt{d})$ is smaller than $d^{1/2-\delta}$.

Problem 69. Find the horizontal distribution of the real parts of the zeros of $\zeta'(s)$ up to a height T on a scale of $1/\log T$.

The analogous problem is open for characteristic polynomials of random $N \times N$ unitary matrices: the radial distribution of zeros of the derivative, on the scale of $1 - 1/N$.

Problem 70. (Hooley's R* conjecture) Let q and a be positive integers with $(a, q) = 1$. Prove that

$$\sum_{h \leq x} e\left(\frac{a\overline{h}}{q}\right) \ll_\epsilon q^\epsilon x^{1/2}.$$

Here $\overline{h}$ is the inverse of h modulo q, i.e. $h\overline{h} \equiv 1 \bmod q$.

Problem 71. What finite groups occur as Galois groups of ring extensions of $\mathbb{F}_p[X]$? Note - necessary conditions known by a conjecture of Abhyankar. What is the smallest group (for each p) satisfying those conditions for which it is not known whether it occurs?

Same question for field extensions.

Asked by Rachel Pries