Complexity of Diophantine Equations

Jeff Lagarias,
University of Michigan
Ann Arbor, Michigan

August 5, 2011 -corrected

Credits

- Work of J. L. partially supported by NSF grants DMS-0801029 and DMS-1101373.

- Some work of J. L. with K. Soundararajan supported by the Mathematical Research Foundation at Stanford University in 2010.

Table of Contents

1. History and Problem Formulation

• Solving Diophantine equations is a long-standing goal of number theorists.

• Focus on possible special role of Diophantine equations from genus zero plane curves.

Diophantus of Alexandria-1

• Diophantus of Alexandria is believed to have lived circa AD 250.

(Error bounds: he lived between BC 150 and AD 350).

• He wrote a collection of thirteen books called together: Arithmetica. Six books known in Greek, include books I, II, III. Four more books in Arabic rediscovered in 1970's, these are books IV, V, VI, VII. Remaining three Greek books fall somewhere among books VIII-XIII.

Diophantus of Alexandria-2

• The Arithmetica consisted of a collection of problems to be solved in rational numbers. These equations reduce to polynomial equations in several indeterminates. These now include over 300 problems.

• Such equations–to solve in rational numbers or integers– are now called Diophantine equations.

Diophantus of Alexandria-3

• From Book IV: "To divide a given number into two numbers such that their product is a cube minus its side."

• Call all the given number a. Diophantus considers the case $a = 6$. The problem is then to find (x, y) such that

$$y(a - y) = x^3 - x.$$

Diophantus's solution: Set $x = ky - 1$, which gives

$$6y - y^2 = k^3y^3 - 3k^2y^2 + 2ky$$

Take $k = 3$ to kill the coefficient of y, obtain: $27y^3 - 26y^2 = 0$. The three roots are $y = 0, 0, \frac{26}{27}$. We get the rational solution $(x, y) = (\frac{17}{9}, \frac{26}{27})$. Thus Diophantus divides $a = 6$ into $\frac{17}{9} + \frac{37}{9}$.

• This problem involves an elliptic curve. At least one example of a hyperelliptic curve occurs (Probem VI.17).

Diophantus of Alexandria-4

• Diophantus Problem III.19. Find four numbers, such that the sum of the squares of all four, plus or minus any one of the numbers, is a square."

• This requires eight conditions to be satisfied:

$$(x_1+x_2+x_3+x_4)^2+(-1)^k x_i^2 = (y_{4k+i})^2, \quad k=1,2;\ i=1,2,3,4.$$

• Diophantus's solution:

$$(x_1,x_2,x_3,x_4) = (\frac{17136600}{163021824}, \frac{12675000}{163021824}, \frac{15615600}{163021824}, \frac{8517600}{163021824})$$

• Diophantus uses integer Pythagorean triples and may well have known the group law on the genus zero projective curve $x^2+y^2=z^2$.

Diophantus of Alexandria-5

• Diophantus Problem II.8. Partition a given square into two squares.

• Famous marginal note of Fermat in Bachet's Diophantus (1621) *"Cubum autem in duos cubos, aut quadratoquadratem in duos quadratoquadratos & generaliter nullam in infinitam ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabelem sane detexi. Hanc marignis exiguitas non caperet."*

• An earlier reader's (13-th Century) marginal note on the same problem: "cursed be Diophantus for the difficulty of this text."

Diophantine Problems

- Instance: A finite system of Diophantine equations S

$$F_i(x_1, .., x_n) = 0, \quad F_i \in \mathbb{Z}[x_1, x_2, ..., x_n].$$

- Question 1. Does S have infinitely many (nonzero) integer solutions?

- Question 2. Does S have a nonnegative integer solution?

- Question 3. Does S have an integer solution in a specified box?

Diophantine Problems: Integer Solutions

- *Example.* Is there a solution to $x^3 + y^3 + z^3 = 29$?

  Answer. Yes. $(x, y, z) = (3, 1, 1)$.

- *Example.* Is there a solution to $x^3 + y^3 + z^3 = 30$?

  Answer. Yes.
  $(x, y, z) = (-283059965, -2218888517, 2220422932)$.
  (Discovered 1999 by E. Pine, K. Yarbrough, W. Tarrant, M. Beck, approach suggested by N. Elkies.)

- *Example.* Is there a solution to $x^3 + y^3 + z^3 = 33$?

  Answer. Unknown

Diophantine Problems: Rational Solutions

- One can ask exactly the same questions for solutions in rational numbers.
- Example $x^2 + y^2 = 1$ has infinitely many rational solutions.
- Example $x^2 + y^2 = 3$ has no rational solutions.
- Homogenize: $x^2 + y^2 = z^2$ has infinitely many nonzero integer solutions.
- Homogenize: $x^2 + y^2 = 3z^2$ has no nonzero integer solutions.

Thesis

• Solving Diophantine equations is an important, long-standing goal of number theorists.

• Solving Diophantine equations motivated important problems in computability theory. (see below)

• David Hilbert's dictum: "We must know. We will know."

• Thesis: The P-NP problem does not seem to fit very well with Diophantine equations. How come?

2. Hilbert's 10-th Problem (1900)

- 10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION

- Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Hilbert's 10-th Problem-2

- A k-ary set $D = \{(m_1, m_2, .., m_k) : m_i \geq 0\} \subset \mathbb{N}^k$ is Diophantine if there is a system S of Diophantine equations

$$f_j(x_1, ..., x_k, y_1, ..., y_l) = 0, \quad 1 \leq j \leq l$$

  such that $(m_1, .., m_k) \in D$ if and only if there exists some $(y_1, ..., y_l) \in \mathbb{N}^l$ for which the equations have a solution.

- Note: Only consider non-negative integer solutions.

- Note: Definition ignores the structure of all other integer solutions to S (which may be complicated).

Hilbert's 10-th Problem-3

- Reduction. Can reduce to case of one Diophantine equation.

  Add sum of squares of equations.

- Reduction. Can reduce integer solution case to nonnegative integer solution case. ($z_i = x_i - x_{i+1}$).

Hilbert's 10-th Problem-4

- Theorem(M. Davis (1949)) Any recursively enumerable set S of the natural numbers $\mathbb{N}$ has the form

$$S = \{m : \exists y \, \forall k_{\leq y} \, \exists \, y_1, y_2, ..., y_l \mid p(a, k, y_1, ..., y_l) = 0.\}$$

for some polynomial
$p(x_1, x_2, y, y_1, y_2, ..., y_l) \in \mathbb{Z}[x_1, x_2, y, y_1, y_2, ..., y_l]$.

- Uses Gödel encoding with the Chinese Remainder Theorem. It has a single bounded universal quantifier.

Hilbert's 10-th Problem-5

- An exponential Diophantine equation is one that allows terms that are of form $c\prod_i x_i^{d_i}\prod_j (n_j)^{x_j}$ in its variables x_i, in which c, d_i, n_j are all nonnegative integers.

- A k-ary set $D = \{(m_1, m_2, .., m_m) : m_i \geq 0\} \subset \mathbb{N}^m$ is exponential Diophantine if there is a system of exponential Diophantine equations

$$g_j(x_1, ..., x_k, y_1, ..., y_l) = 0, \quad 1 \leq j \leq l$$

such that $(x_1, .., x_m) \in D$ if and only if there exists some $(y_1, ..., y_n) \in \mathbb{N}^l$ for which the equations have a solution.

Hilbert's 10-th Problem-6

- Theorem(Davis, Putnam, J. Robinson) Hilbert's 10-th problem is undecidable for exponential Diophantine sets.

- Julia Robinson reduction(1950) : if there exists a Diophantine set D such that $(m, n) \in D$ implies $n < m^m$, and for every $k > 1$ there exists $(m, n) \in D$ with $n > m^k$, then every recursively enumerable set is Diophantine.

- Her proof uses the Pell equation $x_1^2 - Dx_2^2 = n$.

Hilbert's 10-th Problem-7

- Theorem(Matiyasevich (1970))

  (1) Every recursively enumerable set D of nonnegative integers is Diophantine.

  (2) Therefore, Hilbert's 10-th problem is undecidable.

- Method. Matiyasevich showed one can encode the exponentially growing sequence (n, F_{2n}), where $F_n =$ the n-th Fibonacci number, as solutions to a Diophantine equation (having additional variables).

Hilbert's 10-th Problem-Developments

• Hilbert's 10-problem is known to be solvable over local fields: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, finite fields $\mathbb{F}_p$.

• Hilbert's 10-th problem over the rationals $\mathbb{Q}$ is unsolved!

• Even this (important) special case of Hilbert's 10th problem over $\mathbb{Q}$ is unsolved:

Problem. Determine whether an elliptic curve $y^2 = x^3 - Ax - B$ defined over $\mathbb{Q}$ has a rational point.

• Observation: Note the use of Pell type equations in encodings the undecidability proof, both by Julia Robinson and by Matiyasevich.

3. Diophantine Properties of Curves

• The "geometry" of the curve affects its integer and rational solutions.

• Principle of Diophantine Geometry: The complex geometry of a curve defined over an algebraic number field K restricts the structure of algebraic points on a curve.

(Actually, all local fields contribute: real and p-adic points influence arithmetic.)

Diophantine Geometry of Curves-1

• Parameter 1. The (topological) genus of a curve C.

• Note: We will allow curves with singular points; they are then not normal. The genus of such a curve is the genus of a normalization.

(This is well defined, via Riemann, viewing curve as a Riemann surface. Also Hurwitz, Clebsch, Max Noether...

• Genus is a birational invariant of the curve.

Diophantine Geometry of Curves-2

- "Diophantus's Theorem": If a curve over $\mathbb{Q}$ has genus $g = 0$ the number of rational points on it can be very large: it can be infinite and infinitely generated as a group.

  (*) Furthermore there will always exist a number field K where this holds.

- Mordell's Theorem (1922)) If a curve over $\mathbb{Q}$ has genus $g = 1$, then over an algebraic number field K the set of K-points can be infinite, but is always finitely-generated.

- Mordell's Conjecture = Falting's Theorem (1983) If a curve over $\mathbb{Q}$ has genus $g \geq 2$, then over an algebraic number field K, the set of K-points on it is always finite.

Curves of Genus $g \geq 2$

• Finding All Solutions. There is no known effectively computable procedure for locating the finite number of rational solutions to a curve of genus $g \geq 2$ defined over $\mathbb{Q}$.

• Finding One Solution. Moreover, there is no known bound on the "height" of such a point, in terms of height information on the original curve (viewed inside a family of such curves.)

• As far as we know, there could be occasional gigantic "sporadic" solutions to such an equation."

Mordell's Conjecture (regarding Mordell (1922))

- "I was very unfortunate with this paper. It was rejected by the London Mathematical Society; I really don't know why. Perhaps they did not approve of my style..."

- L. J. Mordell, Reminiscences of an octogenarian mathematician, Amer. Math. Monthly **78** (1971), 952–961.

Low Genus Curves

- Leave genus $g = 1$ curves for other speaker(s).

- Fact. (Rational Points) Every genus 0 curve defined over $\mathbb{Q}$ has infinitely many K-rational points on it, for some algebraic number field K.

Plane Curves-1

• A plane curve is a curve in the affine plane cut out by a single polynomial equation $F(x, y) = 0$ with $F(x, y) \in \mathbb{C}[x, y]$.

• An irreducible curve is one for which $F(x, y)$ is irreducible over $\mathbb{C}[x, y]$.

• Parameter 2. Another invariant is the (total) degree of $F(x, y)$.

(It is a projective invariant, not a birational invariant.)

• There are formulas for computing the genus of a plane curve in terms of its degree n and multiplicities of its singular points.

$$g = \frac{(n-1)(n-2)}{2} - \sum_i \frac{r_i(r_i-1)}{2} + (correction).$$

Plane Curves-2

• The property of a curve being a plane curve puts further restrictions on its Diophantine geometry.

• Theorem. (Integer Points) (Runge 1887) Any genus 0 plane curve, that has at least three distinct branches at ∞, has only finitely many integer solutions.

• In addition, there is an algorithm to effectively can determine the integer solutions. See Hilliker and Straus, TAMS **280** (1983), 637–657.

Smale's 5-th Problem

- Smale's list of "Mathematical Problems for the Next Century" (*Mathematics: Frontiers and Perspectives*, AMS: Providence, RI 2000; Also: Wikipedia)

- Smale's 5th Problem: Height bounds for Diophantine curves

Can one decide if a diophantine equation $f(x, y) = 0$ (input $f \in \mathbb{Z}[u, v]$ has an integer solution (x, y) in time 2^{s^c}, where c is a universal constant? That is, can the problem be decided in exponential time?

Here $s(f)$ is the size of f, which is (roughly) the degree plus sum of the logarithms of the coefficients of f.

Smale's 5-th Problem-2

• Smale also asks if curves of genus one or above have a solution of polynomially bounded height.

• Genus 0 is excluded for reasons to be described below.

• Cucker, Koiran, Smale (1999) show solving one-variable Diophantine equations is in P with sparse representation input (in Turing model of computation.)

(Ref. J. Symbolic Computation **27** (1999), 21–29.)

4. Complexity of Binary Quadratic Diophantine Equations (BQDE)

- Binary Quadratic Diophantine Equations are

$$AX^2 + BXY + CY^2 + DX + EY + F = 0$$

- They cut out a genus zero curve.

- These curves may have infinitely many integer points (Runge's theorem does not apply.)

- One may reduce to the case of separated variables $G(X) = H(Y)$ by "completing the square" (and treating several cases instead of one case.)

Binary Quadratic Diophantine Equation Problem

- Problem: Binary Quadratic Diophantine Equation(BQDE)
- Instance: $(A, B, C, D, E, F) \in \mathbb{Z}^6$ specifying a binary quadratic Diophantine equation.
- Question: Does the BQDE have a nonnegative integer solution $(x, y) \in \mathbb{N} \times \mathbb{N}$?

Factoring and BQDE

- Example $(X+2)(Y+2)=N$.

  Answering this solution requires testing if N is composite, a problem which is in complexity class P.

- Example $(X+k)(Y+k)=N$

  Testing for nonnegative integer solutions requires recognizing N having factorization with all factors $\geq k$.

  If BQDE were in complexity class P, for composite N could solve a succession of problems of this kind, varying k by "bisection", to locate the smallest factor of N in polynomial time. Thus factoring would be in complexity class P.

BQDE Solvability

- Solvability. After earlier work of Euler and Legendre, a complete theory developed by Gauss (1801), giving an effective method of finding all integer solutions. Gauss treated the case $B = 2B'$ is even, but this restriction is removable.

BQDE-Exponential Complexity Bound

• Complexity analysis of Gauss's algorithms (Lagarias, J. Algorithms 1980) can be used to show:

• Theorem. If a BQDE has an integer solution, then it can be found in exponential time.

• This gives positive answer to Smale's Problem 5 in this restricted case.

Discriminant-1

- The discriminant

$$\Delta = B^2 - 4AC$$

determines the behavior of the BQDE.

- Three cases, values of Δ determine the geometry of the BQDE:

$\Delta < 0$,

$\Delta > 0$, not a square,

$\Delta = n^2$.

Discriminant-2

- Case 1. (Nonsplit -Definite Torus $\mathbb{G}_m$)

$$\Delta < 0,$$

The real curve is an ellipse.

- Case 2. (Nonsplit-Indefinite Torus $\mathbb{G}_m$)

$$\Delta > 0,$$

with Δ not a perfect square. The real curve is a hyperbola, with irrational slope asymptotes

- Case 3. (Split Torus $\mathbb{G}_m$)

$$\Delta = m^2$$

The real curve is hyperbola with rational slope asymptotes ($m \neq 0$) or two straight lines ($m = 0$).

BQDE is in NP

- Main Theorem (L-1979++) The problem BQDE is in the complexity class NP.

- Strengthened Result The problem is still in NP if one imposes additional congruence side conditions:

$$(x, y) \equiv (a, b) \pmod{N},$$

with (a, b, N) given as extra input data.

Extended Abstract in 1979 FOCS outlining proof.

- References: L, 1979 FOCS; L., Succinct certificates for solutions to BQDE's, `arXiv:math/0611209`

BQDE Difficulty-1

- Major Difficulty. The minimal integer solution (x_0, y_0) of a BQDE may be too large to write down in PSPACE, in the standard binary encoding!

- Example. (negative Pell equation)

$$x^2 - Dy^2 = -1.$$

- Solvability of this problem has long complicated history: see E. Fouvry and J. Klüners, "On the negative Pell equation," Annals of Math. **172** (2010), 2035–2104.

BQDE Difficulty-2

- Example 1. One can show that

$$X^2 - DY^2 = -1$$

with $D = 5^{2k+1}$ has minimal nonnegative solution

$$x_0 + y_0\sqrt{5} = (2+\sqrt{5})^{5^k}$$

- It follows that

$$\log x_0 >> 5^k >> \sqrt{D}.$$

Since input size is $\log D = \log 5^k \approx 2k$, this number requires exponential space to write down in binary.

- Reference: L., Trans. Amer. Math. Soc. **260** (1980), 485–508.

BQDE Difficulty-3

- Example 2. (Other large solutions) The Cohen-Lenstra heuristics for real quadratic fields predict that over 75 percent of real quadratic fields with prime discriminant $D = p \equiv 1 \pmod 4$, have class number $h(D) = 1$.

  The Brauer-Siegel theorem says $h(D) \log \epsilon_D = D^{1/2+o(1)}$ which implies that their fundamental unit $\epsilon_D = x_0 + y_0\sqrt{D}$ is large:

  $$\log \epsilon_D \geq D^{1/2-\epsilon}$$

  These units always have norm -1, and give the minimal solution to the negative Pell equation above.

BQDE Difficulty-4

- Major Difficulty Resolved. We express solution with a succinct certificate. This encodes (x_0, y_0) by a process of repeated exponentiation and twisting. In effect, it is representable by a short straight line program.

- Basic idea comes from the infrastructure of Dan Shanks.

- Infrastructure treated by L. (1981), Hendrik Lenstra, Jr. (1982), Buchmann-Williams (1988).

- Modern form of inftrastructure: Arakelov class group, see Schoof (2008).

Straight Line Programs

• Straight Line Program. Start with $x_0 = 0, x_1 = 1$, and then the m-th line of the program computes $x_m = x_k * x_l$ with $1 \leq k, l < n$ and the operation $*$ at each line can be addition, subtraction or multiplication $(+, -, \times)$. The length of a program is the number of lines.

• Example. One can encode repeated squaring by a straight-line program. Take $x_2 = 1 + 1 = 2$ and, for $n \geq 3$ take

$$x_k = x_{k-1} \times x_{k-1}.$$

This straight line program for n steps ($n \geq 3$) computes $x_n = 2^{2^{n-2}}$.

BQDE Difficulty-5

• Toy Analogue: Repeated Exponentiation. Consider computing the Fibonacci number F_{2^n} (which is doubly-exponentially large in n).

Use for Fibonacci and Lucas numbers F_m, L_m that:

$$(\frac{1+\sqrt{5})}{2})^m = \frac{L_m + F_m\sqrt{5}}{2}.$$

This gives quadratic identities to compute (F_{2m}, L_{2m}) from (F_m, L_m), namely

$$\begin{aligned} L_{2m} &= \frac{1}{2}((L_m)^2 + 5(F_m)^2) \\ F_{2m} &= F_m L_m. \end{aligned}$$

These can be implemented by a straight line program.

BQDE Difficulty-6

• Actual Method for Straight Line Program. More complicated

• Use composition of binary quadratic forms for the "doubling step", and continued fraction reductions for the "twisting substep."

• Second Difficulty Testing if a solution given by straight line program is nonnegative. Not legal to multiply out the straight line program.

BQDE Difficulty-7

- Second Difficulty Resolved. Can determine nonnegativity of the solution using calcuations directly involving the succinct certificate for (x_0, y_0).

- Idea: Either we can compute the solution using a floating point calculation and get enough accuracy. Must rule out floating point underflow.

  Show: The floating point calculation can fail only the solution (x_0, y_0) is sufficiently small that it can be written down and directly checked in polynomial time.

5. Complexity Problems

• What can we learn from the BQDE example? What are open problems?

• Open Problem 1.Is BQDE in complexity class P?

• This does not seem likely to be settled soon since it would require FACTORING to be in P.

Is BQDE an NP-complete problem?

- Open Problem 2.Is the problem BQDE NP-complete?

- There is no evidence for this problem being NP-complete.

- This problem might be a candidate for a problem of intermediate complexity inside NP, neither in P nor NP-complete.

- It shows the (possible) mismatch of "natural" Diophantine problems with the P versus NP question.

BQDE in the Blum-Shub-Smale (BSS) model

• Open Problem 3. In the BSS-model, is the problem BQDE in NP_K for some field K?

• One might choose $K = \mathbb{R}$. Perhaps one wants to consider a number field like $k = \mathbb{Q}$ instead.

• This problem might be easy to resolve, since the current solution involves a straight line program.

• This may provide indirect motivation for studying BSS model for number fields.

BQDE in the Blum-Shub-Smale (BSS) model-2

• Open Problem 4. In the BSS-model, is the problem BQDE a complete problem in a natural BSS-complexity class, e.g. $NP_{\mathbb{R}}$?

Straight Line Program Questions

• Do integers generated by short straight-line programs have restrictions on their additive arithmetic structure (solving Diophantine equations), or on their multiplicative arithmetic structure (factorization properties)?

Shub-Smale Conjecture and Valiant Conjecture

• Conjecture. (Shub and Smale, Duke Math. J. (1994)) There is no short straight-line program that computes a sequence of numbers $f(n) = a_n n!$, of length $<< (\log n)^c$, for any fixed $c \geq 1$.

• Proposition. Shub-Smale (1994) The truth of the Conjecture above implies that the BSS complexity class $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$.

• **Theorem** (Bürgisser) If the Valiant Conjecture is false, then the Pochhammer polynomial $p_n(X) = \prod_{i=j}^{n}(X - j)$ can be computed by a straight line program of length $(\log n)^c$. Therefore $f(n) = n!$ can be computed by a straight line program of polylog length.

BQDE Straight Line Programs-Questions

• The results on BQDE indicate that certain doubly-exponentially large integer solutions of a BQDE can be computed by straight-line programs of polynomial length in the input size.

• Question. Is there a possible converse, whether such numbers necessarily must satisfy some unusually simple Diophantine equation?

• This seems unlikely. But if one believes the Tau Conjecture, such integers must avoid "well-structured" numbers containing all small primes as factors.

BQDE Straight Line Programs-Questions-2

• Some number-theory questions suggested by analogy:

• Question. Is there a possible converse, whether numbers computed by short straight line programs necessarily must satisfy some unusually simple Diophantine equation?

• Question. Another purely number-theoretic direction is whether Diophantine equations can have solutions all having unusually small prime factors.

Smooth Solutions to $A + B = C$

• Consider the linear Diophantine equation $A + B = C$. Define the height of a solution as

$$H(A, B, C) := \max(|A|, |B|, |C|).$$

• One can measure the smoothness of a solution (A, B, C) by the maximal size of a prime dividing ABC. How small can this be made? Define the smoothness

$$S(A, B, C) := \max\{p : p \text{ divides } ABC\}.$$

• Theorem (L-Soundararajan (2011)) There are only finitely many solutions $A + B = C$ having

$$S \leq (3 - \epsilon) \log \log H$$

Smooth Solutions to $A + B = C$ (cont.)

• XYZ Conjecture There is a positive constant c such that the equation $A + B = C$ has infinitely many relatively prime integer solutions with

$$S(A, B, C) \leq (\log H)^c.$$

• Theorem. (L-Soundararajan (2011)) Under the Generalized Riemann Hypothesis (GRH), this conjecture is true for any $c > 8$.

• Theorem. (L- Soundararajan (2011)) Assuming the ABC-conjecture, one cannot take $c < 1$.

• A heuristic argument suggests that the optimal exponent is $c = \frac{3}{2}$.

Thank You!