The ABC Conjecture

David Roe

Department of Mathematics
University of Calgary/PIMS

University of Calgary: Colloquium

Outline

Integer Powers

Goal

Understand **additive** relationships between **integer powers**.

For example, we might ask

Question

Let m, n, k be positive integers and find all solutions to

$$y^m = x^n + k$$

Question

Fix integers A, B, C. Find all solutions to

$$Ax^r + By^s = Cz^t.$$

ABC Triples

Question

Find relationships of the form

$$A + B = C$$

where A, B and C contain ***large powers****.*

$$3^2 + 4^2 = 5^2$$
$$7^2 + 2^6 \cdot 3^2 = 5^4$$
$$3 + 5^3 = 2^7$$
$$1 + 2 \cdot 3^7 = 5^4 \cdot 7$$
$$11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$$
$$x^n + y^n = z^n$$

Interesting Triples

Idea

We can measure how interesting such a relationship is by comparing the **size** of the numbers to the **product of the primes** dividing them.

	radical	size
$3^2 + 4^2 = 5^2$	30	25
$7^2 + 24^2 = 25^2$	210	625
$3 + 5^3 = 2^7$	30	128
$1 + 2 \cdot 3^7 = 5^4 \cdot 7$	210	4375
$11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$	53130	48234496
$x^n + y^n = z^n$	$\leqslant xyz$	z^n

The ABC Conjecture

Definition

An *abc-triple* is a triple of relatively prime positive integers with

$$a + b = c \qquad \text{and} \qquad \mathrm{rad}(abc) < c.$$

The *quality* of an abc-triple is

$$q(a, b, c) = \frac{\log(c)}{\log(\mathrm{rad}(abc))}.$$

ABC Conjecture (Masser (1985), Oesterlé (1988))

Suppose $\epsilon > 0$*. Then there are finitely many abc-triples with quality greater than* $1 + \epsilon$*.*

Highest quality abc-triples

a	b	c	quality
2	$3^{10} \cdot 109$	23^5	1.62991
11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	1.62599
$19 \cdot 1307$	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	1.62349
283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 17^3$	1.58076
1	$2 \cdot 3^7$	$5^4 \cdot 7$	1.56789
7^3	3^{10}	$2^{11} \cdot 29$	1.54708
$7^2 \cdot 41^2 \cdot 311^3$	$11^{16} \cdot 13^2 \cdot 79$	$2 \cdot 3^3 \cdot 5^{23} \cdot 953$	1.54443
5^3	$2^9 \cdot 3^{17} \cdot 13^2$	$11^5 \cdot 17 \cdot 31^3 \cdot 137$	1.53671
$13 \cdot 19^6$	$2^{30} \cdot 5$	$3^{13} \cdot 11^2 \cdot 31$	1.52700
$3^{18} \cdot 23 \cdot 2269$	$17^3 \cdot 29 \cdot 31^8$	$2^{10} \cdot 5^2 \cdot 7^{15}$	1.52216

New proof of FLT

Suppose we had an explicit upper bound on quality, e.g. 2. The quality of $x^n + y^n = z^n$ is

$$\begin{aligned} q &\geqslant \frac{n \log(z)}{\log(xyz)} \\ &\geqslant \frac{n}{3} \end{aligned}$$

So $n \leqslant 6$.

Catalan's Conjecture

Theorem (Tijdeman (1976), Mihăilescu (2002))

There are finitely many solutions to

$$y^m = x^n + 1$$

with $x, y, m, n > 1$. *In fact, there is only one.*

ABC Consequence

There are finitely many solutions to

$$y^m = x^n + k$$

for $x, y, m, n > 1$ *and* $k > 0$ *fixed.*

Hall's Conjecture

Conjecture (Hall)

Suppose

$$y^2 = x^3 + k$$

with $k \neq 0$. *Then there is a constant* C *(independent of* k*) with*

$$\sqrt{|x|} < C \cdot |k|$$

k	x	$\sqrt{\vert x\vert}/\vert k\vert$
17	5234	4.26
24	8158	3.76
225	720114	3.77
-307	939787	3.16
1090	28187351	4.87

Weak form of Hall's Conjecture

ABC Consequence

Suppose $\epsilon > 0$ *and*

$$y^2 = x^3 + k$$

with $k \neq 0$. *Then there is a constant* C_ϵ *(independent of* k*) with*

$$|x|^{1/2-\epsilon} < C_\epsilon |k|.$$

Fix A, B, C and consider

$$Ax^r + By^s = Cz^t.$$

Want **primitive solutions**: x, y, z are relatively prime.

Expected number of solutions

Suppose T large and consider **all** inputs x, y, z with

$$|x| \leqslant T^{1/r} \qquad |y| \leqslant T^{1/s} \qquad |z| \leqslant T^{1/t}$$

Then the value $Ax^r + By^s - Cz^t$ is distributed on an interval of length a constant multiple of T. If this distribution were **uniform** then we would expect

$$T^{(1/r+1/s+1/t)-1}$$

occurrences where $Ax^r + By^s - Cz^t = 0$.

Generalized Fermat Equation

Suppose that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$.

Theorem (Darmon-Granville (1995))

*If r, s, t are **fixed** then there are only finitely many primitive solutions to*

$$Ax^r + By^s = Cz^t.$$

ABC Consequence

There are only finitely many primitive solutions to

$$Ax^r + By^s = Cz^t$$

*as r, s, t **vary**.*

Mordell's Conjecture

Theorem (Faltings (1984))

Suppose that C is a nonsingular curve of genus g over a number field K. Then $C(K)$ is finite.

ABC Consequence

Suppose the maximum quality of any abc-triple is known. Then we can find explicit bounds for the heights of points in $C(K)$.

Szpiro's Conjecture

ABC Consequence

Suppose E is an elliptic curve over $\mathbb{Q}$ with conductor N and minimal discriminant Δ. Then for every $\epsilon > 0$ there is a constant C_ϵ with

$$|\Delta| \leqslant C_\epsilon N^{6+\epsilon}$$

Discriminants

Recall that the discriminant $D_{F/\mathbb{Q}}$ of a number field $F/\mathbb{Q}$ is defined as

$$D_{F/\mathbb{Q}} = \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix},$$

where $\sigma_1, \ldots, \sigma_n$ are the embeddings of F into $\mathbb{C}$, and $\alpha_1, \ldots, \alpha_n$ are a basis for the ring of integers R. The **logarithmic discriminant** is

$$d(F) = \frac{1}{[F : \mathbb{Q}]} |D_{F/\mathbb{Q}}|.$$

Heights

Suppose X is a regular arithmetic surface over R with generic fiber a geometrically irreducible curve. Let D be a divisor on X_F. Then there is a **height function**

$$h_D : X_F(\bar{\mathbb{Q}}) \to R$$

well defined modulo bounded functions. Write $F(P)$ for the field of definition of P.
If X_F is a curve in $\mathbb{P}^2$, D is the restriction of a hyperplane section to X_F and $P = [x : y : z]$, then

$$h_D(P) = \frac{1}{[F(P) : \mathbb{Q}]} \sum_v \log \max(\|x\|_v, \|y\|_v, \|z\|_v).$$

Vojta's Conjecture

Conjecture (Vojta)

Let X be a smooth projective curve defined over a number field F. Let K denote the canonical divisor of X, and $\epsilon > 0$. Then for $P \in X(\bar{\mathbb{Q}})$,

$$h_K(P) \leqslant (1+\epsilon) d(F(P)) + C_{X,\epsilon}.$$

This is equivalent to the ABC conjecture.

Hodge-Arakelov theory

Suppose E is an elliptic curve over a field F of characteristic 0. Write $E^\dagger$ for the "universal" extension of E: the moduli space of pairs (x, ∇_x) of a point x on E and a logarithmic connection on a certain line bundle associated to x.

- $E^\dagger$ is a torsor under the sheaf ω_E of invariant differentials on E.
- Zariski locally, $E^\dagger$ is the spectrum of a polynomial algebra in one variable over $\mathcal{O}_E$, so it makes sense to talk about the relative degree of a function on $E^\dagger$.
- The d-torsion points $E^\dagger[d]$ map isomorphically to $E[d]$.

Theorem (Mochizuki)

Let d be a positive integer and $\eta \in E(F)$ a torsion point of order not dividing d. Define

$$\mathcal{L} = \mathcal{O}_E(d \cdot [\eta]).$$

The natural map

$$\Gamma(E, \mathcal{L})^{<d} \to \mathcal{L}|_{E^{\dagger}[d]}$$

given by restricting sections of degree less than d is a bijection between F-vector spaces of dimension d^2.

We need to modify the **integral structure** of $\Gamma(E, \mathcal{L})^{<d}$ to get an isomorphism for degenerating elliptic curves and curves over the finite and infinite places of a number field.

Near infinity on the moduli stack of elliptic curves (ie over a completed base $\hat{S}$) and for a degenerating elliptic curve E,

$$E|_{\hat{S}} \cong \mathbb{G}_m \qquad\qquad E^\dagger|_{\hat{S}} \cong \mathbb{G}_m \times \mathbb{A}^1.$$

The "standard" integral structure on $E^\dagger$ is

$$\bigoplus_{r \geqslant 0} \mathcal{O}_{\mathbb{G}_m} \cdot T^r$$

(T a coordinate on $\mathbb{A}^1$). To get an isomorphism at finite places:

$$\bigoplus_{r \geqslant 0} \mathcal{O}_{\mathbb{G}_m} \cdot \binom{d \cdot \{T - i_\chi/n\}}{r},$$

where i_χ/n is an invariant determined by η. Near infinity we need to modify this further by scaling by a term asymptotic to

$$q^{-r^2/8d},$$

where q is the Tate parameter of the curve ($E(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times/q^{\mathbb{Z}}$). Mochizuki refers to these terms as "Gaussian poles."

Theorem (Mochizuki)

After modifying the integral structure of $\Gamma(E, \mathcal{L})^{<d}$ as described above, the restriction isomorphism

$$\Gamma(E, \mathcal{L})^{<d} \to \mathcal{L}|_{E^{\dagger}[d]}$$

extends to an isomorphism over the log whole moduli stack of log elliptic curves over $\mathbb{Z}$, with the possible exception of a subscheme determined by η.

Mochizuki then gives an argument for how to use Arakelov theory to prove Vojta's conjecture if one could get rid of these Gaussian poles [3, §1.5.1]

Inter-universal Teichmüller Theory

In [4], Mochizuki develops Interuniversal Teichmüller theory as a way to eliminate these Gaussian poles. The approach is based upon classical and p-adic Teichmüller theory, where the real analytic structure on a manifold is deformed by

$$x + iy \mapsto x + iKy,$$

yielding numerous holomorphic structures.
He begins by fixing **initial Θ-data**, consisting of

- a number field F
- an elliptic curve E over F
- a prime $l \geqslant 5$
- various additional technical data.

From this initial data, he considers hyperbolic orbicurves related by étale covers to $E_F - \{0\}$, with symmetries of the additive and multiplicative structures of $\mathbb{F}_l$ acting on the l-torsion points of E. These yield $\Theta^{\pm\mathbf{ell}}$ **NF-Hodge theaters**, which can be thought of as "miniature models of scheme theory surrounding the number field and theta function". A $\Theta^{\pm\mathrm{ell}}$ NF-Hodge theater is a collection of categories and auxiliary data, indexed by places of F. From an intial Θ-data one can construct a $\Theta^{\pm\mathrm{ell}}$ NF-Hodge theater via certain categories of étale covers of $E_F - \{0\}$.

He then takes a two dimensional lattice of (equivalent) $\Theta^{\pm \mathrm{ell}}$ NF-Hodge theaters by defining (horizontal) Θ-links and (vertical) log-links between Hodge theaters.

$$
\begin{array}{ccccccc}
\ddots & & \vdots & & \vdots & & \iddots \\
 & & \uparrow & & \uparrow & & \\
\cdots & \longrightarrow & \mathrm{HT}^{0,1} & \longrightarrow & \mathrm{HT}^{1,1} & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \\
\cdots & \longrightarrow & \mathrm{HT}^{0,0} & \longrightarrow & \mathrm{HT}^{1,0} & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \\
\iddots & & \vdots & & \vdots & & \ddots
\end{array}
$$

- the Θ-links allow the removal of the Gaussian poles, but do so at the cost of destroying the underlying ring/scheme structure
- the log-links come from p-adic logarithms, and allow the construction of log-shells (containing the images of the local units) that are preserved by the log-link
- These log shells eventually yield bounds on logarithmic volume of certain monoids, which translate to bounds on Arakelov-theoretic heights.

Confused?

Me too.

- ABC@home. http://www.abcathome.com.
- Mazur, Barry. Questions About Number. From: New Directions in Mathematics.
- Mochizuki, Shinichi. Survey of Hodge-Arakelov Theory.
- Mochizuki, Shinichi. Inter-universal Teichmüller Theory I-IV.