Schinzel's hypothesis H

Open problems in number theory

David Kurniadi Angdinata

University College London

Thursday, 31 October 2024

Some fun quotes

Skorobogatov–Morgan (2024):

A notoriously difficult conjecture on prime values of polynomials, deemed to be inaccessible in the current state of analytic number theory.

Bunyakovsky (1857):

Il est à présumer que la démonstration rigoureuse du théorème énoncé sur les progressions arithmétiques des ordres supérieurs conduirait, dans l'état actuel de la théorie des nombres, à des difficultés insurmontables; néanmoins, sa réalité ne peut pas être révoquée en doute.

Primes in arithmetic progressions

Theorem (Dirichlet, 1837)

Let $a, b \in \mathbb{Z}$. Assume no primes p satisfy $p \mid a$ and $p \mid b$. Then there are infinitely many n such that $an + b$ is prime.

Example ($4X + 3$)

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$4n+3$	3	7	11	15	19	23	27	31	35	39	43	47	51
prime	✓	✓	✓		✓	✓		✓			✓	✓	

If there were a finite set $S := \{p \text{ prime} : p \equiv 3 \mod 4\}$, then

$$N := 2 + \prod_{p \in S} p^2 \equiv 3 \mod 4,$$

so N has a prime factor $q \equiv 3 \mod 4$ not in S, which is a contradiction.

Primes in polynomial sequences

Conjecture (Bunyakovsky, 1857)

Let $f \in \mathbb{Z}[X]$ be irreducible. Assume no primes p satisfy "$p \mid f(n)$ for all n". Then there are infinitely many n such that $f(n)$ is prime.

This is Dirichlet's theorem when $f(X) = aX + b$.

Example ($X^2 + 1$)

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$n^2 + 1$	1	2	5	10	17	26	37	50	65	82	101	122	145
prime		✓	✓		✓		✓				✓		

This is one of the four Landau's problems, amongst Goldbach's conjecture, the twin prime conjecture, and Legendre's conjecture.

Simultaneous primes in arithmetic progressions

Conjecture (Dickson, 1904)

Let $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$. Set $f(X) := (a_1 X + b_1) \cdot \dots \cdot (a_k X + b_k)$. Assume no primes p satisfy "$p \mid f(n)$ for all n". Then there are infinitely many n such that $a_1 n + b_1, \dots, a_k n + b_k$ are simultaneously prime.

This is the twin prime conjecture for X and $X + 2$.

Example (X and $2X + 1$)

p	2	3	5	7	11	13	17	19	23	29	31	37	41
$2p+1$	5	7	11	15	23	27	35	39	47	59	63	75	83
prime	✓	✓	✓		✓				✓	✓			✓

This is the Germain prime conjecture, which implies that there are infinitely many composite Mersenne numbers, since $2p + 1 \mid 2^p - 1$ whenever $p \equiv 3 \mod 4$ is a Germain prime.

Density of simultaneous primes

Conjecture (Hardy–Littlewood, 1923)

Let $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$. Set $f(X) := (a_1 X + b_1) \cdot \cdots \cdot (a_k X + b_k)$. Assume no primes p satisfy "$p \mid f(n)$ for all n". Then

$$\#\left\{ n \leq N : \begin{array}{c} a_1 n + b_1, \ldots, a_k n + b_k \\ \textit{are simultaneously prime} \end{array} \right\} \sim C \cdot \frac{N}{\log^k N}.$$

Here,

$$C := \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\#\{n \in \mathbb{F}_p : f(n) = 0\}}{p}\right).$$

If $f_1(X) = X$, then this is the prime number theorem that

$$\#\{n \leq N : n \text{ is prime}\} \sim \frac{N}{\log N}.$$

If $f_1(X) = X$ and $f_2(X) = X + 2$, then C is the twin prime constant.

Simultaneous primes in polynomial sequences

Conjecture (Schinzel's hypothesis H, 1958)

Let $f_1, \ldots, f_k \in \mathbb{Z}[X]$ be irreducible. Set $f := f_1 \cdot \cdots \cdot f_k$. Assume no primes p satisfy "$p \mid f(n)$ for all n". Then there are infinitely many n such that $f_1(n), \ldots, f_k(n)$ are simultaneously prime.

Conjecture (Bateman–Horn, 1962)

Let $f_1, \ldots, f_k \in \mathbb{Z}[X]$ be irreducible. Set $f := f_1 \cdot \cdots \cdot f_k$. Assume no primes p satisfy "$p \mid f(n)$ for all n". Then

$$\# \left\{ n \le N : \begin{array}{c} f_1(n), \ldots, f_k(n) \\ \textit{are simultaneously prime} \end{array} \right\} \sim C \cdot \frac{N}{\prod_i \deg f_i \cdot \log^k N}.$$

Here,

$$C := \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\#\{n \in \mathbb{F}_p : f(n) = 0\}}{p}\right).$$

Multivariate variants

Theorem (Friedlander–Iwaniec, 1997)

There are infinitely many $(x, y) \in \mathbb{Z}^2$ *such that* $x^2 + y^4$ *is prime.*

Theorem (Green–Tao–Ziegler, 2006)

Let $f_1, \ldots, f_k \in \mathbb{Z}[X]$ *such that* $f_i(0) = 0$*. Then there are infinitely many* $(x, y) \in \mathbb{Z}^2$ *such that* $x + f_1(y), \ldots, x + f_k(y)$ *are simultaneously prime.*

Theorem (Bodin–Dèbes–Najib, 2019)

Let R *be a characteristic zero UFD whose fraction field satisfies the product formula, and let* $f_1, \ldots, f_k \in R[X, Y]$*. Then there are* $y \in R[X]$ *such that* $f_1(X, y(X)), \ldots, f_k(X, y(X))$ *are simultaneously irreducible.*

Example ($X^8 + t^3$ over $\mathbb{F}_2[t]$)

$(t^2+t+1)^8+t^3 = (t+1)(t^{15}+t^{14}+t^{13}+t^{12}+t^{11}+t^{10}+t^9+t^8+t^2+t+1)$.

Genericity of simultaneous primes

Let $P_{d,N}$ be the set of $a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$ such that $|a_i| \leq N$.

Theorem (Skorobogatov–Sofos, 2023)

Let $S_{d,N}$ be the set of $f \in P_{d,N}$ such that $X^p - X \nmid f$ in all $\mathbb{F}_p[X]$. Then

$$\lim_{N\to\infty} \frac{\#\left\{(f_1,\ldots,f_k) \in S_{d,N}^k : \begin{array}{c} \exists n \in \mathbb{Z},\ f_1(n),\ldots,f_k(n) \\ \textit{are simultaneously prime} \end{array}\right\}}{\# S_{d,N}^k} = 1.$$

Theorem (Skorobogatov–Sofos, 2023)

Let K be a cyclic number field with integral basis $e_1,\ldots,e_m$ of $\mathcal{O}_K$. Then

$$\lim_{N\to\infty} \frac{\#\left\{f \in P_{d,N} : \begin{array}{c} \mathrm{Nm}_{\mathbb{Q}}^{K}(e_1X_1 + \cdots + e_mX_m) = f(X) \\ \textit{has a rational point} \end{array}\right\}}{\# P_{d,N}} = 1.$$

The Hasse principle

The Hasse principle holds for a variety V over a global field K if it has a point in K whenever it has points in K_v for all places v of K.

Theorem (Hasse–Minkowski theorem)

Let $a_1, \ldots, a_m \in \mathbb{Q}$. Then the Hasse principle holds for

$$a_1 X_1^2 + \cdots + a_m X_m^2.$$

The proof for $m = 4$ reduces to the proof for $m = 3$ by Dirichlet's theorem and the fundamental exact sequence of global class field theory.

Theorem (Hasse norm theorem)

Let K be a cyclic number field. Then there is a short exact sequence

$$1 \to \mathbb{Q}^\times / \operatorname{Nm}_{\mathbb{Q}}^K(K^\times) \to \bigoplus_{p \leq \infty} \mathbb{Q}_p^\times / \operatorname{Nm}_{\mathbb{Q}}^K((K \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times) \to \operatorname{Gal}(K/\mathbb{Q}) \to 1.$$

Thus a local norm everywhere except possibly one place is a global norm.

Application of Dirichlet's theorem

Example ($Y^2 + 3Z^2 = 5X + 7$)

Claim that the Hasse principle holds. By the Hasse norm theorem, it suffices to find some $x \in \mathbb{Q}$ such that $Y^2 + 3Z^2 = 5x + 7$ has points in $\mathbb{Q}_p$ for all places p of $\mathbb{Q}$ except possibly one prime. Observe that

$$(1)^2 + 3(1)^2 \equiv 5(1) + 7 \mod 2^3,$$

$$(3)^2 + 3(1)^2 \equiv 5(1) + 7 \mod 3^3,$$

so it has points in $\mathbb{Q}_2$ and $\mathbb{Q}_3$ by Hensel's lemma. It suffices to find some $x \in \mathbb{Q}$ such that $x \equiv 1 \mod 2^3$ and $x \equiv 1 \mod 3^3$, so that

$$5x + 7 = 5(2^3 \cdot 3^3 \cdot n + 1) + 7 = 2^2 \cdot 3 \cdot (90n + 1).$$

By Dirichlet's theorem, there is some n such that $90n + 1$ is prime. For instance, $n = 2$ gives $Y^2 + 3Z^2 = 2^2 \cdot 3 \cdot 181$, which has points in $\mathbb{Q}_2$, $\mathbb{Q}_3$, and $\mathbb{R}$, but also $\mathbb{Q}_p$ for all primes p except 181.

Application of Schinzel's hypothesis H

Dirichlet's theorem can be replaced by assuming Schinzel's hypothesis H.

Theorem (Colliot-Thélène–Sansuc, 1982)

Let $a_1, \ldots, a_k \in \mathbb{Q}^\times$, and let $f_1, \ldots, f_k \in \mathbb{Q}[X]$ be irreducible. Assume Schinzel's hypothesis H. Then the Hasse principle holds for

$$Y_1^2 + a_1 Z_1^2 = f_1(X), \qquad \ldots, \qquad Y_k^2 + a_k Z_k^2 = f_k(X).$$

Thus the Hasse principle conditionally holds for conic bundles over $\mathbb{P}^1_{\mathbb{Q}}$.

Example (Iskovskikh, 1971)

Let V be the variety over $\mathbb{Q}$ given by $Y^2 + Z^2 = -(X-2)(X-3)$. Then V has points in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p but no points in $\mathbb{Q}$. The failure of the Hasse principle can be detected by $(3 - X^2, -1) \in \mathrm{Br}(V)[2]$.

The Brauer–Manin obstruction

Let V be a variety over a global field K. There is a commutative diagram

$$\begin{array}{ccccccccc}
 & & V(K) & \longrightarrow & V(\mathbb{A}_K) & & & & \\
 & & \downarrow & & \downarrow{\scriptstyle (-)^*} & & & & \\
0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \xrightarrow[\mathrm{inv}_v]{} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0.
\end{array}$$

For any $A \in \mathrm{Br}(V)$, the Brauer–Manin set is

$$V(\mathbb{A}_K)^A := \left\{ (x_v)_v \in V(\mathbb{A}_K) : \sum_v \mathrm{inv}_v(x_v^* A) = 0 \right\}.$$

Example (Iskovskikh, 1971)

Let $A := (3 - X^2, -1) \in \mathrm{Br}(V)$. For any $(x_v)_v \in V(\mathbb{A}_K)$, it can be shown that $\sum_v \mathrm{inv}_v(x_v^* A) = \frac{1}{2}$, so that $V(K) \subseteq V(\mathbb{A}_K)^A = \emptyset$.

Rationally connected varieties

A rationally connected variety is a smooth projective variety such that any two geometric points are connected by a rational curve.

Conjecture (Colliot-Thélène, 2003)

Let V be a rationally connected variety over a number field K. If $V(K) = \emptyset$, then $V(\mathbb{A}_K)^A = \emptyset$ for some $A \in \mathrm{Br}(V)$.

This is known for conic bundles over $\mathbb{P}^1_{\mathbb{Q}}$ with at most five geometric degenerate fibres, due to Colliot-Thélène–Sansuc–Swinnerton-Dyer (1987), Colliot-Thélène (1990), and Salberger–Skorobogatov (1991).

Theorem (Colliot-Thélène–Swinnerton-Dyer, 1994)

Assume Schinzel's hypothesis H. Then Colliot-Thélène's conjecture holds for Severi–Brauer bundles over $\mathbb{P}^1_{\mathbb{Q}}$.