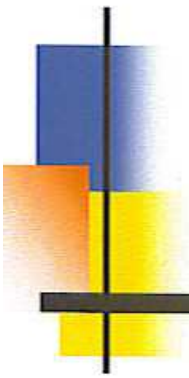


Primes and Orbits

Peter Sarnak

MAA GARDEN STATE
Undergraduate Mathematics
Conference
March 31, 2007

PRIMES AND ORBITS

PETER SARNAK

MAA GARDEN STATE UNDERGRADUATE MATHEMATICS CONFERENCE MARCH/31/2007

PRIMES AND ORBITS

Euclid: There are infinitely many primes:

Proof: $p_1, p_2, \ldots, p_l$,

$p_1 p_2 \cdots p_l + 1$

Euler: $s > 1$

$$\prod_p \frac{1}{1-p^{-s}} = \prod_p \left(1 + p^{-s} + p^{-2s} + \cdots\right)$$

$$= \sum_{n=1}^{\infty} n^{-s}$$

As $s \to 1$, $\sum \frac{1}{n} = \infty$

$$\Rightarrow \prod \frac{1}{1-p^{-1}} = \infty \quad \text{or} \quad \sum \frac{1}{p} = \infty$$

DIRICHLET: (PRIMES IN PROGRESSION)

"Local to global principle"

$A : x \to x + q$ translation

$A^m b = b + mq$, $m \in \mathbb{Z}$

$\mathcal{O} =$ orbit of b under

$L =$ gp generated by $A \leq \mathbb{Z}$

Does this orbit contain infinitely many primes?

If $d = \gcd(b, q) > 1$ then clearly not (local obstruction).

THM: If $\gcd(b, q) = 1$ are then there infinitely many primes in $\mathcal{O}(b, q)$.

TWIN PRIME CONJECTURE

Is x and $x+2$ prime for infinitely many x?

OR If $f(x) = x(x+2)$, is $f(x)$ a product of two primes for infinitely many x?

(no local obstruction)

NOT $x(x+1)$

BRUN finiteness Theorem via the combinatorial sieve:

- $f(x) = x(x+2)$ is a product of at most 18 primes for infinitely many x.

Chen (1970) $f(x)$ is a product of at most 3 primes for infinitely many x.

$$f(n) = n(n+2)$$

$n \leq x$, $z < x$.

$$P_z = \prod_{p \leq z} p$$

$$S(f, P) := \sum_{\substack{n \leq x. \\ (f(n), P) = 1}} 1$$

so $f(n)$ has no prime factors less than z ← want z as big as possible

Mobius inversion

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ distinct} \\ 0 & \text{otherwise} \end{cases}$$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

$$\sum_{\substack{n \le x \\ (f(n),P)=1}} 1 = \sum_{n \le x} \sum_{d \mid (f(n),P)} \mu(d)$$

$$= \sum_{d \mid P} \mu(d) \left(\sum_{\substack{n \le x \\ f(n) \equiv 0 (d)}} 1 \right)$$

$$\beta(d) = \#\{ m \bmod d : f(m) \equiv 0 (d) \}$$

for $d < x$

$$= \sum_{\substack{d \mid P \\ d < x}} \mu(d) \left(\frac{x \, \beta(d)}{d} + \text{error} \right)$$

# of integers in a progression

one can analyze this main term; combinatorial sieve
sieve mog.

if $z = x^{1/100}$ say (B')

$$S(f,P) \geq c \frac{x}{(\log x)^2}, \quad c > 0.$$

So $f(n)$'s in the sum have all their prime factors $\geq x^{1/100}$ and $f(n) \leq x^2$ so such $f(n)$ have a bounded no' of prime factors!

Higher dimensions (linear)

$0 \neq L < \mathbb{Z}^k$, L acting by translation.

$x \to x + l$, $l \in L$.

L is an abelian group

$\cong \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_r$, $w_j \in \mathbb{Z}^k$

linearly indep, $r = \text{rank}(L)$.

Fix $b \in \mathbb{Z}^k$

$$\mathcal{O} = \mathcal{O}_b = b + L$$

seek many points $x = (x_1, \ldots x_k) \in \mathcal{O}$ s.t. x_j are all prime $j = 1, \ldots k$

OR (essentially) $x_1 x_2 \ldots x_n$ is a product of k-primes.

How to measure "many"?

In one variable $S \subset \mathbb{A}^1$ affine space is infinite iff it is Zariski dense.

Zariski topology in $\mathbb{A}^k$ declares the closed sets to be zero sets of polynomials / ϕ (algebraic sets). So S is Zariski dense in $\mathbb{A}^k$ if & the points of S don't satisfy any non trivial polynomial equation.

denote by

$Zcl(S)$ The Zariski closure of S, the smallest algebraic set to contain S.

"HARDY LITTLEWOOD k-tuple conjecture"

$0 \neq L \leq \mathbb{Z}^k$, assume that the coordinate functions $x_j|_L \not\equiv 0$, $j = 1, \dots, k$.

$$\mathcal{O} = \mathcal{O}_b = b + L$$

then

$$Zcl\{x \in \mathcal{O} \mid x_j \text{ is prime for each } j\}$$

$$= Zcl\{x \in \mathcal{O} \mid x_1 x_2 \cdots x_k \text{ is a product of } k\text{-primes}\}$$

$$= Zcl(\mathcal{O})$$

iff there is no local congruence obstruction, IE for each $q \geq 1$ there is $x \in \mathcal{O}$ s.t. $x_1 x_2 \cdots x_k \in (\mathbb{Z}/q\mathbb{Z})^*$.

EG:

$$L = \{(m,m) : m \in \mathbb{Z}\} = \mathbb{Z}(1,1).$$

$\operatorname{rank} L = 1$. $\quad b = (0,2)$

$$b + L = \{(m, m+2) : m \in \mathbb{Z}\}$$

$(x_1, x_2) = x$ $\quad x_1, x_2$ both prime diff for Zariski dense in $Zcl(L) = \{(x_1, x_2) \mid x_1 = x_2 - 1\}$

iff twin prime conj is true.

PROGRESS:

(1) HARDY LITTLEWOOD

(2) I. VINOGRADOV (1930's).

If $L \subset \mathbb{Z}^3$ and $\operatorname{rank}(L) \geq 2$ and is nondegenerate then the Conjecture is true

(He uses H-L circle method + his sieve identity and bilinear estimates).

(3) GREEN-TAO 2006

If $L \subset \mathbb{Z}^4$ and $\text{rank}(L) \geq 2$ and L is nondegenerate then the Conjecture is true.

(uses Vinogradov's methods + Gowers methods in Szemeredi type theorems)

EG: $L = \mathbb{Z}(1,1,1,1) + \mathbb{Z}(0,1,2,3)$

then (x_1, x_2, x_3, x_4)

$= (m, m+n, m+2n, m+3n)$

IE get an arith progression in primes of length 4 (NO LOCAL OBSTRUCTION!)

What is the general problem?

above $A: x \to x + \ell$, $\ell \in L$

action of $\mathbb{A}^k$ preserving $\mathbb{Z}^k$

- Affine linear $A: \mathbb{A}^k \to \mathbb{A}^k$

$$A(x) = xa + \ell,$$

allow mult. and addition

a is an integral $k \times k$ matrix

a^{-1} " "

so $\det a = \pm 1$, i.e. $a \in GL_k(\mathbb{Z})$.

$\ell \in \mathbb{Z}^k$.

$\mathcal{O} = b.L$, L a group of such motion. ← (NO longer ~~super~~ linear)

$f \in \mathbb{Z}[x_1, \ldots, x_k]$ is given.

Given $(\mathcal{O}, f)$ we seek $\wedge$ points means $x \in \mathcal{O}$ for which $f(x)$ has few or even the minimal possible number of prime factors.

$(\mathcal{O}, f)$ given

Definition:

(i) $(\mathcal{O}, f)$ is (factor) finite if there is an $r < \infty$ s.t.

$$\#\{x \in \mathcal{O} \mid f(x) \text{ has at most } r \text{ prime factors}\} = \#\mathcal{O}$$

- Once $(\mathcal{O}, f)$ is finite we can ask for the minimal $r := r_0(\mathcal{O}, f)$.

Enemy (in terms of what we can prove)

TORUS (pure multiplication)

$\mathbb{A}^1$, $R = \mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$

$A(x) = 2x$ gp $\langle A \rangle = \{2^n\}_{n \in \mathbb{Z}}$

$f(x) = x - 1 \in R[x]$.

$\Leftrightarrow$ is $2^n - 1$ prime for infinitely many n? (Mersenne)

is there an $r < \infty$ s.t. $2^n - 1$ is a product of r primes for infinitely many n?

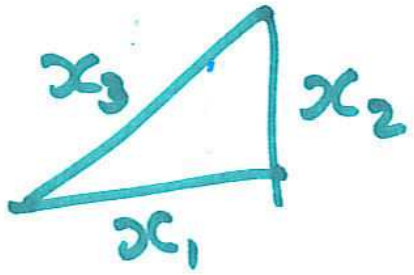
- $2^n - 1$ is too sparse both analytically and algebraically to do a combinatorial sieve.

Bourgain-Gamburd-S (2006/07)

As long as we avoid such tori we can execute a combinatorial sieve to prove $(\mathcal{O}, f)$ finiteness.

Example

PYTHAGORIAN TRIANGLES (TRIPLES)



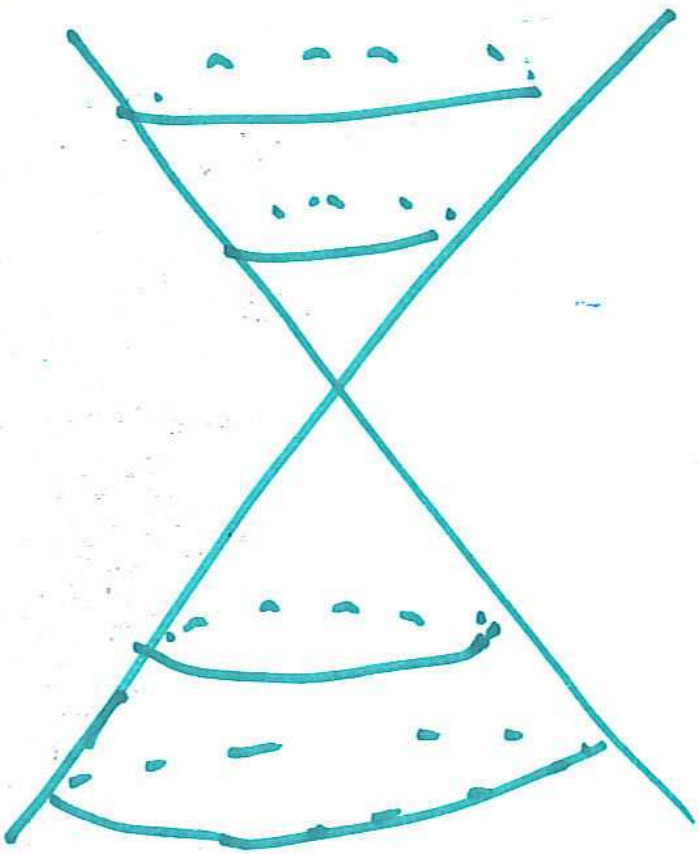
$(x_1, x_2, x_3) = 1$

$$F(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$$

Then $F(x_1, x_2, x_3) = 0$.

C

over $\mathbb{R}$ we have a cone $\wedge$ $F = 0$ in $\mathbb{R}^3$



Let $O_F(\mathbb{Z})$ be the group of 3×3 integer matrices A which preserve F i.e.

$$F(xA) = F(x)$$
$$\det A = \pm 1.$$

eg: $A_1 = \begin{bmatrix} 1 & 2 & 2 \\ -2 & -1 & -2 \\ 2 & 2 & 3 \end{bmatrix}$ $A_2 = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}$

$$A_3 = \begin{bmatrix} -1 & -2 & -2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}.$$

$O_F(\mathbb{Z})$ = gp generated by (A_1, A_2, A_3)

$O = (3,4,5)\, O_F(\mathbb{Z})$.

= all pythagorean triangles.

THM (BGS)

Let $f \in \mathbb{Z}[x_1, x_2, x_3]$ and

$L \leq O_f(\mathbb{Z})$ (L not elementary)

$\mathcal{O} = (3,4,5) \cdot L$

then $(\mathcal{O}, f)$ is finite

Eg: $f(x) = \frac{x_1 x_2}{2}$ = area of the triangle

Then there is a subset of $\mathcal{O}$ which is Zariski dense in $\mathbb{C}$ for whose areas have at most a fixed finite number of prime factors.

What is the minimal divisibility of the areas

I.E. $\tau_0(\mathcal{O}, \text{Area})$

Conjecture (BGS) $\tau_0(\mathcal{O}, \text{Area}) = 6$,

(THERE IS NO LOCAL OBSTRUCTION!)

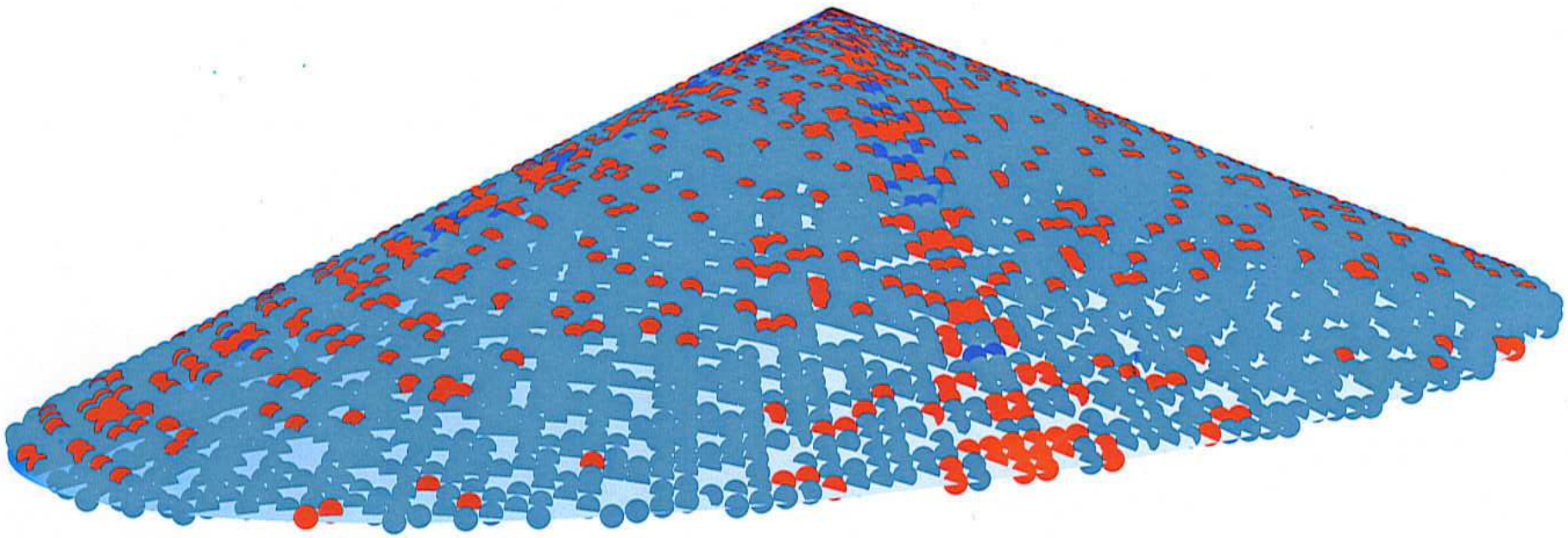
It is elementary (see B. TSOU P.V. junior thesis 2006) that from the Greek (or earlier) parametrization of pythagorean triples

$$x_1 = a^2 - b^2 \quad x_2 = 2ab \quad x_3 = a^2 + b^2$$

that $\tau_0(\mathcal{O}, \text{area}) \geq 6$ (the set with 5 prime factors is NOT Zariski dense in $\mathbb{C}$)

For the <u>full</u> orbit $(3,4,5)\,O_F(\mathbb{Z})$ it follows from the GREEN-TAO THEOREM above that the Conjecture is true.

- The minimal divisibility of the area a Zariski dense (in $\mathbb{C}$) set of pythagorean triangles is 6.



Cone of pythagoream triples
dark blue area ≤ 5 factors
red 6 prime factors
light blue ≥ 7

"thin" orbit of pythagorean triples

Some references:

- I. VINOGRADOV "REPRESENTATIONS OF AN ODD NUMBER AS A SUM OF PRIMES" DOKL. AK. NAUK SSSR 15, 1937, 291-294

- H. IWANIEC + E. KOWALSKI "ANALYTIC NUMBER THEORY" AMS COLLOQ. SERIES 2004 (see COMBINATORIAL SIEVE)

- B. GREEN and T. TAO "LINEAR EQUATIONS IN PRIMES" preprint 2006 see either of their webpages

- J. BOURGAIN, A. GAMBURD and P. SARNAK "SIEVING AND EXPANDERS" C.R. ACAD SCI, PARIS 1343 (2006) 155-159