Averages of multiplicative functions over integer sequences

Peter Koymans
(Joint work with Stephanie Chan, Carlo Pagano, Efthymios Sofos)

Chennai Mathematical Insitute

$\sim$

8 January 2024

Overview

Overview

1. For $f : \mathbb{N} \to [0, \infty)$ and $c_n \in \mathbb{N}$ can we estimate

$$\sum_{n=1}^{N} f(c_n) \ ?$$

Overview

1. For $f : \mathbb{N} \to [0, \infty)$ and $c_n \in \mathbb{N}$ can we estimate

$$\sum_{n=1}^{N} f(c_n) \ ?$$

2. Applications to arithmetic geometry?

Overview

1. For $f : \mathbb{N} \to [0, \infty)$ and $c_n \in \mathbb{N}$ can we estimate
$$\sum_{n=1}^{N} f(c_n) \ ?$$

2. Applications to arithmetic geometry?

3. Applications to algebraic number theory?

Class numbers

B/ If p is a small odd prime, the proportion of imaginary quadratic fields whose class number is divisible by p seems to be significantly greater than $1/p$ (for instance 43 % for $p=3$, 23.5 % for $p=5$).

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.
  - For $n \geq 1$, $\mathrm{Cl}_K[n]$ is the n-torsion subgroup.

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.
  - For $n \geq 1$, $\mathrm{Cl}_K[n]$ is the n-torsion subgroup.
- Interesting properties:
  - If $\#\mathrm{Cl}_K[n] = 1$, then $n \nmid \#\mathrm{Cl}_K[n]$.
  - Average upper bounds: $\#\mathrm{Cl}_K[n] = O(|D|^{\alpha(n)})$ (Soundararajan, Heath-Brown–Pierce, Frei–Widmer, Koymans–Thorner).

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.
  - For $n \geq 1$, $\mathrm{Cl}_K[n]$ is the n-torsion subgroup.
- Interesting properties:
  - If $\#\mathrm{Cl}_K[n] = 1$, then $n \nmid \#\mathrm{Cl}_K[n]$.
  - Average upper bounds: $\#\mathrm{Cl}_K[n] = O(|D|^{\alpha(n)})$ (Soundararajan, Heath-Brown–Pierce, Frei–Widmer, Koymans–Thorner).

Conjecture (Cohen & Lenstra)

- $\#\mathrm{Cl}_K[n]$ has constant average when n odd.

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.
  - For $n \geq 1$, $\mathrm{Cl}_K[n]$ is the n-torsion subgroup.
- Interesting properties:
  - If $\#\mathrm{Cl}_K[n] = 1$, then $n \nmid \#\mathrm{Cl}_K[n]$.
  - Average upper bounds: $\#\mathrm{Cl}_K[n] = O(|D|^{\alpha(n)})$ (Soundararajan, Heath-Brown–Pierce, Frei–Widmer, Koymans–Thorner).

Conjecture (Cohen & Lenstra)

- $\#\mathrm{Cl}_K[n]$ has constant average when n odd.
- $\#\mathrm{Cl}_K[n]$ exhibits average of order $\log |D|$ when n even.

- Consider $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ square-free.
- The ideal class group Cl_K:
  - Finite abelian group encoding crucial arithmetic information.
  - For $n \geq 1$, $\mathrm{Cl}_K[n]$ is the n-torsion subgroup.
- Interesting properties:
  - If $\#\mathrm{Cl}_K[n] = 1$, then $n \nmid \#\mathrm{Cl}_K[n]$.
  - Average upper bounds: $\#\mathrm{Cl}_K[n] = O(|D|^{\alpha(n)})$ (Soundararajan, Heath-Brown–Pierce, Frei–Widmer, Koymans–Thorner).

Conjecture (Cohen & Lenstra)

- $\#\mathrm{Cl}_K[n]$ has constant average when n odd.
- $\#\mathrm{Cl}_K[n]$ exhibits average of order $\log |D|$ when n even.

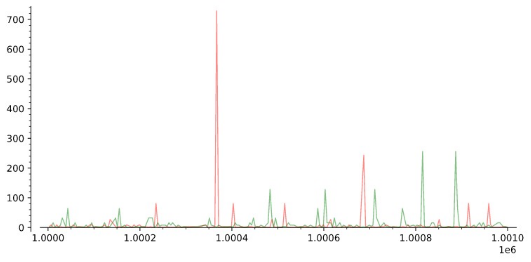
- Known cases:
  - $n = 3$: Davenport–Heilbronn, Bhargava–Shankar–Tsimerman.
  - $n = 2^k$: Fouvry–Klüners, A. Smith.

n-torsion with n divisible by more than one prime?

n-torsion with *n* divisible by more than one prime?
-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.

n-torsion with n divisible by more than one prime?

-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



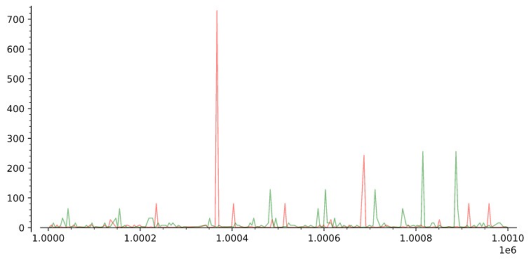
$D \asymp -10^6$

$\#\mathrm{Cl}_K[2]$

$\#\mathrm{Cl}_K[3]$

n-torsion with n divisible by more than one prime?

-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



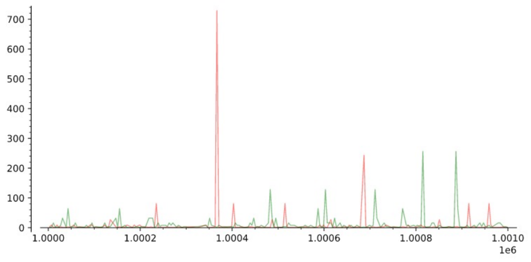
$D \asymp -10^6$

$\#\mathrm{Cl}_K[2]$

$\#\mathrm{Cl}_K[3]$

Theorem (CKPS, 2023) 2- and 3-torsions are independent

n-torsion with n divisible by more than one prime?
-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



$D \asymp -10^6$
$\#\mathrm{Cl}_K[2]$
$\#\mathrm{Cl}_K[3]$

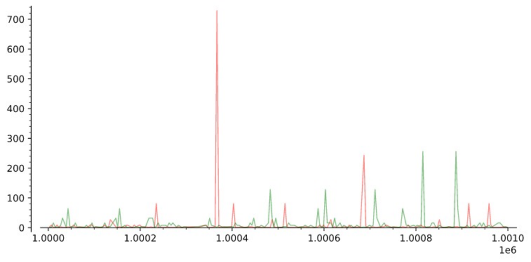
Theorem (CKPS, 2023) 2- and 3-torsions are independent

There are $c, c' > 0$ such that

$$c \log X \leq \frac{1}{X} \sum_{0<D<X} \#\mathrm{Cl}_K[6] \leq c' \log X.$$

n-torsion with n divisible by more than one prime?

-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



$D \asymp -10^6$

$\#\mathrm{Cl}_K[2]$

$\#\mathrm{Cl}_K[3]$

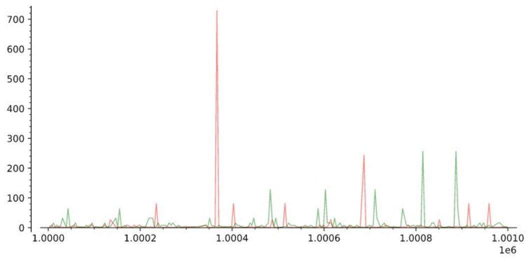
Theorem (CKPS, 2023) 2- and 3-torsions are independent

There are $c, c' > 0$ such that

$$c \log X \leq \frac{1}{X} \sum_{0<D<X} \#\mathrm{Cl}_K[6] \leq c' \log X.$$

n-torsion with n divisible by more than one prime?

-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



$D \asymp -10^6$

$\#\mathrm{Cl}_K[2]$

$\#\mathrm{Cl}_K[3]$

Theorem (CKPS, 2023) 2- and 3-torsions are independent

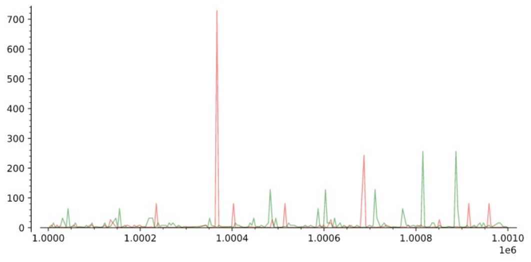
There are $c, c' > 0$ such that

$$c \log X \leq \frac{1}{X} \sum_{0<D<X} \#\mathrm{Cl}_K[6] \leq c' \log X.$$

- First “independence” result for Cohen–Lenstra

n-torsion with n divisible by more than one prime?

-know $\#\mathrm{Cl}_K[6] = \#\mathrm{Cl}_K[2] \cdot \#\mathrm{Cl}_K[3]$ but nothing on averages.



$D \asymp -10^6$

$\#\mathrm{Cl}_K[2]$

$\#\mathrm{Cl}_K[3]$

Theorem (CKPS, 2023) 2- and 3-torsions are independent

There are $c, c' > 0$ such that

$$c \log X \leq \frac{1}{X} \sum_{0<D<X} \#\mathrm{Cl}_K[6] \leq c' \log X.$$

- First "independence" result for Cohen–Lenstra
- same for negative discriminants
- MIXED MOMENTS:
  $\forall s > 0 \sum_{D<X} \#\mathrm{Cl}_K[2]^s \#\mathrm{Cl}_K[3] \asymp X(\log X)^{2^s-1}$.

Multiplicative functions over integer sequences

ON THE SUM $\sum_{k=1}^{x} d\big(f(k)\big)$

P. Erdös*.

1. Let $d(n)$ denote the number of divisors of a positive integer n, and let $f(k)$ be an irreducible polynomial of degree l with integral coefficients. We shall suppose for simplicity that $f(k) > 0$ for $k = 1, 2, \ldots$. In the present paper we prove the following result.

Theorem. *There exist positive constants c_1 and c_2 such that*

$$c_1 x \log x < \sum_{k=1}^{x} d\big(f(k)\big) < c_2 x \log x \tag{1}$$

for $x \geqslant 2$.

- $d(n) = \#\{\text{positive integer divisors of } n\}$

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \quad \rightsquigarrow \quad \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \rightsquigarrow \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

Goal

For "nice" integer sequences c_a, estimate

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) \qquad \text{for } X \geq 1.$$

- $\mathcal{A}$ countable set,

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \rightsquigarrow \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

Goal

For "nice" integer sequences c_a, estimate

$$\sum_{a\in\mathcal{A}} w_X(a) f(c_a) \qquad \text{for } X \geq 1.$$

- $\mathcal{A}$ countable set,
- f multiplicative and $0 \leq f \leq d^s$,

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \rightsquigarrow \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

Goal

For "nice" integer sequences c_a, estimate

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) \qquad \text{for } X \geq 1.$$

- $\mathcal{A}$ countable set,
- f multiplicative and $0 \leq f \leq d^s$,
- $w_X : \mathcal{A} \to [0, \infty)$ finite support function or more general.

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \quad \rightsquigarrow \quad \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

Goal

For "nice" integer sequences c_a, estimate

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) \qquad \text{for } X \geq 1.$$

- $\mathcal{A}$ countable set,
- f multiplicative and $0 \leq f \leq d^s$,
- $w_X : \mathcal{A} \to [0, \infty)$ finite support function or more general.

Asymptotics are very open: ∞ Square-Free values of $t^4 + 2$ open.

- $d(n) = \#\{\text{positive integer divisors of } n\}$
- multiplicative: $d(ab) = d(a)d(b)$ for coprime a, b
- Gauss' genus theory, $\#\mathrm{Cl}_K[2]$ is essentially $d(|D|)$.
- 3-torsion parametrized by polynomials $F(x_1, x_2, x_3, x_4)$

$$\sum_{0<D<X} \#\mathrm{Cl}_K[2]\#\mathrm{Cl}_K[3] \rightsquigarrow \sum_{(a_1,a_2,a_3,a_4)\in\mathbb{Z}^4\cap\mathcal{A}(X)} d(F(a_1, a_2, a_3, a_4))$$

Goal

For "nice" integer sequences c_a, estimate

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) \qquad \text{for } X \geq 1.$$

- $\mathcal{A}$ countable set,
- f multiplicative and $0 \leq f \leq d^s$,
- $w_X : \mathcal{A} \to [0, \infty)$ finite support function or more general.

Asymptotics are very open: ∞ Square-Free values of $t^4 + 2$ open.

- Happy with "correct" bounds
- Erdős (1952), Wolke (1971) special cases

Assumption: sequence "equidistributed" in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \leq M^{\epsilon}$

$$\sum_{\substack{a \in \mathcal{A} \\ c_a \equiv 0 \pmod{d}}} w_X(a) = h(d)M\left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

Assumption: sequence "equidistributed" in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \leq M^{\epsilon}$

$$\sum_{\substack{a \in \mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d) M \left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Assumption: sequence “equidistributed” in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \le M^\epsilon$

$$\sum_{\substack{a \in \mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d) M \left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Theorem (CKPS, 2023) The main tool

Assumption: sequence "equidistributed" in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \le M^\epsilon$

$$\sum_{\substack{a \in \mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d) M \left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Theorem (CKPS, 2023) The main tool

Fix $s > 0$, multiplicative $0 \le f \le d^s$, equidistributed c_a.

Assumption: sequence "equidistributed" in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \le M^\epsilon$

$$\sum_{\substack{a\in\mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d)M\left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Theorem (CKPS, 2023) The main tool

Fix $s > 0$, multiplicative $0 \le f \le d^s$, equidistributed c_a. Then

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) = O\left(M\prod_{p\le M}(1 + (f(p) - 1)h(p)) \right).$$

Assumption: sequence "equidistributed" in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \le M^\epsilon$

$$\sum_{\substack{a\in\mathcal{A} \\ c_a \equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d)M\left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Theorem (CKPS, 2023) The main tool

Fix $s > 0$, multiplicative $0 \le f \le d^s$, equidistributed c_a. Then

$$\sum_{a\in\mathcal{A}} w_X(a) f(c_a) = O\left(M \prod_{p\le M} (1 + (f(p) - 1)h(p)) \right).$$

- $\prod_{p\le M}$ gives the expected logarithms.

Assumption: sequence “equidistributed” in progressions

$\exists M = M(X),\ \epsilon,\ \epsilon' > 0$: for all $d \leq M^{\epsilon}$

$$\sum_{\substack{a\in\mathcal{A} \\ c_a\equiv 0 (\mathrm{mod}\ d)}} w_X(a) = h(d)M\left(1 + O(\log^{-2\kappa} M)\right) + O(M^{1-\epsilon'}).$$

- h multiplicative
- $h(p)$ looks like κ/p over the primes
- $h(p^t) = O_p(1/p^{\delta t})$ for some $\delta > 0$

Theorem (CKPS, 2023) The main tool

Fix $s > 0$, multiplicative $0 \leq f \leq d^s$, equidistributed c_a. Then

$$\sum_{a\in\mathcal{A}} w_X(a)f(c_a) = O\left(M\prod_{p\leq M}(1 + (f(p) - 1)h(p)) \right).$$

- $\prod_{p\leq M}$ gives the expected logarithms.
- 6-torsion: Belabas & Bhargava–Shankar–Tsimerman.

Remarks

- Proved it for more general f (submultiplicative).

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve $+$ Wolke $+$ Nair–Tenenbaum.

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve $+$ Wolke $+$ Nair–Tenenbaum.

- Wolke:

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve $+$ Wolke $+$ Nair–Tenenbaum.

- Wolke:
  - didn't allow twists w ($w_X(D) = \#\mathrm{Cl}_K[3]\mathbf{1}(|D| < X)$ in 6-torsion)

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve $+$ Wolke $+$ Nair–Tenenbaum.

- Wolke:
  - didn't allow twists w ($w_X(D) = \#\mathrm{Cl}_K[3]\mathbf{1}(|D| < X)$ in 6-torsion)
  - assumed polynomial saving; we assume logarithmic

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve $+$ Wolke $+$ Nair–Tenenbaum.

- Wolke:
  - didn't allow twists w ($w_X(D) = \#\mathrm{Cl}_K[3]\mathbf{1}(|D| < X)$ in 6-torsion)
  - assumed polynomial saving; we assume logarithmic
  - assumed $h(p^t) = O(1/p^t)$

$O(1/p^{\delta t})$ crucial applications with singular polynomials:

Remarks

- Proved it for more general f (submultiplicative).
- Obtained matching lower bound if $f(p^t) > g(t)$ for some $g > 0$.
- Proof: Rosser–Iwaniec sieve + Wolke + Nair–Tenenbaum.

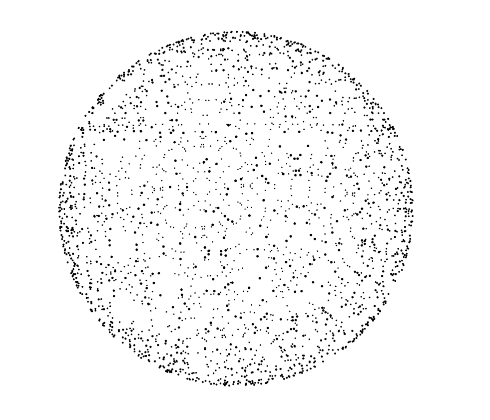
- Wolke:
  - didn't allow twists w ($w_X(D) = \#\mathrm{Cl}_K[3]\mathbf{1}(|D| < X)$ in 6-torsion)
  - assumed polynomial saving; we assume logarithmic
  - assumed $h(p^t) = O(1/p^t)$

$O(1/p^{\delta t})$ crucial applications with singular polynomials:
e.g. for the sequence $(y^2 + x^3)_{x,y \in \mathbb{N}}$ and $t \equiv 0 \pmod 6$:

$$h(p^t) = \frac{\#\left\{y, x \in \mathbb{Z}/p^t\mathbb{Z} : y^2 \equiv -x^3 \left(\bmod p^t\right)\right\}}{p^{2t}} \geq \frac{p^{t/2+2t/3}}{p^{2t}} = \frac{1}{p^{5t/6}}$$

Sums of three squares

Y. Linnik



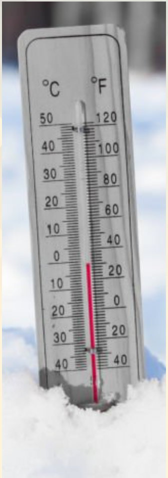
$$x^2 + y^2 + z^2 = 1\,000\,003$$

Goal

Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. <u>Count</u> integer solutions of $F = 0$ in expanding box centered at origin.

Goal

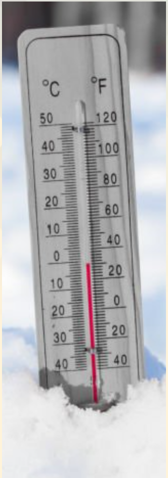
Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. Count integer solutions of $F = 0$ in expanding box centered at origin.



- $\boxed{\dfrac{n}{\deg(F)} > 2^{\deg(F)}}$ OK by circle method

Goal

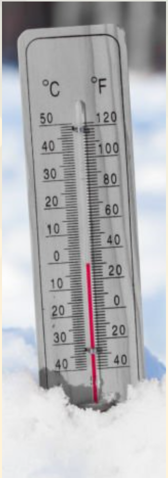
Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. <u>Count</u> integer solutions of $F = 0$ in expanding box centered at origin.



- $\boxed{\dfrac{n}{\deg(F)} > 2^{\deg(F)}}$ OK by circle method
- $\boxed{\dfrac{n}{\deg(F)} < 2}$ circle method “sub-convex” situation

Goal

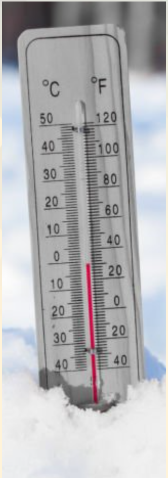
Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. Count integer solutions of $F = 0$ in expanding box centered at origin.



- $\boxed{\dfrac{n}{\deg(F)} > 2^{\deg(F)}}$ OK by circle method
- $\boxed{\dfrac{n}{\deg(F)} < 2}$ circle method "sub-convex" situation
- $\boxed{1 \leq \dfrac{n}{\deg(F)} < 2}$ Manin's conjecture for cubic surfaces, dynamics for Markoff-Hurwitz equations

Goal

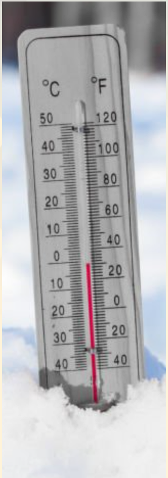
Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. <u>Count</u> integer solutions of $F = 0$ in expanding box centered at origin.



- $\boxed{\dfrac{n}{\deg(F)} > 2^{\deg(F)}}$ OK by circle method
- $\boxed{\dfrac{n}{\deg(F)} < 2}$ circle method "sub-convex" situation
- $\boxed{1 \leq \dfrac{n}{\deg(F)} < 2}$ Manin's conjecture for cubic surfaces, dynamics for Markoff-Hurwitz equations
- $\boxed{\dfrac{n}{\deg(F)} < 1}$ Fermat–Wiles regime: solutions rare

Goal

Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomial. Count integer solutions of $F = 0$ in expanding box centered at origin.



- $\boxed{\dfrac{n}{\deg(F)} > 2^{\deg(F)}}$ OK by circle method
- $\boxed{\dfrac{n}{\deg(F)} < 2}$ circle method "sub-convex" situation
- $\boxed{1 \leq \dfrac{n}{\deg(F)} < 2}$ Manin's conjecture for cubic surfaces, dynamics for Markoff-Hurwitz equations
- $\boxed{\dfrac{n}{\deg(F)} < 1}$ Fermat–Wiles regime: solutions rare
- $\boxed{\dfrac{n}{\deg(F)} < \dfrac{1}{2}}$ Very few examples known: singular planar curves (by determinant method: Bombieri–Pila and Heath-Brown–Salberger)

For $N \in \mathbb{N}$: $L(1, \chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right) \frac{1}{m}$

For $N \in \mathbb{N}$: $L(1,\chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p \mid N}} \left(1+\left(\frac{-1}{p}\right)\frac{1}{p}\right)$

For $N \in \mathbb{N}$: $L(1, \chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right) \frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1 + \left(\frac{-1}{p}\right) \frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N) L(1, \chi_{-N}) N^{\frac{1}{2}} \log N.$$

For $N \in \mathbb{N}$: $L(1,\chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1+\left(\frac{-1}{p}\right)\frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N) L(1,\chi_{-N}) N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\leq c_0$ and $\geq c_1$ for absolute constants c_i.

For $N \in \mathbb{N}$: $L(1,\chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1+\left(\frac{-1}{p}\right)\frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N) L(1,\chi_{-N}) N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\leq c_0$ and $\geq c_1$ for absolute constants c_i.
- Gauss: $L(1,\chi_{-N}) N^{\frac{1}{2}} = \#$ solutions of $x^2 + y^2 + z^2 = N$.

For $N \in \mathbb{N}$: $L(1, \chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right) \frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1 + \left(\frac{-1}{p}\right) \frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N) L(1, \chi_{-N}) N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\leq c_0$ and $\geq c_1$ for absolute constants c_i.
- Gauss: $L(1, \chi_{-N}) N^{\frac{1}{2}} = \#$ solutions of $x^2 + y^2 + z^2 = N$.
- Proof: $\sum_{x,y,z} d(z)$, sum over $x^2 + y^2 + z^2 = N$.

For $N \in \mathbb{N}$: $L(1,\chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1+\left(\frac{-1}{p}\right)\frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N)L(1,\chi_{-N})N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\leq c_0$ and $\geq c_1$ for absolute constants c_i.
- Gauss: $L(1,\chi_{-N})N^{\frac{1}{2}} = \#$ solutions of $x^2 + y^2 + z^2 = N$.
- Proof: $\sum_{x,y,z} d(z)$, sum over $x^2 + y^2 + z^2 = N$.
- Duke's work on cusp forms for equidistribution in progressions

For $N \in \mathbb{N}$: $L(1,\chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1+\left(\frac{-1}{p}\right)\frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

$$x^2 + y^2 + z^2 w^2 = N$$

is

$$\asymp c(N) L(1,\chi_{-N}) N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\le c_0$ and $\ge c_1$ for absolute constants c_i.
- Gauss: $L(1,\chi_{-N})N^{\frac{1}{2}} = \#$ solutions of $x^2 + y^2 + z^2 = N$.
- Proof: $\sum_{x,y,z} d(z)$, sum over $x^2 + y^2 + z^2 = N$.
- Duke's work on cusp forms for equidistribution in progressions
- Friedlander–Iwaniec: $\sum_{x,y,z} \Lambda(x)$ on Elliot–Halberstam & GRH

For $N \in \mathbb{N}$: $L(1, \chi_{-N}) = \sum_{m=1}^{\infty} \left(\frac{-N}{m}\right)\frac{1}{m}$ and $c(N) = \prod_{\substack{p \text{ prime} \\ p|N}} \left(1 + \left(\frac{-1}{p}\right)\frac{1}{p}\right)$

Theorem (CKPS, 2023).

For square-free $N \equiv 3 \pmod 8$ the number of sol's of

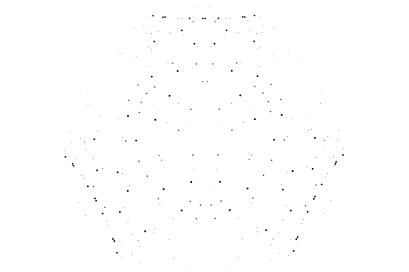
$$x^2 + y^2 + z^2 w^2 = N$$

is

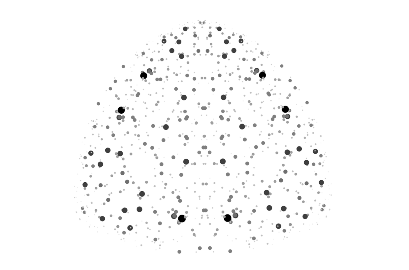
$$\asymp c(N) L(1, \chi_{-N}) N^{\frac{1}{2}} \log N.$$

- $\asymp$ means $\leq c_0$ and $\geq c_1$ for absolute constants c_i.
- Gauss: $L(1, \chi_{-N}) N^{\frac{1}{2}} = \#$ solutions of $x^2 + y^2 + z^2 = N$.
- Proof: $\sum_{x,y,z} d(z)$, sum over $x^2 + y^2 + z^2 = N$.
- Duke's work on cusp forms for equidistribution in progressions
- Friedlander–Iwaniec: $\sum_{x,y,z} \Lambda(x)$ on Elliot–Halberstam & GRH
- also $(x_1 \cdots x_k)^2 + x_{k+1}^2 + x_{k+2}^2 = N$ (where $n/\deg(F) \to 1/2$), and $(x_1 \cdots x_k)^2 + (x_{k+1} \cdots x_{2k})^2 + x_{2k+1}^2 = N$ e.t.c.

$(x, y, z) \in \mathbb{N}^3$ with $x^2 + y^2 + z^2 = N$



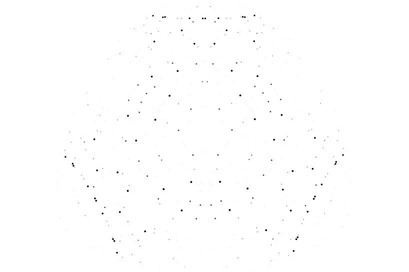
$\boldsymbol{N = 1\,716\,099}$



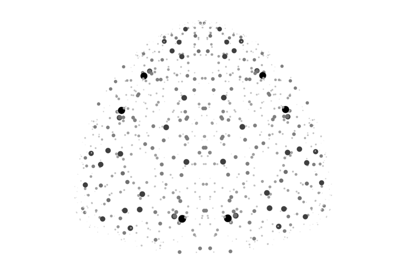
$\boldsymbol{N = 1\,707\,035}$

Color intensity analogous to the size of $\tau(x)\tau(y)\tau(z)$.

$(x, y, z) \in \mathbb{N}^3$ with $x^2 + y^2 + z^2 = N$



$\boldsymbol{N = 1\,716\,099}$

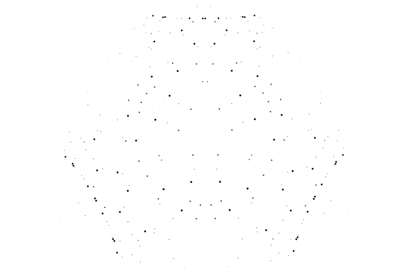


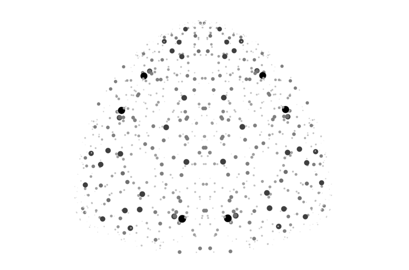
$\boldsymbol{N = 1\,707\,035}$

Color intensity analogous to the size of $\tau(x)\tau(y)\tau(z)$.

- 960 solutions in first image, 936 solutions in second!

$(x, y, z) \in \mathbb{N}^3$ with $x^2 + y^2 + z^2 = N$



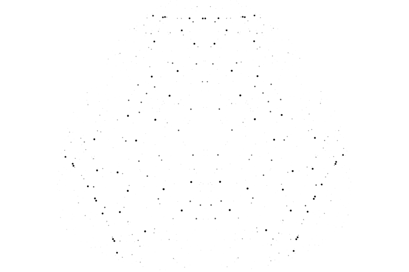


$N = 1\,716\,099$ $\qquad$ $N = 1\,707\,035$

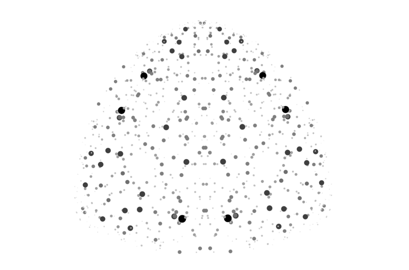
Color intensity analogous to the size of $\tau(x)\tau(y)\tau(z)$.

- 960 solutions in first image, 936 solutions in second!
- $1716099 = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$ (all except 17 are 3 mod 4)

$(x, y, z) \in \mathbb{N}^3$ with $x^2 + y^2 + z^2 = N$



$N = 1\,716\,099$

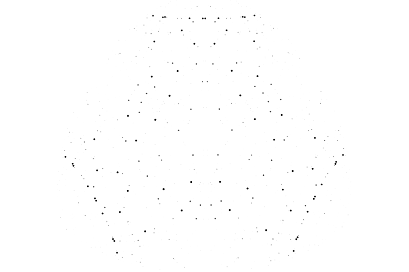


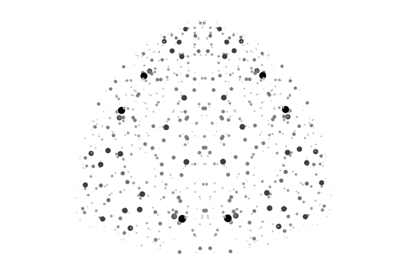
$N = 1\,707\,035$

Color intensity analogous to the size of $\tau(x)\tau(y)\tau(z)$.

- 960 solutions in first image, 936 solutions in second!
- $1716099 = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$ (all except 17 are 3 mod 4)
  $1707035 = 5 \cdot 11 \cdot 41 \cdot 757$ (only 11 is 3 mod 4)

$(x, y, z) \in \mathbb{N}^3$ with $x^2 + y^2 + z^2 = N$





$N = 1\,716\,099$ **$N = 1\,707\,035$**

Color intensity analogous to the size of $\tau(x)\tau(y)\tau(z)$.

- 960 solutions in first image, 936 solutions in second!
- $1716099 = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$ (all except 17 are 3 mod 4)
  $1707035 = 5 \cdot 11 \cdot 41 \cdot 757$ (only 11 is 3 mod 4)
- prefactor $c(N)$ biased against primes 3 mod 4

Summary

1. Tool for general averages.
2. Independent Cohen–Lenstra.
3. Count solutions in few variables.