Results of modern sieve methods in prime number theory and more

Karin Halupczok (WWU Münster)

EWM-Conference 2012, Universität Bielefeld,
1–2 November 2012

1 Basic ideas of sieve theory

2 Classical applications in prime number theory

3 Selected examples of further applications

4 Linnik's problem and the large sieve

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,
then all $n \in A$ with $3 \mid n$,

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,
then all $n \in A$ with $3 \mid n$,
then all $n \in A$ with $5 \mid n$
(multiples of 4 have already been crossed out),

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,
then all $n \in A$ with $3 \mid n$,
then all $n \in A$ with $5 \mid n$
(multiples of 4 have already been crossed out),
and so on ...

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,
then all $n \in A$ with $3 \mid n$,
then all $n \in A$ with $5 \mid n$
(multiples of 4 have already been crossed out),
and so on ...

Stop when all multiples of integers $\leq 10 = \sqrt{100}$ are crossed out.

What is sieve theory about?

Starting Point: The ancient sieve of Eratosthenes producing a list of primes:

Take $A = \{1, \ldots, 100\}$,
then cross out all $n \in A$ with $2 \mid n$,
then all $n \in A$ with $3 \mid n$,
then all $n \in A$ with $5 \mid n$
(multiples of 4 have already been crossed out),
and so on ...

Stop when all multiples of integers $\leq 10 = \sqrt{100}$ are crossed out.

The remaining numbers must be the primes $\in \{10, \ldots, 100\}$, since every composed integer ≤ 100 has a prime divisor $\leq 10 = \sqrt{100}$ and was therefore crossed out in the algorithm.

Animation of the sieve of Eratosthenes

~~01~~	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Animation of the sieve of Eratosthenes

~~01~~	~~02~~	03	~~04~~	05	~~06~~	07	~~08~~	09	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Animation of the sieve of Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	05	~~06~~	07	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Animation of the sieve of Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	07	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Animation of the sieve of Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	~~07~~	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Animation of the sieve of Eratosthenes

~~01~~	~~02~~	~~03~~	~~04~~	~~05~~	~~06~~	~~07~~	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Basic sieve notation

Consider a finite set of objects $\mathcal{A}$ and let $\mathcal{P}$ be a set of positive prime numbers such that for each $p \in \mathcal{P}$ there is associated a subset $\mathcal{A}_p$ of $\mathcal{A}$.

Basic sieve notation

Consider a finite set of objects $\mathcal{A}$ and let $\mathcal{P}$ be a set of positive prime numbers such that for each $p \in \mathcal{P}$ there is associated a subset $\mathcal{A}_p$ of $\mathcal{A}$.

The general sieve problem is then to give upper and lower bounds for the cardinality of the sieved set

$$\mathcal{S}(\mathcal{A}, \mathcal{P}) := \mathcal{A} \setminus \bigcup_{p \in \mathcal{P}} \mathcal{A}_p.$$

Basic sieve notation

Consider a finite set of objects $\mathcal{A}$ and let $\mathcal{P}$ be a set of positive prime numbers such that for each $p \in \mathcal{P}$ there is associated a subset $\mathcal{A}_p$ of $\mathcal{A}$.

The general sieve problem is then to give upper and lower bounds for the cardinality of the sieved set

$$\mathcal{S}(\mathcal{A}, \mathcal{P}) := \mathcal{A} \setminus \bigcup_{p \in \mathcal{P}} \mathcal{A}_p.$$

For a real $z \geq 1$ define $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$. The goal is to estimate $S(\mathcal{A}, \mathcal{P}, z) := \#\left(\mathcal{A} \setminus \bigcup_{p | P(z)} \mathcal{A}_p\right)$, which we call the sieve function.

The sieve function in the sieve of Eratosthenes

The sieve of Eratosthenes is the standard example:

For a real $x \geq 1$ (above: $x = 100$) let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

The sieve function in the sieve of Eratosthenes

The sieve of Eratosthenes is the standard example:

For a real $x \geq 1$ (above: $x = 100$) let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

Further let $\mathcal{A}_p := \{n \in \mathcal{A};\ p \mid n\}$.

The sieve function in the sieve of Eratosthenes

The sieve of Eratosthenes is the standard example:

For a real $x \geq 1$ (above: $x = 100$) let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.
Further let $\mathcal{A}_p := \{n \in \mathcal{A};\ p \mid n\}$. Then the sieve function is

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \#\Big(\mathcal{A} \setminus \bigcup_{p \mid P(z)} \mathcal{A}_p\Big) \\ &= \#\{n \in \mathcal{A};\ (p \mid n \Rightarrow p \geq z) \text{ for all } p \in \mathcal{P}\} \\ &= \#\{n \leq x;\ \gcd(n, P(z)) = 1\} \\ &= \pi(x) - \pi(z), \end{aligned}$$

where $\pi(x) := \#\{p \leq x;\ p \text{ prime}\}$ denotes the prime number counting function.

Results for the prime counting function

Using sieve theory, the expected bounds $C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}$ with constants $0 < C_1 < 1 < C_2$ can be shown, but the prime number theorem

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \lim_{x \to \infty} \frac{\pi(x)}{x / \log x} = 1$$

can not be reached this way.

Results for the prime counting function

Using sieve theory, the expected bounds $C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}$ with constants $0 < C_1 < 1 < C_2$ can be shown, but the prime number theorem

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \lim_{x \to \infty} \frac{\pi(x)}{x / \log x} = 1$$

can not be reached this way.

But if $z \leq \log x$, sieve theory shows that

$$\#\{n \leq x;\ \gcd(n, P(z)) = 1\} \sim \frac{e^{-\gamma} x}{\log z},$$

with $\gamma := \lim_{n \to \infty} (\sum_{k=1}^{n} \frac{1}{k} - \log n) = 0,57721\ldots$ being the Euler–Mascheroni constant.

Another basic example of a sieve

The twin prime sieve:

For a real $x \geq 1$ let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes $p \neq 2$, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

Another basic example of a sieve

The twin prime sieve:

For a real $x \geq 1$ let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes $p \neq 2$, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.
Now let $\mathcal{A}_p := \{n \in \mathcal{A};\ n \equiv 0 \bmod p \text{ or } n \equiv -2 \bmod p\}$.

Another basic example of a sieve

The twin prime sieve:

For a real $x \geq 1$ let $\mathcal{A} := \{n \in \mathbb{N};\ n \leq x\}$, let $\mathcal{P}$ be the set of all primes $p \neq 2$, let $\sqrt{x} < z \leq x$ and $P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.
Now let $\mathcal{A}_p := \{n \in \mathcal{A};\ n \equiv 0 \bmod p \text{ or } n \equiv -2 \bmod p\}$.

Then $\pi_2(x) \leq \pi(z) + S(\mathcal{A}, \mathcal{P}, z)$, where

$$\pi_2(x) := \#\{p \leq x;\ p, p+2 \text{ prime}\}$$

denotes the twin prime counting function.

Sieve theory today

The starting point of the enormous development of modern sieve theory was Brun's sieve in the 1920ies. Applied to the twin prime problem, it shows that the set of twin primes is small compared to the set of all primes: $\pi_2(x) \ll \frac{x}{\log^2 x}$, so that

Sieve theory today

The starting point of the enormous development of modern sieve theory was Brun's sieve in the 1920ies. Applied to the twin prime problem, it shows that the set of twin primes is small compared to the set of all primes: $\pi_2(x) \ll \frac{x}{\log^2 x}$, so that $\sum_{p \in \mathcal{T}} \frac{1}{p}$ converges, if p runs through the set $\mathcal{T}$ of twin primes.

Sieve theory today

The starting point of the enormous development of modern sieve theory was Brun's sieve in the 1920ies. Applied to the twin prime problem, it shows that the set of twin primes is small compared to the set of all primes: $\pi_2(x) \ll \frac{x}{\log^2 x}$, so that $\sum_{p \in \mathcal{T}} \frac{1}{p}$ converges, if p runs through the set $\mathcal{T}$ of twin primes.

Modern sieve theory provides nowadays a collection of sieve theorems giving estimates for sieve functions. Often, they involve very elaborated ideas in their proofs. These theorems can be used as tools in applications, like a "black box".

Sieve theory today

The starting point of the enormous development of modern sieve theory was Brun's sieve in the 1920ies. Applied to the twin prime problem, it shows that the set of twin primes is small compared to the set of all primes: $\pi_2(x) \ll \frac{x}{\log^2 x}$, so that $\sum_{p \in \mathcal{T}} \frac{1}{p}$ converges, if p runs through the set $\mathcal{T}$ of twin primes.

Modern sieve theory provides nowadays a collection of sieve theorems giving estimates for sieve functions. Often, they involve very elaborated ideas in their proofs. These theorems can be used as tools in applications, like a "black box".

Many of them have been applied in the classical branch of prime number theory where they have been created for, but today they also occur in several other branches of mathematics.

1 Basic ideas of sieve theory

2 Classical applications in prime number theory

3 Selected examples of further applications

4 Linnik's problem and the large sieve

1. Primes in short intervals

Does the real interval $[n, n + \sqrt{n}[$ contain primes for all large $n \in \mathbb{N}$? This is an open conjecture.

1. Primes in short intervals

Does the real interval $[n, n + \sqrt{n}[$ contain primes for all large $n \in \mathbb{N}$? This is an open conjecture.

Under assumption of Riemann's hypothesis, there exist primes in all intervals $[n, n + n^{1/2+\varepsilon}[$ with large n, for any $\varepsilon > 0$.

1. Primes in short intervals

Does the real interval $[n, n + \sqrt{n}[$ contain primes for all large $n \in \mathbb{N}$? This is an open conjecture.

Under assumption of Riemann's hypothesis, there exist primes in all intervals $[n, n + n^{1/2+\varepsilon}[$ with large n, for any $\varepsilon > 0$.

Unconditionally, it is proved that there are primes in intervals of the form $[n, n + n^{11/20}[$ for all large n [G. Harman 2007].

1. Primes in short intervals

Does the real interval $[n, n + \sqrt{n}[$ contain primes for all large $n \in \mathbb{N}$? This is an open conjecture.

Under assumption of Riemann's hypothesis, there exist primes in all intervals $[n, n + n^{1/2+\varepsilon}[$ with large n, for any $\varepsilon > 0$.

Unconditionally, it is proved that there are primes in intervals of the form $[n, n + n^{11/20}[$ for all large n [G. Harman 2007].

Further, if Riemann's hypothesis is assumed, almost all intervals $[n, n + \log^2 n[$ with $n \leq X$ (with the exception of $o(X)$ many) contain primes.

2. Primes represented by polynomials

If $f(x) \in \mathbb{Z}[x]$ is a nonconstant irreducible polynomial with positive leading term, and if $f(n)$ has no fixed prime divisor for $n \in \mathbb{N}$, does $f(n)$ will take on infinitely many prime values? This is an open conjecture.

2. Primes represented by polynomials

If $f(x) \in \mathbb{Z}[x]$ is a nonconstant irreducible polynomial with positive leading term, and if $f(n)$ has no fixed prime divisor for $n \in \mathbb{N}$, does $f(n)$ will take on infinitely many prime values? This is an open conjecture.

Dirichlet's Theorem shows that this is true for linear f, but there are no known results for higher degree, except special cases.

2. Primes represented by polynomials

If $f(x) \in \mathbb{Z}[x]$ is a nonconstant irreducible polynomial with positive leading term, and if $f(n)$ has no fixed prime divisor for $n \in \mathbb{N}$, does $f(n)$ will take on infinitely many prime values? This is an open conjecture.

Dirichlet's Theorem shows that this is true for linear f, but there are no known results for higher degree, except special cases.

For polynomials in two variables, the case $m^2 + n^2$ is well understood, and also other quadratic cases.

2. Primes represented by polynomials

If $f(x) \in \mathbb{Z}[x]$ is a nonconstant irreducible polynomial with positive leading term, and if $f(n)$ has no fixed prime divisor for $n \in \mathbb{N}$, does $f(n)$ will take on infinitely many prime values? This is an open conjecture.

Dirichlet's Theorem shows that this is true for linear f, but there are no known results for higher degree, except special cases.

For polynomials in two variables, the case $m^2 + n^2$ is well understood, and also other quadratic cases.

Other results towards higher-degree analogs: $m^2 + n^4$ takes on prime values infinitely often [J. Friedlander and H. Iwaniec 1989].

2. Primes represented by polynomials

If $f(x) \in \mathbb{Z}[x]$ is a nonconstant irreducible polynomial with positive leading term, and if $f(n)$ has no fixed prime divisor for $n \in \mathbb{N}$, does $f(n)$ will take on infinitely many prime values? This is an open conjecture.

Dirichlet's Theorem shows that this is true for linear f, but there are no known results for higher degree, except special cases.

For polynomials in two variables, the case $m^2 + n^2$ is well understood, and also other quadratic cases.

Other results towards higher-degree analogs: $m^2 + n^4$ takes on prime values infinitely often [J. Friedlander and H. Iwaniec 1989].

$x^3 + 2y^3$ similar [D. R. Heath-Brown 2001].

3. Diophantine Approximation

It is known that if $\alpha \in \mathbb{R}$ is irrational, then there are infinitely many pairs of coprime integers m, n with $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

3. Diophantine Approximation

It is known that if $\alpha \in \mathbb{R}$ is irrational, then there are infinitely many pairs of coprime integers m, n with $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

But can we hope to get infinitely many solutions to $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$, for some fixed $0 < \theta \leq 1$?

3. Diophantine Approximation

It is known that if $\alpha \in \mathbb{R}$ is irrational, then there are infinitely many pairs of coprime integers m, n with $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

But can we hope to get infinitely many solutions to $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$, for some fixed $0 < \theta \leq 1$?

Assuming stronger conjectures than the GRH, this is true for $0 < \theta < 1/3$.

3. Diophantine Approximation

It is known that if $\alpha \in \mathbb{R}$ is irrational, then there are infinitely many pairs of coprime integers m, n with $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$.

But can we hope to get infinitely many solutions to $|\alpha - \frac{m}{p}| < \frac{1}{p^{1+\theta}}$, for some fixed $0 < \theta \leq 1$?

Assuming stronger conjectures than the GRH, this is true for $0 < \theta < 1/3$.

The statement is false for $\theta = 1$: There are uncountably many α such that

$$\|\alpha p\| < \frac{\log p}{500p \log \log p}$$

has only finitely many solutions in primes p, where $\|x\| := \min_{m \in \mathbb{Z}} |x - m|$ [G. Harman 1995].

4. Primes in arithmetic progressions

Question: What is the smallest prime in an arithmetic progression?

4. Primes in arithmetic progressions

Question: What is the smallest prime in an arithmetic progression?

So, for a given residue class $a \bmod q$ with $\gcd(a, q) = 1$, we ask for the size of $p_{\min(q,a)} := \min\{p \text{ prime};\ p \equiv a \bmod q\}$.

4. Primes in arithmetic progressions

Question: What is the smallest prime in an arithmetic progression?

So, for a given residue class a mod q with $\gcd(a,q)=1$, we ask for the size of $p_{\min(q,a)} := \min\{p \text{ prime};\ p \equiv a \bmod q\}$.

Y. Linnik showed in [1944] that there is an absolute constant $L>0$ such that $p_{\min(q,a)} \ll q^L$, called Linnik's constant.

4. Primes in arithmetic progressions

Question: What is the smallest prime in an arithmetic progression?

So, for a given residue class $a \bmod q$ with $\gcd(a, q) = 1$, we ask for the size of $p_{\min(q,a)} := \min\{p \text{ prime}; \; p \equiv a \bmod q\}$.

Y. Linnik showed in [1944] that there is an absolute constant $L > 0$ such that $p_{\min(q,a)} \ll q^L$, called Linnik's constant.

This can be done using the classical zero-free region for L-functions.

4. Primes in arithmetic progressions

Question: What is the smallest prime in an arithmetic progression?

So, for a given residue class a mod q with $\gcd(a, q) = 1$, we ask for the size of $p_{\min(q,a)} := \min\{p \text{ prime};\ p \equiv a \bmod q\}$.

Y. Linnik showed in [1944] that there is an absolute constant $L > 0$ such that $p_{\min(q,a)} \ll q^L$, called Linnik's constant.

This can be done using the classical zero-free region for L-functions.

We know today by Bombieri–Vinogradov's theorem, that $p_{\min(q,a)} \ll q^{2+\varepsilon}$ is true for almost all q. This bound is predicted to hold for all q by the GRH.

1 Basic ideas of sieve theory

2 Classical applications in prime number theory

3 Selected examples of further applications

4 Linnik's problem and the large sieve

1. p-adic zeros of quadratic forms

A problem of J.-P. Serre [1990] concerning the quadratic form $\varphi_{a,b}(X, Y, Z) = aX^2 + bY^2 - Z^2$: For how many positive integers a and b does $\varphi_{a,b}$ have a nontrivial rational zero? By the Minkowski local-global principle, one asks for the p-adic solutions for every prime p. There exists a p-adic solution iff the Hilbert symbol satisfies $\left(\frac{a,b}{p}\right) = 1$.

1. p-adic zeros of quadratic forms

A problem of J.-P. Serre [1990] concerning the quadratic form $\varphi_{a,b}(X,Y,Z) = aX^2 + bY^2 - Z^2$: For how many positive integers a and b does $\varphi_{a,b}$ have a nontrivial rational zero? By the Minkowski local-global principle, one asks for the p-adic solutions for every prime p. There exists a p-adic solution iff the Hilbert symbol satisfies $\left(\frac{a,b}{p}\right) = 1$.

Answer: The number of pairs (a,b) with $1 \leq a, b \leq H$ for which $\varphi_{a,b}$ has a nontrivial rational zero is $\ll H^2 / \log\log H$.

1. p-adic zeros of quadratic forms

A problem of J.-P. Serre [1990] concerning the quadratic form $\varphi_{a,b}(X,Y,Z) = aX^2 + bY^2 - Z^2$: For how many positive integers a and b does $\varphi_{a,b}$ have a nontrivial rational zero? By the Minkowski local-global principle, one asks for the p-adic solutions for every prime p. There exists a p-adic solution iff the Hilbert symbol satisfies $\left(\frac{a,b}{p}\right) = 1$.

Answer: The number of pairs (a,b) with $1 \leq a, b \leq H$ for which $\varphi_{a,b}$ has a nontrivial rational zero is $\ll H^2 / \log\log H$.

More accurate: Let $\mathcal{P}$ be an infinite set of odd primes. If the set $\mathcal{P}_b := \{p \in \mathcal{P};\ \left(\frac{b}{p}\right) = -1\}$ is sufficiently large such that $\sum_{p\in\mathcal{P}_b} \frac{1}{p} = \infty$, then for almost all squarefree a being coprime with $2b$, the quadratic form $\varphi_{a,b}$ fails to have a nontrivial p-adic zero for at least one $p \in \mathcal{P}$.

2. Rational points on cubic surfaces

Consider cubic surfaces $F(x) = \varphi(u, v)$, where F is a cubic polynomial and $\varphi(u, v)$ a binary quadratic form.

2. Rational points on cubic surfaces

Consider cubic surfaces $F(x) = \varphi(u, v)$, where F is a cubic polynomial and $\varphi(u, v)$ a binary quadratic form.

Under some mild conditions, there are infinitely many rational points on Châtelet-surfaces where $\varphi(u, v) = u^2 - cv^2$ [H. Iwaniec and R. Munshi, 2010]. Even some strong estimates can be given for the number of such points with bounded height.

2. Rational points on cubic surfaces

Consider cubic surfaces $F(x) = \varphi(u, v)$, where F is a cubic polynomial and $\varphi(u, v)$ a binary quadratic form.

Under some mild conditions, there are infinitely many rational points on Châtelet-surfaces where $\varphi(u, v) = u^2 - cv^2$ [H. Iwaniec and R. Munshi, 2010]. Even some strong estimates can be given for the number of such points with bounded height.

E.g. the case $c = -1$: Let $F(X) = X^3 + \alpha X^2 + \beta X + \gamma \in \mathbb{Z}[X]$ with $\alpha + \beta + \gamma \equiv 0 \bmod 4$. Then $F(x) = u^2 + v^2$ has infinitely many rational points (x, u, v). The number of such rational points having denominators at most y is $\gg y(\log y)^{-3/2}$.

3. Points on elliptic curves

A problem of twin prime type on elliptic curves:
Consider an elliptic curve $E/\mathbb{Q}$.

3. Points on elliptic curves

A problem of twin prime type on elliptic curves:
Consider an elliptic curve $E/\mathbb{Q}$.

Koblitz' conjecture: There are infinitely many p such that the order of $E/\mathbb{F}_p$ is a prime number (after the injection of torsion has been divided out).
Koblitz' conjecture is true on average
[A. Balog, A. C. Cojocaru, C. David 2011].

3. Points on elliptic curves

A problem of twin prime type on elliptic curves:
Consider an elliptic curve $E/\mathbb{Q}$.

Koblitz' conjecture: There are infinitely many p such that the order of $E/\mathbb{F}_p$ is a prime number (after the injection of torsion has been divided out).
Koblitz' conjecture is true on average
[A. Balog, A. C. Cojocaru, C. David 2011].

Further, e. g. for the curve $E: y^2 = x^3 - x$, it can be shown that

$$\#\{p \leq x;\ p \equiv 1\ (4),\ \#(E/\mathbb{F}_p) = 8P_2\} \gg x(\log x)^2,$$

where P_2 is a positive integer having at most two prime factors.

3. Points on elliptic curves

A problem of twin prime type on elliptic curves:
Consider an elliptic curve $E/\mathbb{Q}$.

Koblitz' conjecture: There are infinitely many p such that the order of $E/\mathbb{F}_p$ is a prime number (after the injection of torsion has been divided out).
Koblitz' conjecture is true on average
[A. Balog, A. C. Cojocaru, C. David 2011].

Further, e. g. for the curve $E : y^2 = x^3 - x$, it can be shown that

$$\#\{p \leq x;\ p \equiv 1\ (4),\ \#(E/\mathbb{F}_p) = 8P_2\} \gg x(\log x)^2,$$

where P_2 is a positive integer having at most two prime factors.
The expected asymptotic formula with P_2 replaced by a prime is an unsolved conjecture, considered to be as hard as the twin prime problem itsself.

4. Probabilistic Galois theory

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with leading term 1.
We expect: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ with probability 1.

4. Probabilistic Galois theory

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with leading term 1.
We expect: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ with probability 1.
Consider

$$E_n(H) := \#\{(z_1, \dots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n, \\ \text{such that } f(x) = x^n + z_1 x^{n-1} + \cdots + z_n \\ \text{has } \underline{\text{not}}\ S_n \text{ as Galois group}\}.$$

One can easily show that the number of reducible f with $|z_i| \leq H$ is $\gg H^{n-1}$, so that $E_n(H) \gg H^{n-1}$.

4. Probabilistic Galois theory

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with leading term 1.
We expect: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ with probability 1.
Consider

$$E_n(H) := \#\{(z_1, \ldots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n, \text{ such that } f(x) = x^n + z_1 x^{n-1} + \cdots + z_n \text{ has } \underline{\text{not}}\ S_n \text{ as Galois group}\}.$$

One can easily show that the number of reducible f with $|z_i| \leq H$ is $\gg H^{n-1}$, so that $E_n(H) \gg H^{n-1}$.

It is conjectured that $E_n(H) \ll_{n,\varepsilon} (H^{n-1+\varepsilon})$. This bound has been confirmed for $n = 2, 3, 4$ [P. Lefton 1979, R. Dietmann 2012].

4. Probabilistic Galois theory

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with leading term 1.
We expect: $\mathrm{Gal}(f|\mathbb{Q}) \cong S_n$ with probability 1.
Consider

$$E_n(H) := \#\{(z_1, \dots, z_n);\ |z_i| \leq H,\ 1 \leq i \leq n,\ \text{such that } f(x) = x^n + z_1 x^{n-1} + \dots + z_n \text{ has } \underline{\text{not}}\ S_n \text{ as Galois group}\}.$$

One can easily show that the number of reducible f with $|z_i| \leq H$ is $\gg H^{n-1}$, so that $E_n(H) \gg H^{n-1}$.

It is conjectured that $E_n(H) \ll_{n,\varepsilon} (H^{n-1+\varepsilon})$. This bound has been confirmed for $n = 2, 3, 4$ [P. Lefton 1979, R. Dietmann 2012].

The best known uniform upper bound up to date is $E_n(H) \ll H^{n-1/2}$ [D. Zywina 2010].

5. Example in group theory

Question: "For how many $n \leq x$ is any group of order n cyclic?"

5. Example in group theory

Question: "For how many $n \leq x$ is any group of order n cyclic?"

List of isomorphism classes of groups by order:

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$

...

5. Example in group theory

Question: "For how many $n \leq x$ is any group of order n cyclic?"

List of isomorphism classes of groups by order:

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$

...

We get the following sequence giving the number of isomorphism classes of groups: 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, 2, 1, 14, 1, 2, 2, 14, 1, 6, 1, 4, 2, 2, 1, 52, 2, 5, 1, 5, 1, 15, 2, 13, 2, 2, 1, 13, 1, 2, 4, 267, 1, 4, 1, 5, 1, 4, 1, 50, 1, 2, 3, 4, 1, 6, 1, 52, 15, 2, 1, 15, 1, 2, 1, 12, . . .

5. Example in group theory

Question: "For how many $n \leq x$ is any group of order n cyclic?"

List of isomorphism classes of groups by order:

1	2	3	4	5	6	7
C_1	C_2	C_3	$C_4,\ C_2^2$	C_5	$C_6 = C_3 \times C_2,\ S_3$	C_7

8	9	10
$C_8,\ C_4 \times C_2,\ C_2^3,\ \mathrm{Dih}_4,\ \mathrm{Q}_8$	$C_9,\ C_3^2$	$C_{10} = C_5 \times C_2,\ \mathrm{Dih}_5$

...

We get the following sequence giving the number of isomorphism classes of groups: 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, 2, 1, 14, 1, 2, 2, 14, 1, 6, 1, 4, 2, 2, 1, 52, 2, 5, 1, 5, 1, 15, 2, 13, 2, 2, 1, 13, 1, 2, 4, 267, 1, 4, 1, 5, 1, 4, 1, 50, 1, 2, 3, 4, 1, 6, 1, 52, 15, 2, 1, 15, 1, 2, 1, 12, . . .
For which n is there exactly one class of groups in the list (namely just the cyclic group class)? A theorem in group theory states that this is true iff $\gcd(n, \varphi(n)) = 1$ [Szele 1947].

Example in group theory, the result:

Consider $A(x) := \#\{n \le x;\ \gcd(n, \varphi(n)) = 1\}$.

Example in group theory, the result:

Consider $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Observation: Note that n with $\gcd(n, \varphi(n)) = 1$ is not divisible by a prime $q \equiv 1 \mod p$ for $p \mid n$, since otherwise $p \mid \gcd(n, \varphi(n))$.

Example in group theory, the result:

Consider $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Observation: Note that n with $\gcd(n, \varphi(n)) = 1$ is not divisible by a prime $q \equiv 1 \bmod p$ for $p \mid n$, since otherwise $p \mid \gcd(n, \varphi(n))$.
This can be used for a sieve argument: for each prime p consider the set of n having p as smallest prime divisor. In this set, cross out all multiples of primes $q \equiv 1 \bmod p$.

Example in group theory, the result:

Consider $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Observation: Note that n with $\gcd(n, \varphi(n)) = 1$ is not divisible by a prime $q \equiv 1 \bmod p$ for $p \mid n$, since otherwise $p \mid \gcd(n, \varphi(n))$.
This can be used for a sieve argument: for each prime p consider the set of n having p as smallest prime divisor. In this set, cross out all multiples of primes $q \equiv 1 \bmod p$.
Erdős used this sieve argument and splitted the set of n according to the size of its smallest prime divisor p.

Example in group theory, the result:

Consider $A(x) := \#\{n \leq x;\ \gcd(n, \varphi(n)) = 1\}$.
Observation: Note that n with $\gcd(n, \varphi(n)) = 1$ is not divisible by a prime $q \equiv 1 \bmod p$ for $p \mid n$, since otherwise $p \mid \gcd(n, \varphi(n))$.
This can be used for a sieve argument: for each prime p consider the set of n having p as smallest prime divisor. In this set, cross out all multiples of primes $q \equiv 1 \bmod p$.
Erdős used this sieve argument and splitted the set of n according to the size of its smallest prime divisor p.
By a tricky combination of Brun's sieve and above mentioned result of the number of n having no small prime factors, he showed:

Theorem [Erdős 1948]:

The number $A(x)$ of $n \leq x$, for which every group of order n is cyclic, is $A(x) \sim \frac{e^{-\gamma} x}{\log\log\log x}$ for $x \to \infty$, and γ is the constant of Euler–Mascheroni.

1 Basic ideas of sieve theory

2 Classical applications in prime number theory

3 Selected examples of further applications

4 Linnik's problem and the large sieve

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradov's conjecture: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon) :\ q(p) < p^{\varepsilon}$.

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradov's conjecture: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon) :\ q(p) < p^{\varepsilon}$.

Assuming GRH, it was derived that $q(p) \ll (\log p)^2$ [Ankeny 1952].

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradov's conjecture: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon) :\ q(p) < p^{\varepsilon}$.

Assuming GRH, it was derived that $q(p) \ll (\log p)^2$ [Ankeny 1952].

A theorem of Linnik [1941] shows that exceptions to Vinogradov's conjecture are very rare: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradov's conjecture: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon):\ q(p) < p^{\varepsilon}$.

Assuming GRH, it was derived that $q(p) \ll (\log p)^2$ [Ankeny 1952].

A theorem of Linnik [1941] shows that exceptions to Vinogradov's conjecture are very rare: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

He used a new sieve method which has been developed intensely after him.
Today, in its modern form, it is called the large sieve method.

Linnik's problem

A problem due to Y. Linnik is the size of the smallest nonquadratic residue mod p, namely of $q(p) := \min\{n \in \mathbb{N};\ \left(\frac{n}{p}\right) = -1\}$.

Vinogradov's conjecture: $\forall \varepsilon > 0\ \forall p > p_0(\varepsilon):\ q(p) < p^{\varepsilon}$.

Assuming GRH, it was derived that $q(p) \ll (\log p)^2$ [Ankeny 1952].

A theorem of Linnik [1941] shows that exceptions to Vinogradov's conjecture are very rare: $\#\{p \leq x;\ q(p) \geq p^{\varepsilon}\} \ll_{\varepsilon} \log\log x$.

He used a new sieve method which has been developed intensely after him.
Today, in its modern form, it is called the large sieve method.

The main ingredient of the large sieve method is an inequality of exponential sums, the so-called large sieve inequality:

The large sieve inequality

Let $\{v_n\}$ denote a sequence of complex numbers, let $M, N \in \mathbb{N}$ and let $Q \geq 1$ be a real number. Then

$$\|v\|^{-2} \sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \left| \sum_{M < n \leq M+N} v_n e\left(\frac{a}{q} n\right) \right|^2 \leq Q^2 + N - 1,$$

where $\|v\|^2 := \sum_{M < n \leq M+N} |v_n|^2$, $e(\alpha) := \exp(2\pi i \alpha)$ for $\alpha \in \mathbb{R}$.

The large sieve inequality

Let $\{v_n\}$ denote a sequence of complex numbers, let $M, N \in \mathbb{N}$ and let $Q \geq 1$ be a real number. Then

$$\|v\|^{-2} \sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \Big| \sum_{M < n \leq M+N} v_n e\Big(\frac{a}{q} n\Big) \Big|^2 \leq Q^2 + N - 1,$$

where $\|v\|^2 := \sum_{M<n\leq M+N} |v_n|^2$, $e(\alpha) := \exp(2\pi i \alpha)$ for $\alpha \in \mathbb{R}$.

The most important application of the large sieve (together with combinatorial identities) has been the distribution of primes in APs, namely Bombieri–Vinogradov's theorem. It states that RH holds on average for all "moduli" q up to a big bound.

The large sieve inequality

Let $\{v_n\}$ denote a sequence of complex numbers, let $M, N \in \mathbb{N}$ and let $Q \geq 1$ be a real number. Then

$$\|v\|^{-2} \sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \left| \sum_{M < n \leq M+N} v_n e\left(\frac{a}{q} n\right) \right|^2 \leq Q^2 + N - 1,$$

where $\|v\|^2 := \sum_{M<n\leq M+N} |v_n|^2$, $e(\alpha) := \exp(2\pi i \alpha)$ for $\alpha \in \mathbb{R}$.

The most important application of the large sieve (together with combinatorial identities) has been the distribution of primes in APs, namely Bombieri–Vinogradov's theorem. It states that RH holds on average for all "moduli" q up to a big bound.

Therefore, sieve methods can provide results so strong that they compete with the consequences of the RH: Bombieri–Vinogradov's theorem has many applications.

The large sieve inequality with power moduli

After replacing the moduli q in the large sieve inequality by powers of the form q^k, one can ask also for good upper bounds of the resulting exponential sums.

The large sieve inequality with power moduli

After replacing the moduli q in the large sieve inequality by powers of the form q^k, one can ask also for good upper bounds of the resulting exponential sums.

L. Zhao has shown in [2004] the upper bound

$$Q^{k+1} + (NQ^{1-\delta} + N^{1-\delta}Q^{1+k\delta})N^{\varepsilon},$$

where $\delta := 1/2^{k-1}$, and conjectured that $\delta := 1$ should be the correct exponent in this bound.

The large sieve inequality with power moduli

After replacing the moduli q in the large sieve inequality by powers of the form q^k, one can ask also for good upper bounds of the resulting exponential sums.

L. Zhao has shown in [2004] the upper bound

$$Q^{k+1} + (NQ^{1-\delta} + N^{1-\delta}Q^{1+k\delta})N^{\varepsilon},$$

where $\delta := 1/2^{k-1}$, and conjectured that $\delta := 1$ should be the correct exponent in this bound.

[K. H., 2012] In this bound one can replace δ by $(2k(k-1))^{-1}$.

The large sieve inequality with power moduli

After replacing the moduli q in the large sieve inequality by powers of the form q^k, one can ask also for good upper bounds of the resulting exponential sums.

L. Zhao has shown in [2004] the upper bound

$$Q^{k+1} + (NQ^{1-\delta} + N^{1-\delta}Q^{1+k\delta})N^{\varepsilon},$$

where $\delta := 1/2^{k-1}$, and conjectured that $\delta := 1$ should be the correct exponent in this bound.

[K. H., 2012] In this bound one can replace δ by $(2k(k-1))^{-1}$.

The proof uses Fourier-methods together with a recent deep result of T. Wooley on "efficient congruencing".
[T. Wooley, Ann. of Math. 2012]

The large sieve inequality with power moduli

After replacing the moduli q in the large sieve inequality by powers of the form q^k, one can ask also for good upper bounds of the resulting exponential sums.

L. Zhao has shown in [2004] the upper bound

$$Q^{k+1} + (NQ^{1-\delta} + N^{1-\delta}Q^{1+k\delta})N^{\varepsilon},$$

where $\delta := 1/2^{k-1}$, and conjectured that $\delta := 1$ should be the correct exponent in this bound.

[K. H., 2012] In this bound one can replace δ by $(2k(k-1))^{-1}$.

The proof uses Fourier-methods together with a recent deep result of T. Wooley on "efficient congruencing".
[T. Wooley, Ann. of Math. 2012]
Applications of the new k-bound are in progress. . .

Thank you!

Bibliography:

- A. C. Cojocaru and M. Ram Murty, An Introduction to Sieve Methods and their Applications
- J. Friedlander and H. Iwaniec, Opera de Cribro
- G. Harman, Prime-Detecting Sieves