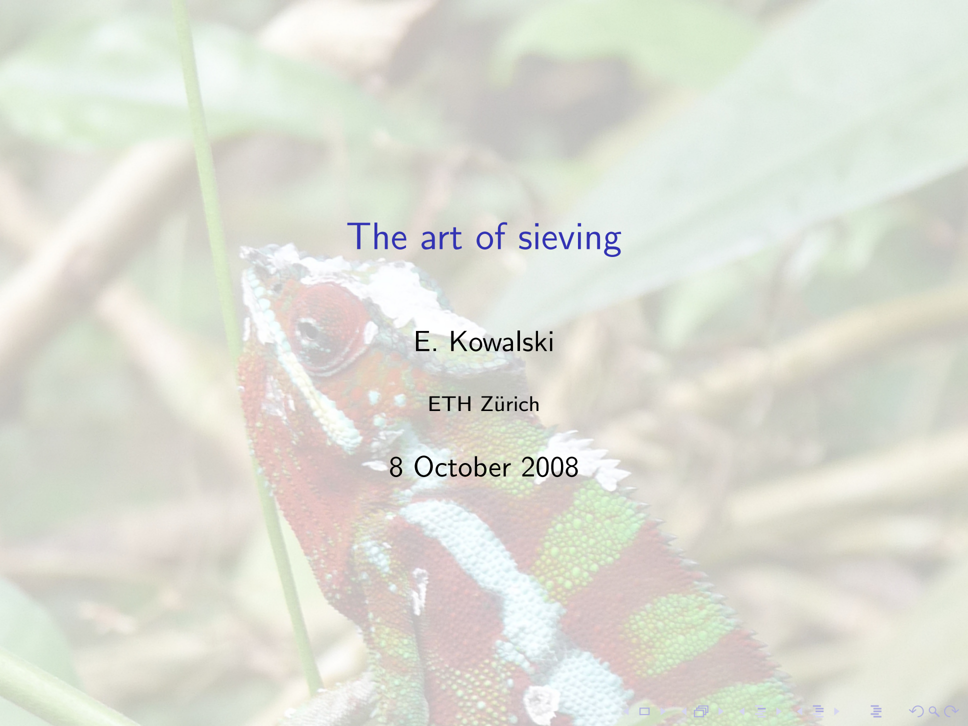


The art of sieving

E. Kowalski

ETH Zürich

8 October 2008

Prime numbers

Prime numbers are natural numbers $p \geq 1$ which can not be split as products of other natural numbers of strictly smaller size.

Prime numbers

Prime numbers are natural numbers $p \geq 1$ which can not be split as products of other natural numbers of strictly smaller size.

For instance:

$$2, \quad 3, \quad 5, \quad 7, \ \ldots \ , 641, \ \ldots \ , 10007, \ \ldots \ , 2^{43112609} - 1, \ \ldots$$

Prime numbers

Prime numbers are natural numbers $p \geq 1$ which can not be split as products of other natural numbers of strictly smaller size.

For instance:

$$2, \quad 3, \quad 5, \quad 7, \ \ldots \ , 641, \ \ldots \ , 10007, \ \ldots \ , 2^{43112609} - 1, \ \ldots$$

but not

$$5007 = 3 \cdot 1669, \qquad 156839 = 2209 \cdot 71, \qquad 8102008 = 8 \cdot 1012751.$$

(The number $2^{43112609} - 1$ is known to be prime since August 2008.)

Factorization

By splitting integers into products of smaller numbers whenever possible, every integer is seen to be a product of primes, possibly with repetition

Factorization

By splitting integers into products of smaller numbers whenever possible, every integer is seen to be a product of primes, possibly with repetition

For example:

$$17179869175 = 5 \cdot 5 \cdot 7 \cdot 7 \cdot 53 \cdot 107 \cdot 2473.$$

Factorization

By splitting integers into products of smaller numbers whenever possible, every integer is seen to be a product of primes, possibly with repetition

For example:

$$17179869175 = 5 \cdot 5 \cdot 7 \cdot 7 \cdot 53 \cdot 107 \cdot 2473.$$

When ordered, the *prime factors* that appear are uniquely determined by n, and so are the number of repetitions of each.

Digression I: why are primes interesting?

Un-historical answer. Constructing primes, and checking that numbers are primes is now *easy* (in some sense).

Digression I: why are primes interesting?

Un-historical answer. Constructing primes, and checking that numbers are primes is now *easy* (in some sense).

```
? p1=1634733645809253848443133883865090859841783670033092312181110852
389333100104508151212118167511579;
? isprime(p1)
time = 137 ms.
%1= 1
? p2=1900871281664822113126851573935413975471896789968515493666638539
0880271038021044989571912614655571;
time = 0 ms.
? isprime(p2)
time = 136 ms.
%2 = 1
```

Digression I: why are primes interesting?

Un-historical answer. Constructing primes, and checking that numbers are primes is now *easy* (in some sense).

```
? p1=163473364580925384844313388386509085984178367003309231218111085
2389333100104508151212118167511579;
? isprime(p1)
time = 137 ms.
%1= 1
? p2=19008712816648221131268515739354139754718967899685154936666385
39088027103802104498957191261465571;
time = 0 ms.
? isprime(p2)
time = 136 ms.
%2 = 1
```

But factoring integers seems to be *extremely hard*.

Digression I: why are primes interesting?

Un-historical answer. Constructing primes, and checking that numbers are primes is now *easy* (in some sense).

```
? p1=163473364580925384844313388386509085984178367003309231218111085
2389333100104508151212118167511579;
? isprime(p1)
time = 137 ms.
%1= 1
? p2=190087128166482211312685157393541397547189678996851549366663853
9088027103802104498957191261465571;
time = 0 ms.
? isprime(p2)
time = 136 ms.
%2 = 1
```

But factoring integers seems to be *extremely hard*.

```
? factor(p1*p2)
^C  *** factor: user interrupt after 1hr, 53mn, 39,129 ms.
```

Digression I: why are primes interesting?

Un-historical answer. Constructing primes, and checking that numbers are primes is now *easy* (in some sense).

```
? p1=163473364580925384844313388386509085984178367003309231218111085
2389333100104508151212118167511579;
? isprime(p1)
time = 137 ms.
%1= 1
? p2=19008712816648221131268515739354139754718967899685154936666385
39088027103802104498957191261465571;
time = 0 ms.
? isprime(p2)
time = 136 ms.
%2 = 1
```

But factoring integers seems to be *extremely hard*.

```
? factor(p1*p2)
^C  *** factor: user interrupt after 1hr, 53mn, 39,129 ms.
```

RSA challenge: Factoring $p_1 \cdot p_2$ (without knowing p_1 and p_2 in advance!) took the equivalent of 30 years of non-stop computation on a fast personal computer in 2005.

Communicating trust

This (and other similar problems) is the foundation of much of today's computer security protocols.

Communicating trust

This (and other similar problems) is the foundation of much of today's computer security protocols.

Say **Agency A** wants to send **Secret Agent B** to some hostile country to meet **Contact C**. How can they be sure that **B** is **B** and **C** is **C**?

Communicating trust

This (and other similar problems) is the foundation of much of today's computer security protocols.

Say **Agency A** wants to send **Secret Agent B** to some hostile country to meet **Contact C**. How can they be sure that **B** is **B** and **C** is **C**?

One way is to give $p_1 p_2$ to **B** (without telling him p_1 or p_2) and communicate p_1 to **C**.

Communicating trust

This (and other similar problems) is the foundation of much of today's computer security protocols.

Say **Agency A** wants to send **Secret Agent B** to some hostile country to meet **Contact C**. How can they be sure that **B** is **B** and **C** is **C**?

One way is to give $p_1 p_2$ to **B** (without telling him p_1 or p_2) and communicate p_1 to **C**.

When they meet, **B** gives $n = p_1 p_2$ to **C**, who *authenticates herself* with almost absolute confidence by immediately returning p_1 (which she already knows) and $p_2 = n/p_1$.

Communicating trust

This (and other similar problems) is the foundation of much of today's computer security protocols.

Say **Agency A** wants to send **Secret Agent B** to some hostile country to meet **Contact C**. How can they be sure that **B** is **B** and **C** is **C**?

One way is to give $p_1 p_2$ to **B** (without telling him p_1 or p_2) and communicate p_1 to **C**.

When they meet, **B** gives $n = p_1 p_2$ to **C**, who *authenticates herself* with almost absolute confidence by immediately returning p_1 (which she already knows) and $p_2 = n/p_1$.

If **C** were an impostor, without knowing p_1, she would not be able to factor n and convince **B**.

Digression II: why are primes interesting?

A more scientific answer. Primes behave in a fascinating way: they show a combination of deterministic description and random answers ("structure" and "randomness").

Digression II: why are primes interesting?

A more scientific answer. Primes behave in a fascinating way: they show a combination of deterministic description and random answers ("structure" and "randomness").

Primes are linked with multiplication; as soon as they interact with *addition*, strange things may happen.

Digression II: why are primes interesting?

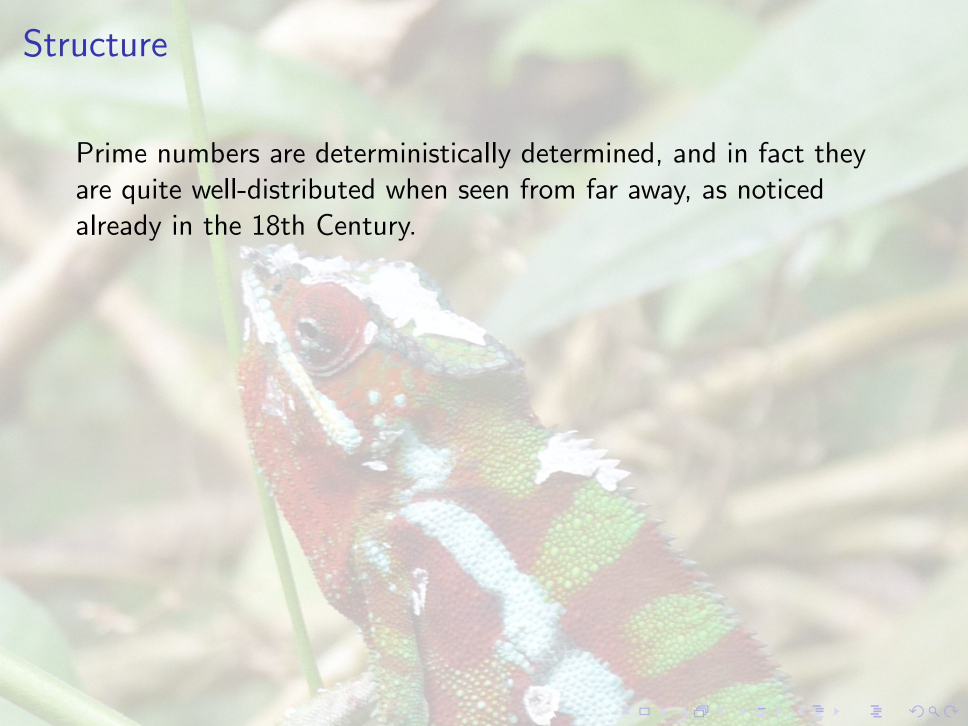
A more scientific answer. Primes behave in a fascinating way: they show a combination of deterministic description and random answers ("structure" and "randomness").

Primes are linked with multiplication; as soon as they interact with *addition*, strange things may happen.

$$2^{30} = 2 \cdot 2 \cdot 2 \cdots 2 \quad \text{(30 times)}$$
$$2^{30} + 1 = 5 \cdot 5 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$$
$$2^{30} + 2 = 2 \cdot 3 \cdot 59 \cdot 3033169$$
$$2^{30} + 3 = 1073741827, \quad 2^{30} + 4 = 2 \cdot 2 \cdot 17 \cdot 15790321$$
$$2^{30} + 5 = 3 \cdot 149 \cdot 2402107$$

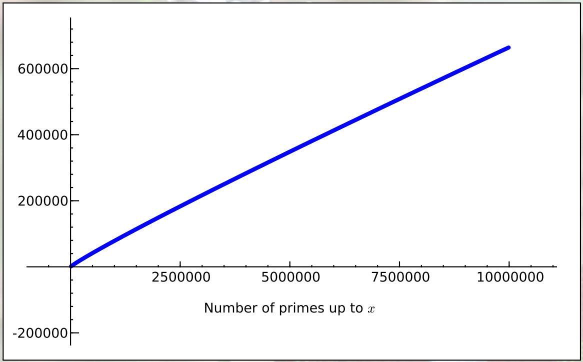
Structure

Prime numbers are deterministically determined, and in fact they are quite well-distributed when seen from far away, as noticed already in the 18th Century.



Structure

Prime numbers are deterministically determined, and in fact they are quite well-distributed when seen from far away, as noticed already in the 18th Century.

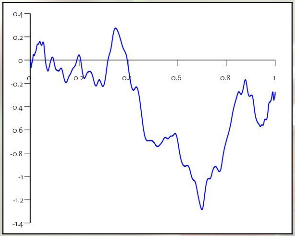


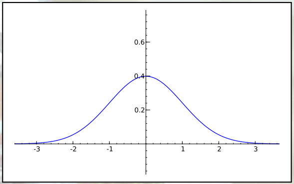
Randomness

But, seen more closely, primes seem to behave chaotically. It seems that any interesting probability distribution may be found naturally within the primes.

The normal gaussian distribution

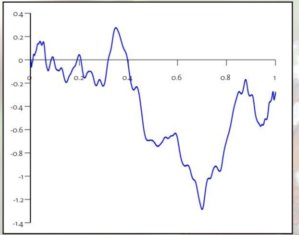
This is for instance the distribution of the position of a random walker (Brownian motion) at time 1.

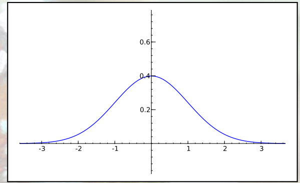




The normal gaussian distribution

This is for instance the distribution of the position of a random walker (Brownian motion) at time 1.





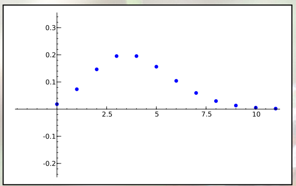
ERDÖS-KÁC theorem:

$$\frac{(\text{nb. of primes dividing } n) - \log\log n}{\sqrt{\log\log n}}$$

is approximately distributed like a normal variable for large n.

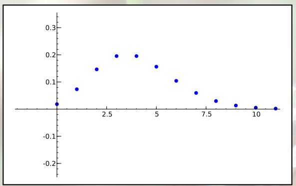
Poisson distribution

This is for instance the distribution of the number of atomic disintegrations (of a given substance) observed during a fixed time.



Poisson distribution

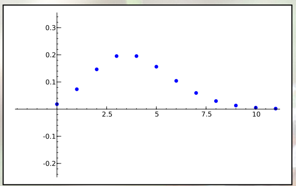
This is for instance the distribution of the number of atomic disintegrations (of a given substance) observed during a fixed time.



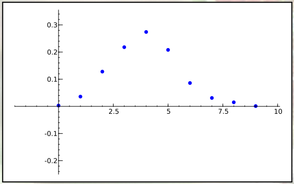
Gaps between primes: the number of primes between x and $x + c \log x$ is (supposed to be) approximately distributed like a Poisson distribution with parameter c.

Poisson distribution

This is for instance the distribution of the number of atomic disintegrations (of a given substance) observed during a fixed time.



Gaps between primes: the number of primes between x and $x + c \log x$ is (supposed to be) approximately distributed like a Poisson distribution with parameter c.

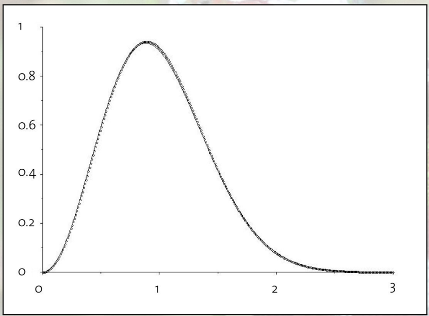


Distribution of spacings of energy levels of large nuclei?

The GUE model for this distribution is conjectured to occur in the zeros of the Riemann zeta function which "controls" the distribution of prime numbers.

Distribution of spacings of energy levels of large nuclei?

The GUE model for this distribution is conjectured to occur in the zeros of the Riemann zeta function which "controls" the distribution of prime numbers.



The continuous line is the theoretical distribution of the normalized spacings of GUE matrices, and the small circles are the data from the Riemann zeta function. (Numerical work and graph by X. Gourdon)

Digression III: why are primes interesting?

Experimental psychology answer.

Human beings have been fascinated by prime numbers since the earliest times in the history of mathematics.

Digression III: why are primes interesting?

Experimental psychology answer.

Human beings have been fascinated by prime numbers since the earliest times in the history of mathematics.

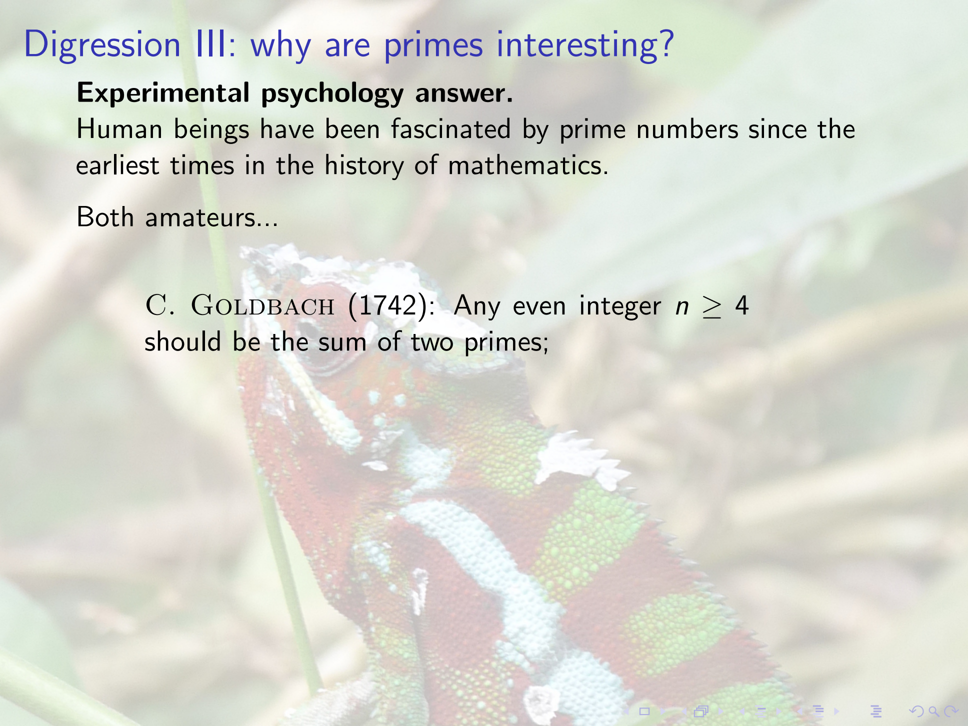
Both amateurs...

Digression III: why are primes interesting?

Experimental psychology answer.
Human beings have been fascinated by prime numbers since the earliest times in the history of mathematics.

Both amateurs...

C. Goldbach (1742): Any even integer $n \geq 4$ should be the sum of two primes;



Digression III: why are primes interesting?

Experimental psychology answer.
Human beings have been fascinated by prime numbers since the earliest times in the history of mathematics.

Both amateurs...

> C. Goldbach (1742): Any even integer $n \geq 4$ should be the sum of two primes;
>
> A. de Polignac (1848): There should exist infinitely many pairs of primes p, $p + 2$ ("twin primes").

Digression III: why are primes interesting?

Experimental psychology answer.

Human beings have been fascinated by prime numbers since the earliest times in the history of mathematics.

Both amateurs...

> C. Goldbach (1742): Any even integer $n \geq 4$ should be the sum of two primes;
>
> A. de Polignac (1848): There should exist infinitely many pairs of primes p, $p+2$ ("twin primes").

... and some of the most renowned scientists:

(The two questions above are still open.)

(cont.)

EUCLID (“there are infinitely many primes”),

(cont.)

EUCLID (“there are infinitely many primes”),

P. DE FERMAT (“if n is an integer, $2^{2^n}+1$ is prime”),

(cont.)

EUCLID ("there are infinitely many primes"),

P. DE FERMAT ("if n is an integer, $2^{2^n} + 1$ is prime"),

L. EULER (contrary to Fermat's opinion, $2^{32} + 1$ is *not* prime),

(cont.)

EUCLID ("there are infinitely many primes"),

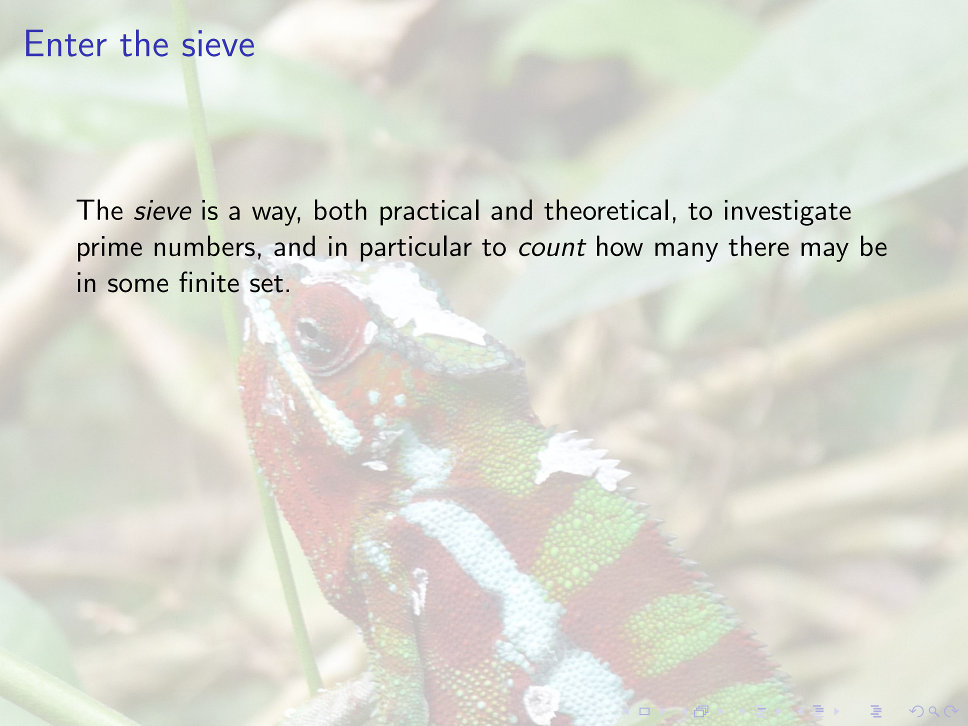
P. DE FERMAT ("if n is an integer, $2^{2^n}+1$ is prime"),

L. EULER (contrary to Fermat's opinion, $2^{32}+1$ is *not* prime),

C.F. GAUSS (the probability that a large integer N be prime is about one chance in $\log N$, which is about three times the number of digits of N).

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set.



Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by Eratosthenes to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

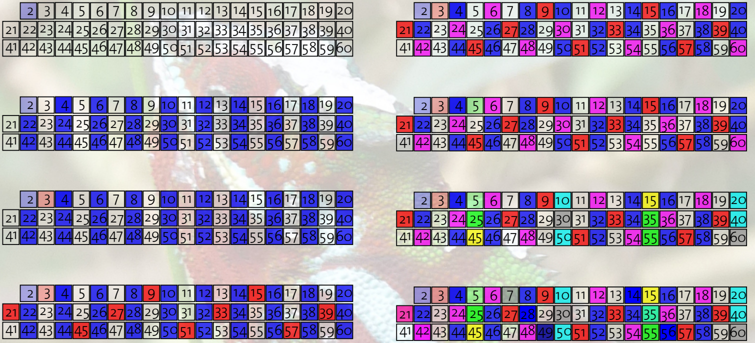
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

	2	3	4	5	6	7	8	9	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

	2	3	4	5	6	7	8	9	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

Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.



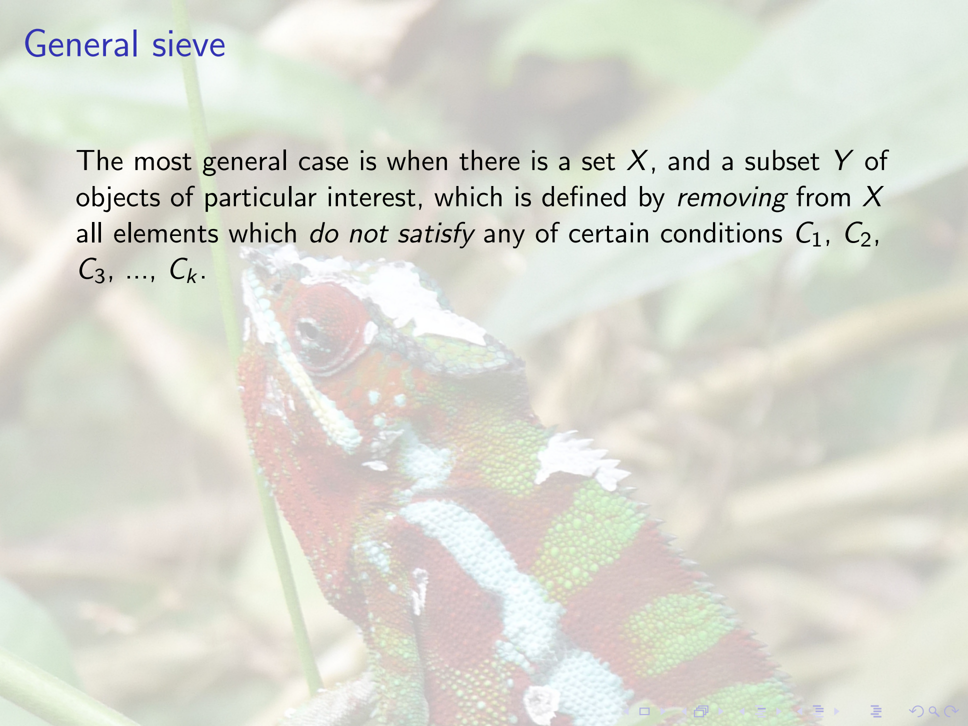
Enter the sieve

The *sieve* is a way, both practical and theoretical, to investigate prime numbers, and in particular to *count* how many there may be in some finite set. The first sieve was used by ERATOSTHENES to make lists of prime numbers.

The primes up to 60 are

$$2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

General sieve



The most general case is when there is a set X, and a subset Y of objects of particular interest, which is defined by *removing* from X all elements which *do not satisfy* any of certain conditions C_1, C_2, C_3, ..., C_k.

General sieve

The most general case is when there is a set X, and a subset Y of objects of particular interest, which is defined by *removing* from X all elements which *do not satisfy* any of certain conditions C_1, C_2, C_3, ..., C_k.

– If there is a "probability" δ_i that the i-th condition holds,

General sieve

The most general case is when there is a set X, and a subset Y of objects of particular interest, which is defined by *removing* from X all elements which *do not satisfy* any of certain conditions C_1, C_2, C_3, ..., C_k.

- If there is a "probability" δ_i that the i-th condition holds,
  - and if the conditions C_i, C_j are nearly *independent* for $i \neq j$,

General sieve

The most general case is when there is a set X, and a subset Y of objects of particular interest, which is defined by *removing* from X all elements which *do not satisfy* any of certain conditions C_1, C_2, C_3, ..., C_k.

– If there is a "probability" δ_i that the i-th condition holds,

– and if the conditions C_i, C_j are nearly *independent* for $i \neq j$,

– then one expects that the probability of Y is about

$$(1-\delta_1)(1-\delta_2)\cdots(1-\delta_k) = 1 - \sum_i \delta_i + \sum_{\{i,j\}} \delta_i\delta_j - \dots$$

General sieve

The most general case is when there is a set X, and a subset Y of objects of particular interest, which is defined by *removing* from X all elements which *do not satisfy* any of certain conditions C_1, C_2, C_3, ..., C_k.

– If there is a "probability" δ_i that the i-th condition holds,

  – and if the conditions C_i, C_j are nearly *independent* for $i \neq j$,

    – then one expects that the probability of Y is about

$$(1-\delta_1)(1-\delta_2)\cdots(1-\delta_k) = 1 - \sum_i \delta_i + \sum_{\{i,j\}} \delta_i\delta_j - \ldots$$

This general "sieve" procedure is based on *inclusion-exclusion*.

Example 1

$$X = \{1, 2, \ldots, N\}$$

Example 1

$$X = \{1, 2, \ldots, N\}$$

$$
\begin{aligned}
C_1 &= (n \text{ is divisible by } 2) && \text{“probability”}\ 1/2 \\
C_2 &= (n \text{ is divisible by } 3) && \text{“probability”}\ 1/3 \\
&\ldots \\
C_k &= (n \text{ is divisible by the } k\text{-th prime}) && \text{“probability”}\ 1/p_k
\end{aligned}
$$

Example 1

$$X = \{1, 2, \ldots, N\}$$

$$C_1 = (n \text{ is divisible by } 2) \qquad \text{“probability”} \ 1/2$$

$$C_2 = (n \text{ is divisible by } 3) \qquad \text{“probability”} \ 1/3$$

$$\ldots$$

$$C_k = (n \text{ is divisible by the } k\text{-th prime}) \qquad \text{“probability”} \ 1/p_k$$

If an integer with $2 \leq n \leq N$ is *not* divisible by a prime number $\ell \leq \sqrt{N}$, then n must itself be a prime, and conversely if $n > \sqrt{N}$.

Example 1

$$X = \{1, 2, \ldots, N\}$$

$$C_1 = (n \text{ is divisible by } 2) \qquad \text{“probability”} \;\; 1/2$$

$$C_2 = (n \text{ is divisible by } 3) \qquad \text{“probability”} \;\; 1/3$$

$$\ldots$$

$$C_k = (n \text{ is divisible by the } k\text{-th prime}) \qquad \text{“probability”} \;\; 1/p_k$$

If an integer with $2 \leq n \leq N$ is *not* divisible by a prime number $\ell \leq \sqrt{N}$, then n must itself be a prime, and conversely if $n > \sqrt{N}$. This is the sieve description with the conditions $C_1, \ldots, C_k$ (up to p_k, with p_k closest to $\sqrt{N}$).

(Cont.)

So the probability that $n \leq N$ be prime should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{p_k}\right)=\prod_{\substack{\ell\leq\sqrt{N}\\ \ell \text{ prime}}}(1-\ell^{-1}).$$

(Cont.)

So the probability that $n \leq N$ be prime should be about

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{p_k}\right) = \prod_{\substack{\ell \leq \sqrt{N} \\ \ell \text{ prime}}} (1 - \ell^{-1}).$$

This is not a bad guess, but it is *wrong*:

(Cont.)

So the probability that $n \leq N$ be prime should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{p_k}\right)=\prod_{\substack{\ell\leq\sqrt{N}\\ \ell \text{ prime}}}(1-\ell^{-1}).$$

This is not a bad guess, but it is *wrong*: on the one hand we have the MERTENS formula (1874):

$$\prod_{\substack{\ell\leq\sqrt{N}\\ \ell \text{ prime}}}(1-\ell^{-1}) \sim \frac{2c}{\log N}, \quad c = 0.561459483566885\ldots$$

(Cont.)

So the probability that $n \leq N$ be prime should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{p_k}\right) = \prod_{\substack{\ell \leq \sqrt{N} \\ \ell \text{ prime}}} (1-\ell^{-1}).$$

This is not a bad guess, but it is *wrong*: on the one hand we have the MERTENS formula (1874):

$$\prod_{\substack{\ell \leq \sqrt{N} \\ \ell \text{ prime}}} (1-\ell^{-1}) \sim \frac{2c}{\log N}, \quad c = 0.561459483566885\ldots$$

but on the other hand

$$(\text{Number of primes } p \leq N) \sim \frac{N}{\log N}$$

(J. HADAMARD and C. DE LA VALLÉE-POUSSIN: Prime Number Theorem, 1896, confirming the intuition of GAUSS).

Example 2: the twin primes

$$X = \{1, 2, \ldots, N\}$$

Example 2: the twin primes

$$X = \{1, 2, \ldots, N\}$$

$$C_1 = (n \text{ or } n + 2 \text{ is divisible by } 2) \quad \text{“probability” } 1/2$$

$$C_2 = (n \text{ or } n + 2 \text{ is divisible by } 3) \quad \text{“probability” } 2/3$$

$$\ldots$$

$$C_k = (n \text{ or } n + 2 \text{ is divisible by the } k\text{-prime}) \quad \text{“probability” } 2/p_k$$

Example 2: the twin primes

$$X = \{1, 2, \ldots, N\}$$

$$C_1 = (n \text{ or } n+2 \text{ is divisible by } 2) \quad \text{“probability” } 1/2$$

$$C_2 = (n \text{ or } n+2 \text{ is divisible by } 3) \quad \text{“probability” } 2/3$$

$$\ldots$$

$$C_k = (n \text{ or } n+2 \text{ is divisible by the } k\text{-prime}) \quad \text{“probability” } 2/p_k$$

The “sifted set” is now the set of twin primes $\sqrt{N} < p \leq N$ such that $p+2$ is also prime.

(Cont.)

So the probability that $n \leq N$ be prime and $n+2$ also should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{2}{3}\right)\cdots\left(1-\frac{2}{p_k}\right)=\frac{1}{2}\prod_{\substack{3\leq\ell\leq\sqrt{N}\\ \ell\text{ prime}}}(1-2\ell^{-1}).$$

(Cont.)

So the probability that $n \leq N$ be prime and $n+2$ also should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{2}{3}\right)\cdots\left(1-\frac{2}{p_k}\right)=\frac{1}{2}\prod_{\substack{3\leq \ell \leq \sqrt{N} \\ \ell \text{ prime}}}(1-2\ell^{-1}).$$

No one knows if this is correct or not!

(Cont.)

So the probability that $n \leq N$ be prime and $n+2$ also should be about

$$\left(1-\frac{1}{2}\right)\left(1-\frac{2}{3}\right)\cdots\left(1-\frac{2}{p_k}\right)=\frac{1}{2}\prod_{\substack{3\leq\ell\leq\sqrt{N}\\ \ell \text{ prime}}}(1-2\ell^{-1}).$$

No one knows if this is correct or not!

It is expected that

$$(\text{Number of primes } p\leq N \text{ such that } p+2 \text{ is prime}) \sim \frac{s_2 N}{(\log N)^2}$$

with

$$s_2=\frac{1}{2}\prod_{\substack{\ell\geq 3\\ \ell \text{ prime}}}\frac{1-2\ell^{-1}}{(1-\ell^{-1})^2}=1.32032469\ldots$$

Some classical results

Here are some highlights of the classical sieve methods.

Some classical results

Here are some highlights of the classical sieve methods.

– I.M. Vinogradov (1937):

For all sufficiently large odd integer n, there are three prime numbers such that $n = p_1 + p_2 + p_3$;

Some classical results

Here are some highlights of the classical sieve methods.

– I.M. Vinogradov (1937):

For all sufficiently large odd integer n, there are three prime numbers such that $n = p_1 + p_2 + p_3$;

– J.R. Chen (1966–73):

There are infinitely many prime numbers p such that $p + 2$ is either prime or a product of two primes;

Some classical results

Here are some highlights of the classical sieve methods.

– I.M. Vinogradov (1937):

For all sufficiently large odd integer n, there are three prime numbers such that $n = p_1 + p_2 + p_3$;

– J.R. Chen (1966–73):

There are infinitely many prime numbers p such that $p + 2$ is either prime or a product of two primes;

Some classical results

Here are some highlights of the classical sieve methods.

– I.M. VINOGRADOV (1937):

For all sufficiently large odd integer n, there are three prime numbers such that $n = p_1 + p_2 + p_3$;

– J.R. CHEN (1966–73):

There are infinitely many prime numbers p such that $p + 2$ is either prime or a product of two primes;

–H. IWANIEC & J. FRIEDLANDER (1998):

There are infinitely many pairs of integers (x, y) such that $x^2 + y^4$ is prime.

The small and large sieves

In the previous examples, the probability of the conditions C_i become small when more and more conditions are involved. This is what is called a "small" sieve.

The small and large sieves

In the previous examples, the probability of the conditions C_i become small when more and more conditions are involved. This is what is called a "small" sieve.

In other problems, one encounters conditions where the probabilities are always roughly similar, for instance each C_i could have probability $1/2$. This is a *large sieve*.

The small and large sieves

In the previous examples, the probability of the conditions C_i become small when more and more conditions are involved. This is what is called a "small" sieve.

In other problems, one encounters conditions where the probabilities are always roughly similar, for instance each C_i could have probability $1/2$. This is a *large sieve*.

This was first developed by LINNIK in 1941, and after many developments, it is now very useful in many (sometimes surprising) applications.

Recent results

During the last few years sieve methods have been applied to many different types of problems. Among these, the most interesting may be those of "hyperbolic" nature.

Recent results

During the last few years sieve methods have been applied to many different types of problems. Among these, the most interesting may be those of "hyperbolic" nature.

J. Bourgain, A. Gamburd, P. Sarnak:
Sieving, expanders and sum product,
(2006–2008);

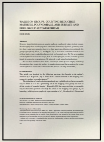
Recent results

During the last few years sieve methods have been applied to many different types of problems. Among these, the most interesting may be those of "hyperbolic" nature.

J. Bourgain, A. Gamburd, P. Sarnak:
Sieving, expanders and sum product,
(2006–2008);


SIEVING, EXPANDERS, AND SUM-PRODUCT

I. Rivin: *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. 2008;


WALKS ON GROUPS, COUNTING REDUCIBLE MATRICES, POLYNOMIALS, AND SURFACE AND FREE GROUP AUTOMORPHISMS

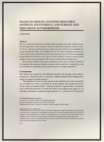
IGOR RIVIN

Recent results

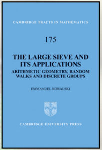
During the last few years sieve methods have been applied to many different types of problems. Among these, the most interesting may be those of “hyperbolic” nature.

J. Bourgain, A. Gamburd, P. Sarnak: *Sieving, expanders and sum product*, (2006–2008);

I. Rivin: *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. 2008;



E. Kowalski: *The large sieve and its applications*, Cambridge Univ. Press (2008).

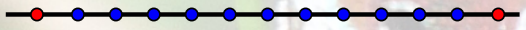


Classical “euclidean” counting

Counting the number of integers in a segment or inside a disc is “easy” because boundaries do not matter much.

Classical “euclidean” counting

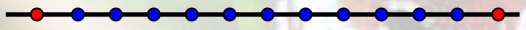
Counting the number of integers in a segment or inside a disc is “easy” because boundaries do not matter much.



The number of points at the boundary of a large interval is quite small.

Classical “euclidean” counting

Counting the number of integers in a segment or inside a disc is “easy” because boundaries do not matter much.



The number of points at the boundary of a large interval is quite small.

The boundary of a large disc has length much smaller than the area: πR^2 is much larger than $2\pi R$ if R is large.

Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.

Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.

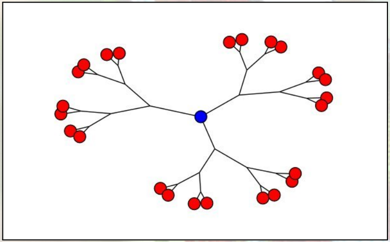
Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.

The hyperbolic area A of a hyperbolic disc of radius R is *smaller* than R.

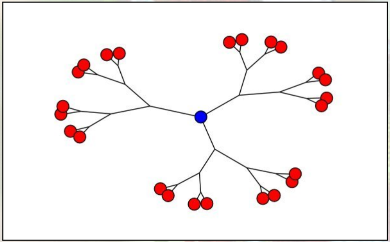
Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.



Hyperbolic counting

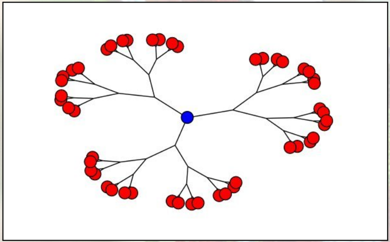
In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.



24 vertices among the 46 are on the "boundary".

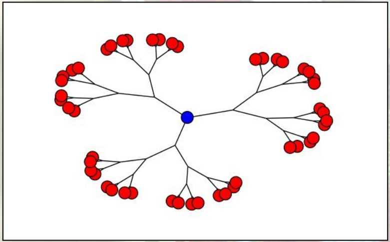
Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.



Hyperbolic counting

In hyperbolic geometry, the length of the boundary of a disc is comparable with the area. Counting discrete points in the interior is much more difficult.



48 vertices among the 94 are on the "boundary".

Apollonian circle packings

The curvature of a circle is the inverse of its radius.

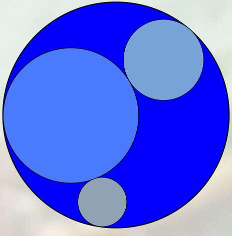
Apollonian circle packings

The curvature of a circle is the inverse of its radius.

There exist sets of four circles with integral curvature which are mutually tangent. Such configurations go back to Apollonius and were studied also by Descartes.

Apollonian circle packings

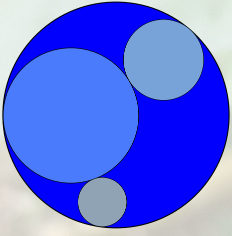
The curvature of a circle is the inverse of its radius.



There exist sets of four circles with integral curvature which are mutually tangent. Such configurations go back to APOLLONIUS and were studied also by DESCARTES.

Apollonian circle packings

The curvature of a circle is the inverse of its radius.

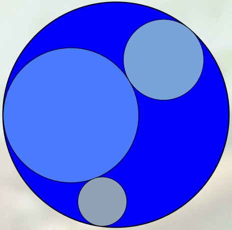


There exist sets of four circles with integral curvature which are mutually tangent. Such configurations go back to APOLLONIUS and were studied also by DESCARTES.

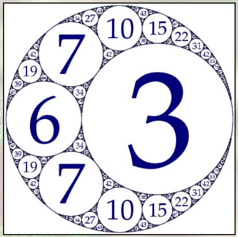
Inserting more and more circles "as large as possible" leads to packings where all circles have integral curvature. Those have many arithmetic properties, and are of a hyperbolic nature.

Apollonian circle packings

The curvature of a circle is the inverse of its radius.



There exist sets of four circles with integral curvature which are mutually tangent. Such configurations go back to Apollonius and were studied also by Descartes.



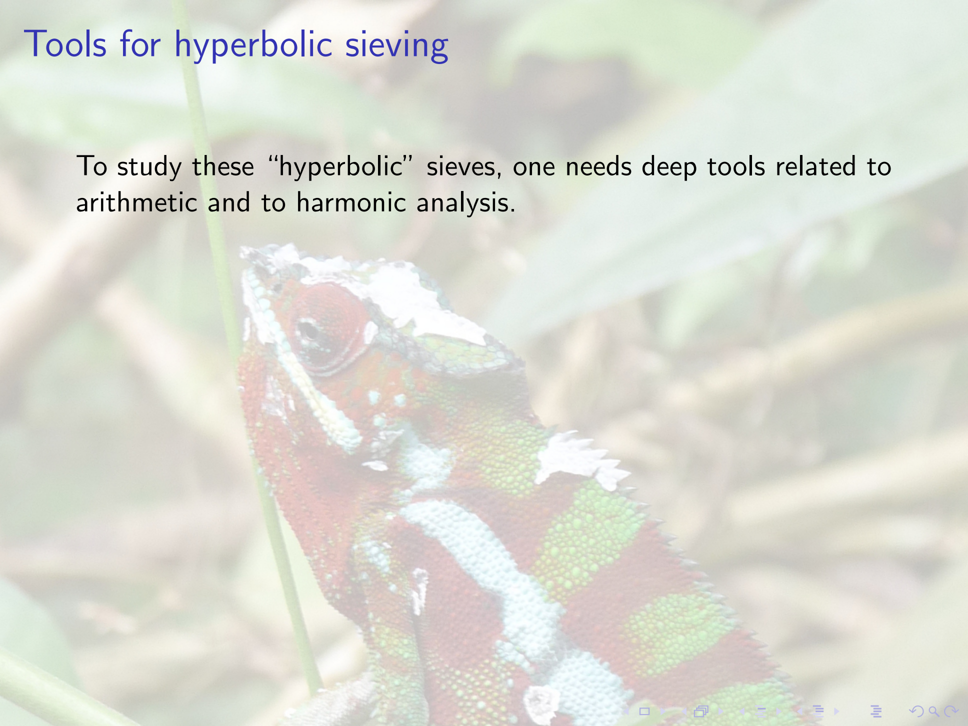
Inserting more and more circles “as large as possible” leads to packings where all circles have integral curvature. Those have many arithmetic properties, and are of a hyperbolic nature.

Diophantine properties of apollonian packings

P. SARNAK (2007), following the methods of Bourgain-Gamburd-Sarnak: for some constant C, in any such packing, there exist infinitely many quadruples of tangent circles, all curvatures of which are product of at most C primes.

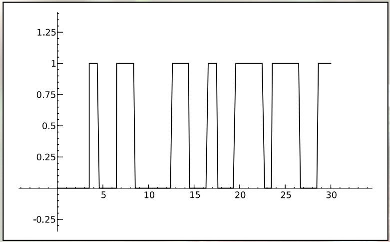
Tools for hyperbolic sieving

To study these "hyperbolic" sieves, one needs deep tools related to arithmetic and to harmonic analysis.



Tools for hyperbolic sieving

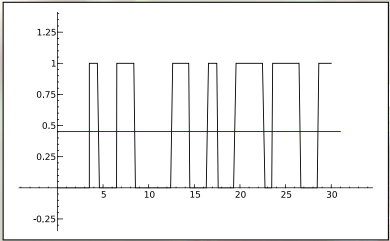
To study these “hyperbolic” sieves, one needs deep tools related to arithmetic and to harmonic analysis.



Harmonic analysis is used to decompose the binary signal that says that a condition holds

Tools for hyperbolic sieving

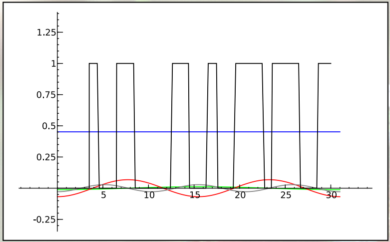
To study these "hyperbolic" sieves, one needs deep tools related to arithmetic and to harmonic analysis.



Harmonic analysis is used to decompose the binary signal that says that a condition holds into a steady "main term" (which corresponds to the probability)

Tools for hyperbolic sieving

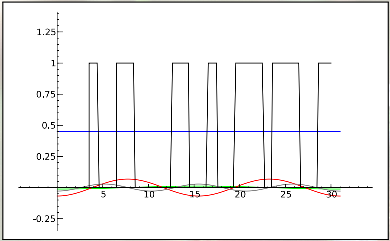
To study these “hyperbolic” sieves, one needs deep tools related to arithmetic and to harmonic analysis.



Harmonic analysis is used to decompose the binary signal that says that a condition holds into a steady “main term” (which corresponds to the probability) and a sum of further oscillating contributions of other harmonics.

Tools for hyperbolic sieving

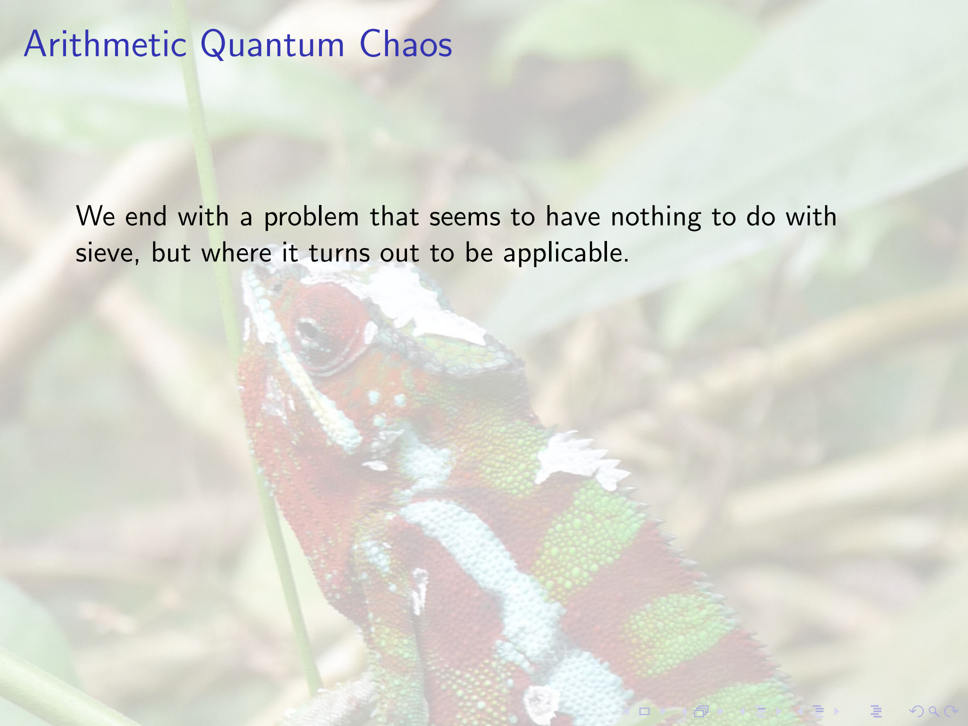
To study these “hyperbolic” sieves, one needs deep tools related to arithmetic and to harmonic analysis.



Harmonic analysis is used to decompose the binary signal that says that a condition holds into a steady “main term” (which corresponds to the probability) and a sum of further oscillating contributions of other harmonics.

The oscillating harmonics must be shown to be negligible in some sense. This often involves very deep results, and most of the work lies here.

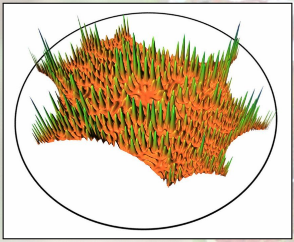
Arithmetic Quantum Chaos



We end with a problem that seems to have nothing to do with sieve, but where it turns out to be applicable.

Arithmetic Quantum Chaos

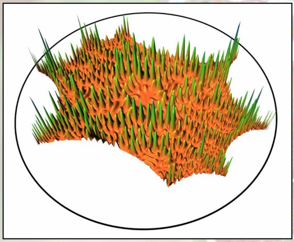
We end with a problem that seems to have nothing to do with sieve, but where it turns out to be applicable.



This shows the density of a “wave function” on a hyperbolic surface.

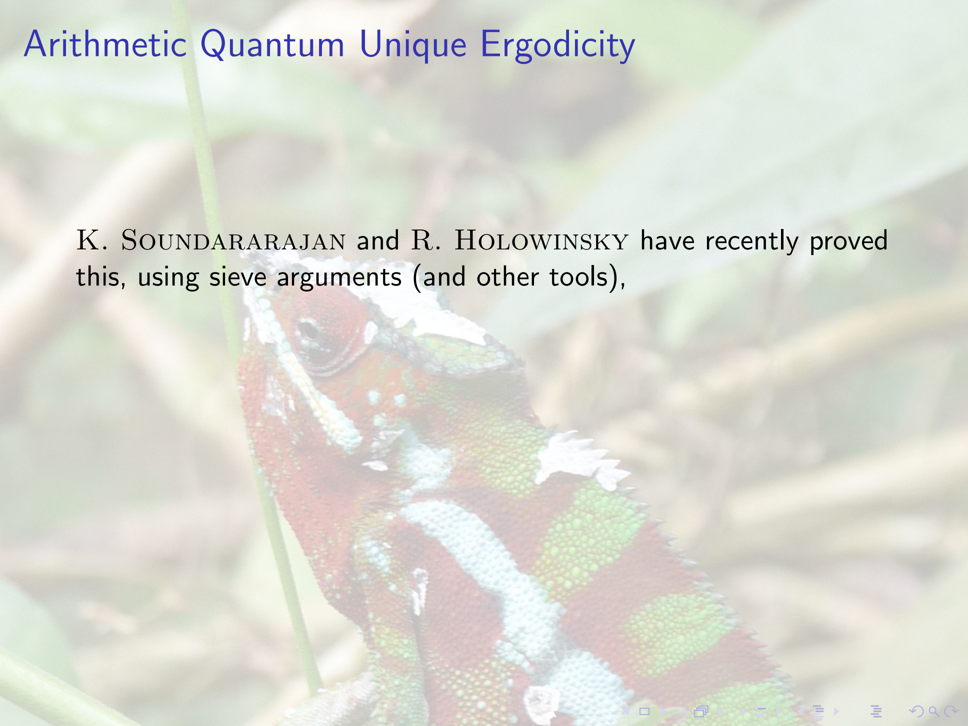
Arithmetic Quantum Chaos

We end with a problem that seems to have nothing to do with sieve, but where it turns out to be applicable.



This shows the density of a “wave function” on a hyperbolic surface. It is expected that for certain surfaces, the wave functions with high energy will be uniformly distributed. (Picture by R. Aurich and F. Steiner.)

Arithmetic Quantum Unique Ergodicity



K. Soundararajan and R. Holowinsky have recently proved this, using sieve arguments (and other tools),

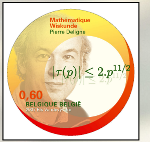
Arithmetic Quantum Unique Ergodicity

K. Soundararajan and R. Holowinsky have recently proved this, using sieve arguments (and other tools), if a certain widely believed conjecture holds.

Arithmetic Quantum Unique Ergodicity

K. Soundararajan and R. Holowinsky have recently proved this, using sieve arguments (and other tools), if a certain widely believed conjecture holds.

For a similar but slightly different problem, they are able to prove completely the analogue result, because the corresponding conjecture is known.



Acknowledgements

Most of the pictures in this document were produced using free mathematical and graphics software, in particular:

– **Inkscape**, `www.inkscape.org`

– **Pari/GP**, `pari.math.u-bordeaux.fr`

– **Sage**, `www.sagemath.org`

– **ImageMagick**, `www.imagemagick.org`

and the whole **GNU** and **Linux** desktop environment.