ARITHMETICAL TRIGONOMETRIC POLYNOMIALS

Olivier Ramaré

October 11, 2023


Flat ground

Primes numbers

- A prime number is not a product of two integers > 1.
- $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.
- THE KEY TO THE MULTIPLICATIVE WORLD:

  Every integer > 1 is a product of prime numbers.

  This product is unique.

Primes numbers

- A prime number is not a product of two integers > 1.
- $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.
- THE KEY TO THE MULTIPLICATIVE WORLD:

  Every integer > 1 is a product of prime numbers.

  This product is unique.
- $6 = 2 \times 3, \;\; 84 = 2 \times 2 \times 3 \times 7$

Primes numbers

- A prime number is not a product of two integers > 1.
- $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.
- THE KEY TO THE MULTIPLICATIVE WORLD:

  Every integer > 1 is a product of prime numbers.

  This product is unique.
- $6 = 2 \times 3, \;\; 84 = 2 \times 2 \times 3 \times 7$
- *Prime numbers are the* ATOMS *of multiplication.*

Primes numbers

- A prime number is not a product of two integers > 1.
- $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.
- THE KEY TO THE MULTIPLICATIVE WORLD:

  Every integer > 1 is a product of prime numbers.

  This product is unique.
- $6 = 2 \times 3, \;\; 84 = 2 \times 2 \times 3 \times 7$
- *Prime numbers are the* ATOMS *of multiplication.*
- Not always easy: try with 2023 or with 14351.

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

Algo (Strassen, 1976/77) ...

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

Algo (Strassen, 1976/77) ...  : (Hittmeir, 2021), (Harvey, 2021).

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

Algo (Strassen, 1976/77) …  : (Hittmeir, 2021), (Harvey, 2021).

Also for primality testing …

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

Algo (Strassen, 1976/77) …  : (Hittmeir, 2021), (Harvey, 2021).

Also for primality testing …  : (Agrawal et al., 2004) *Saxena was the teacher.*

RSA (1991–2007) and Credit Cards

A key point to information exchanges :

Factorising is difficult.

Ron Rivest, Adi Shamir and Len Adleman, in 1977

1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
= 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
× 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

17 969491 597941 066732 916128 449573 246156 367561 808012 600070 888918 835531 726460 341490 933493 372247
868650 755230 855864 199929 221814 436684 722874 052065 257937 495694 348389 263171 152522 525654 410980
819170 611742 509702 440718 010364 831638 288518 852689 = ? × ?

See Wikipedia

Algo (Strassen, 1976/77) …  : (Hittmeir, 2021), (Harvey, 2021).

Also for primality testing …  : (Agrawal et al., 2004) *Saxena was the teacher.*

But this is not what I'm doing:)

Sums of primes

Sums of primes

Goldbach (1742)

$$\begin{array}{ll}
6 = 3 + 3 & 26 = 13 + 13 \\
8 = 3 + 5 & 28 = 23 + 5 \\
10 = 5 + 5 & 30 = 17 + 13 \\
12 = 7 + 5 & 32 = 29 + 3 \\
\vdots & \vdots \\
18 = 11 + 7 & 38 = 19 + 19 \\
20 = 17 + 3 & 40 = 29 + 11 \\
22 = 19 + 3 & 42 = 29 + 13 \\
24 = 13 + 11 & 44 = 31 + 13
\end{array}$$

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Is every even integer a sum of two prime numbers?

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Proved!

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Why study that?

Proved!

Sums of primes

Goldbach (1742)

$6 = 3 + 3$	$26 = 13 + 13$
$8 = 3 + 5$	$28 = 23 + 5$
$10 = 5 + 5$	$30 = 17 + 13$
$12 = 7 + 5$	$32 = 29 + 3$
$\vdots$	$\vdots$
$18 = 11 + 7$	$38 = 19 + 19$
$20 = 17 + 3$	$40 = 29 + 11$
$22 = 19 + 3$	$42 = 29 + 13$
$24 = 13 + 11$	$44 = 31 + 13$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Proved!

Why study that? For the methods!

We had to improve on our knowledge of L-functions, on the large sieve inequality, on the Moebius function...

Sums of primes

Goldbach (1742)

$$\begin{array}{ll}
6 = 3 + 3 & 26 = 13 + 13 \\
8 = 3 + 5 & 28 = 23 + 5 \\
10 = 5 + 5 & 30 = 17 + 13 \\
12 = 7 + 5 & 32 = 29 + 3 \\
\vdots & \vdots \\
18 = 11 + 7 & 38 = 19 + 19 \\
20 = 17 + 3 & 40 = 29 + 11 \\
22 = 19 + 3 & 42 = 29 + 13 \\
24 = 13 + 11 & 44 = 31 + 13
\end{array}$$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Proved!

Why study that? For the methods!

We had to improve on our knowledge of L-functions, on the large sieve inequality, on the Moebius function...
We think the proof of the Goldbach conjecture could reveal treasures: it is worth spending a few hundred years.
Foreseeing? The (combinatorial) result of AKS could have improved the (also combinatorial) sieve, but no, or not yet.

I'll explain later how to determine whether a problem is interesting or not.

Sums of primes

Goldbach (1742)

$$\begin{array}{ll} 6 = 3+3 & 26 = 13+13 \\ 8 = 3+5 & 28 = 23+5 \\ 10 = 5+5 & 30 = 17+13 \\ 12 = 7+5 & 32 = 29+3 \\ \vdots & \vdots \\ 18 = 11+7 & 38 = 19+19 \\ 20 = 17+3 & 40 = 29+11 \\ 22 = 19+3 & 42 = 29+13 \\ 24 = 13+11 & 44 = 31+13 \end{array}$$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Proved!

Why study that? For the methods!

We had to improve on our knowledge of L-functions, on the large sieve inequality, on the Moebius function...
We think the proof of the Goldbach conjecture could reveal treasures: it is worth spending a few hundred years.
Foreseeing? The (combinatorial) result of AKS could have improved the (also combinatorial) sieve, but no, or not yet.
AKS could have "broken" factorization : no.

I'll explain later how to determine whether a problem is interesting or not.

Sums of primes

Goldbach (1742)

$$
\begin{array}{ll}
6 = 3 + 3 & 26 = 13 + 13 \\
8 = 3 + 5 & 28 = 23 + 5 \\
10 = 5 + 5 & 30 = 17 + 13 \\
12 = 7 + 5 & 32 = 29 + 3 \\
\vdots & \vdots \\
18 = 11 + 7 & 38 = 19 + 19 \\
20 = 17 + 3 & 40 = 29 + 11 \\
22 = 19 + 3 & 42 = 29 + 13 \\
24 = 13 + 11 & 44 = 31 + 13
\end{array}
$$

Is every even integer a sum of two prime numbers?

A CONSEQUENCE: *Every odd integer $\geqslant 9$ would be the sum of three prime numbers.*

Proved!

Why study that? For the methods!

We had to improve on our knowledge of L-functions, on the large sieve inequality, on the Moebius function...
We think the proof of the Goldbach conjecture could reveal treasures: it is worth spending a few hundred years.
Foreseeing? The (combinatorial) result of AKS could have improved the (also combinatorial) sieve, but no, or not yet.
AKS could have “broken” factorization : no.
Hittmeir and AKS have robbed banks with cardboard guns!

I’ll explain later how to determine whether a problem is interesting or not.

The main tool for sums of primes

Before 1936: generating series

- Look at
$$r(N) = \#\{(a,b,c) \in \mathbb{N}^3, N = a + 2b + 3c\}.$$
- N-th coefficient of $\sum_{a\geqslant 0} z^a \sum_{b\geqslant 0} z^{2b} \sum_{c\geqslant 0} z^{3c}$.
- $\sum_{a\geqslant 0} z^a \sum_{b\geqslant 0} z^{2b} \sum_{c\geqslant 0} z^{3c} = \dfrac{1}{(1-z)(1-z^2)(1-z^3)} = G(z)$
- Poles at $z = \pm 1$ and at $z = \exp(\pm 2i\pi/3)$.
- Get N-th coefficient by Cauchy's formula:
  integrate on a circle of radius $r < 1$,
  but *close to $r = 1$ to use the poles of $G(z)$.*

This was the leading idea of (Hardy & Ramanujan, 1916), (Hardy & Ramanujan, 2000), (Hardy & Ramanujan, 1917), (Hardy & Ramanujan, 1918).

After 1936: “arithmetical” trigonometric polynomials

Then early 1917: *Ramanujan ill, Littlewood incorporated as a soldier...*

After 1936: “arithmetical” trigonometric polynomials

Then early 1917: *Ramanujan ill, Littlewood incorporated as a soldier...*

Around 1918 – 1923, *Hardy and then Hardy & Littlewood applied this idea to sums of squares, then to Waring’s problem, then to the Goldbach conjecture, then came the series Partitio numerorum ...*

This story is told in details in (Kempner, 1923).

After 1936: “arithmetical” trigonometric polynomials

Then early 1917: *Ramanujan ill, Littlewood incorporated as a soldier...*

Around 1918 – 1923, *Hardy and then Hardy & Littlewood applied this idea to sums of squares, then to Waring’s problem, then to the Goldbach conjecture, then came the series Partitio numerorum ...*

This story is told in details in (Kempner, 1923).

In 1937, *I.M. Vinogradov saw that finite sums are enough:*

$$\sum_{0\leqslant a\leqslant N} z^a \sum_{0\leqslant b\leqslant N} z^{2b} \sum_{0\leqslant c\leqslant N} z^{3c}.$$

We may take $z = \exp(2i\pi\theta)$, *directly on the unit circle!*

After 1936: “arithmetical” trigonometric polynomials

Then early 1917: *Ramanujan ill, Littlewood incorporated as a soldier...*

Around 1918 – 1923, *Hardy and then Hardy & Littlewood applied this idea to sums of squares, then to Waring’s problem, then to the Goldbach conjecture, then came the series Partitio numerorum ...*

This story is told in details in (Kempner, 1923).

In 1937, *I.M. Vinogradov saw that finite sums are enough:*

$$\sum_{0\leqslant a\leqslant N} z^a \sum_{0\leqslant b\leqslant N} z^{2b} \sum_{0\leqslant c\leqslant N} z^{3c}.$$

We may take $z = \exp(2i\pi\theta)$, *directly on the unit circle!*

We study $\boxed{S(\theta) = \sum_{p\leqslant N} \exp(2i\pi p\theta)}$.

p prime

After 1936: "arithmetical" trigonometric polynomials

Then early 1917: *Ramanujan ill, Littlewood incorporated as a soldier...*

Around 1918 – 1923, *Hardy and then Hardy & Littlewood applied this idea to sums of squares, then to Waring's problem, then to the Goldbach conjecture, then came the series Partitio numerorum ...*

This story is told in details in (Kempner, 1923).

In 1937, *I.M. Vinogradov saw that finite sums are enough:*

$$\sum_{0\leqslant a\leqslant N} z^a \sum_{0\leqslant b\leqslant N} z^{2b} \sum_{0\leqslant c\leqslant N} z^{3c}.$$

We may take $z = \exp(2i\pi\theta)$, directly on the unit circle!

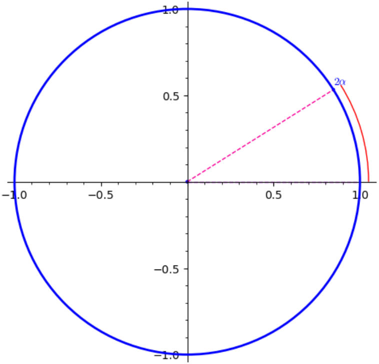
We study $$\boxed{S(\theta) = \sum_{\substack{p\leqslant N \\ p \text{ prime}}} \exp(2i\pi p\theta)}.$$

This is what we use to prove the three prime theorem.

Initiation

Initiation

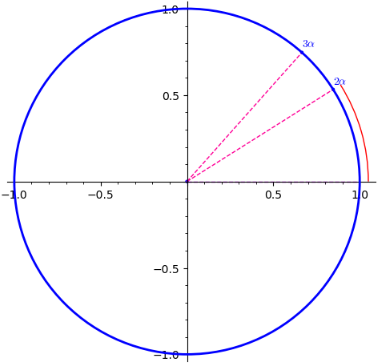
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2$

Initiation

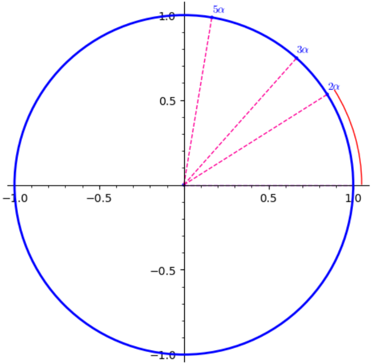
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3$

Initiation

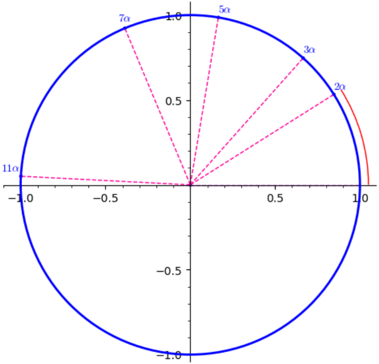
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3, 5$

Initiation

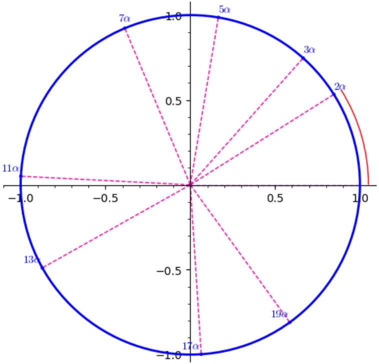
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3, \ldots, 11$

Initiation

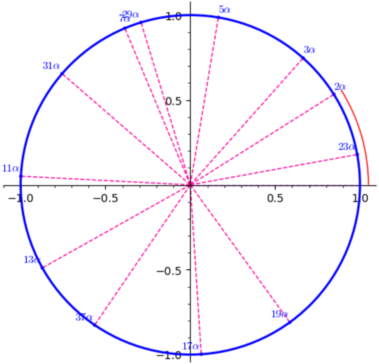
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3, \ldots, 19$

Initiation

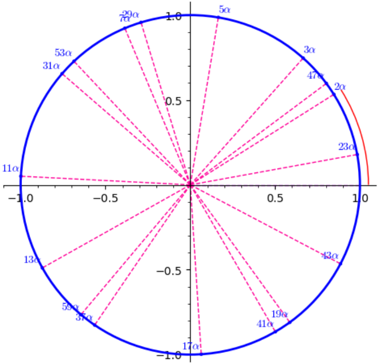
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3, 5, \ldots, 37$

Initiation

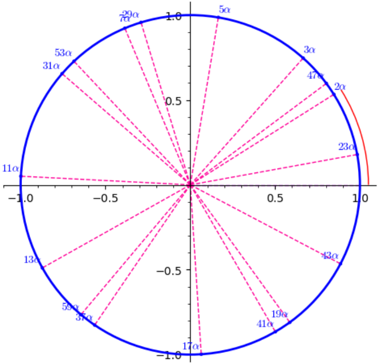
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!



The sequence $(p\alpha)$ for $p = 2, 3, 5, \ldots, 59$

Initiation

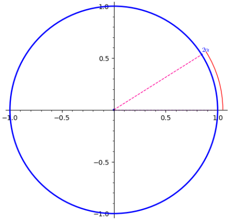
$\alpha = 2\pi/\sqrt{500} = 0.2809\cdots$ for elegant drawings!

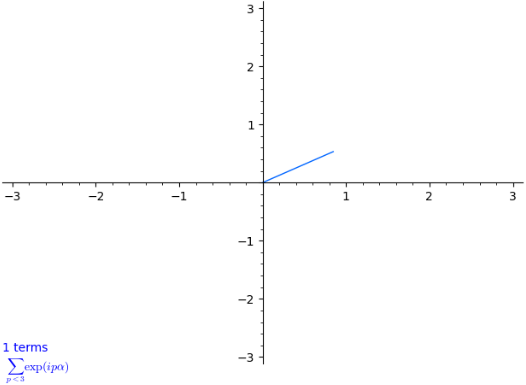


The set $(p\alpha)$ is dense on the unit cercle.

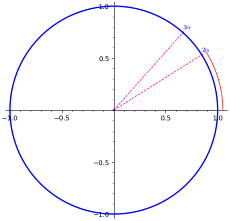
The sequence $(p\alpha)$ for $p = 2, 3, 5, \ldots, 59$

What about the average value?

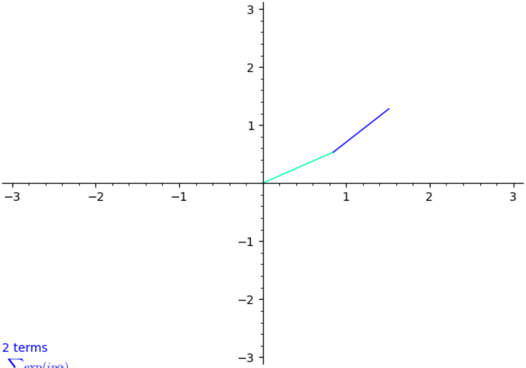




What about the average value?



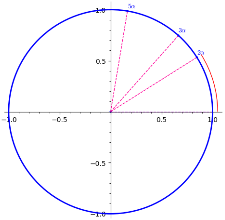
$\longrightarrow$

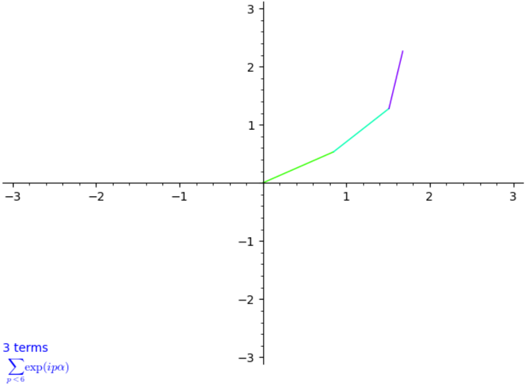


2 terms

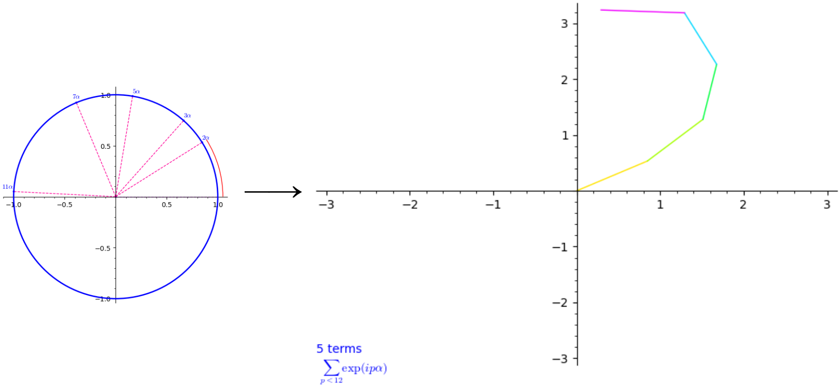
$\sum_{p<4} \exp(ip\alpha)$

What about the average value?

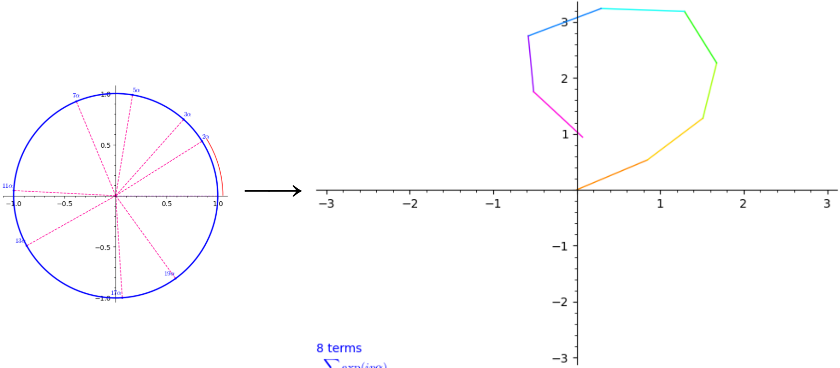




What about the average value?

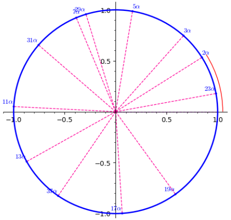


What about the average value?

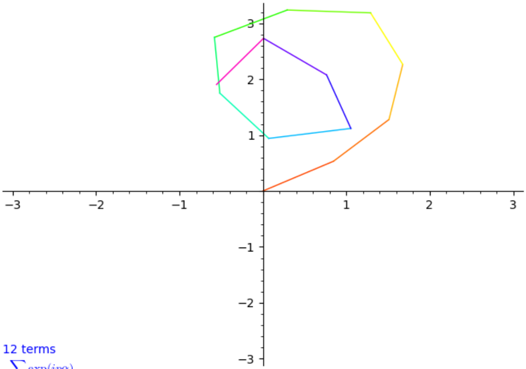


$$\sum_{p<20} \exp(ip\alpha)$$

What about the average value?



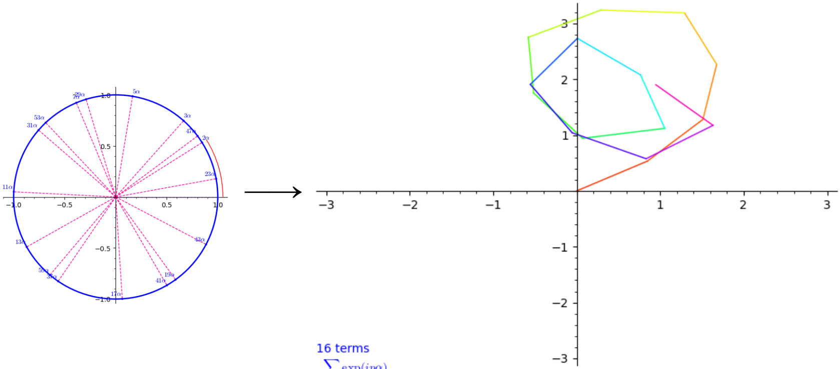
$\longrightarrow$



12 terms

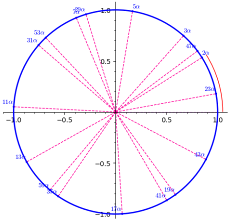
$\sum_{p<38} \exp(ip\alpha)$

What about the average value?

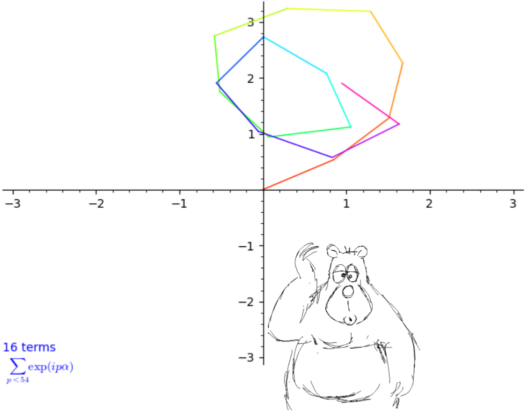


16 terms
$\sum_{p<54} \exp(ip\alpha)$

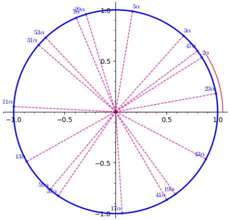
What about the average value?

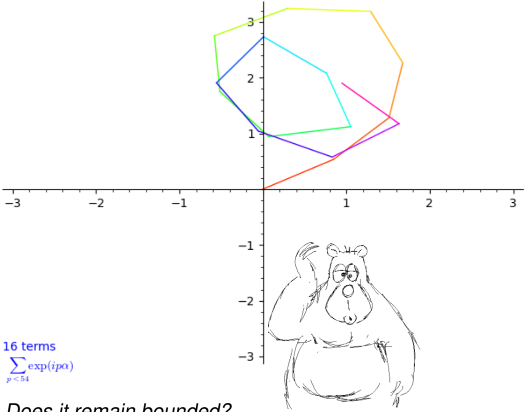


$\longrightarrow$



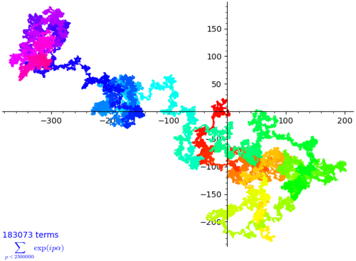
What about the average value?





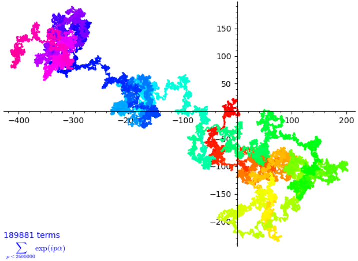
(1) Does it remain bounded?
(2) Does it stay more in some quadrant?
(3) Are there holes?

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 2\,500\,000$

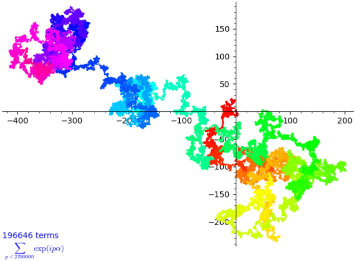
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

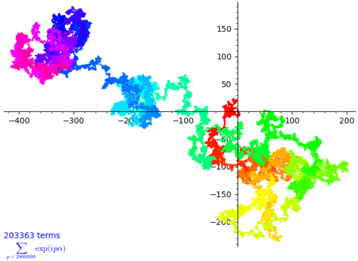
$N = 1, 2, \ldots, 2\,600\,000$

Seen from farther away



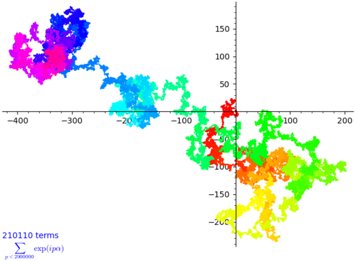
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 2\,700\,000$

Seen from farther away



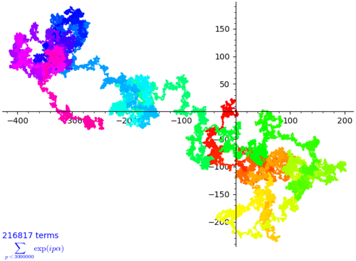
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 2\,800\,000$

Seen from farther away



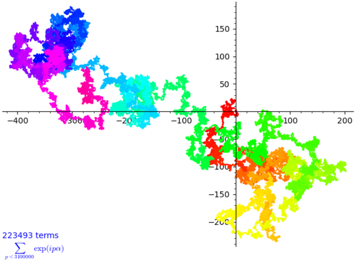
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 2\,900\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,000\,000$

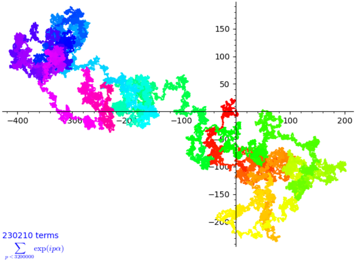
Seen from farther away



The sequence $\sum_{p\leqslant N} \exp(ip\alpha)$ for

$N = 1, 2, \ldots, 3\,100\,000$

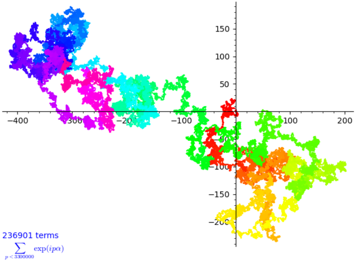
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

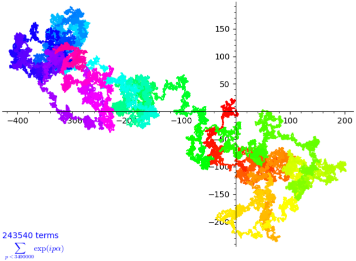
$N = 1, 2, \ldots, 3\,200\,000$

Seen from farther away



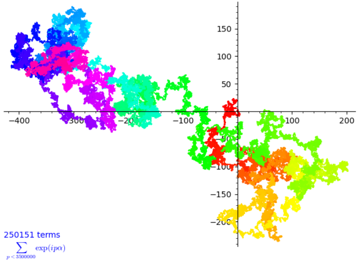
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,300\,000$

Seen from farther away



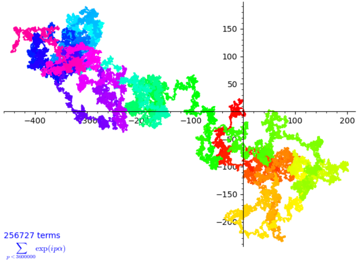
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,400\,000$

Seen from farther away



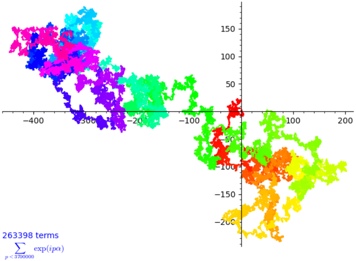
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,500\,000$

Seen from farther away



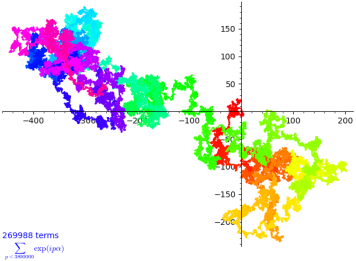
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,600\,000$

Seen from farther away



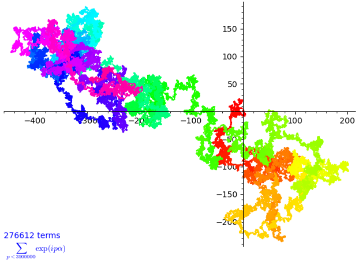
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,700\,000$

Seen from farther away



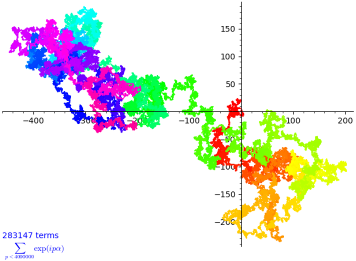
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,800\,000$

Seen from farther away



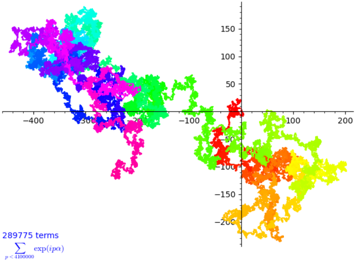
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 3\,900\,000$

Seen from farther away



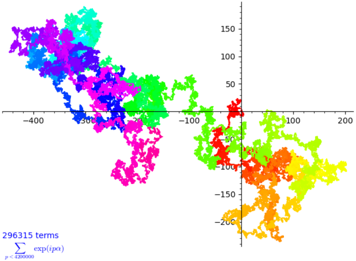
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,000\,000$

Seen from farther away



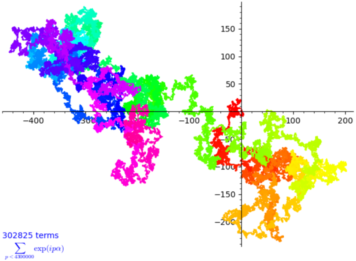
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,100\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,200\,000$

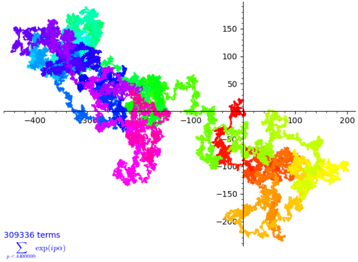
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

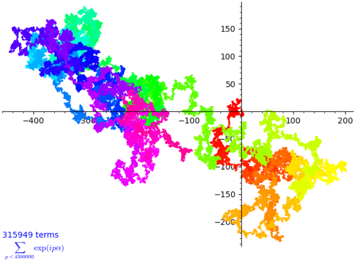
$N = 1, 2, \ldots, 4\,300\,000$

Seen from farther away



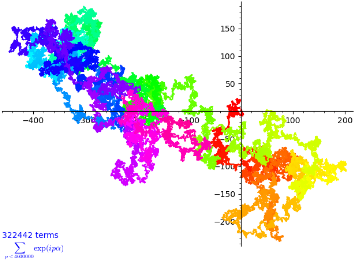
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,400\,000$

Seen from farther away



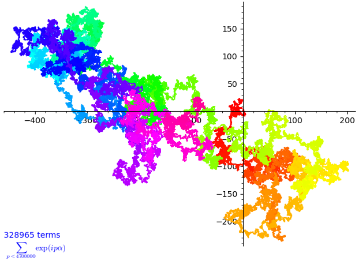
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,500\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 4\,600\,000$

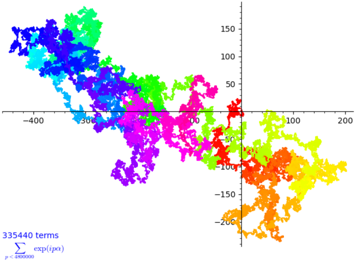
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

$N = 1, 2, \ldots, 4\,700\,000$

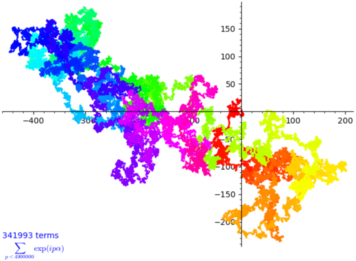
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

$N = 1, 2, \ldots, 4\,800\,000$

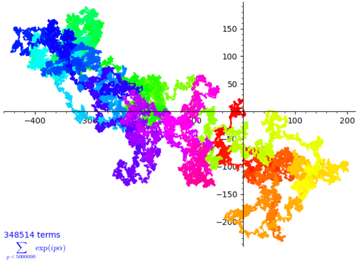
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

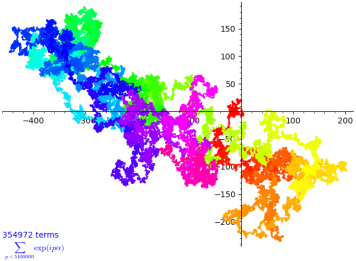
$N = 1, 2, \ldots, 4\,900\,000$

Seen from farther away



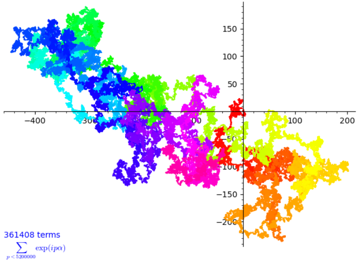
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,000\,000$

Seen from farther away



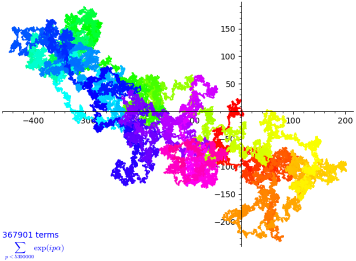
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,100\,000$

Seen from farther away



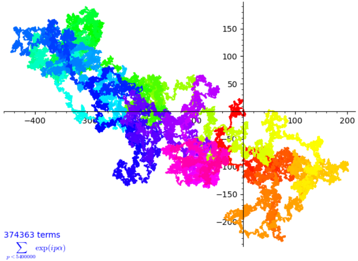
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,200\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,300\,000$

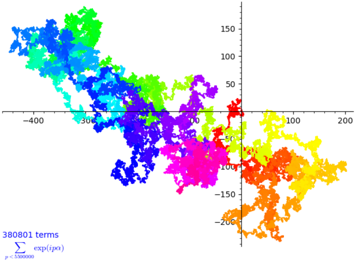
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

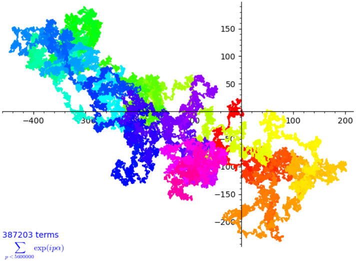
$N = 1, 2, \ldots, 5\,400\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,500\,000$

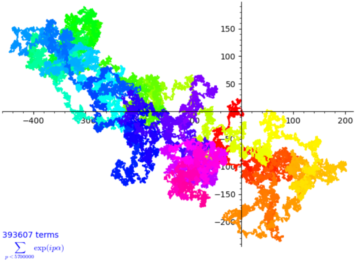
Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

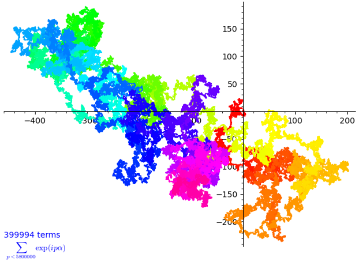
$N = 1, 2, \ldots, 5\,600\,000$

Seen from farther away



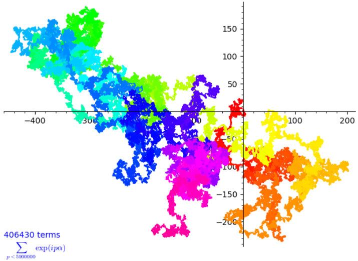
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,700\,000$

Seen from farther away



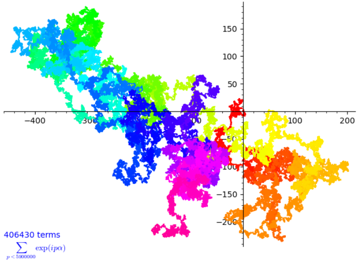
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,800\,000$

Seen from farther away



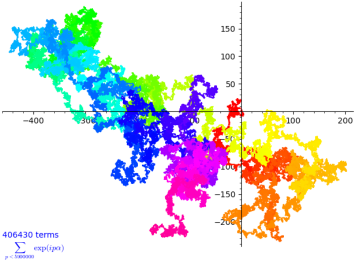
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,900\,000$

Seen from farther away



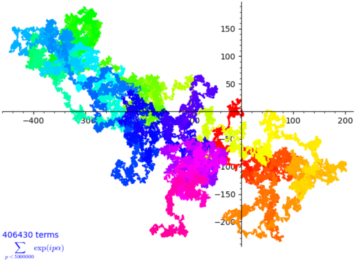
The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,900\,000$

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,900\,000$

Seen from farther away

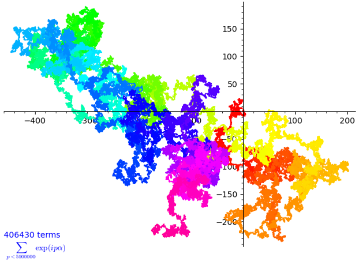


The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for

$N = 1, 2, \ldots, 5\,900\,000$

(1) This sum is very, very small!
(2) Where are the loops coming from?
(3) Does this sum “fill” the space?

Seen from farther away



The sequence $\sum_{p \leqslant N} \exp(ip\alpha)$ for $N = 1, 2, \ldots, 5\,900\,000$

(1) This sum is very, very small!
(2) Where are the loops coming from?
(3) Does this sum “fill” the space?

All what is known: (Vaughan, 1975): $\sum_{p \leqslant N} \exp(ip\alpha) \ll N^{4/5} (\log N)^3$

This is my speciality!

A dynamical viewpoint

Dynamics studies the transform:
$$\begin{aligned} T : [0,2\pi) &\to [0,2\pi) \\ x &\mapsto x+\alpha \mod 2\pi \end{aligned}$$

and the "trajectories" (iterates): $T(x)$, $T^2(x)$, $T^3(x)$, ...

(Starting from $x = 0$, we get $\alpha, 2\alpha, 3\alpha, \ldots$ on the circle).

Take a function $f : [0,2\pi) \to \mathbb{R}$

and study the (Birkhoff) average $\dfrac{1}{N} \displaystyle\sum_{n \leqslant N} f(T^n(x))$.

A dynamical viewpoint

Dynamics studies the transform: $\begin{aligned} T : [0, 2\pi) &\rightarrow [0, 2\pi) \\ x &\mapsto x + \alpha \mod 2\pi \end{aligned}$

and the "trajectories" (iterates): $T(x)$, $T^2(x)$, $T^3(x)$, ...

(Starting from $x = 0$, we get $\alpha, 2\alpha, 3\alpha, \ldots$ on the circle).

Take a function $f : [0, 2\pi) \rightarrow \mathbb{R}$

and study the (Birkhoff) average $\frac{1}{N} \sum_{n \leqslant N} f(T^n(x))$.

(Green & Tao, 2008) considered $\frac{1}{\pi(N)} \sum_{p \leqslant N} f(T^p(x))$.

There are infinitely many solutions to $p_4 - p_3 = p_3 - p_2 = p_2 - p_1$.

A dynamical viewpoint

Dynamics studies the transform: $\begin{aligned} T : [0,2\pi) &\to [0,2\pi) \\ x &\mapsto x+\alpha \mod 2\pi \end{aligned}$

and the "trajectories" (iterates): $T(x)$, $T^2(x)$, $T^3(x)$, ...

(Starting from $x = 0$, we get $\alpha, 2\alpha, 3\alpha, \ldots$ on the circle).

Take a function $f : [0,2\pi) \to \mathbb{R}$

and study the (Birkhoff) average $\frac{1}{N}\sum_{n \leqslant N} f(T^n(x))$.

(Green & Tao, 2008) considered $\frac{1}{\pi(N)}\sum_{p \leqslant N} f(T^p(x))$.

There are infinitely many solutions to $p_4 - p_3 = p_3 - p_2 = p_2 - p_1$.

Then (Bourgain et al., 2013) considered $\frac{1}{N}\sum_{n \leqslant N} \mu(n) f(T^n(x))$.

A dynamical viewpoint

Dynamics studies the transform: $\begin{aligned} T : [0,2\pi) &\to [0,2\pi) \\ x &\mapsto x+\alpha \mod 2\pi \end{aligned}$

and the "trajectories" (iterates): $T(x)$, $T^2(x)$, $T^3(x)$, ...

(Starting from $x = 0$, we get $\alpha, 2\alpha, 3\alpha, \ldots$ on the circle).

Take a function $f : [0,2\pi) \to \mathbb{R}$

and study the (Birkhoff) average $\frac{1}{N}\sum_{n\leqslant N} f(T^n(x))$.

(Green & Tao, 2008) considered $\frac{1}{\pi(N)}\sum_{p\leqslant N} f(T^p(x))$.

There are infinitely many solutions to $p_4 - p_3 = p_3 - p_2 = p_2 - p_1$.

Then (Bourgain et al., 2013) considered $\frac{1}{N}\sum_{n\leqslant N} \mu(n) f(T^n(x))$.

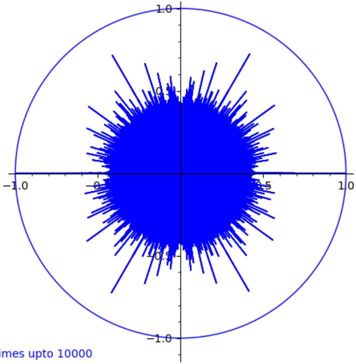
A large body of work emerged on "nilsequences", and on "Sarnak's conjecture".

Varying α / Charted land

Let have α vary

We looked at $S(\alpha) = \sum_{p \leqslant N} \exp(ip\alpha)$ for α fixed and N growing.

Let us look now at $|S(\theta)|$ with θ variable:



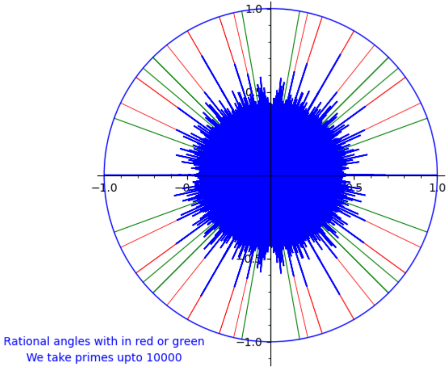
We take primes upto 10000

The normalised module in blue,

Let have α vary

We looked at $S(\alpha) = \sum_{p \leqslant N} \exp(ip\alpha)$ for α fixed and N growing.

Let us look now at $|S(\theta)|$ with θ variable:

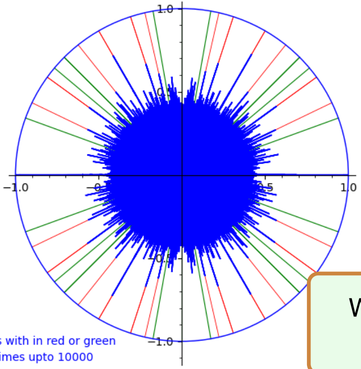


The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

Let have α vary

We looked at $S(\alpha) = \sum_{p \leqslant N} \exp(ip\alpha)$ for α fixed and N growing.

Let us look now at $|S(\theta)|$ with θ variable:



Rational angles with in red or green
We take primes upto 10000

The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

We know how to explain the “cusps”
$\rightarrow$ the Three Primes Theorem

Full sequence: the charted territory

- The value of $\exp(2i\pi pa/q)$ depends only on $p \mod q$.
- Hence PNTAP (Prime Number Theorem in Arithmetic Progressions) controls $S(2\pi a/q)$ when q is “not too large”.

That’s where we see that q squarefree is important.

- Good error term in PNTAP $\rightarrow$ the cusps are sharp.

These are the “major arcs” in Hardy-Littlewood-Ramanujan terminology.

- Away from these? Technique “à la Vinogradov”. Best is $N^{3/4}$.

These are the “minor arcs” in Hardy-Littlewood-Ramanujan terminology.

Cf “sums of type B” in Vinogradov.

- Better bounds? Open territory.
- Angular distribution? Open territory.

Opening the lens

Lack of precision versus generality

We lack of precision,
so maybe we can gain in generality!

(OR+Ruzsa, 98): subsequences $\mathcal{P}^*$ (of the primes) *of density*

for instance, when $N \geqslant 2$, $\#\{p \in \mathcal{P}^* : p \leqslant N\} \geqslant \dfrac{N}{100 \log N}$.

..... Follows lots of work !!! ....

$\bigoplus$ *ergodic aspect (linked to Szemedéri's theorem)*

The leading idea is that primes may be "described" by arithmetic progressions.
Arithmetic progressions share additive properties with the set of every integers.
$\longrightarrow$ "So" primes may share the same properties!
Green set to follow this program on Szemedéri's Theorem.

(Green & Tao, 2008): There are infinitely many solutions to

$$p_4 - p_3 = p_3 - p_2 = p_2 - p_1.$$

And (Tao & Ziegler, 2008), (Green & Tao, 2012), (Tao & Ziegler, 2015), ...

Let us go back to the (theoretical but not historical) beginning!

On the cusps

The number of cusps is finite!

(Green & Tao, 2006): Set $S^*(\alpha) = \sum_{\mathcal{P}^* \ni p \leqslant N} \exp(2i\pi\alpha p)$.

Then

$$\#\left\{\alpha \in \{\tfrac{1}{N}, \tfrac{2}{N}, \cdots, \tfrac{N}{N}\} : |S^*(\alpha)| \geqslant \xi S^*(0)\right\} \ll (1/\xi)^{2+\varepsilon}.$$

Maximum size: $|S^*(\alpha)| \leqslant S^*(0)$.

Number of small Farey points:
$$\#\left\{\tfrac{a}{q} \in [0,1) : q \leqslant 1/\xi\right\} \ll (1/\xi)^2.$$

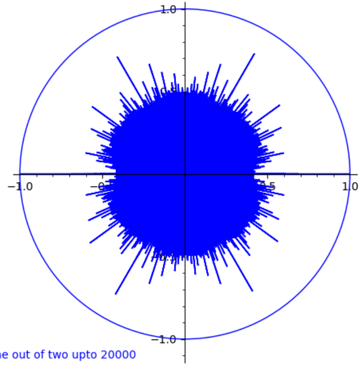
(OR, 2022, 2023):

$$\#\left\{\alpha \in \{\tfrac{1}{N}, \tfrac{2}{N}, \cdots, \tfrac{N}{N}\} : |S^*(\alpha)| \geqslant \xi S^*(0)\right\} \ll (1/\xi)^2.$$

Are all the cusps at Farey points??

A trial

Let us take a prime out of two:

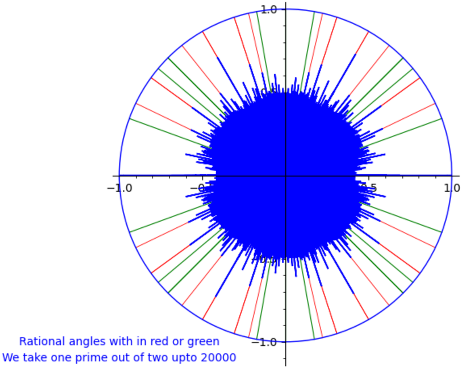


We take one prime out of two upto 20000

The normalised module in blue,

A trial

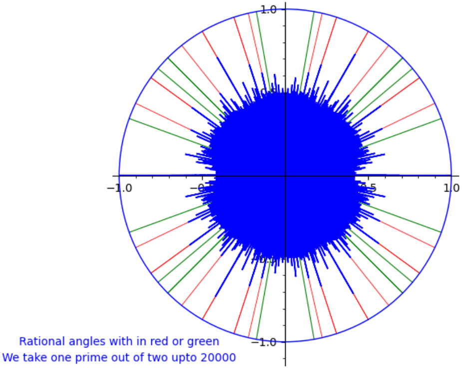
Let us take a prime out of two:



The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

A trial

Let us take a prime out of two:

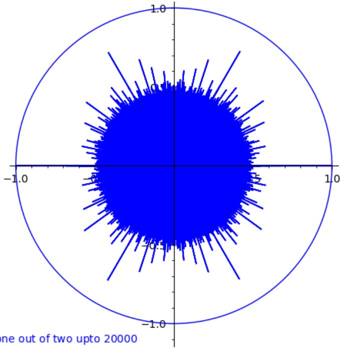


The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

(1) Again the "urchin" structure,
(2) Again cusps at the a/q!!

What about randomly?

Let us take randomly one prime out of two:

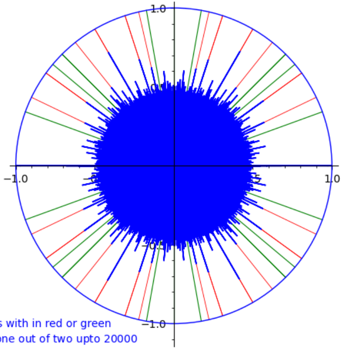


We take random p one out of two upto 20000

The normalised module in blue,

What about randomly?

Let us take randomly one prime out of two:

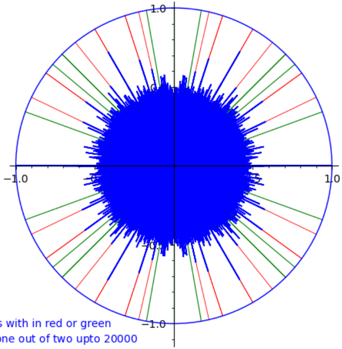


Rational angles with in red or green
We take random p one out of two upto 20000

The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

What about randomly?

Let us take randomly one prime out of two:

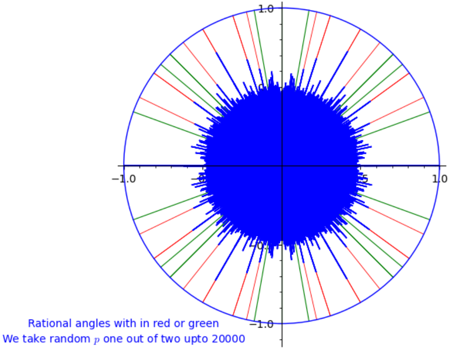


Rational angles with in red or green
We take random p one out of two upto 20000

The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

What about randomly?

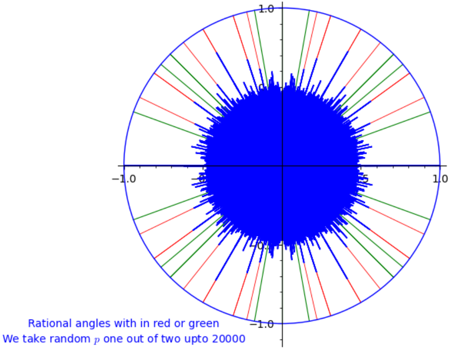
Let us take randomly one prime out of two:



The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

What about randomly?

Let us take randomly one prime out of two:

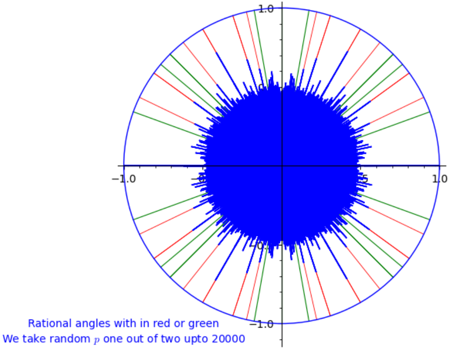


The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

(1) Again the "urchin" structure,
(2) Again cusps at the a/q!!

What about randomly?

Let us take randomly one prime out of two:

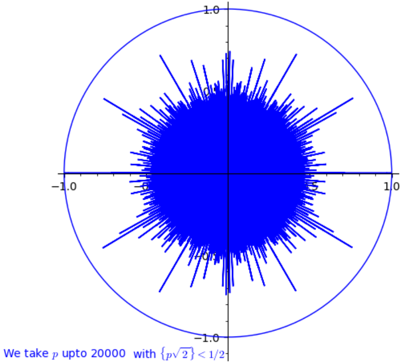


The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

(1) Again the "urchin" structure,
(2) Again cusps at the a/q!!
(3) It can be proved!

May we get a different behaviour???

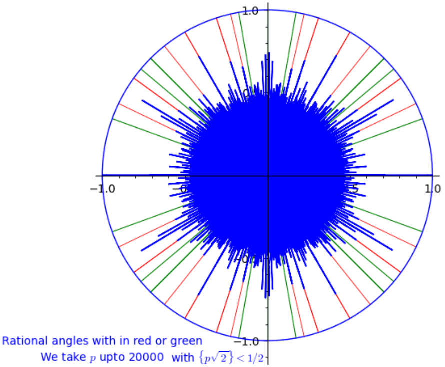
Select the primes p by $\{p\sqrt{2}\} < 1/2$:



The normalised module in blue,

May we get a different behaviour???

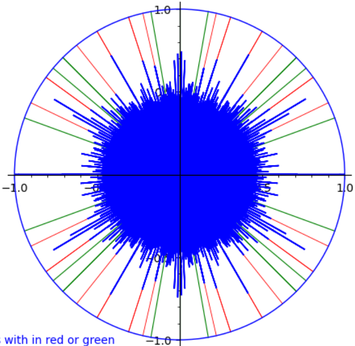
Select the primes p by $\{p\sqrt{2}\} < 1/2$:



The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

May we get a different behaviour???

Select the primes p by $\{p\sqrt{2}\} < 1/2$:



Rational angles with in red or green
We take p upto 20000 with $\{p\sqrt{2}\} < 1/2$

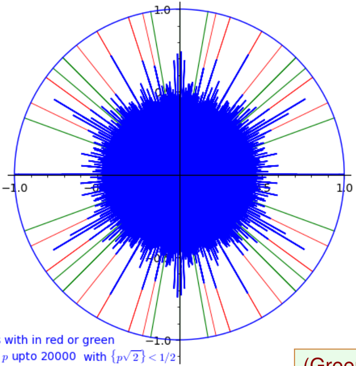
The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

Cusps are few:

(Green & Tao, 2006): For every subsequence of primes of density, the number of "cusps" is finite.

May we get a different behaviour???

Select the primes p by $\{p\sqrt{2}\} < 1/2$:



Rational angles with in red or green
We take p upto 20000 with $\{p\sqrt{2}\} < 1/2$

The normalised module in blue, the angles $2\pi a/q$ are in green when... and in red when...

Cusps are few: (Green & Tao, 2006): For every subsequence of primes of density, the number of "cusps" is finite.

Very few: (OR, 2023): This number of "cusps" is comparable to the number of rationals of small height.

Agrawal, Manindra, Kayal, Neeraj, & Saxena, Nitin. 2004.
PRIMES is in P.
Ann. of Math. (2), **160**(2), 781–793.

Bourgain, J., Sarnak, P., & Ziegler, T. 2013.
Disjointness of Moebius from horocycle flows.
Pages 67–83 of: From Fourier analysis and number theory to Radon transforms and geometry.
Dev. Math., vol. 28.
Springer, New York.

Green, B., & Tao, T. 2006.
Restriction theory of the Selberg sieve, with applications.
J. Théor. Nombres Bordx, **18**(1), 147–182.
Available at `http://fr.arxiv.org/pdf/math.NT/0405581`.

Green, B., & Tao, T. 2008.
The primes contain arbitrarily long arithmetic progressions.
Ann. of Math., 481–547.
Available at `http://fr.arxiv.org/pdf/math.NT/0404188`.

Green, B., & Tao, T. 2012.
The Möbius function is strongly orthogonal to nilsequences.
Ann. of Math. (2), **175**(2), 541–566.

Hardy, G. H., & Ramanujan, S. 1916.
Asymptotic formulae for the distribution of integers of various types. (A problem in the analytic theory of numbers.).
Proc. Lond. Math. Soc. (2), **16**, 112–132.

Hardy, G. H., & Ramanujan, S. 1917.
Une formule asymptotique pour le nombre des partitions de *n*.
C. R. Acad. Sci., Paris, **164**, 35–38.

Hardy, G. H., & Ramanujan, S. 1918.
Asymptotic formulae in combinatory analysis.
Proc. Lond. Math. Soc. (2), **17**, 75–115.

Hardy, G. H., & Ramanujan, S. 2000.
Asymptotic formulæ for the distribution of integers of various types [Proc. London Math. Soc. (2) **16** (1917), 112–132].
Pages 245–261 of: Collected papers of Srinivasa Ramanujan.
AMS Chelsea Publ., Providence, RI.

Harvey, David. 2021.
An exponent one-fifth algorithm for deterministic integer factorisation.
Math. Comp., **90**(332), 2937–2950.

Hittmeir, Markus. 2021.
A time-space tradeoff for Lehman's deterministic integer factorization method.
Math. Comp., **90**(330), 1999–2010.

Kempner, Aubrey J. 1923.
The Development of "Partitio Numerorum," with Particular Reference to the Work of Messrs. Hardy, Littlewood and Ramanujan.
Amer. Math. Monthly, **30**(7), 354–369.

Ramaré, O. 2022.
Notes on restriction theory in the primes.
Israel J. of Math., 22pp.

Strassen, Volker. 1976/77.
Einige Resultate über Berechnungskomplexität.
Jber. Deutsch. Math.-Verein., **78**(1), 1–8.

Tao, Terence, & Ziegler, Tamar. 2008.
The primes contain arbitrarily long polynomial progressions.
Acta Math., **201**(2), 213–305.

Tao, Terence, & Ziegler, Tamar. 2015.
Narrow progressions in the primes.
Pages 357–379 of: Analytic number theory.
Springer, Cham.

Vaughan, R.C. 1975.
Mean value theorems in prime number theory.
J. London Math Soc. (2), **10**, 153–162.