Patterns in the primes

… And dynamics

Andrew Granville

(with animations by *Anthony Doran*)

New York City *27th March 2012*

The primes

$$2, 3, 5, 7, 11, 13, \ldots$$

What? Where? How? Why?
Traditional questions

THE PRIMES

$$2, 3, 5, 7, 11, 13, \ldots$$

What? Where? How? Why?
Traditional questions

We will find them in strange places
Motivated by the use of dynamics

Magic squares

We arrange numbers in a square grid, so that the sum of the rows, and columns, and diagonals all equal. For example we can take the numbers from 1 to 9:

2	7	6
9	5	1
4	3	8

Magic sum is 15

Magic squares

We arrange numbers in a square grid, so that the sum of the rows, and columns, and diagonals all equal. For example we can take the numbers from 1 to 9:

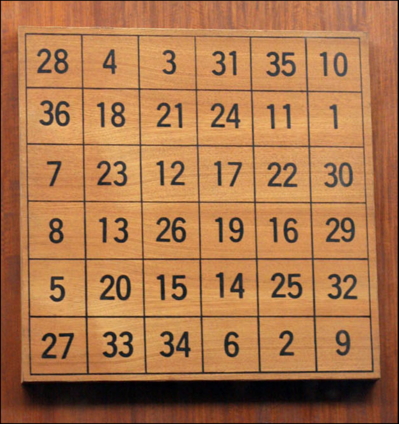
2	7	6
9	5	1
4	3	8

Magic sum is 15

Magic squares have been identified for over 4000 years.

Next slide: A 6-by-6 magic square from the Yuan Dynasty (1271-1368)

And then: Albrecht Dürer's 1514 engraving *Melencolia I*


28 4 3 31 35 10
36 18 21 24 11 1
7 23 12 17 22 30
8 13 26 19 16 29
5 20 15 14 25 32
27 33 34 6 2 9


MELENCOLIA I
16 3 2 13
5 10 11 8
9 6 7 12
4 15 14 1

Magic squares

2	7	6
9	5	1
4	3	8

Magic sum is 15

How about magic squares of primes ?

Magic squares

2	7	6
9	5	1
4	3	8

Magic sum is 15

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

17	89	71
113	59	5
47	29	101

Magic squares

2	7	6
9	5	1
4	3	8

Magic sum is 15

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

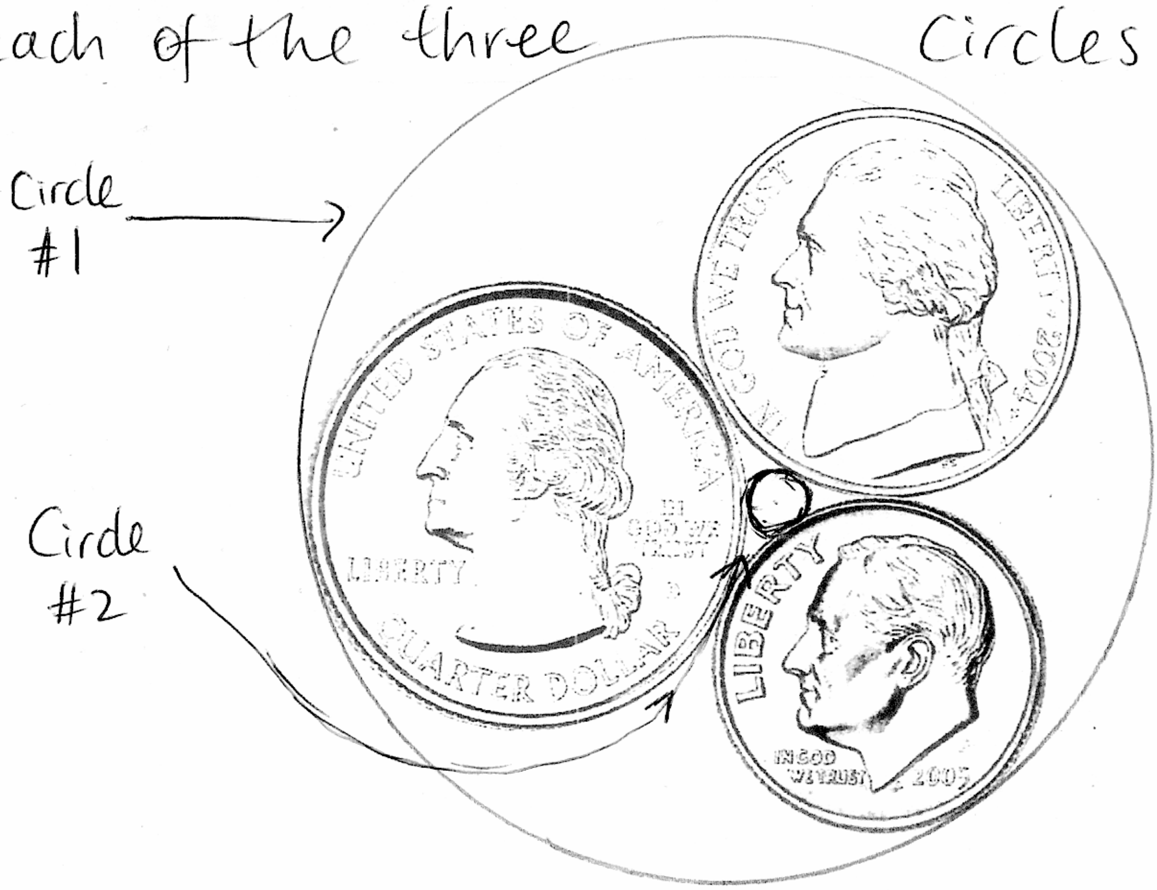
17	89	71
113	59	5
47	29	101

Are there infinitely many?

We begin with 3 circles, each touching each other:

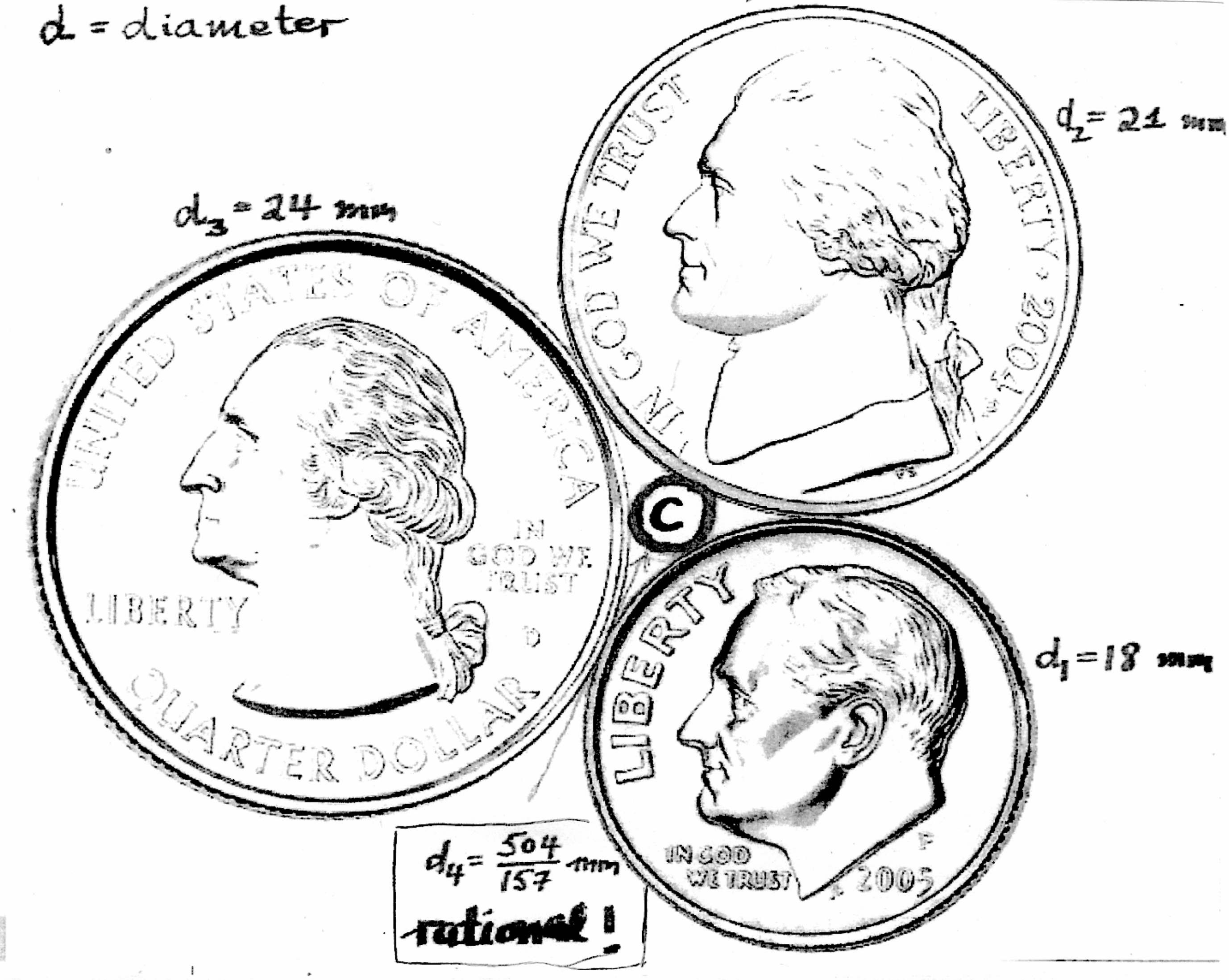
For instance:

Then there are two circles that TOUCH each of the three circles:



Let's check out their diameters:

d = diameter



The outside circle has diameter $\frac{504}{11}$ mm.

Easier to work with integers.

Define Curvature := 504/diameter.

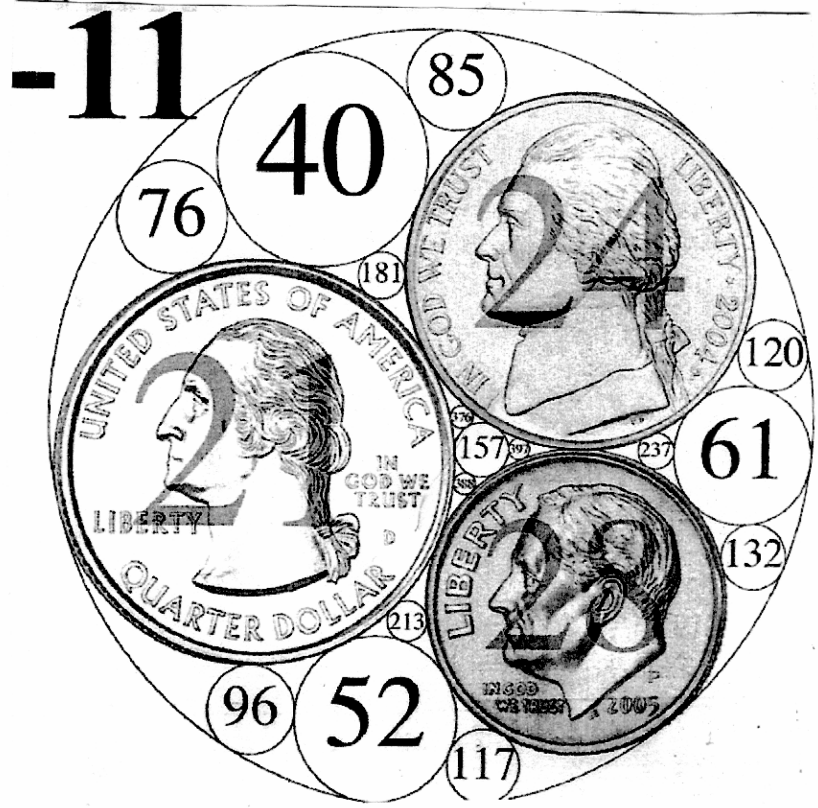
So $c_1 = \frac{504}{d_1} = 28$, $c_2 = 24$, $c_3 = 21$

$c_4 = 157$, $c_5 = 11$

The curvatures of our circles are:

Add more circles (in the same way):

And more



Until you completely fill the circle:

An APOLLONIAN CIRCLE PACKING.

Dynamics and primes?

There are many links ...
We'll start with proving:

There are infinitely many primes

...using dynamical systems

There are infinitely many primes

Want an infinite sequence of integers

$$1 < x_1 < x_2 < x_3 < \dots$$

such that

$$\gcd(x_i, x_j) = 1 \text{ whenever } i \neq j.$$

If prime p_j divides x_j for each j

then $\quad p_1, p_2, p_3 \dots$

is an infinite seq of distinct primes.

There are infinitely many primes

Want an infinite sequence of integers

$$1 < x_1 < x_2 < x_3 < \ldots$$

such that

$$\gcd(x_i, x_j) = 1 \text{ whenever } i \neq j.$$

If prime p_j divides x_j for each j

then $\quad p_1, p_2, p_3 \ldots$

is an infinite seq of distinct primes.

PROOF: If $p_i = p_j$ for $i \neq j$, then

p_i divides x_i and p_j divides x_j,

so that

$p_i = p_j$ divides $\gcd(x_i, x_j) = 1$,

Contradiction.

There are infinitely many primes

So how do we find integers

$$1 < x_1 < x_2 < x_3 < \dots$$

such that

$\gcd(x_i, x_j) = 1$ whenever $i \neq j$?

There are infinitely many primes

So how do we find integers

$$1 < x_1 < x_2 < x_3 < \dots$$

such that

$$\gcd(x_i, x_j) = 1 \text{ whenever } i \neq j?$$

Dynamical systems!

That is using a map like

$$x \hookrightarrow x^2 - x + 1 \dots$$

. We begin by studying remainders under this map

Remainders: $x \hookrightarrow x^2 - x + 1$

$$x = km \hookrightarrow x^2 - x + 1 = (k^2m - k)m + 1$$

Remainder $0 \hookrightarrow$ Remainder 1

$$x = km + 1 \hookrightarrow x^2 - x + 1 = (k^2m + k)m + 1$$

Remainder $1 \hookrightarrow$ Remainder 1

•

And how do we use this?

REMAINDERS: $x \hookrightarrow x^2 - x + 1$

$$x = km \hookrightarrow x^2 - x + 1 = (k^2m - k)m + 1$$

Remainder 0 $\hookrightarrow$ Remainder 1

$$x = km + 1 \hookrightarrow x^2 - x + 1 = (k^2m + k)m + 1$$

Remainder 1 $\hookrightarrow$ Remainder 1

——— Construction ———

Select $x_1 > 1$, say 2, and then

$$x_2 = x_1^2 - x_1 + 1,$$
$$x_3 = x_2^2 - x_2 + 1,$$
$$\ldots$$

And the remainders when we divide by x_i?

Remainders: $x \hookrightarrow x^2 - x + 1$

$$x = km \hookrightarrow x^2 - x + 1 = (k^2m - k)m + 1$$

Remainder 0 $\hookrightarrow$ Remainder 1

$$x = km + 1 \hookrightarrow x^2 - x + 1 = (k^2m + k)m + 1$$

Remainder 1 $\hookrightarrow$ Remainder 1

——— Construction ———

Select $x_1 > 1$, say 2, and then

$$x_2 = x_1^2 - x_1 + 1,$$
$$x_3 = x_2^2 - x_2 + 1,$$
$$\ldots$$

When x_j is divided by x_i $(= m)$:

x_i has remainder 0, so that

$\hookrightarrow x_{i+1} = x_i^2 - x_i + 1$ remainder 1

$\hookrightarrow x_{i+2}$ has remainder 1

$\hookrightarrow x_{i+3}$ has remainder 1. . .

x_i has remainder 0, so that

$\hookrightarrow x_{i+1}$ has remainder 1

$\hookrightarrow x_{i+2}$ has remainder 1

$\hookrightarrow x_{i+3}$ has remainder $1 \ldots$

Therefore x_j has remainder 1 when divided by x_i for all $j > i$

We deduce that

$$\gcd(x_i, x_j) = \gcd(x_i, 1) = 1.$$

——— *Result* ———

Let x_1 be an integer, define

$$x_{i+1} = x_i^2 - x_i + 1$$

for all $i \geq 1$. If x_j has prime divisor p_j for each $j \geq 1$ then

$$p_1, p_2, p_3 \ldots$$

is an infinite seq of distinct primes.

Result

Let x_1 be an integer, define

$$x_{i+1} = x_i^2 - x_i + 1$$

for all $i \geq 1$. If x_j has prime divisor p_j for each $j \geq 1$ then

$$p_1, p_2, p_3 \cdots$$

is an infinite seq of distinct primes.

Result

Let x_1 be an integer, define

$$x_{i+1} = x_i^2 - x_i + 1$$

for all $i \geq 1$. If x_j has prime divisor p_j for each $j \geq 1$ then

$$p_1, p_2, p_3 \cdots$$

is an infinite seq of distinct primes.

Examples

With $x \hookrightarrow x^2 - x + 1$, we have:

$$2 \hookrightarrow 3 \hookrightarrow 7 \hookrightarrow 43 \hookrightarrow \ldots,$$

(Euclid: $2{\cdot}3{+}1 = 7$, $2{\cdot}3{\cdot}7{+}1 = 43$)

Result

Let x_1 be an integer, define

$$x_{i+1} = x_i^2 - x_i + 1$$

for all $i \geq 1$. If x_j has prime divisor p_j for each $j \geq 1$ then

$$p_1, p_2, p_3 \cdots$$

is an infinite seq of distinct primes.

Examples

With $x \hookrightarrow x^2 - x + 1$, we have:

$$2 \hookrightarrow 3 \hookrightarrow 7 \hookrightarrow 43 \hookrightarrow \ldots,$$

(Euclid: $2{\cdot}3{+}1 = 7$, $2{\cdot}3{\cdot}7{+}1 = 43$)

With $x \hookrightarrow x^2 - 2x + 2$, we have:

$$3 \hookrightarrow 5 \hookrightarrow 17 \hookrightarrow 257 \hookrightarrow \ldots,$$

The Fermat numbers, $2^{2^n} + 1$

Formulas that only take prime values?

Fermat (1638): $2^{2^n}+1$ is prime for all $n \geq 0$:

$3, 5, 17, 257, 65537$ are all prime.

Formulas that only take prime values?

Fermat (1638): $2^{2^n}+1$ is prime for all $n \geq 0$:

$3, 5, 17, 257, 65537$ are all prime,

BUT

$2^{2^5} + 1 = 641 \times 6700417$ (Euler)

Formulas that only take prime values?

Fermat (1638): $2^{2^n}+1$ is prime for all $n \geq 0$:

$3, 5, 17, 257, 65537$ are all prime,

BUT

$2^{2^5} + 1 = 641 \times 6700417$ (Euler)

How did Fermat make this mistake?

How much calculation to check whether

$$2^{2^5} + 1$$

is prime?

What about

$$2^{2^6} + 1\ ?$$

Even today: The following are primes:

$$2^2 - 1 = 3$$

$$2^{2^2-1} - 1 = 2^3 - 1 = 7$$

$$2^{2^{2^2-1}-1} - 1 = 2^7 - 1 = 127$$

$$2^{2^{2^{2^2-1}-1}-1} - 1 = 2^{127} - 1.$$

Even today: The following are primes:

$$2^2 - 1 = 3$$

$$2^{2^2-1} - 1 = 2^3 - 1 = 7$$

$$2^{2^{2^2-1}-1} - 1 = 2^7 - 1 = 127$$

$$2^{2^{2^{2^2-1}-1}-1} - 1 = 2^{127} - 1.$$

Conjecture (and challenge)

$$2^{2^{2^{2^{2^2-1}-1}-1}-1} - 1$$

$$= 2^{2^{127}-1} - 1$$

is prime?

• Are there formulas for the primes? Polynomials?

Formulas for primes?

Polynomial with lots of prime values:

$5, 11, 17, 23, 29$, but then $\mathbf{35} = 5 \times 7$

so

$6n + 5$ prime for $n = 0, 1, \ldots, 4$.

Formulas for primes?

Polynomial with lots of prime values:

$5, 11, 17, 23, 29,$ but then $\mathbf{35} = 5 \times 7$

so

$6n + 5$ prime for $n = 0, 1, \ldots, 4.$

More famous is $n^2 + n + 41$ with

$41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, \ldots$

which remains prime until

$$40^2 + 40 + 41 = \mathbf{1681} = 41^2$$

.

Polynomials with only prime values?

$$n^2 + n + 41$$

is prime for $n = 0, 1, \cdots, 39$, but

$$41^2 + 41 + 41$$

is divisible by 41.

Polynomials with only prime values?

$$n^2 + n + 41$$

is prime for $n = 0, 1, \cdots, 39$, but

$$41^2 + 41 + 41$$

is divisible by 41.

Similarly, if $n = 41k$, then

$$n^2 + n + 41 = 41(41k^2 + k + 1),$$

so is divisible by 41.

Polynomials with only prime values?

$$n^2 + n + 41$$

is prime for $n = 0, 1, \cdots, 39$, but

$$41^2 + 41 + 41$$

is divisible by 41.

Similarly, if $n = 41k$, then

$$n^2 + n + 41 = 41(41k^2 + k + 1),$$

so is divisible by 41.

Therefore $n^2 + n + 41$ is *composite* for infinitely many n.

Polynomials with only prime values?

$$n^2 + n + 41$$

is prime for $n = 0, 1, \cdots, 39$, but

$$41^2 + 41 + 41$$

is divisible by 41.

Similarly, if $n = 41k$, then

$$n^2 + n + 41 = 41(41k^2 + k + 1),$$

so is divisible by 41.

Therefore $n^2 + n + 41$ is *composite* for infinitely many n.

Argument can be modified to work for the values of any polynomial $f(n)$.

So, Polynomials **cannot** take **only** prime values

.

Fails. How about infinitely often prime?

Can a polynomial $f(x)$ take prime values infinitely often?

$$n^2 - 1 = (n-1)(n+1)$$

is prime *only for* $n = -2$ and 2, because $x^2 - 1$ is reducible.

So, must assume polynomial $f(x)$ is *Irreducible*

Can a polynomial $f(x)$ take prime values infinitely often?

$$n^2 - 1 = (n-1)(n+1)$$

is prime *only for* $n = -2$ and 2, because $x^2 - 1$ is reducible.

So, must assume polynomial $f(x)$ is *Irreducible*

$$n^2 - n + 2 = 2\left(\binom{n}{2} + 1\right)$$

cannot be prime, as it's always even.

Can a polynomial $f(x)$ take prime values infinitely often?

$$n^2 - 1 = (n-1)(n+1)$$

is prime *only for* $n = -2$ and 2, because $x^2 - 1$ is reducible.

So, must assume polynomial $f(x)$ is

Irreducible

$$n^2 - n + 2 = 2\left(\binom{n}{2} + 1\right)$$

cannot be prime, as it's always even.

So, must assume polynomial $f(x)$ is

Admissible: There is no prime p which divides $f(n)$ for every integer n.

Can a polynomial $f(x)$ take prime values infinitely often?

Admissible: There is no prime p which divides $f(n)$ for every integer n.

CONJECTURE: If a polynomial of degree ≥ 1 is irreducible and admissible then it takes on infinitely many prime values.

.

What do we know about this conjecture?

Can a polynomial $f(x)$ take prime values infinitely often?

Admissible: There is no prime p which divides $f(n)$ for every integer n.

Conjecture: If a polynomial of degree ≥ 1 is irreducible and admissible then it takes on infinitely many prime values.

True for polynomials of degree 1.

CAN A POLYNOMIAL $f(x)$ TAKE PRIME VALUES INFINITELY OFTEN?

Admissible: There is no prime p which divides $f(n)$ for every integer n.

CONJECTURE: If a polynomial of degree ≥ 1 is irreducible and admissible then it takes on infinitely many prime values.

TRUE for polynomials of degree 1.
OPEN for *all* polyns of degree > 1.
The simplest open example is

$$x^2 + 1.$$

• Can't say much more! But as in $n^2 + n + 41$ example, we can ask...

Can a polynomial $f(x)$ take prime values infinitely often?

Admissible: There is no prime p which divides $f(n)$ for every integer n.

Conjecture: If a polynomial of degree ≥ 1 is irreducible and admissible then it takes on infinitely many prime values.

True for polynomials of degree 1.
Open for *all* polyns of degree > 1.
The simplest open example is

$$x^2 + 1.$$

Fix integer $m > 1$

Are there polynomials whose first m values are all prime?

. Return to this later. For now, other ways to find primes.

More complicated formulas

Let

$$p_1 = 2 < p_2 = 3 < p_3 = 5 \ldots$$

be the sequence of primes. Define

$$\alpha := \sum_{m \geq 1} \frac{p_m}{10^{m^2}}$$
$$= .\mathbf{2}00\mathbf{3}0000\mathbf{5}000000\mathbf{7}00000000\mathbf{11}\ldots.$$

Read off the primes from α.

$$p_m = [10^{m^2}\alpha] - 10^{2m-1}[10^{(m-1)^2}\alpha].$$

More complicated formulas

Let

$$p_1 = 2 < p_2 = 3 < p_3 = 5 \ldots$$

be the sequence of primes. Define

$$\alpha := \sum_{m \geq 1} \frac{p_m}{10^{m^2}}$$
$$= .\mathbf{2}00\mathbf{3}0000\mathbf{5}0000000\mathbf{7}000000\mathbf{11}\ldots.$$

Read off the primes from α.

$$p_m = [10^{m^2}\alpha] - 10^{2m-1}[10^{(m-1)^2}\alpha].$$

Magical? Interesting? Artificial?

Wilson's theorem

n is a prime if and only if n divides $(n-1)! + 1$.

- Not useful itself but used in...

Matijasevic (1971):

$$
\begin{aligned}
&F(a,b,\ldots,z) := (k+2)\times \\
&\Big(1-(n+l+v-y)^2-(2n+p+q+z-e)^2 \\
&\quad -(wz+h+j-q)^2-(ai+k+1-l-i)^2 \\
&\quad -((gk+2g+k+1)(h+j)+h-z)^2 \\
&\quad -(z+pl(a-p)+t(2ap-p^2-1)-pm)^2 \\
&\quad -(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2 \\
&\quad -(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2 \\
&\quad -((a^2-1)l^2+1-m^2)^2-((a^2-1)y^2+1-x^2)^2 \\
&\quad -(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2 \\
&\quad -(e^3(e+2)(a+1)^2+1-o^2)^2 \\
&\quad -(16r^2y^4(a^2-1)+1-u^2)^2 \\
&\qquad -(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2\Big).
\end{aligned}
$$

26 variables, degree 20, reducible.

If $a, b, \ldots, z \in \mathbb{N}$ then

$F(a, .., z)$ positive $\Rightarrow F(a, .., z)$ prime.

Each prime is a value of F!

Practical?

Conway

THE NUMBER OF PRIMES UP TO x

Gauss, Christmas eve 1849:

As a boy of 15 or 16, I determined that, at around x*, the primes occur with density* $\frac{1}{\ln x}$.

The number of primes up to x

Gauss, Christmas eve 1849:

As a boy of 15 or 16, I determined that, at around x, the primes occur with density $\frac{1}{\ln x}$.

$$\#\{\text{primes} \leq x\} \approx \sum_{n=2}^{[x]} \frac{1}{\ln n}$$

The number of primes up to x

Gauss, Christmas eve 1849:

As a boy of 15 or 16, I determined that, at around x, the primes occur with density $\frac{1}{\ln x}$.

$$\#\{\text{primes} \leq x\} \approx \sum_{n=2}^{[x]} \frac{1}{\ln n}$$

$$\approx \int_2^x \frac{dt}{\ln t} = \mathrm{Li}(x)$$

The number of primes up to x

Gauss, Christmas eve 1849:

As a boy of 15 or 16, I determined that, at around x, the primes occur with density $\frac{1}{\ln x}$.

$$\#\{\text{primes} \le x\} \approx \sum_{n=2}^{[x]} \frac{1}{\ln n}$$

$$\approx \int_2^x \frac{dt}{\ln t} = \mathrm{Li}(x)$$

$$\approx \frac{x}{\ln x}$$

Gauss's guesstimate:

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\ln t}$$

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\mathrm{Li}(x) - \pi(x)]$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Gauss's guesstimate:

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\ln t}$$

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\mathrm{Li}(x) - \pi(x)]$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Guess: $0 < \mathrm{Li}(x) - \pi(x) < \sqrt{\pi(x)}.$

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\mathrm{Li}(x) - \pi(x)]$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Guess: $0 < \displaystyle\int_2^x \frac{dt}{\ln t} - \pi(x) < \sqrt{\pi(x)}.$

Riemann Hypothesis: $\Leftrightarrow$

$$\left| \int_2^x \frac{dt}{\ln t} \; - \; \pi(x) \right| \leq \sqrt{x} \ln x.$$

.

Back to consecutive prime values

Are there polynomials whose first m values are all prime?

Remember:

$$5, 11, 17, 23, 29$$

or even, $199, 409, 619, 829,$

$1039, 1249, 1459, 1669, 1879, 2089$

$= \{199 + 210n,\ 0 \le n \le 9\}$

ARE THERE POLYNOMIALS WHOSE FIRST m VALUES ARE ALL PRIME?

Remember:

$$5, 11, 17, 23, 29$$

or even, $199, 409, 619, 829,$

$$1039, 1249, 1459, 1669, 1879, 2089$$

$= \{199 + 210n,\ 0 \leq n \leq 9\}$

Dirichlet (1837): Any linear polynomial $mn + a$ with $\gcd(a, m) = 1$, takes infinitely many prime values.

Arbitrarily many consecutive prime values?

ARE THERE POLYNOMIALS WHOSE FIRST m VALUES ARE ALL PRIME?

Remember:

$$5, 11, 17, 23, 29$$

or even, $199, 409, 619, 829,$

$$1039, 1249, 1459, 1669, 1879, 2089$$

$$= \{199 + 210n, \ 0 \le n \le 9\}$$

Dirichlet (1837): Any linear polynomial $mn + a$ with $\gcd(a, m) = 1$, takes infinitely many prime values.

Arbitrarily many consecutive prime values?

Van der Corput (1939): Infinitely many linear polynomials whose first 3 values are prime.

Balog (1990): Infinitely many degree d polynomials whose first $2d+1$ values are prime.

Are there linear polynomials whose first k values are all prime?

ARE THERE LINEAR POLYNOMIALS WHOSE FIRST k VALUES ARE ALL PRIME?

Green and Tao (2007): *Yes.* There are infinitely many k-term arithmetic progressions of primes

In fact the smallest has all primes

$$\leq 2^{2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}} .$$

Record: $43142746595714191 + 5283234035979900n$
for $0 \leq n \leq 25$.

Are there linear polynomials whose first k values are all prime?

Green and Tao (2007): *Yes.* There are infinitely many k-term arithmetic progressions of primes

In fact the smallest has all primes

$$\leq 2^{2^{2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}}}.$$

Record: $43142746595714191 + 5283234035979900n$ for $0 \leq n \leq 25$.

Rephrase as: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$f(0), f(1), \ldots, f(k)$ are all prime.

And for higher degree polynomials?

CONSECUTIVE PRIME VALUES OF POLYNOMIALS, I

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$$f(0), f(1), \ldots, f(k) \text{ are all prime.}$$

Another example: x^2+x+41 prime for $x = 0, 1, 2, \ldots, 39$.

How about quadratic polynomials with 41 consecutive prime values?

Consecutive prime values of polynomials, I

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$$f(0), f(1), \ldots, f(k) \text{ are all prime.}$$

Another example: x^2+x+41 prime for $x = 0, 1, 2, \ldots, 39$.

How about quadratic polynomials with 41 consecutive prime values?

Or 1000 consecutive prime values?

Seems like a very deep question...

Or is it?

Consecutive prime values of polynomials, II

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$$f(0), f(1), \ldots, f(k) \text{ are all prime.}$$

Corollary Fix $N \geq 3$. There are infinitely many quadratic polyns $f(x)$ s.t. $f(0), f(1), \ldots, f(N)$ are all prime.

Consecutive prime values of polynomials, II

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$$f(0), f(1), \ldots, f(k) \text{ are all prime.}$$

Corollary Fix $N \geq 3$. There are infinitely many quadratic polyns $f(x)$ s.t. $f(0), f(1), \ldots, f(N)$ are all prime.

Proof: By Green-Tao, select integers a and b for which

$$aj + b \text{ is prime for } 0 \leq j \leq N^2 + N,$$

Consecutive prime values of polynomials, II

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t.

$f(0), f(1), \ldots, f(k)$ are all prime.

Corollary Fix $N \geq 3$. There are infinitely many quadratic polyns $f(x)$ s.t. $f(0), f(1), \ldots, f(N)$ are all prime.

Proof: By Green-Tao, select integers a and b for which

$aj + b$ is prime for $0 \leq j \leq N^2 + N$,

so that

$a(i^2 + i) + b$ is prime for $0 \leq i \leq N$.

Let $f(x) = ax^2 + ax + b$.

Consecutive prime values of polynomials, II

Green-Tao: There are infinitely many linear polyns $f(x) = ax + b$ s.t. $f(0), f(1), \ldots, f(k)$ are all prime.

Corollary Fix $N \geq 3$. There are infinitely many quadratic polyns $f(x)$ s.t. $f(0), f(1), \ldots, f(N)$ are all prime.

Proof: By Green-Tao, select integers a and b for which

$aj + b$ is prime for $0 \leq j \leq N^2 + N$,

so that

$a(i^2 + i) + b$ is prime for $0 \leq i \leq N$.

Let $f(x) = ax^2 + ax + b$.

Extends to arbitrary degree polyns.

2011 result: Can do this for f monic and degree d .

Balog cubes

Van der Corput (1939): Inf many arithmetic progressions of primes of length 3.

Balog (1990): Inf many 3-by-3 squares of distinct primes, each row and each column in arithmetic progression.

BALOG CUBES

Van der Corput (1939): Inf many arithmetic progressions of primes of length 3.

Balog (1990): Inf many 3-by-3 squares of distinct primes, each row and each column in arithmetic progression.

And 3-by-3-by-3 cubes, eg:

47	383	719
179	431	683
311	479	647

149	401	653
173	347	521
197	293	389

251	419	587
167	263	359
83	107	131

Arithmetic progressions of primes along each row, column, and layer.

Even 3-by-3-by-...-by-3 Balog cubes in arbitrary dimension.

Theorem. There are infinitely many N-by-N-by-$\ldots$-by-N Balog cubes.

Proof: Green-Tao gives

$b + jm$ is prime for $0 \leq j \leq N^d - 1$.

Theorem. There are infinitely many N-by-N-by-$\ldots$-by-N Balog cubes.

Proof: Green-Tao gives

$b + jm$ is prime for $0 \leq j \leq N^d - 1$

The $(a_0, a_1, \ldots, a_{d-1})$ entry of our Balog cube, with $0 \leq a_i \leq N - 1$ for each i is

$b + (a_0 + a_1 N + \ldots + a_{d-1} N^{d-1})m.$

Theorem. There are infinitely many N-by-N-by-$\ldots$-by-N Balog cubes.

Proof: Green-Tao gives

$b + jm$ is prime for $0 \le j \le N^d - 1$

The $(a_0, a_1, \ldots, a_{d-1})$ entry of our Balog cube, with $0 \le a_i \le N - 1$ for each i is

$b + (a_0 + a_1 N + \ldots + a_{d-1} N^{d-1})m.$

Now if

$j = a_0 + a_1 N + \ldots + a_{d-1} N^{d-1}$

with each

$$0 \le a_i \le N - 1$$

then

$$0 \le j \le N^d - 1$$

so each entry, $b + jm$, is prime.

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

17	89	71
113	59	5
47	29	101

and

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

These are magic squares of primes.

How about n-by-n?

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

17	89	71
113	59	5
47	29	101

and

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

These are magic squares of primes.

How about n-by-n?

There are n-by-n magic squares of integers, say with (i, j)th entry, $m_{i,j}$.

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

17	89	71
113	59	5
47	29	101

and

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

These are magic squares of primes.

How about n-by-n?

There are n-by-n magic squares of integers, say with (i, j)th entry, $m_{i,j}$.

Then square $a + dm_{i,j}$ is magic

Magic squares of primes

Magic square: Sum of each row, column, and diagonal, is identical:

17	89	71
113	59	5
47	29	101

and

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

These are magic squares of primes.

How about n-by-n?

There are n-by-n magic squares of integers, say with (i, j)th entry, $m_{i,j}$.

Then square $a + dm_{i,j}$ is magic

Green-Tao theorem $\Rightarrow$ Magic Square of Primes.

Many other fun corollaries

-11


204
85
156
189
40
76
24
IN GOD WE TRUST
LIBERTY
132
181
205
208
120
UNITED STATES OF AMERICA
21
IN GOD WE TRUST
LIBERTY
QUARTER DOLLAR
157
237
61
LIBERTY
28
132
237
213
244
160
96
52
117
216
253

Apollonian packings

Three circles touching – create two new circles tangent to them.

DESCARTES: If three curvatures are a, b, c, the two tangent circles' curvatures are solutions to

$$2(x^2+a^2+b^2+c^2) = (x+a+b+c)^2$$

Apollonian packings

Three circles touching – create two new circles tangent to them.

Descartes: If three curvatures are a, b, c, the two tangent circles' curvatures are solutions to

$$2(x^2+a^2+b^2+c^2) = (x+a+b+c)^2$$

Given solution t, other is

$$x = 2(a+b+c) - t$$

Apollonian packings

Three circles touching – create two new circles tangent to them.

Descartes: If three curvatures are a, b, c, the two tangent circles' curvatures are solutions to

$$2(x^2+a^2+b^2+c^2) = (x+a+b+c)^2$$

Given solution t, other is

$$x = 2(a+b+c) - t$$

View this as a map:

$$t \;\rightarrow\; 2(a+b+c) - t$$

Apollonian packings

Three circles touching – create two new circles tangent to them.

Descartes: If three curvatures are a, b, c, the two tangent circles' curvatures are solutions to

$$2(x^2+a^2+b^2+c^2) = (x+a+b+c)^2$$

Given solution t, other is

$$x = 2(a+b+c) - t$$

View this as a map:

$$t \;\rightarrow\; 2(a+b+c) - t$$

Starting with $(21, 24, 28, -11)$ use map, and re-orderings, to find all the numbers in the packing!

Apollonian packings

Starting with $(21, 24, 28, -11)$ use

$$x = 2(a + b + c) - t$$

and re-orderings, to find all the numbers in the packing!

Apollonian packings

Starting with $(21, 24, 28, -11)$ use

$$x = 2(a + b + c) - t$$

and re-orderings, to find all the numbers in the packing!

Sarnak (2010): Infinitely many primes.

Apollonian packings

Starting with $(21, 24, 28, -11)$ use

$$x = 2(a + b + c) - t$$

and re-orderings, to find all the numbers in the packing!

Sarnak (2010): Infinitely many primes.

Sarnak (2010): Infinitely many pairs of "kissing" primes.

Apollonian packings

Starting with $(21, 24, 28, -11)$ use

$$x = 2(a+b+c) - t$$

and re-orderings, to find all the numbers in the packing!

Sarnak (2010): Infinitely many primes.

Sarnak (2010): Infinitely many pairs of "kissing" primes.

Can generalize this to other linear maps of this type, and by allowing several such maps

Bourgain, Kontorovic (2012): If these maps do not "repel points too fast" then there are indeed infinitely many such primes

GAPS BETWEEN PRIMES, I

Difference 1?

GAPS BETWEEN PRIMES, I

Difference 1?

Difference 2?

$\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$.

Gaps between primes, I

Difference 1?

Difference 2?

$\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$.

Infinitely many such prime *twins*?

That is, n for which $p_{n+1} - p_n = 2$?

Open question

. And how short gaps can we prove? Smaller than average?

Gaps between primes, I

Difference 1?

Difference 2?

$\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$.

Infinitely many such prime *twins*?

That is, n for which $p_{n+1} - p_n = 2$?

Open question

Prime number theorem:

About $\frac{x}{\ln x}$ primes up to x.

Therefore average gap is about $\ln x$.

Gaps between primes, I

Difference 1?

Difference 2?

$\{3,5\}$, $\{5,7\}$, $\{11,13\}$, $\{17,19\}$, $\{29,31\}$.

Infinitely many such prime *twins*?

That is, n for which $p_{n+1} - p_n = 2$?

Open question

Prime number theorem:

About $\frac{x}{\ln x}$ primes up to x.

Therefore average gap is about $\ln x$.

Goldston, Pintz, Yildirim (2007)

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = 0.$$

. Pathetic? Expect 2. Can get $\leq \sqrt{\log x}$.

Large Gaps?

Prime number theorem:

About $\frac{x}{\ln x}$ primes up to x.

Therefore average gap is about $\ln x$.

Larger gaps? None of

$$m! + 2, m! + 3, \ldots, m! + m,$$

is prime as they are divisible by $2, 3, \ldots, m$, respectively.

If p_n is the largest prime $\leq m! + 1$ then $p_{n+1} \geq m! + m + 1 \geq p_n + m$.

Large Gaps?

Prime number theorem:

About $\frac{x}{\ln x}$ primes up to x.

Therefore average gap is about $\ln x$.

Larger gaps? None of

$$m! + 2, m! + 3, \ldots, m! + m,$$

is prime as they are divisible by $2, 3, \ldots, m$, respectively.

If p_n is the largest prime $\le m! + 1$ then $p_{n+1} \ge m! + m + 1 \ge p_n + m$.

By a variant on this argument, **Westzynthius** (1931)

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = \infty.$$

What's the largest a gap can be?

Summary

Westzynthius (1931)

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = \infty.$$

Goldston, Pintz, Yildirim (2007)

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = 0.$$

Summary

Westzynthius (1931)

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = \infty.$$

Goldston, Pintz, Yildirim (2007)

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = 0.$$

Largest Gaps?

Riemann Hypothesis:

$$p_{n+1} - p_n \le \sqrt{p_n}(\ln p_n).$$

Summary

Westzynthius (1931)

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = \infty.$$

Goldston, Pintz, Yildirim (2007)

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\ln p_n} = 0.$$

Largest Gaps?

Riemann Hypothesis:

$$p_{n+1} - p_n \le \sqrt{p_n}(\ln p_n).$$

Is there always a prime between two squares?

is an Open question

Prime k-tuplets conjecture, I

Are there inf many prime tuples

$$p, p+2N?$$

Prime k-tuplets conjecture, I

Are there inf many prime tuples

$$p, p + 2N?$$

$$p, 2p + 1?$$

PRIME k-TUPLETS CONJECTURE, I

Are there inf many prime tuples

$$p, p + 2N?$$

$$p, 2p + 1?$$

$$p - 6, p, p + 6?$$

A common generalization?

PRIME k-TUPLETS CONJECTURE, I

Are there inf many prime tuples

$$p, p + 2N?$$

$$p, 2p + 1?$$

$$p - 6, p, p + 6?$$

A common generalization?

$$a_1x + b_1,\ a_2x + b_2,\ \ldots,\ a_kx + b_k$$

Linear polyns, integer coeffs.

ADMISSIBLE: No prime p divides $\prod_{i=1}^{k}(a_in + b_i)$ for every n; a_i's> 0.

PRIME k-TUPLETS CONJECTURE, I

Are there inf many prime tuples

$$p, p+2N?$$

$$p, 2p+1?$$

$$p-6, p, p+6?$$

A common generalization?

$$a_1x+b_1,\ a_2x+b_2,\ \ldots,\ a_kx+b_k$$

Linear polyns, integer coeffs.

ADMISSIBLE: No prime p divides $\prod_{i=1}^{k}(a_in+b_i)$ for every n; a_i's>0.

Prime k-tuplets conjecture

Infinitely many integers n for which $a_1n+b_1,\ a_2n+b_2,\ \ldots,$ and a_kn+b_k are all prime.

PRIME k-TUPLETS CONJECTURE, I

Are there inf many prime tuples

$$p, p + 2N?$$

$$p, 2p + 1?$$

$$p - 6, p, p + 6?$$

A common generalization?

$$a_1x + b_1,\ a_2x + b_2,\ \ldots,\ a_kx + b_k$$

Linear polyns, integer coeffs.

ADMISSIBLE: No prime p divides $\prod_{i=1}^{k}(a_in + b_i)$ for every n; a_i's> 0.

Prime k-tuplets conjecture

Infinitely many integers n for which $a_1n+b_1,\ a_2n+b_2,\ \ldots,$ and a_kn+b_k are all prime.

(Only case proved: $k = 1$)

Green, Tao and Ziegler

No attack on

- $p, p+2$ (*twin prime*);
- $p, N-p$ (*Goldbach*),
- $p, 2p+1$ (*Sophie Germain twins*).

Green, Tao and Ziegler

No attack on

$p, p+2$ (*twin prime*);
$p, N-p$ (*Goldbach*),
$p, 2p+1$ (*Sophie Germain twins*).

These are all *difficult pairs*: Here one requires primes p and q for which

$$ap + bq = c$$

for some fixed non-zero a, b.

Green, Tao and Ziegler

No attack on

$p, p+2$ (*twin prime*);
$p, N-p$ (*Goldbach*),
$p, 2p+1$ (*Sophie Germain twins*).

These are all *difficult pairs*: Here one requires primes p and q for which

$$ap + bq = c$$

for some fixed non-zero a, b.

Green-Tao-Ziegler, 2012:

The prime k-tuplets conjecture holds for any admissible k-tuple of linear forms that does not contain a difficult pair.

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Example 1: $a, a+d, a+2d \ldots, a+kd$

The original Green-Tao Theorem

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Example 1: $a, a+d, a+2d \ldots, a+kd$

The original Green-Tao Theorem

Example 2: $b,\ b+a+1,\ b+2a+4 \ldots, b+ka+k^2$

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Example 2: $b,\ b+a+1,\ b+2a+4$ $\ldots, b+ka+k^2$

These are the values of x^2+ax+b for $x=0,1,\ldots,k$

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Example 2: $b, \ b+a+1, \ b+2a+4$ $\dots, b+ka+k^2$

These are the values of x^2+ax+b for $x=0,1,\dots,k$

Consequence: Existence of infinitely many *monic* polynomials $f(x)$ of degree d, for which $f(0), f(1), \dots, f(m)$ are all prime.

Green-Tao-Ziegler Theorem

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Consequence: Existence of infinitely many *monic* polynomials $f(x)$ of degree d, for which $f(0), f(1), \ldots, f(m)$ are all prime.

Example 3: $p, q, 2p + 3q, 2p - 3q$

Pythagorean triples

A Pythagorean triangle has sides

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

with area

$$A := rs(r+s)(r-s).$$

Pythagorean triples

A Pythagorean triangle has sides

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

with area

$$A := rs(r+s)(r-s).$$

How few prime factors can $A/6$ have?

.

Note that 6 always divides A

Pythagorean triples

A Pythagorean triangle has sides

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

with area

$$A := rs(r+s)(r-s).$$

How few prime factors can $A/6$ have?

Three, if $s = 6$ and $r-6, r, r+6$ are all prime.

. Difficult pairs. No chance of proving this.

Pythagorean triples

A Pythagorean triangle has sides

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

with area

$$A := rs(r+s)(r-s).$$

How few prime factors can $A/6$ have?

Three, if $s = 6$ and $r-6, r, r+6$ are all prime.

Ben Tsou (2007, junior thesis) $A/6$ has four prime factors infinitely often: Take $r = 2p, \ s = 3q$ when

$$p, q, 2p+3q, \text{ and } 2p-3q$$

are all prime.

PYTHAGOREAN TRIPLES

A Pythagorean triangle has sides

$$r^2 - s^2, \quad 2rs, \quad r^2 + s^2$$

with area

$$A := rs(r+s)(r-s).$$

How few prime factors can $A/6$ have?

Three, if $s = 6$ and $r-6, r, r+6$ are all prime.

Ben Tsou (2007, junior thesis) $A/6$ has four prime factors infinitely often: Take $r = 2p, \; s = 3q$ when

$$p, q, 2p+3q, \text{ and } 2p-3q$$

are all prime.

This follows from the GREEN-TAO-ZIEGLER Theorem

GREEN-TAO-ZIEGLER THEOREM

The prime k-tuplets conjecture for any admissible k-tuple of linear forms that does not contain a difficult pair.

Further consequences:

You find them!