

PATTERNS IN THE PRIMES

Andrew Granville

(with animations by *Anthony Doran*)

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 x_j has prime divisor $p_j \forall j$ then

$$p_1, p_2, p_3 \dots$$

is an infinite seq of distinct primes.

THERE ARE INFINITELY MANY PRIMES

Want an infinite sequence of integers

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

such that

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

If x_j has prime divisor $p_j \forall j$ then

$$p_1, p_2, p_3 \dots$$

is an infinite seq of distinct primes.

PROOF: If $p_i = p_j$ for $i \neq j$, then p_i divides x_i and $p_i = p_j$ divides x_j , so that

$$p_i \text{ divides } \gcd(x_i, x_j) = 1,$$

Contradiction.

THERE ARE INFINITELY MANY PRIMES

So how do we find integers

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

such that

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

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

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

.

We begin by studying remainders under this map

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

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

Remainder 0 \mapsto Remainder 1

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

Remainder 1 \mapsto Remainder 1

.

And how do we use this?

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

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

Remainder 0 \mapsto Remainder 1

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

Remainder 1 \mapsto Remainder 1

————— Construction —————

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

$$x_2 = x_1^2 - x_1 + 1,$$

$$x_3 = x_2^2 - x_2 + 1,$$

...

.

And the remainders when we divide by x_i ?

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

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

Remainder 0 \mapsto Remainder 1

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

Remainder 1 \mapsto Remainder 1

————— Construction —————

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

$$x_2 = x_1^2 - x_1 + 1,$$

$$x_3 = x_2^2 - x_2 + 1,$$

...

Remainders, x_j divided by $x_i (= m)$:

x_i has remainder 0, so that

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

$$\mapsto x_{i+2} \text{ has remainder } 1$$

$$\mapsto x_{i+3} \text{ has remainder } 1 \dots$$

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...

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

$$p_1, p_2, p_3 \dots$$

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

$$p_1, p_2, p_3 \dots$$

is an infinite seq of distinct primes.

.

Examples?

————— *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

$$p_1, p_2, p_3 \dots$$

is an infinite seq of distinct primes.

————— *Examples* —————

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

$$2 \mapsto 3 \mapsto 7 \mapsto 43 \mapsto \dots,$$

(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

$$p_1, p_2, p_3 \dots$$

is an infinite seq of distinct primes.

————— *Examples* —————

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

$$2 \mapsto 3 \mapsto 7 \mapsto 43 \mapsto \dots,$$

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

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

$$3 \mapsto 5 \mapsto 17 \mapsto 257 \mapsto \dots,$$

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

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

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

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

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 **35** = 5×7

so

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

FORMULAS FOR PRIMES?

Polynomial with lots of prime values:

5, 11, 17, 23, 29, but then **35** = 5×7

so

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

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

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, ...

which remains prime until

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

.

.

Can polynomials only take prime values?

POLYNOMIALS WITH ONLY PRIME VALUES?

$$n^2 + n + 41$$

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

$$41^2 + 41 + 41$$

is divisible by 41.

POLYNOMIALS WITH ONLY PRIME VALUES?

$$n^2 + n + 41$$

is prime for $n = 0, 1, \dots, 39$, 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 $n = 0, 1, \dots, 39$, 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 $n = 0, 1, \dots, 39$, 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 ,
since $x^2 - 1$ 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 ,
since $x^2 - 1$ is reducible.

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

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

is never prime, since it is 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 admis-
sible 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 admis-
sible 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 admis-
sible 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 admis-
sible 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

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

be the sequence of primes. Define

$$\begin{aligned} \alpha &:= \sum_{m \geq 1} \frac{p_m}{10^{m^2}} \\ &= .\mathbf{2003000050000007000000011} \dots \end{aligned}$$

Read off the primes from α .

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

MORE COMPLICATED FORMULAS

Let

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

be the sequence of primes. Define

$$\begin{aligned}\alpha &:= \sum_{m \geq 1} \frac{p_m}{10^{m^2}} \\ &= .\mathbf{2003000050000007000000011} \dots\end{aligned}$$

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):

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

26 variables, degree 20, reducible.

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

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

Each prime is a value of F !

Practical?

RECOGNIZING PRIMES QUICKLY

Fermat's Little Theorem (1640)

If p is a prime then

p divides $a^p - a$ for all integers a .

RECOGNIZING PRIMES QUICKLY

Fermat's Little Theorem (1640)

If p is a prime then

p divides $a^p - a$ for all integers a .

Reversing that for $a = 2$ gives

$n \nmid 2^n - 2 \Rightarrow n$ composite

Does this identify every composite n ?

If so then this is a primality test

RECOGNIZING PRIMES QUICKLY

Fermat's Little Theorem (1640)

If p is a prime then

p divides $a^p - a$ for all integers a .

Reversing that for $a = 2$ gives

$n \nmid 2^n - 2 \Rightarrow n$ composite

Does this identify every composite n ?

No, since 341 divides $2^{341} - 2$

and $341 = 31 \times 11$.

RECOGNIZING PRIMES QUICKLY

Fermat's Little Theorem (1640)

If p is a prime then

p divides $a^p - a$ for all integers a .

Reversing that for $a = 2$ gives

$n \nmid 2^n - 2 \Rightarrow n$ composite

Does this identify every composite n ?

No, since 341 divides $2^{341} - 2$

and $341 = 31 \times 11$.

But 341 does not divide $3^{341} - 3$,

so 341 cannot be prime

.

How about using the test for $a = 2, 3, 5, 7, \dots$?

RECOGNIZING PRIMES QUICKLY

Fermat's Little Theorem (1640)

If p is a prime then

p divides $a^p - a$ for all integers a .

Reversing that for $a = 2$ gives

$n \nmid 2^n - 2 \Rightarrow n$ composite

Does this identify every composite n ?

No, since 341 divides $2^{341} - 2$

and $341 = 31 \times 11$.

But 341 does not divide $3^{341} - 3$,

so 341 cannot be prime

There are infinitely many integers n
which divide $a^n - a$ for all integers a ,
starting with $n = 561, 1105, 1729$.

RECOGNIZING PRIMES QUICKLY, II

Polynomial time : d^C for d digit integers

The best tests, until recently:

$d^{c \ln \ln d}$ steps.

In the real world $\ln \ln d < 7$.

.

But we want an actual theorem!

RECOGNIZING PRIMES QUICKLY, II

Polynomial time : d^C for d digit integers

The best tests, until recently:

$$d^{c \ln \ln d} \text{ steps.}$$

In the real world $\ln \ln d < 7$.

Agrawal, Kayal and Saxena (2002):

$$d^{7\frac{1}{2}} \text{ steps.}$$

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 $\frac{1}{\ln x}$.*

$$\begin{aligned}\#\{\text{primes} \leq x\} &\approx \sum_{n=2}^{[x]} \frac{1}{\ln n} \\ &\approx \int_2^x \frac{dt}{\ln t} = \text{Li}(x)\end{aligned}$$

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 $\frac{1}{\ln x}$.*

$$\begin{aligned}\#\{\text{primes} \leq x\} &\approx \sum_{n=2}^{[x]} \frac{1}{\ln n} \\ &\approx \int_2^x \frac{dt}{\ln t} = \text{Li}(x) \\ &\approx \frac{x}{\ln x}\end{aligned}$$

Gauss's guesstimate:

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

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\text{Li}(x) - \pi(x)]$
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:

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

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\text{Li}(x) - \pi(x)]$
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: $0 < \text{Li}(x) - \pi(x) < \sqrt{\pi(x)}$.

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\text{Li}(x) - \pi(x)]$
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: $0 < \int_2^x \frac{dt}{\ln t} - \pi(x) < \sqrt{\pi(x)}$.

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

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

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

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

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

Arbitrarily many consecutive prime values?

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

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

Record: $468395662504823 + 45872132836530n$
for $0 \leq n \leq 23$.

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

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

Record: $468395662504823 + 45872132836530n$
for $0 \leq n \leq 23$.

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

$f(0), f(1), \dots, f(k)$ 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.

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

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

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.

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

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

How about quadratic polynomials with 41 consecutive prime values?

Or 1000 consecutive prime values?

Seems like a very deep question...

CONSECUTIVE PRIME VALUES OF POLYNOMIALS, II

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

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

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

CONSECUTIVE PRIME VALUES OF POLYNOMIALS, II

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

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

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

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

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

CONSECUTIVE PRIME VALUES OF POLYNOMIALS, II

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

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

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

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

Corollary Fix $N \geq 3$. There are infinitely many quadratic polyns $f(x)$ s.t. $f(0), f(1), \dots, f(N)$ 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-...-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- \dots -by- N Balog cubes.

Proof: Green-Tao gives

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

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

$b + (a_0 + a_1N + \dots + a_{d-1}N^{d-1})m.$

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

Proof: Green-Tao gives

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

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

$b + (a_0 + a_1N + \dots + a_{d-1}N^{d-1})m.$

Now if

$j = a_0 + a_1N + \dots + a_{d-1}N^{d-1}$

with each

$$0 \leq a_i \leq N - 1$$

then

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

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.

SETS WITH ALL AVERAGES PRIME

Averages of subsets of $\{7, 19, 67\}$ are

$$\begin{aligned}\frac{7}{1} &= 7, & \frac{19}{1} &= 19, & \frac{67}{1} &= 67, \\ \frac{7+19}{2} &= 13, & \frac{7+67}{2} &= 37, & \frac{19+67}{2} &= 43, \\ & & \frac{7+19+67}{3} &= 31,\end{aligned}$$

which are all prime. Other exs?

$$\{5, 17, 89, 1277\};$$

$$\{209173, 322573, 536773, 1217893, 2484733\}.$$

SETS WITH ALL AVERAGES PRIME

Averages of subsets of $\{7, 19, 67\}$ are

$$\begin{aligned}\frac{7}{1} &= 7, & \frac{19}{1} &= 19, & \frac{67}{1} &= 67, \\ \frac{7+19}{2} &= 13, & \frac{7+67}{2} &= 37, & \frac{19+67}{2} &= 43, \\ & & \frac{7+19+67}{3} &= 31,\end{aligned}$$

which are all prime. Other exs?

$$\{5, 17, 89, 1277\};$$

$$\{209173, 322573, 536773, 1217893, 2484733\}.$$

YOUR CHALLENGE: Show there are such sets of primes of any size k .

SETS WITH ALL AVERAGES PRIME

Averages of subsets of $\{7, 19, 67\}$ are

$$\begin{aligned}\frac{7}{1} &= 7, & \frac{19}{1} &= 19, & \frac{67}{1} &= 67, \\ \frac{7+19}{2} &= 13, & \frac{7+67}{2} &= 37, & \frac{19+67}{2} &= 43, \\ & & \frac{7+19+67}{3} &= 31,\end{aligned}$$

which are all prime. Other exs?

$$\{5, 17, 89, 1277\};$$

$$\{209173, 322573, 536773, 1217893, 2484733\}.$$

YOUR CHALLENGE: Show there are such sets of primes of any size k .

ANOTHER CHALLENGE: Prove existence of other interesting sets of primes, using the Green-Tao theorem.

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)

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

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

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

is prime as they are divisible by $2, 3, \dots, m$, 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

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

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

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

By a variant on this argument,

Westzynthius (1931)

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

What's the largest a gap can be?

Summary

Westzynthius (1931)

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

Goldston, Pintz, Yıldırım (2007)

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

Summary

Westzynthius (1931)

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

Goldston, Pintz, Yildirim (2007)

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

LARGEST GAPS?

Riemann Hypothesis:

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

Summary

Westzynthius (1931)

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

Goldston, Pintz, Yildirim (2007)

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

LARGEST GAPS?

Riemann Hypothesis:

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

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?

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

Linear polyns, integer coeffs.

ADMISSIBLE: No prime p divides $\prod_{i=1}^k (a_i n + b_i)$ 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?

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

Linear polyns, integer coeffs.

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

Prime k -tuplets conjecture

Infinitely many integers n for which $a_1n + b_1, a_2n + b_2, \dots$, 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?

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

Linear polyns, integer coeffs.

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

Prime k -tuplets conjecture

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

(Only case proved: $k = 1$)

PRIME k -TUPLETS CONJECTURE, II

Further generalization:

$$f_1, f_2, \dots, f_k$$

irreducible polyns with integer coefficients in several variables, admissible, simultaneously positive valued.

Conjecture: There are infinitely many distinct sets of integer values for the variables so that all the polynomials are prime valued.

PRIME k -TUPLETS CONJECTURE, II

Further generalization:

$$f_1, f_2, \dots, f_k$$

irreducible polyns with integer coefficients in several variables, admissible, simultaneously positive valued.

Conjecture: There are infinitely many distinct sets of integer values for the variables so that all the polynomials are prime valued.

True for any admissible, irreducible

- Quadratic polyn in two variables.
- $x^2 + y^4$ (Friedlander and Iwaniec)
- Cubic polynomial in two variables.
(Heath-Brown)

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: $a, a+d, a+2d, \dots, a+kd$
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: $a, a+d, a+2d, \dots, a+kd$
The original Green-Tao Theorem

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

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

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

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 $f(0), f(1), \dots, f(m)$ are all prime.

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

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 $f(0), f(1), \dots, f(m)$ are all prime.

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

Further consequences:

You find them!

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