Prime numbers

What we know, and what we know we think

Greg Martin
University of British Columbia

College of Staten Island Mathematics Colloquium
April 30, 2010

slides can be found on my web page
`www.math.ubc.ca/~gerg/index.shtml?slides`

Outline

Outline

1. Introduction: A subject sublime
2. Single prime numbers, one at a time
3. Multiple prime numbers—partners in crime
4. Random prime questions

Outline

1. Introduction: A subject sublime
2. Single prime numbers, one at a time
3. Multiple prime numbers—partners in crime
4. Random prime questions

Outline

1. Introduction: A subject sublime
2. Single prime numbers, one at a time
3. Multiple prime numbers—partners in crime
4. Random prime questions

Outline

1. Introduction: A subject sublime
2. Single prime numbers, one at a time
3. Multiple prime numbers—partners in crime
4. Random prime questions *(this one doesn't rhyme)*

A tale of two subjects

Questions about the distribution of prime numbers, and about the existence of prime numbers of special forms, have been stymieing mathematicians for over two thousand years. It's almost necessary to study two different subjects:

- the theorems about prime numbers that we have been able to prove
- the (vastly more numerous) conjectures about prime numbers that we haven't yet succeeded at proving

Let's look at the most central questions concerning the distribution of primes, seeing which ones have been answered already and what mathematical techniques have been used to attack them.

A tale of two subjects

Questions about the distribution of prime numbers, and about the existence of prime numbers of special forms, have been stymieing mathematicians for over two thousand years. It's almost necessary to study two different subjects:

- the theorems about prime numbers that we have been able to prove
- the (vastly more numerous) conjectures about prime numbers that we haven't yet succeeded at proving

Let's look at the most central questions concerning the distribution of primes, seeing which ones have been answered already and what mathematical techniques have been used to attack them.

A tale of two subjects

Questions about the distribution of prime numbers, and about the existence of prime numbers of special forms, have been stymieing mathematicians for over two thousand years. It's almost necessary to study two different subjects:

- the theorems about prime numbers that we have been able to prove
- the (vastly more numerous) conjectures about prime numbers that we haven't yet succeeded at proving

Let's look at the most central questions concerning the distribution of primes, seeing which ones have been answered already and what mathematical techniques have been used to attack them.

A tale of two subjects

Questions about the distribution of prime numbers, and about the existence of prime numbers of special forms, have been stymieing mathematicians for over two thousand years. It's almost necessary to study two different subjects:

- the theorems about prime numbers that we have been able to prove
- the (vastly more numerous) conjectures about prime numbers that we haven't yet succeeded at proving

Let's look at the most central questions concerning the distribution of primes, seeing which ones have been answered already and what mathematical techniques have been used to attack them.

Lots of primes

Theorem (Euclid)

There are infinitely many primes.

Proof.

If not, multiply them all together and add one:

$$N = p_1 p_2 \cdots p_k + 1$$

This number N must have some prime factor, but is not divisible by any of the p_j, a contradiction. □

Lots of primes

Theorem (Euclid)

There are infinitely many primes.

Proof.

If not, multiply them all together and add one:

$$N = p_1 p_2 \cdots p_k + 1$$

This number N must have some prime factor, but is not divisible by any of the p_j, a contradiction. □

Lots of primes

Theorem (Euclid)

There are infinitely many primes.

Proof.

If not, multiply them all together and add one:

$$N = p_1 p_2 \cdots p_k + 1$$

This number N must have some prime factor, but is not divisible by any of the p_j, a contradiction. □

This slide contains a joke. . .

Theorem

There are infinitely many composites.

Proof.

If not, multiply them all together and don't add one. □

This slide contains a joke. . .

Theorem

There are infinitely many composites.

Proof.

If not, multiply them all together and don't add one. □

How many primes?

Question

Approximately how many primes are there less than some given number x?

- Legendre and Gauss conjectured the answer.
- Riemann wrote a groundbreaking memoir describing how one could prove it using functions of a complex variable.

Prime Number Theorem (Hadamard and de la Vallée-Poussin independently, 1898)

The number of primes less than x is asymptotically $x/\ln x$.

How many primes?

Question

Approximately how many primes are there less than some given number x?

- Legendre and Gauss conjectured the answer.
- Riemann wrote a groundbreaking memoir describing how one could prove it using functions of a complex variable.

Prime Number Theorem (Hadamard and de la Vallée-Poussin independently, 1898)

The number of primes less than x is asymptotically $x/\ln x$.

How many primes?

Question

Approximately how many primes are there less than some given number x?

- Legendre and Gauss conjectured the answer.
- Riemann wrote a groundbreaking memoir describing how one could prove it using functions of a complex variable.

Prime Number Theorem (Hadamard and de la Vallée-Poussin independently, 1898)

The number of primes less than x is asymptotically $x/\ln x$.

How many primes?

Question

Approximately how many primes are there less than some given number x?

- Legendre and Gauss conjectured the answer.
- Riemann wrote a groundbreaking memoir describing how one could prove it using functions of a complex variable.

Prime Number Theorem (Hadamard and de la Vallée-Poussin independently, 1898)

The number of primes less than x is asymptotically $x/\ln x$.

Proof of the Prime Number Theorem

Riemann's plan for proving the Prime Number Theorem was to study the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

This sum converges for every complex number s with real part bigger than 1, but there is a way to nicely define $\zeta(s)$ for all complex numbers $s \neq 1$.

The proof of the Prime Number Theorem boils down to figuring out where the zeros of $\zeta(s)$ are. Hadamard and de la Vallée-Poussin proved that there are no zeros with real part equal to 1, which is enough to prove the Prime Number Theorem.

Proof of the Prime Number Theorem

Riemann's plan for proving the Prime Number Theorem was to study the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

This sum converges for every complex number s with real part bigger than 1, but there is a way to nicely define $\zeta(s)$ for all complex numbers $s \neq 1$.

The proof of the Prime Number Theorem boils down to figuring out where the zeros of $\zeta(s)$ are. Hadamard and de la Vallée-Poussin proved that there are no zeros with real part equal to 1, which is enough to prove the Prime Number Theorem.

Proof of the Prime Number Theorem

Riemann's plan for proving the Prime Number Theorem was to study the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

This sum converges for every complex number s with real part bigger than 1, but there is a way to nicely define $\zeta(s)$ for all complex numbers $s \neq 1$.

The proof of the Prime Number Theorem boils down to figuring out where the zeros of $\zeta(s)$ are. Hadamard and de la Vallée-Poussin proved that there are no zeros with real part equal to 1, which is enough to prove the Prime Number Theorem.

Proof of the Prime Number Theorem

Riemann's plan for proving the Prime Number Theorem was to study the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

This sum converges for every complex number s with real part bigger than 1, but there is a way to nicely define $\zeta(s)$ for all complex numbers $s \neq 1$.

The proof of the Prime Number Theorem boils down to figuring out where the zeros of $\zeta(s)$ are. Hadamard and de la Vallée-Poussin proved that there are no zeros with real part equal to 1, which is enough to prove the Prime Number Theorem.

Proof of the Prime Number Theorem

Riemann's plan for proving the Prime Number Theorem was to study the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

This sum converges for every complex number s with real part bigger than 1, but there is a way to nicely define $\zeta(s)$ for all complex numbers $s \neq 1$.

More is suspected, however. Other than some "trivial zeros" $s = -2, -4, -6, \dots,$ Riemann conjectured:

Riemann Hypothesis

All nontrivial zeros of $\zeta(s)$ have real part equal to $1/2$.

Primes of the form $4n+3$

Let's begin to look at primes of special forms.

Theorem

There are infinitely many primes $p \equiv -1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4p_1p_2\cdots p_k - 1.$$

The product of numbers that are all $1 \pmod 4$ is still $1 \pmod 4$, but $N \equiv -1 \pmod 4$. Therefore N must have some prime factor that's congruent to $-1 \pmod 4$, a contradiction. $\square$

Primes of the form $4n + 3$

Let's begin to look at primes of special forms.

Theorem

There are infinitely many primes $p \equiv -1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4p_1p_2 \cdots p_k - 1.$$

The product of numbers that are all $1 \pmod 4$ is still $1 \pmod 4$, but $N \equiv -1 \pmod 4$. Therefore N must have some prime factor that's congruent to $-1 \pmod 4$, a contradiction. □

Primes of the form $4n+3$

Let's begin to look at primes of special forms.

Theorem

There are infinitely many primes $p \equiv -1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4p_1p_2\cdots p_k - 1.$$

The product of numbers that are all $1 \pmod 4$ is still $1 \pmod 4$, but $N \equiv -1 \pmod 4$. Therefore N must have some prime factor that's congruent to $-1 \pmod 4$, a contradiction. $\square$

Primes of the form $4n + 3$

Let's begin to look at primes of special forms.

Theorem

There are infinitely many primes $p \equiv -1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4p_1p_2 \cdots p_k - 1.$$

The product of numbers that are all $1 \pmod 4$ is still $1 \pmod 4$, but $N \equiv -1 \pmod 4$. Therefore N must have some prime factor that's congruent to $-1 \pmod 4$, a contradiction. $\square$

Primes of the form $4n+1$

Theorem

There are infinitely many primes $p \equiv 1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \dots, p_k$ be all such primes, and define

$$N = 4(p_1 p_2 \cdots p_k)^2 + 1,$$

so that none of the primes congruent to $1 \pmod 4$ divides N. If q is a prime factor of N, then $4(p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod q$. But it can be shown that $4x^2 \equiv -1 \pmod q$ has a solution x if and only $q \equiv 1 \pmod 4$. Therefore N has all prime factors congruent to $1 \pmod 4$, a contradiction. □

Primes of the form $4n+1$

Theorem

There are infinitely many primes $p \equiv 1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4(p_1 p_2 \cdots p_k)^2 + 1,$$

so that none of the primes congruent to $1 \pmod 4$ divides N. If q is a prime factor of N, then $4(p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod q$. But it can be shown that $4x^2 \equiv -1 \pmod q$ has a solution x if and only $q \equiv 1 \pmod 4$. Therefore N has all prime factors congruent to $1 \pmod 4$, a contradiction. □

Primes of the form $4n+1$

Theorem

There are infinitely many primes $p \equiv 1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \dots, p_k$ be all such primes, and define

$$N = 4(p_1 p_2 \cdots p_k)^2 + 1,$$

so that none of the primes congruent to $1 \pmod 4$ divides N. If q is a prime factor of N, then $4(p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod q$. But it can be shown that $4x^2 \equiv -1 \pmod q$ has a solution x if and only $q \equiv 1 \pmod 4$. Therefore N has all prime factors congruent to $1 \pmod 4$, a contradiction. □

Primes of the form $4n + 1$

Theorem

There are infinitely many primes $p \equiv 1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4(p_1 p_2 \cdots p_k)^2 + 1,$$

so that none of the primes congruent to $1 \pmod 4$ divides N. If q is a prime factor of N, then $4(p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod q$. But it can be shown that $4x^2 \equiv -1 \pmod q$ has a solution x if and only $q \equiv 1 \pmod 4$. Therefore N has all prime factors congruent to $1 \pmod 4$, a contradiction. □

Primes of the form $4n+1$

Theorem

There are infinitely many primes $p \equiv 1 \pmod 4$.

Proof.

If not, let $p_1, p_2, \ldots, p_k$ be all such primes, and define

$$N = 4(p_1 p_2 \cdots p_k)^2 + 1,$$

so that none of the primes congruent to $1 \pmod 4$ divides N. If q is a prime factor of N, then $4(p_1 p_2 \cdots p_k)^2 \equiv -1 \pmod q$. But it can be shown that $4x^2 \equiv -1 \pmod q$ has a solution x if and only $q \equiv 1 \pmod 4$. Therefore N has all prime factors congruent to $1 \pmod 4$, a contradiction. $\square$

Similar proofs

Elementary arguments like this can address many, but not all, arithmetic progressions.

Theorem (Schur 1912; R. Murty 1988)

The existence of infinitely many primes $p \equiv a \pmod{m}$ can be proved in this way if and only if $a^2 \equiv 1 \pmod{m}$.

- For example, such proofs exist for each of $1 \pmod{8}$, $3 \pmod{8}$, $5 \pmod{8}$, and $7 \pmod{8}$. (Note that it doesn't make sense to look for infinitely many primes $p \equiv a \pmod{m}$ unless $\gcd(a,m) = 1$.)
- No such proof exists for $2 \pmod{5}$ or $3 \pmod{5}$.

Similar proofs

Elementary arguments like this can address many, but not all, arithmetic progressions.

Theorem (Schur 1912; R. Murty 1988)

The existence of infinitely many primes $p \equiv a \pmod{m}$ can be proved in this way if and only if $a^2 \equiv 1 \pmod{m}$.

- For example, such proofs exist for each of $1 \pmod{8}$, $3 \pmod{8}$, $5 \pmod{8}$, and $7 \pmod{8}$. (Note that it doesn't make sense to look for infinitely many primes $p \equiv a \pmod{m}$ unless $\gcd(a, m) = 1$.)
- No such proof exists for $2 \pmod{5}$ or $3 \pmod{5}$.

Similar proofs

Elementary arguments like this can address many, but not all, arithmetic progressions.

Theorem (Schur 1912; R. Murty 1988)

The existence of infinitely many primes $p \equiv a \pmod{m}$ can be proved in this way if and only if $a^2 \equiv 1 \pmod{m}$.

- For example, such proofs exist for each of $1 \pmod{8}$, $3 \pmod{8}$, $5 \pmod{8}$, and $7 \pmod{8}$. (Note that it doesn't make sense to look for infinitely many primes $p \equiv a \pmod{m}$ unless $\gcd(a, m) = 1$.)
- No such proof exists for $2 \pmod{5}$ or $3 \pmod{5}$.

Dirichlet's theorem

Theorem (Dirichlet, 1837)

If $\gcd(a,m)=1$*, then there are infinitely many primes* $p \equiv a \pmod{m}$*.*

In fact, the proof of the Prime Number Theorem provided more information: if $\phi(m)$ denotes the number of integers $1 \le a \le m$ such that $\gcd(a,m)=1$, then the primes are equally distributed among the $\phi(m)$ possible arithmetic progressions:

Theorem

If $\gcd(a,m)=1$*, then the number of primes* $p \equiv a \pmod{m}$ *that are less than* x *is asymptotically* $x/(\phi(m)\ln x)$*.*

Dirichlet's theorem

Theorem (Dirichlet, 1837)

If $\gcd(a, m) = 1$*, then there are infinitely many primes* $p \equiv a \pmod{m}$.

In fact, the proof of the Prime Number Theorem provided more information: if $\phi(m)$ denotes the number of integers $1 \le a \le m$ such that $\gcd(a, m) = 1$, then the primes are equally distributed among the $\phi(m)$ possible arithmetic progressions:

Theorem

If $\gcd(a, m) = 1$*, then the number of primes* $p \equiv a \pmod{m}$ *that are less than* x *is asymptotically* $x/(\phi(m) \ln x)$.

Dirichlet's theorem

Theorem (Dirichlet, 1837)

If $\gcd(a,m)=1$, then there are infinitely many primes $p \equiv a \pmod{m}$.

In fact, the proof of the Prime Number Theorem provided more information: if $\phi(m)$ denotes the number of integers $1 \le a \le m$ such that $\gcd(a,m)=1$, then the primes are equally distributed among the $\phi(m)$ possible arithmetic progressions:

Theorem

If $\gcd(a,m)=1$, then the number of primes $p \equiv a \pmod{m}$ that are less than x is asymptotically $x/(\phi(m)\ln x)$.

Proof of Dirichlet's theorem

To be able to pick out individual arithmetic progressions, Dirichlet introduced the dual group of group characters, namely homomorphisms $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$. Each group character gives rise to a Dirichlet L-function

$$L(s,\chi) = \sum_{\substack{n=1 \\ \gcd(n,m)=1}}^{\infty} \chi(n)n^{-s}.$$

By showing that $\lim_{s\to1} L(s,\chi)$ exists and is nonzero for every (nontrivial) character χ, Dirichlet could prove that there are infinitely many primes $p \equiv a \pmod{m}$ when $\gcd(a,m)=1$. Later, when the analytic techniques for proving the Prime Number Theorem were established, Dirichlet's algebraic innovations could be incorporated to prove the asymptotic formula for primes in arithmetic progressions.

Proof of Dirichlet's theorem

To be able to pick out individual arithmetic progressions, Dirichlet introduced the dual group of group characters, namely homomorphisms $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$. Each group character gives rise to a Dirichlet L-function

$$L(s,\chi) = \sum_{\substack{n=1 \\ \gcd(n,m)=1}}^{\infty} \chi(n)n^{-s}.$$

By showing that $\lim_{s\to1} L(s,\chi)$ exists and is nonzero for every (nontrivial) character χ, Dirichlet could prove that there are infinitely many primes $p \equiv a \pmod m$ when $\gcd(a,m) = 1$. Later, when the analytic techniques for proving the Prime Number Theorem were established, Dirichlet's algebraic innovations could be incorporated to prove the asymptotic formula for primes in arithmetic progressions.

Proof of Dirichlet's theorem

To be able to pick out individual arithmetic progressions, Dirichlet introduced the dual group of group characters, namely homomorphisms $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$. Each group character gives rise to a Dirichlet L-function

$$L(s,\chi) = \sum_{\substack{n=1 \\ \gcd(n,m)=1}}^{\infty} \chi(n)n^{-s}.$$

By showing that $\lim_{s\to1} L(s,\chi)$ exists and is nonzero for every (nontrivial) character χ, Dirichlet could prove that there are infinitely many primes $p \equiv a \pmod m$ when $\gcd(a,m) = 1$. Later, when the analytic techniques for proving the Prime Number Theorem were established, Dirichlet's algebraic innovations could be incorporated to prove the asymptotic formula for primes in arithmetic progressions.

Proof of Dirichlet's theorem

To be able to pick out individual arithmetic progressions, Dirichlet introduced the dual group of group characters, namely homomorphisms $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$. Each group character gives rise to a Dirichlet L-function

$$L(s,\chi) = \sum_{\substack{n=1 \\ \gcd(n,m)=1}}^{\infty} \chi(n)n^{-s}.$$

By showing that $\lim_{s\to1} L(s,\chi)$ exists and is nonzero for every (nontrivial) character χ, Dirichlet could prove that there are infinitely many primes $p \equiv a \pmod{m}$ when $\gcd(a,m) = 1$. Later, when the analytic techniques for proving the Prime Number Theorem were established, Dirichlet's algebraic innovations could be incorporated to prove the asymptotic formula for primes in arithmetic progressions.

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does "reasonable" mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn't be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining "reasonable"...

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does “reasonable” mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn’t be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining “reasonable”…

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does “reasonable” mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn't be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining “reasonable”...

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does "reasonable" mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn't be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining "reasonable"...

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does “reasonable” mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn’t be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining “reasonable”. . .

Prime values of polynomials

Conjecture

If $f(n)$ is a reasonable polynomial with integer coefficients, then $f(n)$ should be prime infinitely often.

What does "reasonable" mean?

- $f(n)$ should be irreducible over the integers (unlike, for example, n^3 or $n^2 - 1$).
- $f(n)$ shouldn't be always divisible by some fixed integer (unlike, for example, $15n + 35$ or $n^2 + n + 2$).

So for example, $n^2 + 1$ is a reasonable polynomial.

To measure the second property defining "reasonable"...

Prime values of polynomials

Definition

$\sigma_f(p)$ is the number of integers $1 \le k \le p$ such that $f(k) \equiv 0 \pmod{p}$.

Conjecture

If $f(n)$ is an irreducible polynomial with integer coefficients such that $\sigma_f(p) < p$ for all primes p, then $f(n)$ should be prime infinitely often. In fact, the number of integers $1 \le n \le x$ such that $f(n)$ is prime should be asymptotically

$$\frac{x}{\ln x} \frac{1}{\deg f} \prod_p \left(1 - \frac{\sigma_f(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-1}.$$

Prime values of polynomials

Definition

$\sigma_f(p)$ is the number of integers $1 \le k \le p$ such that $f(k) \equiv 0 \pmod{p}$.

Conjecture

If $f(n)$ is an irreducible polynomial with integer coefficients such that $\sigma_f(p) < p$ for all primes p, then $f(n)$ should be prime infinitely often. In fact, the number of integers $1 \le n \le x$ such that $f(n)$ is prime should be asymptotically

$$\frac{x}{\ln x} \frac{1}{\deg f} \prod_p \left(1 - \frac{\sigma_f(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-1}.$$

Prime values of polynomials

Definition

$\sigma_f(p)$ is the number of integers $1 \le k \le p$ such that $f(k) \equiv 0 \pmod{p}$.

Conjecture

If $f(n)$ is an irreducible polynomial with integer coefficients such that $\sigma_f(p) < p$ for all primes p, then $f(n)$ should be prime infinitely often. In fact, the number of integers $1 \le n \le x$ such that $f(n)$ is prime should be asymptotically

$$\frac{x}{\ln x} \frac{1}{\deg f} \prod_p \left(1 - \frac{\sigma_f(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-1}.$$

Prime values of polynomials

Question

What does this conjecture assert when $f(n) = mn + a$ is a linear polynomial?

Since $\sigma_f(p) = p$ for any prime p dividing $\gcd(m, a)$, the product contains a factor $(1 - p/p)(1 - 1/p)^{-1} = 0$ if $\gcd(m, a) > 1$.

Prime values of polynomials

Question

What does this conjecture assert when $f(n) = mn + a$ is a linear polynomial?

Since $\sigma_f(p) = p$ for any prime p dividing $\gcd(m, a)$, the product contains a factor $(1 - p/p)(1 - 1/p)^{-1} = 0$ if $\gcd(m, a) > 1$.

Prime values of polynomials

Question

What does this conjecture assert when $f(n) = mn + a$ is a linear polynomial?

If $\gcd(m, a) = 1$, then $\sigma_f(p) = 0$ if p divides m and $\sigma_f(p) = 1$ otherwise, and the conjecture asserts that the number of integers $1 \le n \le x/m$ such that $mn + a$ is prime should be asymptotically

$$\frac{x/m}{\ln(x/m)} \frac{1}{1} \prod_{p \mid m} \left(1 - \tfrac{0}{p}\right)\left(1 - \tfrac{1}{p}\right)^{-1} \prod_{p \nmid m} \left(1 - \tfrac{1}{p}\right)\left(1 - \tfrac{1}{p}\right)^{-1}.$$

This is the asymptotic formula for primes less than x that are congruent to $a \pmod{m}$, as described earlier.

Prime values of polynomials

Question

What does this conjecture assert when $f(n) = mn + a$ is a linear polynomial?

If $\gcd(m,a) = 1$, then $\sigma_f(p) = 0$ if p divides m and $\sigma_f(p) = 1$ otherwise, and the conjecture asserts that the number of integers $1 \le n \le x/m$ such that $mn + a$ is prime should be asymptotically

$$\frac{x/m}{\ln(x/m)} \frac{1}{1} \prod_{p \mid m} \left(1 - \tfrac{0}{p}\right)\left(1 - \tfrac{1}{p}\right)^{-1} \prod_{p \nmid m} \left(1 - \tfrac{1}{p}\right)\left(1 - \tfrac{1}{p}\right)^{-1}.$$

This is the asymptotic formula for primes less than x that are congruent to $a \pmod{m}$, as described earlier.

Prime values of polynomials

Question

What does this conjecture assert when $f(n) = mn + a$ is a linear polynomial?

If $\gcd(m, a) = 1$, then $\sigma_f(p) = 0$ if p divides m and $\sigma_f(p) = 1$ otherwise, and the conjecture asserts that the number of integers $1 \le n \le x/m$ such that $mn + a$ is prime should be asymptotically

$$\frac{x/m}{\ln x} \prod_{p \mid m} \left(1 - \tfrac{1}{p}\right)^{-1} = \frac{x}{m \ln x} \frac{m}{\phi(m)}.$$

This is the asymptotic formula for primes less than x that are congruent to $a \pmod{m}$, as described earlier.

Sieve methods

One can count the number of primes in a set of integers using inclusion-exclusion; however, each inclusion/exclusion step comes with an error term in practice, and they add up to swamp the main term.

Sieve methods use approximate inclusion-exclusion formulas to try to give upper and lower bounds for the number of primes in the set.

For prime values of polynomials, these bounds tend to look like:

- upper bound: at most 48 times as many primes as expected
- lower bound: at least -46 times as many primes as expected

Sieve methods

One can count the number of primes in a set of integers using inclusion-exclusion; however, each inclusion/exclusion step comes with an error term in practice, and they add up to swamp the main term.

Sieve methods use approximate inclusion-exclusion formulas to try to give upper and lower bounds for the number of primes in the set.

For prime values of polynomials, these bounds tend to look like:

- upper bound: at most 48 times as many primes as expected
- lower bound: at least -46 times as many primes as expected

Sieve methods

One can count the number of primes in a set of integers using inclusion-exclusion; however, each inclusion/exclusion step comes with an error term in practice, and they add up to swamp the main term.

Sieve methods use approximate inclusion-exclusion formulas to try to give upper and lower bounds for the number of primes in the set.

For prime values of polynomials, these bounds tend to look like:

- upper bound: at most 48 times as many primes as expected
- lower bound: at least -46 times as many primes as expected

Sieve methods

One can count the number of primes in a set of integers using inclusion-exclusion; however, each inclusion/exclusion step comes with an error term in practice, and they add up to swamp the main term.

Sieve methods use approximate inclusion-exclusion formulas to try to give upper and lower bounds for the number of primes in the set.

For prime values of polynomials, these bounds tend to look like:

- upper bound: at most 48 times as many primes as expected
- lower bound: at least -46 times as many primes as expected

Pairs of linear polynomials

We could choose a reasonable pair of polynomials $f(n)$ and $g(n)$ and ask whether they are simultaneously prime infinitely often.

- $f(n) = n$ and $g(n) = n + 1$: unreasonable
- $f(n) = n$ and $g(n) = n + 2$: the Twin Primes Conjecture
- $f(n) = n$ and $g(n) = 2n + 1$: Sophie Germaine primes
- $f(n) = n$ and $g(n) = 2K - n$ for some big even integer $2K$: Goldbach's Conjecture asserts that they're simultaneously prime at least once

Pairs of linear polynomials

We could choose a reasonable pair of polynomials $f(n)$ and $g(n)$ and ask whether they are simultaneously prime infinitely often.

- $f(n) = n$ and $g(n) = n + 1$: unreasonable
- $f(n) = n$ and $g(n) = n + 2$: the Twin Primes Conjecture
- $f(n) = n$ and $g(n) = 2n + 1$: Sophie Germaine primes
- $f(n) = n$ and $g(n) = 2K - n$ for some big even integer $2K$: Goldbach's Conjecture asserts that they're simultaneously prime at least once

Pairs of linear polynomials

We could choose a reasonable pair of polynomials $f(n)$ and $g(n)$ and ask whether they are simultaneously prime infinitely often.

- $f(n) = n$ and $g(n) = n + 1$: unreasonable
- $f(n) = n$ and $g(n) = n + 2$: the Twin Primes Conjecture
- $f(n) = n$ and $g(n) = 2n + 1$: Sophie Germaine primes
- $f(n) = n$ and $g(n) = 2K - n$ for some big even integer $2K$: Goldbach's Conjecture asserts that they're simultaneously prime at least once

Pairs of linear polynomials

We could choose a reasonable pair of polynomials $f(n)$ and $g(n)$ and ask whether they are simultaneously prime infinitely often.

- $f(n) = n$ and $g(n) = n + 1$: unreasonable
- $f(n) = n$ and $g(n) = n + 2$: the Twin Primes Conjecture
- $f(n) = n$ and $g(n) = 2n + 1$: Sophie Germaine primes
- $f(n) = n$ and $g(n) = 2K - n$ for some big even integer $2K$: Goldbach's Conjecture asserts that they're simultaneously prime at least once

Pairs of linear polynomials

We could choose a reasonable pair of polynomials $f(n)$ and $g(n)$ and ask whether they are simultaneously prime infinitely often.

- $f(n) = n$ and $g(n) = n + 1$: unreasonable
- $f(n) = n$ and $g(n) = n + 2$: the Twin Primes Conjecture
- $f(n) = n$ and $g(n) = 2n + 1$: Sophie Germaine primes
- $f(n) = n$ and $g(n) = 2K - n$ for some big even integer $2K$: Goldbach's Conjecture asserts that they're simultaneously prime at least once

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \ldots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and n^2+1: product is always divisible by 2
- n and $2n^2+1$ and $4n^2+1$: product is always divisible by 3
- n and $4n^2+1$ and $6n^2+1$: product is always divisible by 5
- n and $4n^2+1$ and $10n^2+1$: product has no fixed prime factor

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \dots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and $n^2 + 1$: product is always divisible by 2
- n and $2n^2 + 1$ and $4n^2 + 1$: product is always divisible by 3
- n and $4n^2 + 1$ and $6n^2 + 1$: product is always divisible by 5
- n and $4n^2 + 1$ and $10n^2 + 1$: product has no fixed prime factor

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \dots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and $n^2 + 1$: product is always divisible by 2
- n and $2n^2 + 1$ and $4n^2 + 1$: product is always divisible by 3
- n and $4n^2 + 1$ and $6n^2 + 1$: product is always divisible by 5
- n and $4n^2 + 1$ and $10n^2 + 1$: product has no fixed prime factor

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \dots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and n^2+1: product is always divisible by 2
- n and $2n^2+1$ and $4n^2+1$: product is always divisible by 3
- n and $4n^2+1$ and $6n^2+1$: product is always divisible by 5
- n and $4n^2+1$ and $10n^2+1$: product has no fixed prime factor

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \ldots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and $n^2 + 1$: product is always divisible by 2
- n and $2n^2 + 1$ and $4n^2 + 1$: product is always divisible by 3
- n and $4n^2 + 1$ and $6n^2 + 1$: product is always divisible by 5
- n and $4n^2 + 1$ and $10n^2 + 1$: product has no fixed prime factor

Systems of polynomials

We could even choose any number of polynomials $f_1, f_2, \ldots$ of any degrees and ask that they are all simultaneously prime infinitely often. We need them all to be irreducible, and we also need their product to have no fixed prime divisor.

Example polynomial triples

- n and $n^2 + 1$: product is always divisible by 2
- n and $2n^2 + 1$ and $4n^2 + 1$: product is always divisible by 3
- n and $4n^2 + 1$ and $6n^2 + 1$: product is always divisible by 5
- n and $4n^2 + 1$ and $10n^2 + 1$: product has no fixed prime factor

Even more wishful thinking

Schinzel's "Hypothesis H"

If $f_1(n),\dots,f_k(n)$ are distinct irreducible polynomials with integer coefficients such that $\sigma_{f_1\cdots f_k}(p) < p$ for all primes p, then $f_1(n),\dots,f_k(n)$ should be simultaneously prime infinitely often.

Bateman/Horn Conjecture

In the above situation, the number of integers $1 \le n \le x$ such that $f_1(n),\dots,f_k(n)$ is simultaneously prime should be asymptotically

$$\frac{x}{(\ln x)^k}\frac{1}{(\deg f_1)\cdots(\deg f_k)}\prod_p\left(1-\frac{\sigma_{f_1\cdots f_k}(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-k}.$$

Even more wishful thinking

Schinzel's "Hypothesis H"

If $f_1(n), \dots, f_k(n)$ are distinct irreducible polynomials with integer coefficients such that $\sigma_{f_1 \cdots f_k}(p) < p$ for all primes p, then $f_1(n), \dots, f_k(n)$ should be simultaneously prime infinitely often.

Bateman/Horn Conjecture

In the above situation, the number of integers $1 \le n \le x$ such that $f_1(n), \dots, f_k(n)$ is simultaneously prime should be asymptotically

$$\frac{x}{(\ln x)^k} \frac{1}{(\deg f_1) \cdots (\deg f_k)} \prod_p \left(1 - \frac{\sigma_{f_1 \cdots f_k}(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k}.$$

One polynomial in more than one variable

Quadratic forms are known to represent primes infinitely often; in fact the set of prime values often has quite a bit of structure.

Example 1

The prime values of the polynomial $4m^2 + n^2$ are exactly the primes congruent to $1 \pmod 4$.

Example 2

The prime values of the polynomial $2m^2 - 2mn + 3n^2$, other than 2, are exactly the primes whose last digit is 3 or 7 and whose second-to-last digit is even.

However, unless the number of variables is large relative to the degree, there are only a few examples known of polynomials with infinitely many prime values; two are $m^2 + n^4$ and $m^3 + 2n^3$.

One polynomial in more than one variable

Quadratic forms are known to represent primes infinitely often; in fact the set of prime values often has quite a bit of structure.

Example 1

The prime values of the polynomial $4m^2 + n^2$ are exactly the primes congruent to $1 \pmod 4$.

Example 2

The prime values of the polynomial $2m^2 - 2mn + 3n^2$, other than 2, are exactly the primes whose last digit is 3 or 7 and whose second-to-last digit is even.

However, unless the number of variables is large relative to the degree, there are only a few examples known of polynomials with infinitely many prime values; two are $m^2 + n^4$ and $m^3 + 2n^3$.

One polynomial in more than one variable

Quadratic forms are known to represent primes infinitely often; in fact the set of prime values often has quite a bit of structure.

Example 1

The prime values of the polynomial $4m^2 + n^2$ are exactly the primes congruent to $1 \pmod 4$.

Example 2

The prime values of the polynomial $2m^2 - 2mn + 3n^2$, other than 2, are exactly the primes whose last digit is 3 or 7 and whose second-to-last digit is even.

However, unless the number of variables is large relative to the degree, there are only a few examples known of polynomials with infinitely many prime values; two are $m^2 + n^4$ and $m^3 + 2n^3$.

One polynomial in more than one variable

Quadratic forms are known to represent primes infinitely often; in fact the set of prime values often has quite a bit of structure.

Example 1

The prime values of the polynomial $4m^2 + n^2$ are exactly the primes congruent to $1 \pmod 4$.

Example 2

The prime values of the polynomial $2m^2 - 2mn + 3n^2$, other than 2, are exactly the primes whose last digit is 3 or 7 and whose second-to-last digit is even.

However, unless the number of variables is large relative to the degree, there are only a few examples known of polynomials with infinitely many prime values; two are $m^2 + n^4$ and $m^3 + 2n^3$.

Primes in arithmetic progressions

The k polynomials $m, m+n, m+2n, \dots, m+(k-1)n$ in two variables define an arithmetic progression of length k.

Example

With $k = 5$, taking $m = 199$ and $n = 210$ gives the quintuple 199, 409, 619, 829, 1039 of primes in arithmetic progression.

For $k = 3$, it was proved by Vinogradov and van der Corput (1930s) that there are infinitely many triples of primes in arithmetic progression. But even the case $k = 4$ was elusive.

Theorem (Ben Green and Fields Medal winner Terry Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

Primes in arithmetic progressions

The k polynomials $m, m+n, m+2n, \dots, m+(k-1)n$ in two variables define an arithmetic progression of length k.

Example

With $k = 5$, taking $m = 199$ and $n = 210$ gives the quintuple 199, 409, 619, 829, 1039 of primes in arithmetic progression.

For $k = 3$, it was proved by Vinogradov and van der Corput (1930s) that there are infinitely many triples of primes in arithmetic progression. But even the case $k = 4$ was elusive.

Theorem (Ben Green and Fields Medal winner Terry Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

Primes in arithmetic progressions

The k polynomials $m, m+n, m+2n, \ldots, m+(k-1)n$ in two variables define an arithmetic progression of length k.

Example

With $k=5$, taking $m=199$ and $n=210$ gives the quintuple 199, 409, 619, 829, 1039 of primes in arithmetic progression.

For $k=3$, it was proved by Vinogradov and van der Corput (1930s) that there are infinitely many triples of primes in arithmetic progression. But even the case $k=4$ was elusive.

Theorem (Ben Green and Fields Medal winner Terry Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

Primes in arithmetic progressions

The k polynomials m, $m+n$, $m+2n$, $\ldots$, $m+(k-1)n$ in two variables define an arithmetic progression of length k.

Example

With $k=5$, taking $m=199$ and $n=210$ gives the quintuple 199, 409, 619, 829, 1039 of primes in arithmetic progression.

For $k=3$, it was proved by Vinogradov and van der Corput (1930s) that there are infinitely many triples of primes in arithmetic progression. But even the case $k=4$ was elusive.

Theorem (Ben Green and Fields Medal winner Terry Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

Primes in arithmetic progressions

Theorem (Green/Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

The methods used to prove this theorem were, for the most part, very different from usual proofs in number theory. Green and Tao formulated a generalization of Szemeredi's Theorem, which tells us that "large" subsets of the integers always contain long arithmetic progressions, to "large" subsubsets of "nice" subsets of the integers.

They used some sieve method weights to construct the "nice" subset of the integers inside which the primes sit as a "large" subsubset.

Primes in arithmetic progressions

Theorem (Green/Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

The methods used to prove this theorem were, for the most part, very different from usual proofs in number theory. Green and Tao formulated a generalization of Szemeredi's Theorem, which tells us that "large" subsets of the integers always contain long arithmetic progressions, to "large" subsubsets of "nice" subsets of the integers.

They used some sieve method weights to construct the "nice" subset of the integers inside which the primes sit as a "large" subsubset.

Primes in arithmetic progressions

Theorem (Green/Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

The methods used to prove this theorem were, for the most part, very different from usual proofs in number theory. Green and Tao formulated a generalization of Szemeredi's Theorem, which tells us that “large” subsets of the integers always contain long arithmetic progressions, to “large” subsubsets of “nice” subsets of the integers.

They used some sieve method weights to construct the “nice” subset of the integers inside which the primes sit as a “large” subsubset.

Primes in arithmetic progressions

Theorem (Green/Tao, 2004)

For any k, there are infinitely many k-tuples of primes in arithmetic progression.

The methods used to prove this theorem were, for the most part, very different from usual proofs in number theory. Green and Tao formulated a generalization of Szemeredi's Theorem, which tells us that “large” subsets of the integers always contain long arithmetic progressions, to “large” subsubsets of “nice” subsets of the integers.

They used some sieve method weights to construct the “nice” subset of the integers inside which the primes sit as a “large” subsubset.

Mersenne primes

Consider numbers of the form $2^n - 1$. Since

$$2^{uv} - 1 = (2^u - 1)(2^{(v-1)u} + 2^{(v-2)u} + \cdots + 2^{2u} + 2^u + 1),$$

we see that $2^n - 1$ cannot be prime unless n itself is prime.

We currently know 47 values of n for which $2^n - 1$ is prime: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, …, 43,112,609.

Conjecture

There are infinitely many n for which $2^n - 1$ is prime.

Mersenne primes

Consider numbers of the form $2^n - 1$. Since

$$2^{uv} - 1 = (2^u - 1)(2^{(v-1)u} + 2^{(v-2)u} + \cdots + 2^{2u} + 2^u + 1),$$

we see that $2^n - 1$ cannot be prime unless n itself is prime.

We currently know 47 values of n for which $2^n - 1$ is prime: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, ..., 43,112,609.

Conjecture

There are infinitely many n for which $2^n - 1$ is prime.

Mersenne primes

Consider numbers of the form $2^n - 1$. Since

$$2^{uv} - 1 = (2^u - 1)(2^{(v-1)u} + 2^{(v-2)u} + \cdots + 2^{2u} + 2^u + 1),$$

we see that $2^n - 1$ cannot be prime unless n itself is prime.

We currently know 47 values of n for which $2^n - 1$ is prime: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, . . . , 43,112,609.

Conjecture

There are infinitely many n for which $2^n - 1$ is prime.

Connection with perfect numbers

Definition

A number is perfect if it equals the sum of its proper divisors.

Example

$28 = 1 + 2 + 4 + 7 + 14$ is a perfect number.

Each Mersenne prime $2^n - 1$ gives rise to a perfect number $2^{n-1}(2^n - 1)$, and all even perfect numbers are of this form.

Conjecture

There are no odd perfect numbers.

Connection with perfect numbers

Definition

A number is perfect if it equals the sum of its proper divisors.

Example

$28 = 1 + 2 + 4 + 7 + 14$ is a perfect number.

Each Mersenne prime $2^n - 1$ gives rise to a perfect number $2^{n-1}(2^n - 1)$, and all even perfect numbers are of this form.

Conjecture

There are no odd perfect numbers.

Connection with perfect numbers

Definition

A number is perfect if it equals the sum of its proper divisors.

Example

$28 = 1 + 2 + 4 + 7 + 14$ is a perfect number.

Each Mersenne prime $2^n - 1$ gives rise to a perfect number $2^{n-1}(2^n - 1)$, and all even perfect numbers are of this form.

Conjecture

There are no odd perfect numbers.

Connection with perfect numbers

Definition

A number is perfect if it equals the sum of its proper divisors.

Example

$28 = 1 + 2 + 4 + 7 + 14$ is a perfect number.

Each Mersenne prime $2^n - 1$ gives rise to a perfect number $2^{n-1}(2^n - 1)$, and all even perfect numbers are of this form.

Conjecture

There are no odd perfect numbers.

Fermat primes

Consider numbers of the form $2^n + 1$. Since

$$2^{uv} + 1 = (2^u + 1)(2^{(v-1)u} - 2^{(v-2)u} + \cdots + 2^{2u} - 2^u + 1)$$

if v is odd, we see that $2^n + 1$ cannot be prime unless n itself is a power of 2.

We currently know 5 values of n for which $2^n + 1$ is prime: 1, 2, 4, 8, 16.

Conjecture

There is no other n for which $2^n + 1$ is prime.

Gauss proved that a regular k-sided polygon can be constructed with a straightedge and compass if and only if the odd prime factors of k are distinct Fermat primes $2^n + 1$.

Fermat primes

Consider numbers of the form $2^n + 1$. Since

$$2^{uv} + 1 = (2^u + 1)(2^{(v-1)u} - 2^{(v-2)u} + \cdots + 2^{2u} - 2^u + 1)$$

if v is odd, we see that $2^n + 1$ cannot be prime unless n itself is a power of 2.

We currently know 5 values of n for which $2^n + 1$ is prime: 1, 2, 4, 8, 16.

Conjecture

There is no other n for which $2^n + 1$ is prime.

Gauss proved that a regular k-sided polygon can be constructed with a straightedge and compass if and only if the odd prime factors of k are distinct Fermat primes $2^n + 1$.

Fermat primes

Consider numbers of the form $2^n + 1$. Since

$$2^{uv} + 1 = (2^u + 1)(2^{(v-1)u} - 2^{(v-2)u} + \cdots + 2^{2u} - 2^u + 1)$$

if v is odd, we see that $2^n + 1$ cannot be prime unless n itself is a power of 2.

We currently know 5 values of n for which $2^n + 1$ is prime: 1, 2, 4, 8, 16.

Conjecture

There is no other n for which $2^n + 1$ is prime.

Gauss proved that a regular k-sided polygon can be constructed with a straightedge and compass if and only if the odd prime factors of k are distinct Fermat primes $2^n + 1$.

Fermat primes

Consider numbers of the form $2^n + 1$. Since

$$2^{uv} + 1 = (2^u + 1)(2^{(v-1)u} - 2^{(v-2)u} + \cdots + 2^{2u} - 2^u + 1)$$

if v is odd, we see that $2^n + 1$ cannot be prime unless n itself is a power of 2.

We currently know 5 values of n for which $2^n + 1$ is prime: 1, 2, 4, 8, 16.

Conjecture

There is no other n for which $2^n + 1$ is prime.

Gauss proved that a regular k-sided polygon can be constructed with a straightedge and compass if and only if the odd prime factors of k are distinct Fermat primes $2^n + 1$.

Artin's Conjecture

Some decimal expansions of fractions take a long time to start repeating:

$$\tfrac{1}{7} = 0.\overline{142857} \qquad \tfrac{1}{19} = 0.\overline{052631578947368421}$$

When p is a prime, the period of $1/p$ is equal to the order of 10 modulo p, that is, the smallest positive integer t such that $10^t \equiv 1 \pmod{p}$. This order is always some divisor of $p-1$.

Artin's Conjecture

There are infinitely many primes p for which the order of 10 modulo p equals $p-1$, that is, for which the period of the decimal expansion for $1/p$ is as large as possible.

Artin's Conjecture

Some decimal expansions of fractions take a long time to start repeating:

$$\tfrac{1}{7} = 0.\overline{142857} \qquad \tfrac{1}{19} = 0.\overline{052631578947368421}$$

When p is a prime, the period of $1/p$ is equal to the order of 10 modulo p, that is, the smallest positive integer t such that $10^t \equiv 1 \pmod{p}$. This order is always some divisor of $p-1$.

Artin's Conjecture

There are infinitely many primes p for which the order of 10 modulo p equals $p-1$, that is, for which the period of the decimal expansion for $1/p$ is as large as possible.

Artin's Conjecture

Some decimal expansions of fractions take a long time to start repeating:

$$\tfrac{1}{7} = 0.\overline{142857} \qquad \tfrac{1}{19} = 0.\overline{052631578947368421}$$

When p is a prime, the period of $1/p$ is equal to the order of 10 modulo p, that is, the smallest positive integer t such that $10^t \equiv 1 \pmod{p}$. This order is always some divisor of $p-1$.

Artin's Conjecture

There are infinitely many primes p for which the order of 10 modulo p equals $p-1$, that is, for which the period of the decimal expansion for $1/p$ is as large as possible.

The end

These slides

www.math.ubc.ca/~gerg/index.shtml?slides