Prime Numbers

Maths and Physics Club

IIT Bombay

December 24, 2020

Prime Numbers

- Definition: A natural number greater than 1 that is not a product of two smaller natural numbers.
- How to determine whether a number is a prime or not?
- Distribution of primes
- Applications of primes
- Some 'beautiful' facts about primes

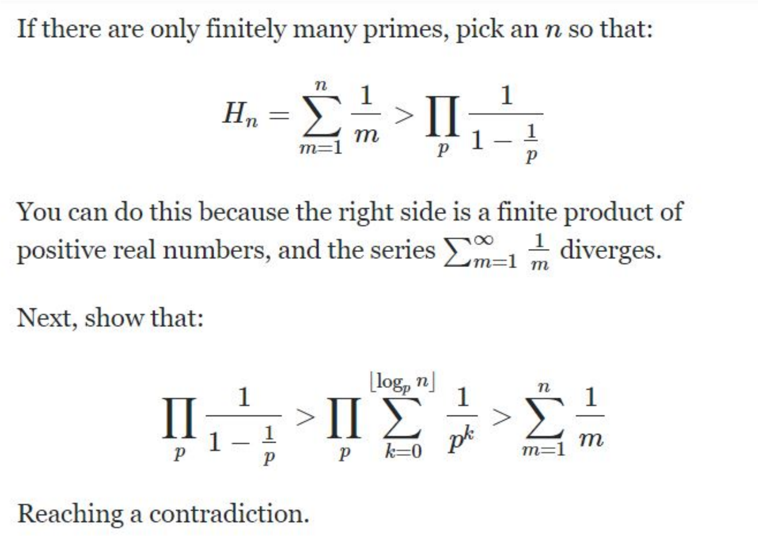
Distribution of Primes

How many prime numbers are there?

- Proof 1: Prime divisor of $\prod p_i + 1$. Food for thought- how about $\prod p_i - 1$? (Proof?)
- Proof 2: $n! + 1$ has a prime factor greater than n (Proof?)

Infinitude of Primes

- Proof 3: Divergence of harmonic series $\Sigma 1/n$



If there are only finitely many primes, pick an n so that:

$$H_n = \sum_{m=1}^{n} \frac{1}{m} > \prod_p \frac{1}{1-\frac{1}{p}}$$

You can do this because the right side is a finite product of positive real numbers, and the series $\sum_{m=1}^{\infty} \frac{1}{m}$ diverges.

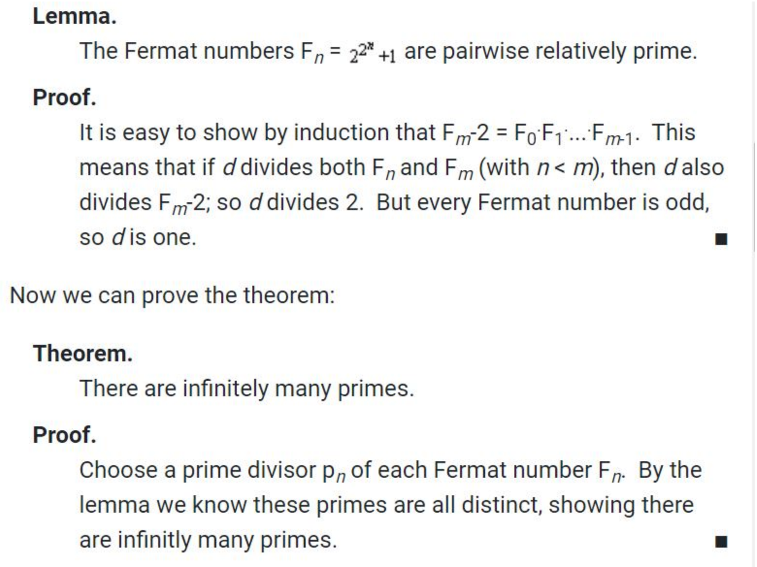
Next, show that:

$$\prod_p \frac{1}{1-\frac{1}{p}} > \prod_p \sum_{k=0}^{\lfloor \log_p n \rfloor} \frac{1}{p^k} > \sum_{m=1}^{n} \frac{1}{m}$$

Reaching a contradiction.

Infinitude of Primes

Proof 4: Goldbach's Proof.



Lemma.

The Fermat numbers $F_n = 2^{2^n}+1$ are pairwise relatively prime.

Proof.

It is easy to show by induction that $F_m - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1}$. This means that if d divides both F_n and F_m (with $n < m$), then d also divides $F_m - 2$; so d divides 2. But every Fermat number is odd, so d is one. ■

Now we can prove the theorem:

Theorem.

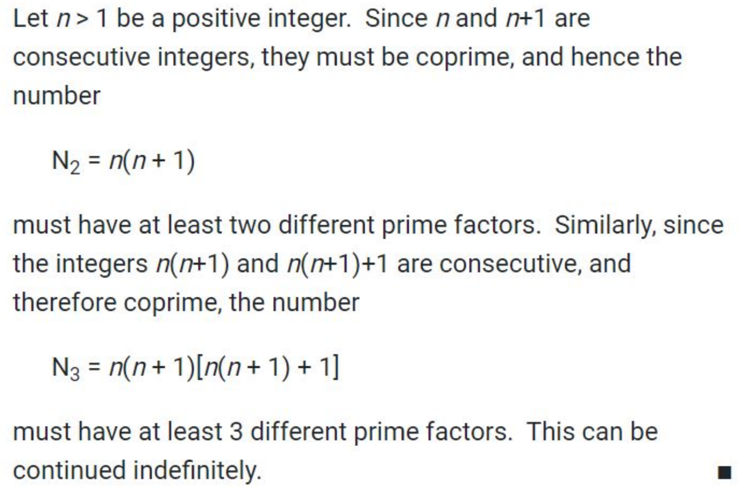
There are infinitely many primes.

Proof.

Choose a prime divisor p_n of each Fermat number F_n. By the lemma we know these primes are all distinct, showing there are infinitly many primes. ■

Infinitude of Primes

Proof 5: Filip Saidak's Proof



Let $n > 1$ be a positive integer. Since n and $n+1$ are consecutive integers, they must be coprime, and hence the number

$$N_2 = n(n + 1)$$

must have at least two different prime factors. Similarly, since the integers $n(n+1)$ and $n(n+1)+1$ are consecutive, and therefore coprime, the number

$$N_3 = n(n + 1)[n(n + 1) + 1]$$

must have at least 3 different prime factors. This can be continued indefinitely. ■

Infinitude of Primes

- Proof 6: Using topology
- Proof 7: Infinitely many primes of the form $4k + 1$? (Proof?)
  $N = (2p_1 p_2 ... p_k)^2 + 1$
- Proof 8: Infinitely many primes of the form $4k + 3$? (Proof?)
  $N = 4p_1 p_2 ... p_k - 1$
- Can we continue this way?
  Infinitely many proofs for the infinitude of primes?! Indeed, we can!

Dirichlet's Theorem

- Given natural numbers a, b, when is it possible that there are infinitely many primes of the form $ak + b$?
- Necessary condition: $(a, b) = 1$
- And it is the sufficient condition indeed!
- Proof? No elementary proof!
- Introducing a fancy field: Analytical Number Theory! Analytic number theory is the branch of number theory which uses real and complex analysis to investigate various properties of integers and prime numbers. Examples of topics falling under analytic number theory include Dirichlet L-series, the Riemann zeta function, the totient function, and the prime number theorem.

Prime Number Theorem

- Define $\pi(x)$ as the number of primes upto x.
- Averages the function: statistical technique. $\frac{\pi(x)}{x}$
- Prime number theorem: asymptotically, $\pi(x) = \frac{x}{logx}$
- Proof: using complex analysis and Riemann Zeta Function!
- Later on, an 'elementary proof' was discovered.

Prime Numbers and Conjectures

- Every number can be written as a sum of powers of two- binary representation.
  base n representation
  Every number can be written as a sum of at most four square numbers
- Can every number be written as a sum of prime numbers?
- Goldbach conjecture: Every even number greater than 3 can be written as a sum of two prime numbers.
- Proved result: every even integer greater than 3 can be written as in the form $p_1 + p_2 p_3$ where p_1 is a prime, and p_2, p_3 are either primes or equal to 1.
- Waring's prime number conjecture: every odd number greater than 3 is either a prime number or the sum of three prime numbers

Prime Number Conjectures

- Twin Prime Conjecture
- Chebyshev's biase: Prime number races
- There are infinitely many primes of the form $n^2 + 1$.
  It is proven that there are infinitely many primes of the form $n^2 + m^2 + 1$ and $n^2 + m^2$.
- There is always a prime between n^2 and $(n + 1)^2$
- Prime spirals conjecture.

Generating Prime Numbers

- Is there a polynomial that takes only prime values?
- Story of $n^2 + n + 41$
- Matiyasevich: a polynomial in 10 variables is sufficient!
- So far, we have seen how to 'construct primes'

Frame Title

But the questions that we have not addressed so far are, can every prime be constructed in such a way? Can every number constructed in a way is a prime? How to determine whether a number is a prime or not?
PRIMALITY TESTING!

Sieve of Eratosthenes

- Eratosthenes: Make a list of all the integers less than or equal to n (greater than one) and strike out the multiples of all primes less than or equal to the square root of n, then the numbers that are left are the primes
- Trial division: divisibility tests of 3, 9, 7, 11 (Proofs)
- Base vs divisibility test
- Trial division upto $\sqrt{n}$
- How to make it optimal?
- Divide by primes less than n
- WHEELING!
- Wheel of 30: residues modulo 1, 7, 11, 13, 17, 19, 23, and 29.

Pseudoprimes

- "If n is a prime, then statement S is true about n"
- If the statement fails, the number is composite.
- How about the converse?
- Pseudoprimes!

Fermat's Test

- Fermat's (Little) Theorem: If p is a prime and if a is any integer, then $a^p \equiv a(modp)$. In particular, if p does not divide a, then $a^{p-1} \equiv 1(modp)$ (Proofs (many:P))
- Converse: Fermat Pseudoprimes. (Rare!!)
- Combining Fermat tests for various bases a.
- 341 is a pseudoprime base 2, but not base 3. 91 is a pseudoprime in base 3 but not in base 2.
- Alas! the number 561 is a Fermat Pseudoprime in every base a
- Carmichael number: a composite integer n for which $a^n \equiv a(modn)$ for every integer a.

Carmichael Numbers

- Carmichael number: a composite integer n for which $a^n \equiv a(modn)$ for every integer a
- An integer n is a Carmichael number iff n is positive, composite, squarefree, and for each prime p dividing n, $p-1$ divides $n-1$. (Proof)
- There are infinitely many Carmichael numbers (Proof)
- Carmichael numbers are not as rare as we expect (Proof)
- First few Carmichael numbers: 561, 1105, 1729, 2465, 2821.
- Can we 'generalize' the Fermat's little theorem in order to 'avoid' pseudoprimes?

Some results about prime numbers

- $p > 1$ is a prime iff every number modulo p is invertible. (Proof?)
- $p > 1$ is a prime iff $\phi(p) = p - 1$. (Proof?)
- $p > 1$ is a prime iff the only solutions to the congruence $x^2 \equiv 1(mod p)$ are $x = 1, x = p - 1$ modulo p. (Proof?)

Some results about prime numbers

Given any natural number a, if p is a prime, then:

- a, a^2, a^3,...,a^{p-1} are incongruent modulo p, and are precisely the numbers $1, 2, ..., p-1$ in some order. (Proof)
- There is an integer a such that $a^{p-1} \equiv 1 (modp)$ AND a^k is NOT congruent to 1 modulo p for any $1 \leq k < p-1$ (Primitive root) (Proof?)
- Generator, order, periodicity

Luca's Theorem

- Lucas theorem: Let $n > 1$. If for every prime factor q of n-1 there is an integer a such that $a^{n-1} \equiv 1 (mod n)$, and $a^{(n-1)/q}$ is not congruent to $1 (mod n)$; then n is prime.
- Converse is not true! $(n = p^k, 2p^k)$
- Proof: n is a prime, if $\phi(n) = n - 1$, or $\phi(n) | n - 1$
- If not, there is a prime q and exponent $r > 0$ such that $q^r | n - 1$ but q^r does not divide $\phi(n)$.
- For this q, there exists a that satisfies the condition above.
- Then $ord_n(a)$ divides $n - 1$ but not $\frac{n-1}{q}$.
- So q^r divides $ord_n(a)$ which divides $\phi(n)$.
- Contradiction to existence of prime q dividing n. Hence, n is a prime.

The n-1 test

Suppose $n - 1 = FR$, where $F > R$, $gcd(F, R) = 1$ and the factorization of F is known. If for every prime factor q of F there is an integer $a > 1$ such that $a^{n-1} \equiv 1 (modn)$, and $gcd(a^{(n-1)/q-1}, n) = 1$; then n is prime.
Pepin's Test, Proth's Theorem, Lucas-Lehmer Test, n+1 tests

A quick application of Lucas-Lehmer test

- Lucas numbers: $L(1) = 1, L(2) = 3. L(n) = L(n-1) + L(n-2)$
- First few Lucas numbers: 1, 3, 4, 7, 11, 18...
- If n does not divide $L(n) - 1$, then it is not a prime.
- Computing largest prime number by hand:
- Lucas Lehmer series: $l(1) = 4$, $l(n) = l(n-1)^2 - 2$. 4, 14, 194,...
- Primality test: let p be a prime. Let $n = 2^p - 1$. Then n is a prime iff $p|l(p-1)$.
- Used to prove that $2^{67} - 1$ is not a prime
- Used to prove that $2^{127} - 1$ is a prime
  Largest prime computed by hand!

Mersenne's Primes

- Incorrect conjecture: (Mersenne) Every integer of the form $2^n - 1$ is a prime.
- Mersenne's Primes: If $2^n - 1$ is a prime, then it is called as a Mersenne's Prime.
- Some small values of n: n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 and 127.
- Perfect number: A positive integer n is called a perfect number if it is equal to the sum of all of its positive divisors, excluding n itself.
- First few perfect numbers: 6, 28, 496 and 8128.
- That is, 2.3, 4.7, 16.31, 64.127. Coincidence?!
- If $2^n - 1$ is prime, then so is n.
- Proof: Factorization!

Antiprimes

- Antiprimes (Highly composite numbers): Any number less than n has less number of divisors.
- City number, clock. First few antiprimes- 1,2,4,6,12,24,36,48,60,...,360.
- Number of divisors of $n = \Pi p_i^{a_i}$ is $d(n) = \Pi(a_i + 1)$. Proof?
- Primes dividing an antiprime: consecutive primes. Proof?
- $a_i \geq a_j$ when $i < j$. Proof?
- Ramanujan: If n has k divisors, then $a_k = 1$.

Prime Numbers

- Building blocks of the number system. Fundamental Theorem of Arithmetic
- Number theoretic functions. Euler's totient function, number of divisors, sum of divisors
- Applications in cryptography: it is easy to take a product of two integers compared to factoring an integer
- Structure of integers modulo prime p. Forms a 'ring'. Algebraic number theory
- Ring theory: primes, irreducibles. eg. Polynomial ring
- Some beautiful theorems: quadratic law of reciprocity, cyclotomic polynomials, primitive roots and what not!
- Many many conjectures and fancy results. eg. Riemann Hypothesis
- Prime numbers are mysterious, intimidating, useful and beautiful in their own fasion!