Prime numbers

*Carl Friedrich Gauss, the *Prince of Mathematicians*, once said:*
"Mathematics is the queen of the sciences—and [prime] number theory is the queen of mathematics."

Prime Numbers in Cryptography

Whenever you make a payment and receive an OTP, you are actually using cryptography. Why do we use primes? Because multiplying two large prime numbers is easy but factoring the product back into the original primes is extremely difficult—even for supercomputers. This property is the basis of many encryption algorithms. One famous example is the RSA algorithm (named after Rivest, Shamir, and Adleman), widely used for securing online data. Read more:
https://www.geeksforgeeks.org/maths/why-prime-numbers-are-used-in-cryptography/

Prime Gaps and Conjectures

The distribution of primes can be approximated as: $\pi(N) \sim N / \log(N)$, where $\pi(N)$ is the prime-counting function (the number of primes less than or equal to N) and log(N) is the natural logarithm of N. This means that for large N, the probability that a random integer $\leq N$ is prime is roughly: 1 / log(N). Among the positive integers of at most 1000 digits, about one in 2300 is prime ($\log(10^{1000}) \approx 2302.6$).

- Cramér's Conjecture: The maximum size of prime gaps is bounded by $(\log p)^2$, where p is prime.
- Twin Prime Conjecture: At the minimum, gaps can be as small as 2.

Both remain open problems in mathematics.

Algorithms for Prime Numbers

Even though we have a proof that there are infinitely many prime numbers, finding very large prime numbers is a very difficult task. Thus, it would be of great interest if there was a simple formula or function that produced prime numbers. One famous such "formula" was proposed by Fermat, who famously claimed that the numbers of the form $Fn = 2^{2^n}+1$, known as Fermat numbers, are always prime. The first few Fermat numbers $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ are, indeed, prime numbers. However, Fermat's claim has been proven to be fantastically wrong, since every single other Fermat number that we have been able to factor has turned out to be a composite number. For instance, Euler proved in 1732 that $F_5 = 4294967297 = 641*6700417$. The conjecture that there is no other Fermat number is an open problem.

Prime Number Formulas

There exist prime number generation formulas, but they are impractical for computation. Willans formula is based on Wilson's theorem in that a number $p > 1$ is prime iff $(p-1)! + 1$ is divisible by p. This is impractical as factorials grow extremely fast. $10! \approx 3.6 \times 10^6$. $70! > 10^{100}$ (one googol). Even the fastest supercomputers can compute factorial primality only up to ~200 numbers using this method, and thus it is not useful in practice.

Efficient Methods

1. Sieve of Eratosthenes is a classical method for generating primes and checking them.
   https://www.geeksforgeeks.org/dsa/sieve-of-eratosthenes/
2. Improved Sieves: Optimizations exist, but still slow for very large numbers.
3. Miller-Rabin Primality Test: Probabilistic test. Not 100% accurate but fast and practical.
   https://www.geeksforgeeks.org/dsa/primality-test-set-3-miller-rabin/

Conclusion

Prime numbers remain central to both pure mathematics and modern-day cryptography. While exact formulas exist, practical prime testing relies on efficient algorithms like the Miller-Rabin algorithm. We will now discuss your assignment problems.

1. A prime number is 123456789**10**987654321. Here n is 10. Find the next number that follows this pattern. That number n lies between 1000 and 3000. This was discovered by an Indian.
2. 11 is prime, 111 is not prime. We use the notation, 1_N means N ones. For example, 1_7, we mean seven ones:1111111. 1_N is represented by $(10^N-1)/9$. If N is prime 1_N might be prime. If N is not prime, 1_N can not be prime. Thus we have to check only for N being prime. Determine the 5 primes between N=2 and N=1040.
3. We are interested in Mersenne primes. A Mersenne prime is a prime number that is one less than a power of two. The largest Mersenne prime discovered was on Oct 12, 2024 when 2^p-1 where p=136,279,841. This has 41,024,320 digits. Find the two primes where p lies between 2201 and 2299. These primes were discovered in 1952.
4. Brocard's conjecture is the conjecture (open problem) that there are at least four prime numbers between $(p_n)^2$ and $(p_{n+1})^2$, where p_n is the n^{th} prime number, for every $n \geq 2$. Use the two prime numbers you obtained in #3 and determine at least four prime numbers between the squares of those numbers.
5. Palindromic prime numbers are prime numbers that are also palindromes. The simpler ones are 11 and 122333221. More interesting ones are 1223334444555554444333221 and 12233355555333221. The largest found so far is $10^{1888529} - 10^{944264} - 1$ which has 1,888,529 digits. Find a palindromic prime that has at least 50 digits.
6. A perfect number is a positive integer that is equal to the sum of its positive proper divisors, that is, divisors excluding the number itself. For instance, 6 has proper divisors 1, 2 and 3, and 1 + 2 + 3 = 6, so 6 is a perfect number. The next perfect number is 28, since 1 + 2 + 4 + 7 + 14 = 28. Euclid proved that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number and then Euler proved that all even perfect numbers followed this form. The existence of odd perfect numbers is an open problem and it can be shown if such a number exists it should be $> 10^{1500}$. Using the primes in #3, prove that the above expression yields a perfect number.
7. Take some interesting problem in prime numbers, which are all open problems. Some are as follows and prove them for a number that has greater than 50 digits. Take one of the following conjectures or choose one of your own.
    a) A Wieferich prime is a prime p such that p^2 is a divisor of $2^{(p-1)} - 1$. We only know two Wieferich primes: 1093 and 3511. The crazy thing is that we conjecture that there are infinitely many Wieferich primes… but we only know two of them!
    b) Goldbach's conjecture: Every even $n > 2$ is the sum of two primes.
    c) The Weak Goldbach Problem: Every odd $n > 5$ is the sum of three primes.
    d) Every even number is the difference of two primes.
    e) Legendre's conjecture that there is a prime between consecutive integer squares directly implies that there are at least two primes between prime squares for $p_n \geq 3$ since $p_{n+1} - p_n \geq 2$.
    f) Oppermann's conjecture is that for any integer n greater than 1, there is always a prime number between $n(n - 1)$ and n^2, and another between n^2 and $n(n + 1)$.