SmallSEOTools

PLAGIARISM SCAN REPORT

Words	724	Date	February 24,2019
Characters	4196	Exclude Url	

3% Plagiarism	97% Unique	1 Plagiarized Sentences	36 Unique Sentences

Content Checked For Plagiarism

Large Primes How to check them??? â€œGod may not play dice with the universe, but something strange is going on with the prime numbers.â€▯ -Paul Erdos â€œDecember 21, 2018 -- The largest known prime number 2^82589933 - 1 has being discovered by The Great Internet Mersenne Prime Search (GIMPS) which has 24,862,048 digits. A computer volunteered by Patrick Laroche from Ocala, Florida made the find on December 7, 2018.â€▯[1] Primes, whole numbers with two factors, have always influenced the mathematical world with its beauty. It has made cryptography an enigma. Large primes are used in encryption to make networks more secure. And who can forget the million-dollar problem of Riemann Hypothesis, which is based on the distribution of primes? Also, there is a sort of joy in finding the large prime numbers in society. The layman’s way for checking a number to be prime is, trial division of the number n with 2,3 and odd numbers of the form 6kÂ±1 (k>=1) less than or equal to âˆšn. But time complexity for executing this is exponential (O(2^n/2)) to the size of n and is not acceptable for large numbers. Let’s take a try if we assume that in one second 1016 iterations execute on a supercomputer and we run this program for 24x7x365, it would not have completed till the moment, even if we started at the big-bang to check the primality of largest prime known till date. The question is, how the primality of numbers with such a huge size is checked? Some methods like using Fermat’s Little Theorem and Miller-Rabin test exist, but there is some error/probability associated with them. Lucas-Lehmer test, developed by Édouard Lucas and improved by him and Derrick Henry Lehmer[2] is used to check the primality of special types of numbers known as Mersenne numbers. These are the numbers of the form 2n â€“ 1. Under this test, a Mersenne number, 2n -1 is prime, if and only if, n is odd prime and (n-1)th element of the Lucas-Lehmer sequence (given below) is divisible by the number. The Lucas-Lehmer sequence is given as â€“ L(i) = 4, i = 1 L(i) = (L(i-1))2 â€“ 2, i > 1 It grows very fast, first few elements of the sequence are 4, 14, 194, 37634, 1416317954,.â€¦. So, instead of first calculating the (n-1)th element of the sequence and then checking it’s divisibility. We keep on passing just the remainders from ith iteration to (i+1)th, which makes calculation somewhat fast. Let’s check the primality of 27-1. 27-1 = 127, n = 7 L(1)=4 Incrementing till L(6) by taking remainders from one iteration to next. 4 mod 127 = 4 â€¦L(1) 42-2 mod 127 = 14 mod 127 = 14 â€¦L(2) 142-2 mod 127 = 194 mod 127 = 67 â€¦L(3) 672-2 mod 127 = 4487 mod 127 = 42 â€¦L(4) 422-2 mod 127 = 1762 mod 127 = 111 â€¦L(5) 1112-2 mod 127 = 12319 mod 127 = 0 â€¦L(6) As L(6) mod 127 equals zero. 127 is a prime number. This is the main idea behind the construction of GIMPS’s algorithm, which is generally used to find large Mersenne primes. GIMPS gives thousands of dollars as prize money for finding large primes to the enthusiasts. An algorithm for primality checking of all types of numbers is also of theoretical interest known as AKS primality test, founded by IIT Kanpur’s professors named Manindra Agrawal, Neeraj Kayal and Nitin Saxena, in 2002[3]. It is a generalization of Fermat’s Little Theorem polynomial. It states that a number n is prime if all the coefficients of polynomial (x - 1)n - (xn - 1) are divisible by n. This algorithm runs in polynomial time with the size of n. AKS’s correctness is based on the generalized Riemann Hypothesis. It is not much used in practice as other fast algorithms also exist which works on a particular type of number. Some amusing facts : The largest prime found without using a computer is, 117*(2148+1) (a Proth number)by Aime Ferrier. He used a mechanical calculator and Proth’s theorem for this.[4] The largest prime checked just by hand calculations is 2127-1 by Lucas. Using his Lucas-Lehmer sequence. It is difficult (but scientifically possible) to remember all the digits of the largest prime known till date in decimal by humans. But you may remember it in binary ;)

Sources	Similarity

God may not play dice with the universe, but something strange is...=1) less than or equal to âˆšn. But time complexity for executing this is exponential (O(2^n/2)) to the size of n and is not acceptable for large numbers. Let’s take a try if we assume that in one second 1016 iterations execute on a supercomputer and we run this program for 24x7x365, it would not have completed till the moment, even if we started at the big-bang to check the primality of largest prime known till date. The question is, how the primality of numbers with such a huge size is checked? Some methods like using Fermat’s Little Theorem and Miller-Rabin test exist, but there is some error/probability associated with them. Lucas-Lehmer test, developed by Édouard Lucas and improved by him and Derrick Henry Lehmer[2] is used to check the primality of special types of numbers known as Mersenne numbers. These are the numbers of the form 2n â€“ 1. Under this test, a Mersenne number, 2n -1 is prime, if and only if, n is odd prime and (n-1)th element of the Lucas-Lehmer sequence (given below) is divisible by the number. The Lucas-Lehmer sequence is given as â€“ L(i) = 4, i = 1 L(i) = (L(i-1))2 â€“ 2, i > 1 It grows very fast, first few elements of the sequence are 4, 14, 194, 37634, 1416317954,.â€¦. So, instead of first calculating the (n-1)th element of the sequence and then checking it’s divisibility. We keep on passing just the remainders from ith iteration to (i+1)th, which makes calculation somewhat fast. Let’s check the primality of 27-1. 27-1 = 127, n = 7 L(1)=4 Incrementing till L(6) by taking remainders from one iteration to next. 4 mod 127 = 4 â€¦L(1) 42-2 mod 127 = 14 mod 127 = 14 â€¦L(2) 142-2 mod 127 = 194 mod 127 = 67 â€¦L(3) 672-2 mod 127 = 4487 mod 127 = 42 â€¦L(4) 422-2 mod 127 = 1762 mod 127 = 111 â€¦L(5) 1112-2 mod 127 = 12319 mod 127 = 0 â€¦L(6) As L(6) mod 127 equals zero. 127 is a prime number. This is the main idea behind the construction of GIMPS’s algorithm, which is generally used to find large Mersenne primes. GIMPS gives thousands of dollars as prize money for finding large primes to the enthusiasts. An algorithm for primality checking of all types of numbers is also of theoretical interest known as AKS primality test, founded by IIT Kanpur’s professors named Manindra Agrawal, Neeraj Kayal and Nitin Saxena, in 2002[3]. It is a generalization of Fermat’s Little Theorem polynomial. It states that a number n is prime if all the coefficients of polynomial (x - 1)n - (xn - 1) are divisible by n. This algorithm runs in polynomial time with the size of n. AKS’s correctness is based on the generalized Riemann Hypothesis. It is not much used in practice as other fast algorithms also exist which works on a particular type of number. Some amusing facts : The largest prime found without using a computer is, 117*(2148+1) (a Proth number)by Aime Ferrier. He used a mechanical calculator and Proth’s theorem for this.[4] The largest prime checked just by hand calculations is 2127-1 by Lucas. Using his Lucas-Lehmer sequence. It is difficult (but scientifically possible) to remember all the digits of the largest prime known till date in decimal by humans. But you may remember it in binary ;) ">Compare text God may not play dice with the universe, but something strange is going on with the prime numbers. https://www.allgreatquotes.com/quote-359925/	10%