Primality in Number Theory

Janet Flume

Friedley Senior High School

INTRODUCTION

The concept of primality is central to the number theory concepts. Prime numbers are the natural integers with no positive divisors apart from one and itself. Natural numbers greater than one, which are not prime numbers are commonly referred to as composite numbers. For instance, five is a prime number solely because five and one are its lone positive, numerical factors. On the other hand, six is not a prime number because two and three are its divisors in addition to one and itself. The fundamental theorem establishes the principle role of primality in the number theory. It states that integers greater than one may be expressed as products of primes uniquely in terms of ordering. The distinctiveness of the conception requires the exclusion of one as a prime number because of the possibility of including one in factorization. For instance, 3, 1•3, 1• 1 c3 and so on, are legitimate factorization of three. The trial division is a slow but simple approach for the verification of the primality of any given integer. The process entails ascertaining whether an integer is a multiple of any number between two and the root of the integer. However, algorithms are considered to be much more effective in the testing of primality of relatively larger integers. Even numbers greater than two are not considered as prime numbers because, by definition, such numbers have at minimum three discrete divisors, namely one, two, and itself.

FUNDAMENTAL THEOREM OF ARITHMETIC

The critical importance of primality to mathematics and number theory in particular stems from the arithmetic fundamental theorem. The conception asserts that integers larger than one may be expressed as prime products in ways that are unique with regards to the order of the factors of primality. For instance, 23244 is equivalents to 149 • 13 • 3 • 22. In the example, it is evident that similar prime factors may transpire multiple times. It may be decomposed as follows: n = p1 • p2 • p3• p4• p5• p6... • pt. The concept implies that factorization of prime numbers is identical except in the ordering of the constituent factors. Therefore, despite the numerous algorithms as far as prime factorization is concerned, the results are identical. The early Greeks did not consider one as a number, as well as prime. However, by the Renaissance and Middle Age, most mathematicians began to regard one as a prime number. Derrick Norman included one in his list of prime numbers. During the twentieth century, however, that has changed because one has assumed a special category referred to as a unit.

PRIME FACTORIZATION PROOF

The prime factors, in the number theory, are prime numbers that divide integers precisely without a remainder. The prime factorization of integers is a list of prime factor numbers and their resulting multiplicities, which are often in powers. For instance, 420 is equivalent to 2*2*3*5*7, also expressed as 22*3*5*7, whereby 5, 3 and 2 have multiplicities of one, two and three, respectively. The concept of gcd of two integers will used in proving that when p is a prime and p | mb, then p | m or p | n. The key step in the theorem is proving the above statement.

Let gcd (r, n) = max {d | r and d | n}, unless both r and n are zero whereby gcd (0, 0) is equivalent to zero. For instance, gcd (1, 2) is equivalent to one, gcd (6, 27) is equivalent to three and gcd (0, m) is equivalent to m. When m is not equivalent to zero, the gcd is existent primarily because when d |m then d is less than or equivalent to | m|, and | m| is the only existing positive integer less than or equivalent to | r |. Additionally, gcd will exist when n is not equivalent to zero. For any numbers r and n, the gcd (r, n) will be equivalent to gcd (n, r), gcd (±r, ±n), gcd (r, n – r), and gcd (r, n + r). It proves that gcd (r, n) is equivalent to gcd (r, n –r) because other cases are already proved using a similar approach.

EUCLID'S PROOF

The tenets of Euclid's theorem is that the two, there, five, seven, eleven, thirteen ... series of prime number succession or sequence never ends. The statement is in honor of Euclid, a mathematician of the ancient Greek. The proof considers any predetermined set of S prime numbers. The idea is to take into consideration the product of numbers concerned plus one.

N 1+ Π pєS p•

Just as other integers, the term N is certainly divisible by, at minimum, one prime and itself. Of the prime divisors of N, none is a member of the predetermined set, S, of prime numbers because of the remainder left behind. Consequently, the fixed sets of prime extend to larger predetermined set of prime numbers. Most often

it is erroneously suggested that Euclid's proof is grounded on the supposition that the initial set comprises solely of prime numbers, resulting to contradictions, or that it consists of smaller primes as opposed to arbitrary fixed sets of prime numbers. Today, nth Euclid number is considered to be the multiple of the least n prime numbers plus one.

EULER'S PROOF

The Euler's proof makes use of the sum of the reciprocals of prime numbers: S = ½ + 1/3 + 1/5 + 1/7...1/p. The sum becomes bigger than arbitrary real numbers as long as p is significantly big. The scenario demonstrates that primes are infinitely many, because otherwise the sum would only grow up to the point where the ultimate prime is achieved. The S (p) growth is quantified in the second theorem of Mertens. For comparison purposes, the sum S = ½2 + 1/ (32) + 1/ (52) + 1/ (72...1/ (n2) does not lead to infinity as n approaches infinity. In that case, the frequency of occurrence of primes is higher compared to the squares of ordinary numbers. The Brun's theorem asserts that the sum of the twin primes' reciprocals, (1/3 + 1/5) + (1/5 + 1/7) + (1/7 + 1/11) + (1/11 + 1/13) is finite.

APPLICATIONS

For years, the number theory and the concept of primality are considered as the canonical illustrations of pure mathematics. These concepts can be used in the development of cryptography algorithms, and most notably in the generation of pseudorandom numbers and hash tables. Modulo arithmetic alters arithmetic using numbers {0, 1, 2, 3.....n-1}, with modulus being a fixed natural integer. Calculating products, sums, and differences is executed as usual. However, when handling a negative integer or numbers greater than n-1, the modulus is substituted by the remainder after being divided by n. For example, when n is equivalent to seven, the sum of five and three is one rather than eight because eight divided by seven has one as its remainder. Therefore, it can be said that the sum of five and seven is congruent to one modulo eleven. The statement is denoted as 5 + 7 = 1(mod 11). At the same time the sum of six and one is 0 (mod 7). The standard properties of multiplication and addition are still applicable in modular arithmetic.

A range of mathematical domains apply prime numbers, with Sylow theorems being some of the areas of application. According to the conception, when G is a predetermined set and pn is the greatest power of p, a prime that subdivides the ordering of G, then the finite group has a subset of order pn. In addition, group consisting of prime order are considered as cyclic. Several algorithms of public-key cryptography, including the RSA, are founded on big prime numbers. This is based on the assumption that it is relatively easier and efficient to multiply two large integers (m and an) than to calculate m and n when only the product (mn) is predetermined. The evolutionary strategy applied by the cicadas uses the concept of primality.

CONCLUSION

As it has been demonstrated, the concept of primality is profound in the number theory.

Prime numbers find many uses in different scientific areas including cryptography. One of the most interesting assertions around prime numbers is that every positive integer can be uniquely expressed as a product of prime numbers, although the assertion is extremely difficult to prove. Prime numbers exhibit unique characteristics, as they seem to grow, just like weed grows, among natural numbers, obeying no other law other than that of chance.