Combinatorial Primality Test

Maheswara Rao Valluri
School of Mathematical and Computing Sciences
Fiji National University, Derrick Campus, Suva, Fiji.
maheswara.valluri@fnu.ac.fj

Abstract

This paper provides proofs of the results of Laisant - Beaujeux: (1) If an integer of the form $n = 4k + 1$, $k > 0$ is prime, then $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv 1(mod\, n), m = \frac{n-1}{2}$, and (2) If an integer of the form $n = 4k+3$, $k \geq 0$ is prime, then $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv -1(mod\, n), m = \frac{n-1}{2}$. In addition, the author proposes important conjectures based on the converse of the above theorems which aim to establish primality of n. These conjectures are scrutinized by the given combinatorial primality test algorithm which can also distinguish patterns of prime n whether it is of the form $4k + 1$ or $4k + 3$.

1 Introduction

A positive integer n is to be called a *prime* if it has only divisor of 1 and itself, otherwise n is called a *composite*. There are, by Euclid's theorem (about 350BC) infinitely many primes. Primes are mainly categorized into three patterns of the form $4k + 1, 4k + 2$ and $4k + 3$. The integer 2 is only the even prime that is of the form $4k + 2$. Primes of the form $4k + 1$ are $5, 13, 17, 29, 37, 41, ...$etc., and of the form $4k + 3$ are $3, 7, 11, 19, 23, 31, 43, ...$etc. There are also many other patterns of primes which are listed on the Online Encyclopedia Integer Sequence (OEIS). Readers are referred to search for any prime pattern on the OEIS [9]. Primes are building blocks for any composite. A composite is composed by primes in some order. For instance, 143 is composed by primes, 11 and 13. It is clear that one can easily compose any composite by multiplication of primes but decomposition of the composite is a challenging computational problem, so called the *integer factorization problem*. The RSA cryptosystem [11] was constructed based on the *integer factorization problem*. This is an NP-intermediate problem on a classical computer. However, this problem can be reduced to a polynomial time problem on a quantum computer due to Shor's algorithm [12].

In 1808, a French mathematician, Christian Kramp introduced the notation ! for factorials. The *factorial* of n is the product of all positive integers less than or equal to n. In Kramp's notation, $n! = n(n-1)(n-2)...3.2.1.0!$. By convention, one defines $0! = 1! = 1$. Suppose that a set S contains n distinct objects. Then, one obtains that there are exactly $n!$ permutations of S. If there are r objects chosen from the set S that contains n objects, this is equal to $\begin{pmatrix} n \\ r \end{pmatrix} = \frac{n!}{(n-r)!r!}$. We now recall the Wilson's theorem [6, Theorem 80] which is based on factorials.

Theorem 1. (Wilson's Theorem) *An integer n is prime if and only if* $(n-1)! \equiv -1(mod\, n)$.

The Wilson's theorem is not helpful to employ in practice, since the Wilson's primality test requires $O(n)$ operations to compute it. Later, a variant of the Wilson's theorem was discovered in 1961 [8] which is stated as follows:

Lemma 1. *Let $n = 4k + 1$ be a prime. Then $(\frac{n-1}{2})! \equiv (-1)^v (mod\, n)$, where v is the number of quadratic non-residue less than $\frac{1}{2}n$.*

We recall the Fermat's Little Theorem and Fermat-Euler Theorem [3] which are used to prove the main theorems in the next section.

Theorem 2. (Fermat's Little Theorem) *Let n be a prime and integer a is a primitive such that $gcd(a, n) = 1$. Then, $a^{n-1} \equiv 1(mod\, n)$.*

The Fermat's Little Theorem is a probablistic primality test. The origin of Carmichael numbers is based on the cases where the Fermat's Little Theorem fails [2]. However, the Fermat's Little Theorem became a basis to establish many primality tests.

There is a special case of the Fermat's Little Theorem which is given as follows:

Theorem 3. (Fermat-Euler Theorem) *If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1(mod\, n)$.*

Remark 1. For n is a prime, we have $\phi(n) = n - 1$.

The purpose of the paper is to provide proofs of the results of Laisant-Beaujeux [4, page 277]:

(1) If an integer of the form $n = 4k + 1$, $k > 0$ is prime, then $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv 1(mod\, n), m = \frac{n-1}{2}$.

(2) If an integer of the form $n = 4k + 3$, $k \geq 0$ is prime, then $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv -1(mod\, n), m = \frac{n-1}{2}$.

Furthermore, this paper conjectures statements based on the converse of the above theorems, and also presents an algorithm for combinatorial primality test. This test requires $O(2^{\frac{(n-1)}{2}})$ operations for its primality.

2 Main Results

This section presents proofs of the results of Laisant - Beaujeux [4, page 277].

Theorem 4. *If an integer of the form $n = 4k + 1$, $k > 0$ is prime, then $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv 1(mod\, n), m = \frac{n-1}{2}$.*

Proof. Suppose that n is prime of the form $4k + 1$. Then, n has a primitive root. Let a be a primitive root modulo n. Then the integers $1, a, a^2, ..., a^{n-2}$ are congruence modulo n, to some order, $1, 2, 3, ..., n-1$. Hence, we have $(n-1)! \equiv 1 \cdot a \cdot a^2 \cdots a^{n-2} (mod\, n) \equiv a^{\frac{(n-2)(n-1)}{2}} (mod\, n)$. Consequently, we have $m! \equiv a^{\frac{(n-1)(n+1)}{8}} (mod\, n)$.

And,

$$\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv \frac{(n-1)!}{[(\frac{n-1}{2})!]^2} \equiv \frac{a^{\frac{(n-2)(n-1)}{2}}}{a^{\frac{(n-1)(n+1)}{4}}} \equiv a^{\frac{(n-1)(n-5)}{4}} (mod\, n).$$

To analyze further the expression, we employ $n = 4k + 1$, where k is a natural number. As $k < 4k = n - 1$, then $a^k \not\equiv 1 (mod\, n)$. However, $a^{4k} \equiv a^{n-1} \equiv 1(mod\, n)$, by Fermat's Little Theorem. As $(a^k)^4 \equiv a^{4k} \equiv 1(mod\, n)$, then $a^{2k} \equiv \pm 1(mod\, n)$, So $a^k \equiv -1(mod\, n)$.

Hence,

$$\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv a^{\frac{(n-1)(n-5)}{4}} \equiv a^{\frac{(4k+1-1)(4k+1-5)}{4}} \equiv (a^k)^{4k-4} \equiv (-1)^{4(k-1)} \equiv 1(mod\, n).$$

Example 1. For prime $n = 17$, $\begin{pmatrix} 16 \\ 8 \end{pmatrix} \equiv 1(mod\, 17)$ and for composite $n = 27$, $\begin{pmatrix} 26 \\ 13 \end{pmatrix} \equiv 11 \not\equiv 1(mod\, 27)$.

Theorem 5. *If an integer of the form $n = 4k + 3$, $k \geq 0$ is prime, then* $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv -1(mod\, n), m = \frac{n-1}{2}$.

Proof. Extracting from the above proof,

$$\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv a^{\frac{(n-1)(n-5)}{4}} (mod\, n)$$

also holds for this case. To analyze the expression, we use $n = 4k + 3$, where k is a natural number. As $k < 2(2k + 1) = n - 1$, then $a^k \not\equiv 1(mod\, n)$. However, $a^{2(2k+1)} \equiv a^{n-1} \equiv 1(mod\, n)$, by Fermat's Little Theorem. As $a^{4k+2} \equiv a^{(n-1)} \equiv 1(mod\, n)$, then $a^{2k+1} \equiv -1(mod\, n)$.

Hence,

$$\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv a^{\frac{(n-2)(n-1)}{4}} \equiv a^{\frac{(4k+3-1)(4k+3-5)}{4}} \equiv a^{\frac{(4k+2)(4k-2)}{4}}$$

$$\equiv a^{(2k+1)(2k-1)} \equiv (-1)^{(2k-1)} \equiv -1(mod\, n).$$

Example 2. For $n = 31$, $\begin{pmatrix} 30 \\ 15 \end{pmatrix} \equiv -1(mod\, 31)$.

Remark 2. Algorithm 1 checks the validity of the converse of the theorem 4 and 5. Thus, the author proposes Conjectures 1 and 2.

Conjecture 1. *If* $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv 1(mod\, n), m = \frac{n-1}{2}$, *then $n = 4k + 1$ is a prime.*

Conjecture 2. *If* $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv -1(mod\, n), m = \frac{n-1}{2}$, *then $n = 4k+3$ is a prime, except for $n = 5907$.*

Remark 3. It was found that the Conjecture 2 fails at $n = 5907$. Note that the composite numbers that satisfy the Conjecture 2 are Laisant - Beaujeux pseudoprimes. These numbers could be rarer than Carmichael numbers.

3 Combinatorial Primality Test

An important challenge in number theory is to efficiently determine whether an integer n is prime or composite. Miller-Rabin Primality Test [7,10] and Elliptic Curve Primality Test [5] are well known efficient primality tests. However, these are probabilistic primality tests. In 2002, Agrawal et al., discovered an unconditional deterministic primality test [1] which requires $O((log\, n)^{6+\epsilon})$ steps on a classical computer. The Wilson's primality test is also a deterministic test but it is not computationally efficient. In the algorithm 1, we provide a primality test based on combinatorics which requires $O(2^{\frac{(n-1)}{2}})$ steps in order to test whether n is prime or composite.

Algorithm 1 Algorithm for Combinatorial Primality Test

Input : An integer n
Runtime : $O(2^{\frac{(n-1)}{2}})$ operations
Procedure :
1: Compute $\begin{pmatrix} n-1 \\ m \end{pmatrix} \equiv r(mod\, n), m = \frac{n-1}{2}$
2 : **if** $r = 1$, **then**
3: Declare n is prime of the form $4k + 1$
4: **else if** $r = -1$, **then**
5: Declare n is prime of the form $4k + 3$
6: **else**
7: Declare n is composite.
8: **end if**
9:**end if**
Output : Declare whether the integer n is prime or composite

4 Conclusion

This paper has provided proofs of the results of Laisant - Beaujeux on primality and proposed corresponding conjectures based on their converse statements. Furthermore, the paper has presented an algorithm for combinatorial primality test which checks the validity of the conjectures. The test requires $O(2^{\frac{(n-1)}{2}})$ operations to test whether n is prime or composite. It is also noted that this test could also distinguish patterns of prime whether it is of the form $4k + 1$ or $4k + 3$.

Acknowledgement

The author of the paper thanks Oliver Knill for his comments and suggestions on the Conjecture 2.

References

[1] Agrawal, M., Kayal, N., and Saxena, N., "PRIMES is in P", Ann. of Math., 160(2), 781–793 (2004).

[2] Carmichael, R.D. Note on a number theory function. Bull. Amer. Math. Soc., 16:232–238, 1910.

[3] Crandall, R., and Pomerance, C., "Prime Numbers: A Computational Perspective", Springer-Verlag, New York (2001).

[4] Dickson, L.E., "History of the theory of numbers. Vol. I: Divisibility and primality", New York: Dover Publications, ISBN 978-0-486-44232-7, MR 0245499, Zbl 1214.11001(1919).

[5] Goldwasser, S.; Kilian, J. "Primality Testing Using Elliptic Curves", Journal of the ACM 46(4), 450-472 (1999). MR1812127 (2002e:11182).

[6] Hardy, G.H., and Wright, E.M., "An Introduction to the Theory of Numbers", Oxford University Press, 4th Edition, (1960).

[7] Miller, G.L., "Riemann's hypothesis and tests for primality", Journal of Computer and System Sciences, 13 (3): 300–317 (1976).

[8] Mordell, L. J., "The congruence $(p - 1/2)! \equiv \pm 1 (mod\, p)$". Amer. Math. Monthly 68, 145-146 (1961).

[9] Online Encyclopedia Integer Sequence, http://oeis.org/

[10] Rabin, M.O., "Probabilistic algorithms for testing primality", J. Number Theory 12, 128-138 (1980).

[11] Rivest, R., Shamir, A, and Adleman, L., "A method for obtaining digital signature and public-key cryptosystem", Communication of the ACM, 21(2), 120-126 (1978).

[12] Shor, P.W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing, 26(5), 1484-1509 (1997).