Generalization of Fermat's Little Theorem

MJ Sanada Khumanthem[1] and Kh. Manglem Singh[2]
[1,2]Department of Computer Science & Engineering, MIT Manipur

Abstract
There are different methods to decide whether an integer is prime. Fermat's little theorem is the generalization of $2^{n-1} \equiv 1 \, mod \, n$, while AKS test is the generalization of Fermat's little theorem. Fermat's little theorem is probabilistic method, while AKS test is deterministic one.
The first method is faster, but not guaranteed, and the second one is guaranteed, but slow.

Keywords : Prime, Fermat's little theorem, AKS test, Pascal' triangle, Binomial expansion

I. Introduction

Binomial expansion of $(x+a)^n$ contains $n+1$ terms with the first and the last coefficients equal to 1 and other coefficients greater than 1.

$$(x+a)^n = C(n,0)x^n + C(n,1)x^{n-1}a + C(n,2)x^{n-2}a^2 + \cdots + C(n,n)a^n$$

$$= \sum_{i=0}^{n} C(n,i)x^{n-i}a^i \qquad (1)$$

$$\text{where} C(n,i) = \frac{n!}{i!(n-i)!} \qquad (2)$$

If $x = 1$and $a = 1$, then $\sum_{i=0}^{n} C(n,i) = 2^n$, that is, the sum of all coeffients is equal to 2^n.
On the other hand, if $x = 1$and $a = -1$, then $C(n,0) - C(n,1) + C(n,2) - \cdots + (-1)^n C(n,n) = 0$. Since sum of all coefficients is equal 2^n and their difference is 0. Rearranging the terms, we have

$$C(n,0) + C(n,2) + \cdots = C(n,1) + C(n,3) + \cdots = 2^{n-1} \qquad (3)$$

If n is odd, then the total number of terms in the expansion is even so the total numbers of terms for odd and even coefficients are same and each is equal to $\frac{n+1}{2}$. The coefficients for binomial expansion are shown below in Figure 1 as Pascal's triangle:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 120 495 792 924 792 495 120 66 12 1

Figure 1 Pascal's triangle.

All the prime numbers except 2 are odd primes and the total number of coefficients in binomial expansion is even if n is an odd integer. These coefficients are symmetrical in Pascal's triangle and so a maximum of only the first half coefficients is sufficient for analysis. Sum of the first half coefficients for odd n is

$$C(n,0) + C(n,1) + C(n,2) + \cdots + C(n,\tfrac{n+1}{2}) = 2^{n-1} \qquad (4)$$

Each coefficient except the first and the last is divisible by n if n is prime. Therefore the number 2^{n-1} when divided by n gives a remainder 1 if n is prime, that is

$2^{n-1} \equiv 1 \; mod \; n$ (5)

II. Fermat's Little Theorem

If n is prime and $gcd(a, n) = 1$, then

$a^{n-1} \equiv 1 \; mod \; n$ (6)

This is, $a^{n-1} \equiv 1 \; mod \; n$ is equal to $2^{n-1} \equiv 1 \; mod \; n$ in Equation (5) for $a = 2$.

Let us take some examples. Take $n = 391$and $a = 2$.

$2^{391-1} \; mod \; 391 = 285$reveals that $n = 391$ is composite.

Take another $n = 397$and $a = 2$.

$2^{397-1} \; mod \; 397 = 1$reveals that $n = 397$ is prime.

Take another $n = 341$and $a = 2$.

$2^{341-1} \; mod \; 341 = 1$indicates that $n = 341$ is prime, but 341 is composite as $341 = 11 \times 31$.

This is due to the fact that all coefficients in binomial expansion are not divisible by n, but their sum excluding the first and last coefficients may be divisible by n for some values of n. Such exception shows that $2^{341-1} \; mod \; 341 = 1$.

To test a number n for primality, values for a from the set $\{2,3,4, \ldots, n-1\}$ may be used. If any one of these values yields anything other than 1, it can be concluded that n is composite.

Putting $a = 3$, $3^{341-1} \; mod \; 341 = 56$ reveals that $n = 341$ is composite. Sometimes neither $a = 2$ nor $a = 3$ nor some other values of a will reveal that n is composite.

Take another example, $n = 1729$.

$2^{1729-1} \; mod \; 1729 = 1$and $3^{1729-1} \; mod \; 1729 = 1$. We cannot draw an immediate conclusion that $n = 1729$ is prime, because, n can be factored as $n = 1729 = 7 \times 13 \times 19$.

A composite number n that passes Fermat's little theorem is called a Carmichael number. For examples, 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585 etc. are Carmichael numbers. Total number of Carmichael numbers less than 10^{21} is 20,138,200, that is, about 0.000000000002% of the total. Thus probability that an integer will be a Carmichael number is extremely low.

III. AKS Test

Agrawal, Kayal and Saxena developed AKS test that was named after them in 2002 [2] and their method is based on the generalization of Fermat's little theorem. Each term in the denominator of binomial coefficient in Equation (2) is strictly less than n. If n is a prime, it cannot be factored, but the other terms in numerator such as 2,3,4,…,$(p-1)$ have common factors with all those terms in denominator. Therefore n divides $C(n, i)$ if n is prime.

$n$is prime if and only if [1] the following congruence holds.

$(x + a)^n \equiv x^n + a \; mod \; n$ (7)

Let us take some examples. Take $n = 3$and $a = 2$. Then

$$\begin{aligned}(x+2)^3 \; mod \; 3 &\equiv x^3 + 6x^2 + 12x + 8 \; mod \; 3 \\ &\equiv x^3 + 2 \; mod \; 3\end{aligned}$$

which is $x^n + a$. So the identity holds and we conclude that $n = 3$ is prime.

Take $n = 7$and $a = 1$. Then

$$(x+1)^7 \bmod 7 \equiv x^7 + 7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x + 1 \bmod 7$$
$$\equiv x^7 + 1 \bmod 7$$

Since the identity holds, $n = 7$ is prime.

We can verify that $n = 6$ is composite.

$$(x+1)^6 \bmod 6 \equiv x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 \bmod 6$$
$$\equiv x^6 + 3x^4 + 2x^3 + 3x^2 + 1 \bmod 6$$

Since the congruence (7) is not satisfied, $n = 6$ is composite.

But there are too many coefficients in binomial expansion of $(x+a)^n$ and this way of testing may not be practical.

AKS test is for ensuring faster result to test whether $n$is prime or composite [3]. Their method works not only with $mod\ n$, but also mod a polynomial $x^r - 1$, where r is a reasonably smaller prime. Instead of computing $(x+a)^n$, AKS test computes the remainder when $(x+a)^n$ is divided by $x^r - 1$. It has only $r+1$ terms. AKS test provides restriction, which guarantees that the congruence $(x+a)^n \equiv x^n + a\ (mod\ x^r - 1, n)$ cannot hold for composite n. Their algorithm is given below [1,2] :

Input: integer $n > 1$.

1. If $n = a^b$ for $a \in N$and $b > 1$, output COMPOSITE.
2. Find the smallest r such that $O_r(n) > log^2 n$.
3. If $1 < (a, n) < n$ for some $a \le r$, output COMPOSITE.
4. If $n \le r$, output PRIME.
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   If $(x+a)^n \neq x^n + a\ (mod\ x^r - 1, n)$, output COMPOSITE;
6. Output PRIME.

where

- $O_r(n)$is the order of n modulo r, that is, the smallest value k such that $n^k = 1\ mod\ r$.
- $\phi$is Euler phi function.
- log denotes a base 2 logarithm.
- $(mod\ x^r - 1, n)$means divide by the polynomial $x^r - 1$ and take the remainder.

Let us an example. Take $n = 77$.

1. $n = 77$cannot be expressed in the form a^b, where a is an integer and b is another integer. A conclusion cannot be drawn at this point.
2. Find the smallest r such that $O_r(n) > log^2 n = (\log 77)^2 \approx 39.27$.

The order of $n = 77$ modulo r should be 40 or higher. The order of an element divides the order of the group, so we need a group with 40 or more elements. We can start with $r = 41$, since the multiplicative group of integers modulo 41 has 40 elements. The order of 77 mod 41 is 41.

3. Next check if $1 < (a, 77) < 77$ for some $a \le r = 41$.

This happens for $a = 7$ (and other values), so we stop and declare that 77 is composite.

Take another example, $n = 29$.

1. $n$cannot be expressed in the form a^b, so a conclusion cannot be drawn here.
2. Find the smallest r such that $O_r(n) > log^2 n = (\log 29)^2 = 23.6$.

We need the order of 29 modulo r to be 24 or higher. We find that $r = 31$ is the smallest possibility. The order of 29 mod 31 is 31.

3. Next check if $1 < (a, 29) < 29$ for some $a \le r = 31$. It is not there.
4. Because $n < r$, we conclude n is prime.

IV. Conclusions

There are different methods to decide whether an integer is prime. Fermat's little theorem is the generalization of $2^{n-1} \equiv 1 \; mod \; n$, while AKS test is the generalization of Fermat's little theorem. Fermat's little theorem is a probabilistic method and AKS test deterministic one.

References

[1] C.P. Bauer, Secret history, the story of cryptology, CRC Press, 2013.
[2] M. Agrawal, N. Kayal and N. Saxena, PRIMES is in P, Ann. of Math., 160(2), 781-793, 2004.
[3] S. Aaronson, The prime facts: from Euclid to AKS, 2003, https://www.scottaaronson. com/writings/prime.pdf (accessed on 07/07/2019).