Generalization In primality Testing

M.Sc :Haythem Ghani Ahmad
Diyala University
College of Science
Mathematic Dep.

Abstract

There are several methods to test the number whether it is prime number or not (composite). One of these methods by using Libnez's theorem or Willson's theorem.
This paper is new contribution represented the general mathematical form for this kind of primality testing .

المستخلص

توجد العديد من الطرق لأختبار العدد هل هو أولي أم لا(مركب). واحدة من هذه الطرق هي باستخدام نظرية لبنز أو نظرية ولسن. في هذا البحث نجد الصيغة الرياضية العامة لهذا النوع من الاختبارات.

1. Introduction:

The factoring numbers is so hard, "is n prime?" is a much easier question to answer than the more complicated quotations, "what are the factors of n?" there are several probabilistic primality testing.
Libnez proposed his theorem to test the prime number "if p is prime number then $(p-2)! \equiv 1 \pmod{p}$" [1]. And Willson propose his

theorem to test the prime number "if p is prime number then
$(p-1)! \equiv -1 \pmod p$" [2].
Haythem in his M.Sc thesis proposed that "if $p \geq 3$ is a prime number
then
$(p-3)! \equiv \frac{p-1}{2} \pmod p$" [3].
The aim of this paper is to provide new mathematical idea according to
the three previous theorems and proposed the general form of them .
This paper contains two sections in addition to the first section, section
two contains new proposed results and section three contains the conclusion.

2.New results in primality testing :

In this section great efforts have been concentrated on finding new results
primality testing, The three theorems above are considered as a basic key
for the new results.

2.1. Result 1:

If $p>4$ is prime number then
$6(p-4)! \equiv 1 \pmod p$

Proof:

By libnez theorem:-

$$(p-2)! \equiv 1 \pmod p$$
$$(p-2)(p-3)(p-4)! \equiv 1 \pmod p$$
$$(p-5p+6)(p-4)! \equiv 1 \pmod p$$
$$(p-4)! \equiv \frac{1 \pmod p}{p(p-5) \bmod p + 6 \bmod p}$$

$6(p-4)! \equiv 1 \pmod p$

(Notice the relationship between 4&6)

2.2. Result 2:

If $p \geq 5$ is prime number then

$24(p-5)! \equiv (p-1) \pmod p$

Proof:

By using the theorem:

$(p-3)! \equiv \frac{p-1}{2} \pmod p$

$(p-3)(p-4)(p-5)! \equiv \frac{p-1}{2} \pmod p$

$2(p^2-7p+12)(p-5)! \equiv (p-1) \pmod p$

$2(p-5)! \equiv \frac{(p-1) \pmod p}{p(p-7) \bmod p + 12 \bmod p}$

$24(p-5)! \equiv (p-1) \pmod p$

(Notice the relationship between 5&24)

2.3 Result 3:

If $p>6$ is prime number then:-

$120(p-6)! \equiv 1 \pmod p$

Proof:

By result no.1:

$6(p-4)! \equiv 1 \pmod p$

$6(p-4)(p-5)(p-6)! \equiv 1 \pmod p$

$6(p^2-9p+20)(p-6)! \equiv 1 \pmod p$

$6(p-6)! \equiv \frac{1 \pmod p}{p(p-9) \bmod p + 20 \bmod p}$

$120(p-6)! \equiv 1 \pmod p$

(Notice the relationship between 6&120)

2.4 Result 4:

If $p \geq 7$ is prime number then:

$720(p-7)! \equiv (p-1) \pmod{p}$

Proof :

By result 2:

$24(p-5)! \equiv 1 \pmod{p}$

$24(p-5)(p-6)(p-7)! \equiv (p-1) \pmod{p}$

$24(p^2-11p+30)(p-7)! \equiv (p-1) \pmod{p}$

$$24(p-7)! \equiv \frac{(p-1) \pmod{p}}{p(p-11) \bmod p + 30 \bmod p}$$

$720(p-7)! \equiv (p-1) \pmod{p}$

(Notice the relationship between 7&720)

Note:

1- We can go ahead in these results and prove it for any number more than 7.

2- The relation between the pair in any result is:
Let us say the first number is n then the second one must be $(n-1)!$

3 Conclusions:

We can obtained from all these theorems and results and from the relationship between the pair of numbers the general form to them which is:

$(n-1)!(p-n)! \equiv 1 \pmod{p}$ if n is even number

$(n-1)!(p-n)! \equiv -1 \pmod{p}$ if n is an odd number

References:

[1]Allenby and Redfern "Introduction to number theory with computing" 1989.

[2] Schroeder "number theory in Science and communication" Second edition, 1986.

[3] Haythem G. Ahmad "mathematical Analysis of RSA and Rabin cryptosystems" Al_mustansiria University, M.Sc 1999.