American Journal of Computational Mathematics, **2013, 3, 59-60**
http://dx.doi.org/10.4236/ajcm.2013.31009 Published Online March 2013 (http://www.scirp.org/journal/ajcm)

Primality Test

Gabriele Martino
Via Cornelia, Rome, Italy
Email: martino.gabri@gmail.com

Received October 12, 2012; revised November 27, 2012; accepted December 5, 2012

ABSTRACT

In this paper we will give an algorithm that in the worst case solve the question about the primality of a number in $O\left(\frac{\sqrt{N}}{2}\right)$ but that gives better result if the number is not prime (constant operation). Firstly, we will introduce an equation on which are based not prime numbers. With this equation it is possible to deduce the prime number that generates a not prime number and to establish an equation in which if exists a certain integer the number is not prime and therefore vice versa to deduce if it is prime.

Keywords: Prime Numbers; Equation

1. Introduction

There exist different primality test [1,2]. The most simple is to check all the divisors of a given number *N*. If the number has some divisor with remainder 0, then the number is not prime. Another method uses the Wilson Theorem, but it is quiets inefficient. Some methods certificate the primality with some probability. Those methods can assure certify always if a number is prime and in some case certify than a number is prime even if it is not. Those methods take a value *a* from a set previously calculated. One example is the Miller Rabin Test. Given a number *n*, we choose a number *a* and state the even number $n-1=2^s\cdot d$ with *s* positive integer and *d* positive odd integer. If $a^d \not\equiv 1$ (mod *n*) and $a^{2rd} \not\equiv -1$ (mod n) the number is composite. As deterministic, the most successful algorithm is the Manindra Agrawal, Neeraj Kayal, and Nitin Saxena Test [3]. The algorithm is based on the equation $(x+a)^p$ mod $p=(x^p+a)$ mod *p* for *a*, *p* prime and for each *x*. They were able to reasonably speed up the expansion of the binomial terms. To do this they state that the formula is valid also for the polynomial divided by x^r-1 with *r* small prime: $(x+a)^p$ mod $(p,x^r-1)=(x^p+a)$ mod (p,x^r-1). In this way the remainder has only *r* + 1 terms.

An Equation for Not Prime

The algorithm is based on the fact that a number is not prime when is even or when it has a form of the kind $n=p^2+2\cdot k\cdot p$ where *n* is the generated number, *p* is an integer prime >1 and $k=0,1,2,\cdots$. Therefore it is necessary to solve the equation

$$n=p^2+2\cdot k\cdot p \tag{1}$$

with variable *p* that gives the positive solution

$$p=\frac{-4k+\sqrt{4\cdot k^2+4\cdot n}}{2}=-2+\sqrt{k^2+n} \tag{2}$$

In general we have

$$\frac{n-p^2}{2\cdot p}=k \tag{3}$$

If *k* is an integer for a certain prime the number is generated. The set of primes is in the set of odds. If a condition is valid for the odds we can assert that it is valid for the prime and therefore if *k* is integer for an odd number is integer for a prime and therefore the number is generated.

2. Method

It is based on statement (3)

```
number
isprime
$isprime = true$
if number mod 2 == 0 then
    $isprime = false$
end if
for $odd = 3$, $odd < \sqrt{N}$ And $isprime$, $odd = odd + 2$
    if $\frac{(number - odd^2)}{2\cdot odd}$ integer then
        $isprime = false$
    end if
end for
```

return isprime.

3. Computational Complexity

The method requires $O\left(\frac{\sqrt{N}}{2}\right)$.

4. Results

The test has been done with

- Asus notebook
- Intel i7 processor
- 4 GB Ram
- Java Programming Language
- Windows 7 OS

For the number 99999989 that is prime the result is run: true BUILD SUCCESSFUL (total time: 0 seconds).

Not counted by the machine as significative.

5. Discussion

If we apply L'Hopital's rule [4] for the asymptotic analysis with $O\left(\log_2^3(N)\right)$ as confront term. We obtain derivative ratio

$$\lim_{x\to\infty} c\cdot\frac{\frac{\mathrm{d}\left(\log_2^3 x\right)}{\mathrm{d}x}}{\frac{\mathrm{d}\sqrt{x}}{\mathrm{d}x}} = \lim_{x\to\infty} c\cdot\frac{\left(\log_2 x\right)^2}{x^{1/2}},$$

where c is a constant value, so applying again L'Hopital's rule the ratio became $\lim_{x\to\infty} c\cdot\frac{\log_2 x}{x^{1/2}}$ and applying again $\lim_{x\to\infty} c\cdot\frac{1}{x^{1/2}}$ that goes to zero for x that goes to infinity. The result is not asymptotically better than $O\left(\log_2^3(N)\right)$, if we estimate the plot of the two functions we reach the asymptotic cross-over after the interval [2, 192823208].

REFERENCES

[1] S. Aaronson, "The Prime Facts: From Euclid to AKS," *Lecture Notes*, 2003.

[2] Wikipedia. http://en.wikipedia.org/wiki/Primality_test

[3] Wikipedia. http://en.wikipedia.org/wiki/AKS_primality_test

[4] Wikipedia. http://en.wikipedia.org/wiki/L'Hopital's Rule