A-020

An algorithm to reduce primality testing cost

Kaede Sasaki *

Abstract: We examined a new method giving a reduced set including all prime numbers. Our new method shows superior property by combining with other algorithms comparing with the original algorithms. We calculated prime numbers in the formular of the Pythagorean theorem. This equation expresses that the product of two numbers equidistant from one prime number equals the height squared. We can get prime numbers at a hypotenuse from the square root of the sum of the base squared and the height squared. The number that is odd and not multiple of three is chosen for the base in our method. Particularly we used a number one for the base. And, the height squared is always the product of a constant and an integer. All prime numbers and some series of composit numbers are calculated as integers. We exclude some composit numbers by combining with other algorithms.

Introduction

Primality testing is a practical method to get new prime numbers for applications [3] . Practically computable primality testing algorithms are progressing and more advancement is desirable. We examined a new method giving a reduced set including all prime numbers. Our new method shows superior property by combining with other algorithms comparing with the original algorithms.

Method

We calculated a new set including all prime numbers p in the formular of the Pythagorean theorem.

Theorem 0.1 (Pythagorean theorem) *This is a theorem about a right triangle of a hypotenuse p of a base b and a height h.*

$$p^2 = b^2 + h^2$$

$$(p - b)(p + b) = h^2$$

Theorem 0.2 *Let $p > 4$ be a prime number then $(p - 1)(p + 1)$ is a multiple of* 24.

This Polynomial expresses that product of two numbers equidistant from one prime number equals the height squared. We can get a prime number at a hypotenuse from the square root of the sum of base squared and height squared on the right triangle. The number that is odd and not multiple of three is chosen for the base in our method, particularly one is most suitable to find smaller prime numbers. And, the height is always the product of a constant and an integer. Prime numbers and some composit numbers are calculated as integers. We exclude some composit numbers by combining with other algorithms, F: Fermat [1], MR: Miller-Rabins [2].

Results

Table 1 shows the calculated results of the numbers p_K satisfies the equation with known prime numbers and those selected by other algorithms for comparisons. Prime numbers smaller than 32 and some composit numbers are calculated. We exclude some composit numbers by combining with other algorithms .

Table 2 shows the results of all prime numbers and some composit numbers calculated for $540 < p < 580$. Our method does not select a composit number 561 which are made output by other algorithms.

Our new method shows superior property by combining with other algorithms comparing with the original algorithms. Our method does not select some composit numbers which are made output by other algorithms.

Discussions

Known practical algorithms make selecton of composite numbers [1] . We showed some composite numbers, Carmichael numbers, were excluded by our new method. We expect our new algorithm use polynominal time for the calculation. We can reduce the primality testing cost by use of our new algorithm for the pre-processing selection of the testing numbers for the MR-algorithm, for example.

References

[1] William R Alford, Andrew Granville, and Carl Pomerance. There are infinitely many carmichael numbers. *Annals of Mathematics*, pages 703–722, 1994.

[2] Michael O Rabin. Probabilistic algorithm for testing primality. *Journal of number theory*, 12(1):128–138, 1980.

[3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

*(ndependent), kpoakh@gmail.com

Table 1: All prime numbers smaller than 32 and some composit numbers are calculated. We exclude some composit numbers by combining with other algorithms, F: Fermat [1] , MR: Miller-Rabins [2] .

odd	known	our	other		combined	
	p	p_K	p_F	p_{MR}	p_K—p_F	p_K—p_{MR}
3	3		3	3	3	3
5	5	5	5	5	5	5
7	7	7	7	7	7	7
9						
11	11	11	11	11	11	11
13	13	13	13	13	13	13
15						
17	17	17	17	17	17	17
19	19	19	19	19	19	19
21						
23	23	23	23	23	23	23
25		25				
27						
29	29	29	29	29	29	29
31	31	31	31	31	31	31

Table 2: All prime numbers and some composit numbers are calculated for $540 < p < 580$. Our method does not select a composit number 561 which are made output by other algorithms.

odd	known	our	other		combined	
	p	p_K	p_F	p_{MR}	p_K—p_F	p_K—p_{MR}
541	541	541	541	541	541	541
543						
545		545				
547	547	547	547	547	547	547
549						
551		551				
553		553				
555						
557	557	557	557	557	557	557
559		559				
561			561	561		
563	563	563	563	563	563	563
565		565				
567						
569	569	569	569	569	569	569
571	571	571	571	571	571	571
573						
575		575				
577	577	577	577	577	577	577
579						