REPORT
ON THE LARGEST KNOWN TWIN PRIMES

T. Csajbók, G. Farkas, A. Járai, Z. Járai and J. Kasza

(Budapest, Hungary)

Abstract. $16869987339975 \cdot 2^{171690} \pm 1$ are the largest known twin primes ever found.

1. Introduction

Prime numbers are of fundamental importance in number theory and cryptography. Many encryption methods are based on the theory of prime numbers. A famous unsolved problem of number theory is to prove that there are infinitely many twin primes, i.e. pairs of primes which differ by two. It is a serious challenge for the science of computational number theory to find large primes or to produce a huge number of primes.

2. Purposes

Our goal was to find large twin primes greater than the known ones. In order to reach this, we had to use high speed sieving methods and primality testing.

Our investigations were based on some theoretical conceptions described by K.-H. Indlekofer and A. Járai in the papers [1] and [2]. We used "triple-sieving". This method gave us a chance to find large Sophie Germain primes, too. The number p is called Sophie Germain prime, if p and $p + 2$ are both primes.

3. Results

We have been looking for twin and Sophie Germain primes by checking the primality of

$$p = (5775 + h \cdot 30030) \cdot 2^{171960} - 1$$

for $0 \leq h < 2^{33}$. Sieving out all candidates for which p, $p + 2$ or $2p + 1$ has a divisor less then 2^{48}, their number decreased from 8.5 billion to about 5 million. After testing about 370000 candidates we have found

$$16869987339975 \cdot 2^{171960} \pm 1,$$

which are 51779 of digits, to be primes.

At the time of submitting this paper the tests are going on in the expectation of finding large Sophie Germain primes, too. We are going to present details about the applied methods and computations elsewhere.

References

[1] **Indlekofer K.-H. and Járai A.,** Largest known twin primes and Sophie Germain primes, *Mathematics of Computation,* **68** (1999), 1317-1324.

[2] **Indlekofer K.-H. and Járai A.,** Largest known twin primes, *Mathematics of Computation,* **65** (1996), 427-428.

(Received September 9, 2005)

T. Csajbók, G. Farkas, A. Járai, Z. Járai and J. Kasza
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter s. 1/C
H-1117 Budapest, Hungary
`farkasg@compalg.inf.elte.hu`