Annales Univ. Sci. Budapest., Sect. Comp. 26 (2006) 181-183

REPORT ON THE LARGEST KNOWN SOPHIE GERMAIN AND TWIN PRIMES

T. Csajbók, G. Farkas, A. Járai, Z. Járai and J. Kasza
(Budapest, Hungary)

Abstract. The the largest known Sophie Germain prime is

$$137211941292195 \cdot 2^{171960} - 1$$

and the largest known twin primes are

$$100314512544015 \cdot 2^{171690} \pm 1.$$

Introduction

Last year we published the largest known twin prime pair in [2]. We continued the hunting for large prime combinations. Besides the twin primes we focused our attention to the Sophie Germain primes. An integer p is a Sophie Germain prime if p and $2p+1$ are simultaneously primes. As a matter of fact we can consider p and $2p+1$ as a Cunningham chain of length 2 of the first kind. A Cunningham chain of length k (of the first kind) is sequence of k primes, each which is twice the proceeding one plus one. A Cunningham chain of length k (of the second kind) is a sequence of k primes, each of which is twice the proceeding one minus one. This prime combinations play important role in the number theory and cryptography. For example J. Gonda points out an interesting fact in [1]: let us consider an RSA public key cryptographic algorithm, where p and q are odd primes, $n = pq$, e positive integer relatively prime to $\varphi(n)$. Then the cycling attack on the RSA is successful only in a very few cases if n is a product of only two factors of the same magnitude that are doubly Sophie Germain pairs (e.g. p and q are the first member of a Cunningham chain of length 3 of the first kind), and e is a primitive root with respect to $p-1$ and $q-1$ as moduli.

Results

We have found

$$100314512544015 \cdot 2^{171690} \pm 1,$$

which are 51780 of digits, to be a twin prime pair and

$$137211941292195 \cdot 2^{171960} - 1$$

to be a 51780 of digits Sophie Germain prime.

Since the goal of this paper exclusively was to report on the new world record, we are going to present details about the applied methods and computations elsewhere.

Acknowledgment. This work was carried out under the HPC-EUROPA project (RII3-CT-2003-506079) with the support of the European Community - Research Infrastructure Action under the FP6 "Structuring the European Research Area" Programme and by OTKA T043657.

References

[1] **Gonda J.,** The number of the modulo n roots of the polynomial $x^v - x^u$ and the RSA, *J. of Universal Computer Science,* **12** (2006), 1215-1228.

[2] **Csajbók T., Farkas G., Járai A., Járai Z. and Kasza J.,** Report on the largest known twin primes, *Annales Univ. Sci. Budapest. Sect. Comp.,* **25** (2005), 247-248.

(Received December 4, 2006)

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