LARGEST KNOWN TWIN PRIMES

KARL-HEINZ INDLEKOFER AND ANTAL JÁRAI

ABSTRACT. The numbers $697053813 \cdot 2^{16352} \pm 1$ are twin primes.

A search for large prime pairs of the form $(3 + 30h) \cdot 2^{16352} \pm 1$ was performed at the University of Paderborn, Germany in the framework of a project for parallel computing in computational number theory supported by the Heinz Nixdorf Institute, Paderborn. We used the arithmetic routines developed in this project for fast parallel and sequential computations with very large numbers. The search was done until the first large prime pair $697053813 \cdot 2^{16352} \pm 1$ was found. These numbers have 4932 digits starting with $1930880535\ldots$. To our best knowledge the earlier records were $1692923232 \cdot 10^{4020} \pm 1$ (4030 digit), $4655478828 \cdot 10^{3429} \pm 1$ (3439 digit) found by Dubner [1] and $1706595 \cdot 2^{11235} \pm 1$ (3389 digit) found by Parady, Smith, Zarantonello [3] in 1990. The search consisted of the following steps:

1. We started with the 2^{25} nonnegative values of h below 2^{25}. The exponent 16352 was fixed during the calculations.

2. Both the case $+1$ and the case -1 were sieved with factors from 7 up to 2^{37}. After sieving, 209571 candidates remained.

3. Using the probabilistic Miller–Rabin primality test (see Knuth [2, pp. 379–380]), the candidates were tested, first the $+1$ case and then the -1 case, until a "probable twin prime pair" was found.

4. This "probable twin prime pair" was tested with exact tests: the -1 case using a Lucasian test (see Riesel [5]) and the $+1$ case using the test of Brillhart, Lehmer and Selfridge and the test of Proth (see Ribenboim [4, pp. 37–40]).

The number $\pi_2(x)$ of twin primes below x is conjectured to be $\pi_2(x) \sim 2C_2 x / \ln^2(x)$ where $C_2 = \prod_{p>2}(1 - 1/(p-1)^2) \approx 0.66016\ldots$. Computer experiments support this conjecture: see Ribenboim [4, p. 202]. Here we test a sequence of numbers $N \pm 1$, $N = (h_0 + 30h) \cdot 2^n$, where n is a large but fixed natural number, h runs through the positive integers smaller than $2^{32}/30$, and where $h_0 \equiv 3 \bmod 30$, $n \equiv 0 \bmod 4$ or $h_0 \equiv 9 \bmod 30$, $n \equiv 1 \bmod 4$, or $h_0 \equiv 21 \bmod 30$, $n \equiv 3 \bmod 4$ or $h_0 \equiv 27 \bmod 30$, $n \equiv 2 \bmod 4$ is satisfied, because only in these cases is it true that $N - 1$ and $N + 1$ both are not divisible by 2, 3 and 5 and a simple exact Lucas test works for $N - 1$. Our experiments with a simple Maple® program show that $11/\ln^2 N$ is a good lower estimate for the probability that $N - 1$ and $N + 1$ both are primes for the range $N \leq 2^{512}$, where n is fixed and h runs up to $2^{32}/30$. If we assume that this approximation holds up to $N \approx 2^{16000}$, we get $\approx 1/11\,000\,000$ for

---

the lower density of such twin primes in this range. The amount of work is reduced drastically by sieving out the candidates which have a "small" prime divisor below some constant. This constant can be choosen between 2^{37} and 2^{41}.

The above twin primes were found in November, 1994. The test was running on several Sun® workstations with the SuperSPARC® processor of Texas Instruments with clock frequency from 33 MHz to 50 MHz. The low-level routines of the sieving, the multiplication routine for the tests and some other parts of the modular reduction were written in assembly language using the properties of the SuperSPARC processor. The multiplication routine uses Karatsuba's method (see Knuth [2, pp. 278–279]). Other parts of the program were written in C. The running time for one probabilistic test was ≈ 5 minutes for one number (33 MHz). The running time of the sieving was ≈ 8 day (33 MHz). The probabilistic test was performed for 63119 pairs altogether. We did not find any number which was not prime but passed the probabilistic test.

References

1. H. Dubner, *e-mail* (1994).
2. D. E. Knuth, *The art of computer programming*, Vols. 1–3, 2nd ed., Addison-Wesley, Reading, MA, 1981. MR **83i:**68003
3. B. K. Parady, J. F. Smith, and S. E. Zarantonello, *Largest known twin primes*, Math. Comp. **55** (1990), 381–382. MR **90j:**11013
4. P. Ribenboim, *The book of prime number records*, Springer-Verlag, Berlin and New York, 1989. MR **90g:**11127
5. H. Riesel, *Lucasian criteria for the primality of $N = h \cdot 2^n - 1$*, Math. Comp. **23** (1969), 869–875. MR **41:**6773

Universität GH Paderborn, FB 17, D-33095 Paderborn, Germany
E-mail address: k-heinz@uni-paderborn.de
E-mail address: jarai@uni-paderborn.de