Annales Univ. Sci. Budapest., Sect. Comp. 51 (2020) 69–75

JÁRAI'S PRIME HUNTING METHODS RELOADED (THE LARGEST KNOWN CUNNINGHAM CHAIN OF LENGTH 2 OF THE 2nd KIND)

Gábor Farkas (Budapest, Hungary)
Gábor Gévay (Berlin, Germany)
Péter Magyar (Szombathely, Hungary)
Béla Szekeres (Budapest, Hungary)

Dedicated to Professor Antal Járai on his 70th birthday

Communicated by Imre Kátai

(Received June 6, 2020; accepted July 8, 2020)

Abstract. Antal Járai established three research groups that dealt with computational number theory. Due to his brilliant ideas these teams were very successful. Moreover, he implemented the world's fastest arithmetic routines. He focused mainly on large prime combinations and his teams reached 19 world records from 1992 to 2014, namely they set the record for the largest known twin primes 9 times and Sophie Germain primes 7 times and a Cunningham chain of length 3 of the first kind. Furthermore they proved the primality of the largest known number of the form $n^4 + 1$ and a number which is simultaneously twin and Sophie Germain prime. In this paper, we report on a new project proving that Járai's methods and routines are cutting edge tools for effective manipulation of large numbers even in 2020. We are celebrating Prof. Járai's 70th birthday with his 20th world record.

Key words and phrases: Computational number theory, Cunningham chains, prime records, sieving methods.
2010 Mathematics Subject Classification: 11Y11.
The project has been supported by the European Union, cofinanced by the European Social Fund. EFOP-3.6.1.-16-2016-0023.

1. Introduction

In 1994 Járai joined a contest that started when S. Yates introduced the concept of "Titanic Prime" [16] which is a prime number with at least 1 000 decimal digits. The essence of this competition is finding large numbers and proving their primality. The contest welcomes both single numbers and curious prime combinations too, e.g. twin primes, Sophie Germain primes, Cunningham chains or primes in arithmetic progression. The exact rules, concepts, definitions and top lists can be found on C. Kaldwell's page [17].

We can have a look at Járai's world records in Figure 1, details are found in papers [2, 3, 4, 6, 15]. To understand it assume that p is a prime number. We say that p is a *twin prime*, if $p+2$ is also a prime. If $2p+1$ is a prime then p is a *Sophie Germain prime* and we speak about a *Cunningham chain of length* k *of the first kind* (notation: $Cck1$) if we have a sequence of primes

$$\{p, 2p+d, 4p+3d, 8p+7d, ..., 2^{k-1}p+(2^{k-1}-1)d\},$$

where $k \geq 2$ and $d=1$. This sequence is a *Cunningham chain of the second kind* (notation: $Cck2$) if $d=-1$ holds.

The Prime Number	Type	Date	Digits
Submitted by Karl-Heinz Indlekofer and Antal Járai			
$697053813 \cdot 2^{16352} - 1$	twin prime	November, 1994	4 932
$157324389 \cdot 2^{16352} - 1$	Sophie Germain prime	February, 1995	4 931
$470943129 \cdot 2^{16352} - 1$	Sophie Germain prime	February, 1995	4 932
$242206083 \cdot 2^{38880} - 1$	twin prime	November, 1995	11 713
$2375063906985 \cdot 2^{19380} - 1$	Sophie Germain prime	December, 1995	5 847
$4610194180515 \cdot 2^{5056} - 1$	Sophie Germain & twin prime	January, 1996	1 535
$(235 \cdot 2^{18400})^4 + 1$	n^4+1	1996	22 166
Submitted by Karl-Heinz Indlekofer, Antal Járai and Heinz-Georg Wassing			
$871892617365 \cdot 2^{48000} - 1$	twin prime	January, 2000	14 462
$2230907354445 \cdot 2^{48000} - 1$	twin prime	January, 2000	14 462
$2409110779845 \cdot 2^{60000} - 1$	twin prime	January, 2000	18 075
$3714089895285 \cdot 2^{60000} - 1$	Sophie Germain prime	March, 2000	18 075
$4648619711505 \cdot 2^{60000} - 1$	twin prime	March, 2000	18 075
Submitted by Tímea Csajbók, Gábor Farkas, Antal Járai, Zoltán Járai and János Kasza			
$16869987339975 \cdot 2^{171960} - 1$	twin prime	September, 2005	51 779
$137211941292195 \cdot 2^{171960} - 1$	Sophie Germain prime	May, 2006	51 780
$100314512544015 \cdot 2^{171960} - 1$	twin prime	Jun, 2006	51 780
$194772106074315 \cdot 2^{171960} - 1$	twin prime	Jun, 2006	51 780
$620366307356565 \cdot 2^{253824} - 1$	Sophie Germain prime	November, 2009	76 424
$648621027630345 \cdot 2^{253824} - 1$	Sophie Germain prime	November, 2009	76 424
Submitted by Gábor Farkas, Gábor Gévay, Antal Járai and Emil Vatai			
$5110664609396115 \cdot 2^{34944} - 1$	Cunningham chain of length 3 of the 1st kind	April, 2014	10 535

Figure 1. Járai's world records from 1992 to 2014.

1.1. New projects and difficulties

The authors of this paper thought the 20th prime record would the best present for Prof. Járai's 70th birthday. Therefore, at the end of 2019 we started to redesign and rewrite the program codes used earlier and at the beginning of 2020 we were ready to "hunt" for new large primes. We endeavoured to apply some ideas and fast arithmetic routines designed by Járai. We planned to find the largest known $Cc31$, but there were some factors holding back the progress. The most serious problem was the fact that the world record held since 2016 was broken on 18th February 2020. Therefore, our work was almost completely wasted, so we had to redesign our project. We focused our attention to $Cc22$'s, but the nightmare come true again. This world record was broken by another team in May 2020.

In spite of difficulties, still bursting with enthusiasm, continuing the project *the largest known* $Cc22$ was found on 30 May, 2020. Our new record consists of 77 078 decimal digits.

2. The plan

Due to the two restarts our time to meet the submission deadline to the special issue of this journal to celebrate Prof. Járai's 70th birthday was significantly reduced. As we calculated, the largest known Cunningham chain of length 2 of the 2nd kind takes the least time to discover. Although we touched upon this type of prime combinations in the paper [13] published in 2012, we technically redesigned and rewrote our routines and recalculated expected running time because of some significant differences. For example, in order to increase the effectiveness of the process we carried out so called triple-sieving in 2012. This means that the sieving was performed for not only Cunningham chains but also twin primes simultaneously. So we could expect at least two world recorder $Cc22$ and two bronze-medalist twin primes. In the recent project the large difference between the magnitude of twin prime record and Cunningham chain record excluded the possibility of triple-sieving.

2.1. Hyperparameters

The work [13] includes lot of details about classical and modern mathematical results which are indispensable tools to carry out a successful prime hunting project. In this paper, we consider exclusively the redesigned parts. Consider first the generator polynomial:

$$f_0(x) = (h_0 + c \cdot x) \cdot 2^e + d,$$

where d is equal 1 or -1. The numbers generated by a generator polynomial are called "candidates". Observe that if we set $d = 1$ then for the polynomials

$$f_i(x) = (h_0 + c \cdot x) \cdot 2^{e+i} + 1,$$

where $i = 0, 1$, the equation $f_1 = 2f_0 - 1$ is valid because

$$(h_0 + c \cdot x) \cdot 2^{e+1} + 1 = 2 \cdot ((h_0 + c \cdot x) \cdot 2^e + 1) - 1,$$

i.e. if for an arbitrary x $f_0(x)$ and $f_1(x)$ are simultaneously prime then they form a $Cc22$. Furthermore, we can realize that both polynomials generate numbers of form $k \cdot 2^n + 1$. This means that we could ignore the Riesel test for proving the primality of the candidates, so the parameter h_0 become unnecessary. We kept the constant $c = 30030$, thus the primes 2, 3, 5, 7, 11, 13 are not divisors of the numbers generated by f_0 and f_1. The constant $e = 256000$ guarantees numbers with at least 77 069 digits. Since the product $c \cdot x$ has a factor 2^j, where $x \in H$ and $j \geq 1$ therefore the final published numbers are of the form $h \cdot 2^{e+j}$ for an odd integer $h < 2^{e+j}$.

2.2. Expected values

As usual we denote the complete set of possible values of x by H. The details of calculations which were based on the Bateman–Horn conjecture [1] were published in [13]. In that work, $|H| = 2^{35}$ was chosen. In the new project the cardinality of H could be reduced because the double-sieve, unlike the triple-sieve, does not eliminate $Cc22$'s. Furthermore the magnitude of the candidates could be slightly increased. Finally, we obtain that if $H = \{1, 2, \ldots 2^{31} - 1\}$ then the expected value of the number of $Cc22$'s is:

$$Cc_{exp} \approx 1.82.$$

Furthermore, the compression factor of the sieve can be approximated as described in [13]. Denote the expected value of the candidates by CS_{exp} after sieving with the primes up to 2^{27} and by CM_{exp} after sieving with the primes up to 2^{54}. We obtained that

$$CS_{exp} = 51601691 \text{ and } CM_{exp} = 12900422.$$

We assumed that a primality test takes 100 seconds in average and the programs run in 1000 threads. Thus, we could hope that after sieving the project will be finished in two weeks even in the worst case scenario.

3. The reality

We started running the programs on a server (Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz. CPU features: RDTSC, CMOV, PREFETCH, MMX, SSE,

SSE2, AVX, FMA3. L1 cache size: 32 KB, L2 cache size: 1024 KB.) owned by our research group AAK. We had an idyllic beginning, the results were generated smoothly. During the implementation we used some fast arithmetic routines designed by A. Járai. Due to Járai's functions our program generated 2^{27} primes in 6 seconds and finished the sieve with these primes in 349 seconds. For the real value of candidates after the sieving with primes up to 2^{27} we got that

$$CS_{real} = 51609622,$$

i.e. the difference from the approximated value CS_{exp} less than 0.00154%.

Unfortunately, after the small prime sieve we had a lot of difficulty in continuing our work. We could not reach such a super computer having sufficient operative memory as needed for the parallelization of the large prime sieve. Since the candidates were numbers of the form $k \cdot 2^n + 1$, we used Proth primality test which takes approximately 80 seconds in average per number. Although the expected running time increased, we began to run the primality tests because rewriting the program would have taken more time.

3.1. Results

Finally, on Saturday 30 May 2020, at 12:59 a test program running on the supercomputer of ELTE named "Atlasz" stopped with a positive result. Thus, we reached our goal, the largest known Cunningham chain of length 2 of the 2nd kind was found, consisting of the following primes:

$$p = 3622179275715 \cdot 2^{256002} + 1 \qquad 77\,077 \text{ decimal digits,}$$

$$p = 3622179275715 \cdot 2^{256003} + 1 \qquad 77\,078 \text{ decimal digits.}$$

References

[1] **Bateman, P.T. and R.A. Horn,** A heuristic asymptotic formula concerning the distribution of prime numbers, *Mathematics of Computation*, **16** (79), (1962), 363–367.

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

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

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

[5] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known twin primes of the World, $16869987339975 \cdot 2^{171960} \pm 1$ (51779 digits), `http://primes.utm.edu/top20/page.php?id=1`, (2005).

[6] **T. Csajbók, G. Farkas, A. Járai, Z. Járai, J. Kasza,** Report on the largest known Sophie Germain and twin primes, *Annales Univ. Sci. Budapest, Sect. Comp.*, **26**, (2006) 181–183.

[7] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known twin primes of the World, $100314512544015 \cdot 2^{171960} \pm 1$ (51780 digits), `http://primes.utm.edu/top20/page.php?id=1`, (2006).

[8] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known Sophie Germain prime of the World, $137211941292195 \cdot 2^{171960} - 1$ (51780 digits), `http://primes.utm.edu/top20/page.php?id=2`, (2006).

[9] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known twin primes of the World, $194772106074315 \cdot 2^{171960} \pm 1$ (51780 digits), `http://primes.utm.edu/top20/page.php?id=1`, (2007).

[10] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known Sophie Germain prime of the World, $620366307356565 \cdot 2^{253824} - 1$ (76424 digits), `http://primes.utm.edu/top20/page.php?id=2`, (2009).

[11] **Csajbók, T., G. Farkas, A. Járai, Z. Járai and J. Kasza,** The largest known Sophie Germain prime of the World, $648621027630345 \cdot 2^{253824} - 1$ (76424 digits), `http://primes.utm.edu/top20/page.php?id=2`, (2009).

[12] **Járai, A. and E. Vatai,** Cache optimized linear sieve, *Acta Universitatis Sapientiae Informatica*, **3(2)** (2011), 205–223.

[13] **Csajbók, T., G. Farkas and J. Kasza,** Sieving for large twin primes and Cunningham chains of length 2 of the second kind, *Annales Univ. Sci. Budapest., Sect. Comp.*, **38** (2012), 117–128.

[14] **Farkas, G. and E. Vatai,** Sieving for large Cunningham chains of length 3 of the first kind, *Annales Univ. Sci. Budapest., Sect. Comp.*, **40** (2013), 215–222.

[15] **Farkas, G., G. Gévay, A. Járai and E. Vatai,** The largest known Cunningham chain of length 3 of the first kind, *Studia Universitatis Babes-Bolyai Mathematica*, **59(4)** (2014), 457–462.

[16] **Yates, S,** Titanic primes, *J. Recreational Math.*, **16(4)**, (1984) 250–262.

[17] **Caldwell, C.K.,** The Prime Pages, `http://primes.utm.edu`

[18] **Járai, J.,** World records in computational number theory, `http://compalg.inf.elte.hu/~ajarai/worldr.htm`

G. Farkas
Department of Computer Algebra
Eötvös Loránd University
Budapest
Hungary
farkasg@inf.elte.hu

G. Gévay
Technische Universität
Berlin
Germany
ggab90@gmail.com

P. Magyar
Eötvös Loránd University
Szombathely
Hungary
z47mli@inf.elte.hu

B. Szekeres
Department of Numerical Analysis
Eötvös Loránd University
Budapest
Hungary
szekeres@inf.elte.hu