NEW LARGEST KNOWN FACTOR OF FERMAT NUMBERS

JOHN B. COSGRAVE AND YVES GALLOT

ABSTRACT. The prime number $3 \cdot 2^{382449} + 1$ divides the Fermat number $F_{382447} = 2^{2^{382447}} + 1$.

COMMENTS

On July 23, 1999, John Cosgrave discovered a new prime $P = 3 \cdot 2^{382449} + 1$ using Yves Gallot's program Proth.exe. The program started to test P as a possible factor of a generalized Fermat number $F_{b,m} = b^{2^m} + 1$ for some $b \leq 12$, by using "a time saving device" [2]. On July 25, we discovered that P is a factor of F_{382447}, $F_{382447,3}$, $F_{382443,6}$ and $F_{382447,12}$. P is not a factor of any $F_{m,5}$ and $F_{m,10}$. A verification was made by checking directly that $12^{2^{382447}} \equiv -1 \pmod{P}$. Previously the largest known composite Fermat number was F_{303088}, with factor $3 \cdot 2^{303093} + 1$ [9].

The new factor was found on a 350 MHz Pentium II computer, one of a number of machines in St. Patrick's College of Dublin City University running the program.

The program is named Proth.exe because one of the theorems of the self-taught farmer François Proth (1852-1879) is the heart of the program (see [7], [6, Theorem 102, page 79] or [8, page 52]):

Theorem. *Let $n > 1$, $k < 2^n$ and $N = k \cdot 2^n + 1$ be a quadratic non-residue* (mod a) *for some odd prime a. Then the necessary and sufficient condition for N to be a prime is that $a^{(N-1)/2} \equiv -1 \pmod{N}$.*

Proth.exe is written as a Windows 9x/NT/2000 program (because more than 90% of the computers can run it) available on the internet [5].

The test is simple, in practice the difficulty is multiplying the large numbers involved. The program is based on an efficient right-angle convolution [3]. The Fast Fourier Transform is written in assembler and optimized to take into account the size of the cache-memory of the computer.

Ray Ballinger and Wilfrid Keller organize the search of the primes of the form $k \cdot 2^n + 1$ on the internet [1]. Because of the important result "It appears that the probability of each prime of the form $k \cdot 2^n + 1$ dividing a Fermat number is $1/k$" [4], the search is particularly extended for small values of k.

Date: August 4, 1999.

1991 *Mathematics Subject Classification.* Primary 11Y05, 11Y11; Secondary 11A51, 11A41.

Key words and phrases. Prime numbers, Fermat numbers, primality proving algorithms.

(C) Copyright 1999, Yves Gallot. You may make unlimited copies of the document and give copies to other persons as long as the copies you make and distribute contain the unaltered and unabridged document.

Four factors were already found with Proth.exe by some contributors to the search: - $165 \cdot 2^{49095} + 1$ divides F_{49093} (Yves Gallot) - $169 \cdot 2^{63686} + 1$ divides F_{63679} (Harvey Dubner) - $99 \cdot 2^{83863} + 1$ divides F_{83861} (Gennady Gusev) - $39 \cdot 2^{113549} + 1$ divides F_{113547} (John Renze) -.

The discovery is the fruit of an international collaborative effort. The credit goes to all the contributors to the search: Ed Adamson, Mark Alfonso, Bojan Antonovic, Ray Ballinger, Brian Beesley, Christer Berg, Steve Bird, Lars Blomberg, Didier Boivin, Jack Brennen, Bryon Buck, Ingo Buechel, Robert Burrowes, Chris Caldwell, Kevin Carton, John Chatzikonstantinou, Robert Clark, John Cosgrave, Joseph Cox, Nick Craig-Wood, Mike Curtis, Chad Davis, Daval Davis, Mike Dawson, John DeCuir, Sébastien Desnault, Olivier Dodinval, Pete Dodson, Harvey Dubner, Rüdiger Eckhard, Germano Vale Filho, Matt Fischer, Martin Freiss, Brandon Galbraith, Yves Gallot, Michael Graef, Gennady Gusev, Henry Hamilton, Michael Hannigan, David Hanson, Bill Hodgeman, Chris Jeppesen, Jo Yeong Uk, Paul Jobling, Craig Johnston, Rick Jones, Henk-Jan de Jong, Wilfrid Keller, Chip Kerchner, Skip Key, Eduard Kostolansky, Richard Kowalski, Henri Lifchitz, Lars Lindley, Dave Linton, Jud McCranie, Bryan McIntyre, Sven Meinhardt, Michal Misztal, Dan Morenus, Chris Nash, Peter Neugebauer, Takahiro Nohara, Alexis Nunes, Michael O'Brien, Kevin O'Hare, Anton Oleynick, Nicolas Pagnier, Charlie Partin, Michael Peake, Kirk Pearson, Andy Penrose, Richard Quelle, John Renze, Stephen Scott, Rob Simmons, Chris St.Clair, Ola Svallmark, Aaron Swihart, Janusz Szmidt, Tadashi Taura, Manfred Toplic, Steven Whitaker, Vincent Wighman, Jeff Wolski, Helmut Zeisel, Bruce Ziemienski.

Acknowledgments

The first author wishes to acknowledge the use of his College's computer facilities during the relatively quiet Summer months.

References

1. R. Ballinger and W. Keller, *Proth Search Page*, 1997, http://vamri.xray.ufl.edu/proths/
2. A. Björn and H. Riesel, *Factors of generalized Fermat numbers*, Math. Comp. **67** (1998), 441-446.
3. R. Crandall and B. Fagin, *Discrete Weighted Transforms and Large-Integer Arithmetic*, Math. Comp. **62** (1994), 305-324.
4. H. Dubner and W. Keller, *Factors of generalized Fermat numbers*, Math. Comp. **64** (1995), 397-404.
5. Y. Gallot, *Proth.exe: a Windows program for finding very large primes*, 1997, http://www.utm.edu/research/primes/programs/gallot/
6. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, 1979.
7. F. Proth, *Théorèmes sur les nombres premiers*, Comptes Rendues Acad. des Sciences, Paris, **87** (1878), 926.
8. P. Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer-Verlag, New York, 1995.
9. J. Young, *Large primes and Fermat factors*, Math. Comp. **67** (1998), 1735-1738.

Mathematics Department, St. Patrick's College, Drumcondra, Dublin 9, Ireland
E-mail address: John.Cosgrave@spd.ie

E-mail address: galloty@wanadoo.fr