Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
August 22, 2022

Six "Most Wanted" numbers from the wanted lists issued with Page 140 were factored on Page 141. NFS@Home factored 10,323−, 10,323+, 3,677−, 5,463+, 7,383−, and 11,311−, all by the Special Number Field Sieve.

No "More Wanted" number from the wanted lists issued with Page 140 was factored on Page 141.

One "Smaller-but-Needed" number from the wanted lists issued with Page 140 was factored on Page 141. NFS@Home factored 2,2822M by the General NFS.

New wanted lists are enclosed.

ECMNET means Paul Zimmermann, Alex Kruppa, Torbjörn Granlund, Michel Quercia, Witold Grabysz, Vilmar Trevisan and many helpers who use the GMP-ECM program of Kruppa and Zimmermann. NFS@Home is a group led by Greg Childers.

There were no new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. A list of recent champions is enclosed.

The first holes factored on Page 141 are in # 6635, # 6636, # 6641, # 6643, # 6644, # 6657, # 6660 and # 6662. No second, third, fourth or fifth hole was factored on Page 141.

The smallest new factor reported on Page 141 has 59 digits. See # 6639. The largest number factored on Page 141 has 378 digits. See # 6645.

See the URL `http://www.prothsearch.net/fermat.html` for a list of all known Fermat factors.

No new Mersenne prime was found since the last page. The current largest known prime is $2^{82589933} - 1$. See the URL `http://primes.utm.edu/primes/` for Chris Caldwell's database of the largest known primes (updated hourly).

See the URL `http://homes.cerias.purdue.edu/~ssw/cun/index.html` for the online Cunningham book.

John Brillhart was born on November 13, 1930, and died on May 21, 2022. When John was in the Army, his drill sergeant asked why he was scribbling numbers next to his rifle. John explained that he was factoring the serial number of his gun—branding himself as a potential trouble maker in the eyes of the surprised sergeant. This fascination with factoring stayed with John for the rest of his life. He and Michael Morrison described the continued fraction factoring method, CFRAC, the first subexponential running time algorithm, in their 1975 article. They introduced the factor base and showed how to combine the relations in this algorithm by using Gaussian elimination on vectors of exponents over the field with 2 elements. These ideas led Pomerance to invent the quadratic sieve. The number field sieve, the fastest known factoring method for general numbers, stemmed from the quadratic sieve. John was one of the members of the Cunningham Project. He was a coauthor of the book **Factorizations of** $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ **up to high powers**, and wrote most of the text of the first edition.

Please send me any address changes.

Keep the factors coming!

Sam Wagstaff