Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
June 2, 2006

Two “Most” and six “More Wanted” numbers from the wanted lists issued with Page 100 were factored on Page 102. Using the Special Number Field Sieve, Franke factored 6,274+ and NFSNET′′ factored 2,764+. Also with SNFS, Kleinjung factored 11,220+, Franke factored 7,257+ and 7,257−, CWI factored 10,238+ and Silverman factored 2,1406M. Kleinjung used the General Number Field Sieve to factor 11,218+.

Two “Smaller-but-Needed” numbers were factored on Page 102, both by some form of the Number Field Sieve. CWI factored 5,715M and Reynolds factored 6,798L.

The factorization of 2,764+ completes the factorization of all numbers $2^n \pm 1$ with $n \leq 768$, which is a milestone for cryptographers, who once used keys of length 768 bits.

New wanted lists, prepared by John Selfridge, are enclosed.

CWI means Peter Montgomery, Herman te Riele and Willemien Ekkelkamp at the Centrum voor Wiskunde en Informatica in Amsterdam. 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. NFSNET′′ is a group of factorers lead by Don Leclair, Paul Leyland and Richard Wackerbarth and with contributions from many volunteer workers. See their URL `http://www.nfsnet.org` .

There was one new champion for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. The factorization of 5,349− in # 5373 is a new champion (second place) for largest penultimate prime factor. A list of recent champions is enclosed.

The first holes done on Page 102 are in # 5371, # 5372, # 5374 # 5377, # 5378, # 5382, # 5384, # 5385 and # 5394. The only second hole done on Page 102 is in # 5357. The third holes done on Page 102 are in # 5359 and # 5360. The fourth holes done on Page 102 are in # 5369 and # 5391. No fifth holes were done on Page 102.

The smallest new factor reported on Page 102 has 44 digits. See # 5387. The largest number factored on Page 102 has 307 digits. See # 5364.

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

See the URL `http://www.utm.edu/research/primes/largest.html` for Chris Caldwell’s list of all of the largest known Mersenne primes. The largest known Mersenne prime, the forty-third one to be disovered, is $2^{30402457} - 1$.

See the URL `http://www.cerias.purdue.edu/homes/ssw/cun/index.html` for the online Cunningham book. The full text is available at the AMS web site: `http://www.ams.org/online_bks/conm22` .

It is with sadness that I note the passing of George Sassoon. In 1993–1999 he mustered the computing power of all the PCs on the Isle of Mull in Scotland, where he lived, and factored more than a dozen numbers from the Cunningham Project. His factoring group was called MullFac.

Please send me any address changes.

Keep the factors coming!

Sam Wagstaff