Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
February 4, 2010

One “More Wanted” number from the wanted lists issued with Page 112 was factored on Page 114. NFS@Home factored 2,1678M by the Special Number Field Sieve.

Six “Most Wanted” numbers from the wanted lists issued with Page 113 were factored on Page 114. NFS@Home factored 6,323+, 3,548+ and 5,361+. Batalov and Dodson factored 10,248+ and 11,241−. Batalov, NFS@Home and Dodson factored 10,269−. All were done by the SNFS.

Ten “More Wanted” numbers from the wanted lists issued with Page 113 were factored on Page 114. NFS@Home factored 2,1714M, 5,373+, 6,331+, 6,332+, 7,311− and 10,268+. Batalov and Dodson factored 3,551− and 12,247−. Raman factored 7,320+. All were done by the SNFS. Dodson found a small factor of 6,338+ by the Elliptic Curve Method and NFS@Home finished the remaining cofactor with SNFS.

Two “Smaller-but-Needed” numbers were factored on Page 114. My student Fang-Yu Rao and I sieved 2,2074M by the General NFS and Greg Childers finished it. Al Edwards factored 11,275−, also by GNFS.

The factorization of 10,248+ in # 5801 was the last of the numbers $b^n \pm 1 < 10^{250}$.

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. Mersenneforum is a group with a section interested in factoring. See `http://www.mersenneforum.org` . NFS@Home is a group led by Greg Childers.

There were two new champions for factoring Cunningham numbers on this page, both the same factorization. Recall that a champion is one of the best two records in its class. The C280 of 2,941− split in # 5811 was a new champion (second place) for Special Number Field Sieve by size and also by SNFS Difficulty. A list of recent champions is enclosed.

The first holes done on Page 114 are in # 5794, # 5795, # 5797, # 5801, # 5802, # 5803, # 5804, # 5808, # 5809, # 5812, # 5817, # 5819, # 5820, # 5824 and # 5825. The only second hole done on Page 114 is in # 5815. The only third hole done on Page 114 is in # 5823. The only fourth hole done on Page 114 is in # 5799. No fifth holes were done on Page 114.

The smallest new factor reported on Page 114 has 55 digits. See # 5807. The largest number factored on Page 114 has 282 digits. See # 5807. (The two records just happened to come from the same number.)

See the URL `http://www.prothsearch.net/fermat.html` for Wilfrid Keller’s list of all known Fermat factors. Of particular note is the recently discovered 54-digit factor of F_{14}, the first prime factor known for that number.

No new Mersenne primes have been found since the last page. The current largest known prime is $2^{43112609} - 1$. See the URL `http://primes.utm.edu/primes/` for Chris Caldwell’s database of the largest known primes (updated hourly).

See the URL `http://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` .

Dik Winter passed away on December 28, 2009. He was part of CWI since 1969. As a programmer, he was part of the teams that set records for factoring large integers by the quadratic sieve in the 1980s and by the special and general number field sieves in the 1990s. He was the first to code the APR-CL primality test. He was also known for writing programs to solve Rubik’s Cube and to compute pi to many decimal places by the spigot algorithm.

Please send me any address changes.

Keep the factors coming!

Sam Wagstaff