

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
February 29, 2008

Five “Most Wanted” numbers from the wanted lists issued with Page 106 were factored on Page 107. NFSNET” factored 2,787–, 2,787+ and 10,239–. Kruppa et al. factored 7,269–. Silverman factored 6,299–. All were factored using the Special Number Field Sieve.

Four “More Wanted” numbers from the wanted lists issued with Page 106 were factored on Page 107. NFSNET” factored 10,239+, Raman factored 6,305– and CWI factored 12,229–. Those three numbers were factored using the SNFS. Finally, Leyland used the General Number Field Sieve to factor 2,1574L.

Four “Smaller-but-Needed” numbers were factored on Page 107. Irvine and Littin factored 6,329–. Irvine factored 10,375+. Davis and Womack factored 5,775M and 7,366+. The first three numbers were factored by GNFS, but 7,366+ was done with SNFS.

New wanted lists are enclosed.

CWI means Peter Montgomery, Herman te Riele, Willemien Ekkelkamp and Andrey Timofeev 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 Richard Wackerbarth and Paul Leyland. They are supported in the sieving effort by Bruce Dodson (Lehigh U), Jeroen Demeyer (U Gent) and Greg Childers (Cal State Fullerton), as well as the contributions of a number of additional volunteer sievers. See their URL <http://www.nfsnet.org>.

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. The closest factorization to being a champion on Page 107 was the P66 factor of 5,725L in # 5589, which was just a bit smaller than the record (second place) for the Elliptic Curve Method. A list of recent champions is enclosed.

The first holes done on Page 107 are in # 5564, # 5565, # 5578, # 5581, # 5590, # 5591 and # 5598. The second holes done on Page 107 are in # 5566 and # 5585. The only third hole done on Page 107 is in # 5594. The fourth holes done on Page 107 are in # 5579 and # 5584. The only fifth hole done on Page 107 is in # 5563.

The smallest new factor reported on Page 107 has 48 digits. See # 5592. The largest number factored on Page 107 has 306 digits. See # 5576.

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. No new Mersenne primes have been found since $2^{32,582,657} - 1$.

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.

Please send me any address changes.

Keep the factors coming!

Sam Wagstaff