Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
November 4, 2006

One "Most" and six "More Wanted" numbers from the wanted lists issued with Page 102 were factored on Page 103. Using the Special Number Field Sieve, NFSNET″ factored 3,479+. Also with SNFS, NFSNET″ factored 2,797+ and Silverman factored 2,1426L, 2,1454L, 2,1462L and 5,314+. CWI used the General Number Field Sieve to factor 12,229+.

Eight "Smaller-but-Needed" numbers were factored on Page 103, all by some form of the Number Field Sieve. T. Shimoyama et al. factored 7,352+, CWI factored 10,396+, G. Reynolds factored 7,539L, S. Hoogendorn factored 10,372+, and S. Irvine factored 6,384+, 2,1666L, 2,1634L and 6,289+.

The factorization of 2,1526L completes the factorization of all base 2 numbers with size $\leq 2^{768}$, a milestone for cryptographers, who once used keys of length 768 bits.

New wanted lists 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 67-digit factor of 10,381+ in # 5418 is a new champion for largest penultimate prime factor. A list of recent champions is enclosed.

The first holes done on Page 103 are in # 5405, # 5412, # 5423, # 5427, # 5430, # 5431 and # 5433. The only second hole done on Page 103 is in # 5413. The third holes done on Page 103 are in # 5408, # 5411, # 5434, and # 5438. The fourth holes done on Page 103 are in # 5407 and # 5409. The only fifth hole done on Page 103 is in # 5414.

The smallest new factor reported on Page 103 has 44 digits. See # 5429. The largest number factored on Page 103 has 299 digits. See # 5425.

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. GIMPS has discovered that $2^{32,582,657}-1$ is prime. It is the forty-fourth Mersenne prime to be discovered and is the largest known prime. It has 9,808,358 digits. It was found at Central Missouri State University by Curtis Cooper and Steve Boone, who also found the previous prime record holder, $2^{30,402,457}-1$.

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