Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
May 21, 2002

Many “Wanted” numbers were factored on Page 88, all but one by the Number Field Sieve. From the wanted lists mailed with Page 86 on May 31, 2001, T. Granlund and CWI factored the “Most Wanted” numbers 2,641− and 2,641+. CWI factored the “Most Wanted” number 2,643−. A.K. Lenstra, CWI, B. Dodson, T. Granlund, P. Leyland and J. Klos factored the “Most Wanted” number 5,283+.

J. Franke and T. Kleinjung factored the “More Wanted” number 3,386+. T. Granlund factored the “More Wanted” number 5,284+. These factorizations finished the entire wanted lists of May 31, 2001.

T. Granlund and CWI also factored the “Smaller-but Needed” number 11,407M.

New wanted lists were issued with the third edition. Since it is not yet on-line, its wanted lists are given on a separate sheet enclosed. Three numbers from the new lists have been factored. N. Daminelli of ECMNET used the Elliptic Curve Method to find a factor of the “Most Wanted” number 11,197+. The 161-digit composite cofactor remains on the “Most Wanted” list. B. Dodson, A.K. Lenstra and CWI factored the “Most Wanted” number 2,647+. CWI factored the “More Wanted” number 6,244+.

CWI means Henk Boender, Stefania Cavallar, Walter Lioen, Peter Montgomery, Herman te Riele and Dik Winter at the Centrum voor Wiskunde en Informatica in Amsterdam. ECMNET means Paul Zimmermann, Torbjörn Granlund, Michel Quercia, Witold Grabysz, Vilmar Trevisan and many helpers who use Granlund’s GMP-ECM program. The *tmpqs* in # 4682 means that three large primes were used in the Quadratic Sieve.

There were seven new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. The factorization of 2,727− was a champion (second place) for SNFS by size and also by difficulty. It was also a champion (first place) for largest penultimate prime factor. The factorization of 2,1606L was a champion for Quadratic Sieve. The factorization of 2,953+ was a champion for GNFS. The factorization of 2,751− was a champion (first place) for SNFS by size and also by difficulty.

The number 2,751− had been the smallest Mersenne number with no known prime divisor. Its replacement in that category is 2,809−.

The first holes done on Page 88 are in # 4678, # 4679, # 4680, # 4683, # 4688, # 4696 and # 4711. The second holes done on Page 88 are in # 4674, # 4675, # 4676 and # 4720. No third or fourth holes were done on Page 88. The fifth holes done on Page 88 are in # 4685, # 4687 and # 4702. (Note that 2,727− was a sixth hole and 2,751− was a seventh hole when factored.)

The smallest new factor reported on Page 88 has 37 digits. See # 4698 and # 4689. The largest number factored on Page 88 has 338 digits. See # 4684.

See the URL `http://www.prothsearch.net/fermat.html` for Wilfrid Keller’s list of all known Fermat factors. Several new factors were added since last summer.

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 new largest Mersenne prime is $2^{13466917} - 1$.

I will put Updates to the Third Edition on my web page. There is no Update there yet, but I will put Update 3.1 there this summer. See the URL `http://www.cerias.purdue.edu/homes/ssw/cun/index.html`. The Factor Calculator on that page seems to be working again.

I sent the Third Edition of the book to the AMS on September 18, 2001. They claim it will appear as an electronic book on their web site soon. When it appears, I will put a link to it from my web page.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff