Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
July 30, 1997

Many 'Wanted' numbers were factored on Page 76. From the lists in Update 2.A, the group NFSNET factored the 'Most Wanted' numbers 3,344+, 5,233−, 6,209+, 10,166+ and 12,148+, all with the Number Field Sieve. The same group also factored the 'More Wanted' numbers 2,998L, 7,191+ and 11,149+ with the Number Field Sieve. NFSNET is factoring 2,569− and 7,199− now, so these two numbers have been removed from the 'Wanted' lists. New Wanted lists are given on the Champions page.

All four of the 'Smaller but Needed' numbers were done on Page 76. MullFac factored 2,725− by the Quadratic Sieve. I factored 2,917− by QS. M. Mambo, E. Okamoto and R. Peralta factored 2,655− by QS. CWI factored 2,685+ by NFS. These were the last two numbers with 108 digits in the Cunningham Tables. No new 'Smaller but Needed' list is issued at this time.

One Page 76, Tables 6+, 11+ and 12+ joined Tables 3−, 6− and 11− in being completed up to the second edition limit.

The Number Field Sieve categories on the champions page have been redefined. The new definitions are explained in the enclosed Note to Newcomers. There were new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. There was a new champion (second place) for Special NFS by size of number factored, that of 10,166+ by NFSNET. There were also new champions in the new category of Hybrid Special/General NFS, factorizations of 2,1650L and 2,1095+ by CWI. A list of recent champions and the first holes in each table is given on another sheet.

MullFac means Isle of Mull Factoring Group. It includes George Sassoon, Vivian Stevens and Richard Edwards. CWI means Henk Boender, Stefania Cavallar, Marije Elkenbracht-Huizing, Walter Lioen, Peter Montgomery, Herman te Riele and Dik Winter at the Centrum voor Wiskunde en Informatica in Amsterdam. NFSNET is a group which uses NFS and includes Bob Silverman, Peter Montgomery, Marije Elkenbracht-Huizing, Stefania Cavallar, Richard Wackerbarth, me and many volunteer sievers. M+O+P means Masahiko Mambo, Eiji Okamoto and Rene Peralta. ERWW means Andreas Erdmann, Jonas Rathert, Hannes Wettig and Georg Wambach.

The first holes done on Page 76 are in # 3987, # 3999, # 4000, # 4007, # 4008, # 4014, # 4015, # 4017, # 4038, # 4040 and # 4041. The only second hole done on Page 76 is in # 3990. The third holes done on Page 76 are in # 4006, # 4012, # 4016 and # 4020. No fourth holes were done on Page 76. The fifth holes done on Page 76 are in # 4025 and # 4035.

The smallest new factor reported on Page 76 has 27 digits. See # 4002. The largest number factored on Page 76 has 355 digits. See # 4009.

Richard Crandall, Karl Dilcher and Chris van Halewyn have found a new 33-digit factor of F_{15} by the Elliptic Curve Method. It is 168768817029516972383024127016961. Two other factors of F_{15} were already known. Richard Brent has shown that the remaining cofactor is composite with 9808 digits.

Let me correct two typos in the table of Fermat factors in Update 2.A. k should be 79707 rather than 7970 for $m = 1225$. The last entry should have $n = 157169$ and $m = 157167$ rather than the reverse.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff