

February 20, 1996

Many 'Wanted' numbers were factored on Page 73. From the old lists mailed with Page 71 in December, 1994, the group CWI factored 2,565- c115 using the Number Field Sieve.

New 'Wanted' lists were issued with Update 2.9 last August. For the first time in the history of these Pages, all ten of the 'Most Wanted' numbers were factored on one page. On Page 73, NFSNET, a new group started by Bob Silverman and Marije Elkenbracht-Huizing, factored 3,316+, 3,317+, 2,527-, 2,521+ and 10,158+ by NFS. CWI factored 3,317+ and 10,163- by NFS. CWI factored 5,256+ and 2,563- by ECM. Richard Brent found the most wanted factorization of all: he factored $F_{10} = 2,1024+$ by ECM. This number and 5,256+ were the last numbers from the wanted lists published in the Second Edition of the book to be factored. NFSNET factored the 'More Wanted' number 2,524+ by NFS and CWI found a factor of the 'More Wanted' number 2,974L by ECM, leaving a c114 cofactor. New wanted lists are enclosed. Five numbers that were on the Update 2.9 wanted lists do not appear on the new lists because they are being factored now. They are 2,934L, 2,962M, 5,223+, 11,142+ and 12,137-. They will appear on Page 74.

Two of the 'Smaller but Needed' numbers were done on Page 73. Scott Contini and Carl Pomerance factored 5,280+ c104 by MPQS. CWI factored 12,157+ c106 by the general NFS. The latest list of 'Smaller but Needed' numbers appears on the 'Champions' page. It contains all Cunningham composite numbers having 105, 106 or 107 digits.

Our goal of factoring all the higher base ($b > 2$) numbers listed in the first (1983) edition of the book has been achieved. The last three of these numbers were factored on Page 73. CWI factored 3,317+ c151 by NFS. NFSNET factored 3,313+ c129 and 3,316+ c127 by NFS.

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. CWI factored 10,163- c138 by the Special NFS. CWI factored 12,157+ c106 by the General NFS. Hidenori Kuwakado found a p43 factor and CWI found a p47 factor by ECM. A list of recent champions and the first holes in each table is given on another sheet.

FactOregon or FO means Peter Montgomery, Robby Robson and Russell Ruby at Oregon State University, Corvallis, Oregon, and Joe Buhler and Scott Huddleston at Reed College, Portland, Oregon. CWI means Henk Boender, 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, Marije Elkenbracht-Huizing, Richard Wackerbarth, me and a few dozen volunteer sievers. We use mpecm to refer to an Elliptic Curve program for the MasPar computer written by Arjen Lenstra and Brandon Dixon.

The first holes done on Page 73 are in # 3834, # 3842, # 3844, # 3845, # 3846, # 3856 and # 3857. The second holes done on Page 73 are in # 3841 and # 3850. The third holes done on Page 73 are in # 3811, # 3824, # 3828, # 3836 and # 3853. The only fourth hole done on Page 73 is in # 3816. The only fifth hole done on Page 73 is in # 3859.

The smallest new factor reported on Page 73 has 25 digits. See # 3815 and # 3823. The largest number factored on Page 73 was 2,2302L c331. See # 3815.

Only two Cunningham numbers with b^n smaller than 10^{150} remain to be done. They are 11,142+ c141 and 12,137- c123. One number of this type, 3,313+ c129, was done on Page 73. See # 3842. (The two remaining numbers are being factored now. They will appear on Page 74.)

The last two numbers with 104 digits, 3,385- and 5,280+, were factored on Page 73. See # 3809 and # 3821. All of the smallest composite numbers in the Cunningham table (105 digits) appear in the 'Smaller but Needed' list.

Three new factors of Fermat numbers were discovered since Page 72 was issued. All were found by Richard Brent. The first two are shown in line # 3840 and complete the factorization of F_{10} . The third is the factor 319546020820551643220672513 of F_{13} , found on 19 June 1995. The cofactor is a composite number with 2391 decimal digits.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff