Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
September 16, 1996

Many 'Wanted' numbers were factored on Page 74. From the old lists in Update 2.9, the group CWI factored 5,223+ using ECM and the Quadratic Sieve. The group NFSNET factored 11,142+, 12,137− and 2,934L with the Number Field Sieve. Scott Contini used the Quadratic Sieve to factor 2,962M. These numbers were not given in the 'Wanted' lists issued with Page 73 last February because their factorizations all were in progress then.

From the 'Wanted' lists issued with Page 73 eight 'Most Wanted' and six 'More Wanted' numbers were factored. NFSNET factored the 'Most Wanted' numbers 2,559−, 2,536+, 6,199−, 5,226+, 7,187−, 10,163+ and 12,139−, all by NFS. Marije Elkenbracht-Huizing, Richard Wackerbarth and Paul Zimmermann factored 3,331− by NFS. The number 10,167− has been removed from the 'Most Wanted' list because NFSNET is doing it now. It will appear on Page 75. Only 2,569− remains 'Most Wanted'.

E. Okamoto and R. Peralta factored the 'More Wanted' number 6,209− by QS. Paul Leyland factored 2,982L by QS. NFSNET factored 2,974L, 6,206+, 7,181+ and 11,146+ by NFS. New wanted lists are enclosed.

All seven of the 'Smaller but Needed' numbers were done on Page 74. E. Okamoto and R. Peralta factored the 'Needed' numbers 2,1890M, 3,831L, 2,625− and 2,1662L, all by QS. Georg Wambach, Andreas Erdmann and Jonas Rathert factored 3,395+ by QS. I factored 11,363L and 2,717− by QS. These seven numbers were the last numbers with 105, 106 and 107 digits in the Cunningham Tables. The latest list of 'Smaller but Needed' numbers appears on the 'Champions' page. It contains all Cunningham composite numbers having 108, 109 or 110 digits.

Several milestones were reached on Page 74. The last two numbers with $b^n < 10^{150}$, namely, 11,142+ and 12,137−, were factored. Also, the factorization of 6,199− completes work on 6,n± with $n \leq 200$.

There were two new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. Scott Contini set a new record for factoring 2,962M c116 by QS. Marije Elkenbracht-Huizing and Peter Montgomery set a new General NFS record with 10,193− c108. A list of recent champions and the first holes in each table is given on another sheet.

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, Peter Montgomery, Marije Elkenbracht-Huizing, Richard Wackerbarth, me and a few dozen volunteer sievers. MEH+PM means Marije Elkenbracht-Huizing and Peter Montgomery. GW+AE+JR means Georg Wambach, Andreas Erdmann and Jonas Rathert. EO+RP means Eiji Okamoto and Rene Peralta. M+O+P means Masahiko Mambo and EO+RP. 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 74 are in # 3865, # 3866, # 3871, # 3874, # 3876, # 3877, # 3880, # 3883, # 3884, # 3885, # 3886, # 3887, # 3900, # 3901, # 3902, # 3903, # 3904, # 3906, # 3920, # 3921, # 3922 and # 3923. The only second hole done on Page 74 is in # 3899. No third or fourth holes were done on Page 74. The fifth holes done on Page 73 are in # 3861 and # 3905.

The smallest new factor reported on Page 74 has 28 digits. See # 3869, # 3870, # 3914 and # 3924.

David Slowinski and Paul Gage found the Mersenne prime $2^{1257787} - 1$.

I plan to issue the next Update in November or December, 1996. Several tables (bases 5, 7 and 11, at least) will be lengthened in it.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff