Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
February 6, 1997

This mailing includes Update 2.A as well as Page 75. Page 75 became filled just when I received the Update from the printer.

Many 'Wanted' numbers were factored on Page 75. From the old lists issued with Page 73, the group NFSNET factored the 'Most Wanted' number 10,167− with the Number Field Sieve. This number was not given in the 'Wanted' lists issued with Page 74 last September because its factorization was in progress then.

From the 'Wanted' lists issued with Page 74 two 'Most Wanted' and six 'More Wanted' numbers were factored. NFSNET factored the 'Most Wanted' numbers 3,332+ and 7,188+ and the 'More Wanted' numbers 2,982M, 11,148+, 3,349− and 2,986L, all by NFS. The group CWI factored the 'More Wanted' number 2,998M by the Elliptic Curve Method. Bob Silverman and the group CWI factored the 'More Wanted' number 7,205− by NFS. New wanted lists appear in Update 2.A. While the Update was being printed, CWI factored the new 'More Wanted' number 2,1022L by NFS. Another new 'More Wanted' number, 2,998L, is in progress at this writing by NFSNET.

Five of the 'Smaller but Needed' numbers were done on Page 75. M. Mambo, E. Okamoto and R. Peralta factored the 'Needed' numbers 2,649+ and 5,253−, both by the Quadratic Sieve. NFSNET factored 5,505M by NFS. CWI factored 2,855− by NFS. I factored 6,211− by QS. It was the last number with 108 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 up to 111 digits.

One Page 75, Tables 3− and 6− joined 11− in being completed up to the second edition limit.

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. Two new records for the (Special) Number Field Sieve were the factorizations of 10,167− and 3,349−. It is not easy to compare record factorizations by SNFS. I list them in order of $b^n - 1$, because SNFS did not use any known factors and had to factor the full $b^n - 1$ and $10^{167} - 1 > 3^{349} - 1$. The factorization of 3,349− produced a new record penultimate factor, one with 80 digits. 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 many volunteer sievers. M+O+P means Masahiko Mambo, Eiji Okamoto and Rene Peralta.

The first holes done on Page 75 are in # 3929, # 3941, # 3947, # 3950, # 3954, # 3967, # 3980 and # 3983. The second holes done on Page 75 are in # 3925, # 3958 and # 3975. The third holes done on Page 75 are in # 3966 and # 3977. The fourth holes done on Page 75 are in # 3939, # 3940 and # 3968. The fifth holes done on Page 75 are in # 3939, # 3938, # 3962 and # 3970.

The smallest new factor reported on Page 75 has 27 digits. See # 3956. The largest number factored on Page 75 has 324 digits. See # 3959.

Armengaud, Woltman et al. found the Mersenne prime $2^{1398269} - 1$.

Several more new Fermat factors are listed in Update 2.A. While it was being printed, I received seven more of them from Tadashi Taura via W. Keller. They include a factor of F_{28}, the second smallest Fermat number (after F_{24}) whose character was previously unknown. We list them here as triples (m, k, n) meaning the factor $k \cdot 2^n + 1$ of $F_m = 2^{2^m}$: (28,25709319373,36), (1990,150863,1993), (13250,351,13252), (14276,157,14280), (17906,135,17909), (24651,99,24653), (28281,81,28285). These factors have been verified by H. Dubner and W. Keller.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff