December 13, 1993

Peter Montgomery reported two typos in Update 2.7. Scott Huddleston's name was misspelled. In the 'More Wanted' list, '5,316+' should be '3,316+'. Several people reported the latter typo.

Two 'Most Wanted' numbers were factored on Page 69. From the wanted lists in Update 2.7, Arjen Lenstra and Dan Bernstein factored 11,127+ c120 and Bob Silverman factored 7,169− c132 using the Number Field Sieve.

Eight 'More Wanted' numbers were factored on Page 69. From the old wanted lists mailed with Page 66, Bob Silverman factored 5,193+ c124 by NFS. From the wanted lists in Update 2.7, he factored 6,173− c119, 6,176+ c125, 6,178+ c137 and 7,163+ c117, all by NFS. Bruce Dodson used the Elliptic Curve Method to find a factor of 10,158+ c153, leaving a 120-digit composite cofactor. He also factored 2,898M c115 by ECM. Arjen Lenstra, Mark Manasse and the network factored 3,311+ c111 by the Quadratic Sieve. New wanted lists appear on the 'Champions' page. Omitted from these lists are two numbers, 7,172+ and 7,173−, whose factorizations are in progress now, by the network and by Silverman, respectively.

F. Morain and R. Lercier factored one of the 'Smaller but Needed' numbers, 2,529− c101, by QS. The group 'MullFac' factored 5,213+ c98 by QS. The latest list of 'Smaller but Needed' numbers appears on the 'Champions' page.

Our current goal is to factor all the higher base ($b > 2$) numbers listed in the first (1983) edition of our book. Nine of these numbers were factored on Page 69. Silverman factored 5,193+ c124, 6,173− c119, 6,176+ c125, 6,178+ c137, 7,163+ c117, and 7,169− c132, all by NFS. Arjen Lenstra and Dan Bernstein factored 11,127+ c120 by NFS. Arjen Lenstra, Mark Manasse and the network factored 3,311+ c111 and 3,329+ by QS. At this writing, 15 of these numbers remain to be factored.

Only one number with b^n smaller than 10^{140} remain unfinished. It is 11,131+ c129.

There are two new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. The new champion Quadratic Sieve factorization is the c116 of 3,329+. The new (second-place) champion penultimate prime factor is the p68 of 6,178+. A list of recent champions and the first holes in each table is given on another sheet.

The abbreviation AKL+MM means Arjen Lenstra and Mark Manasse. The abbreviation MullFac means Isle of Mull Factoring Group; it includes George Sassoon, Vivian Stevens and Richard Edwards. 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 69 are in # 3548, 3557, 3576, 3582, 3590, 3600 and 3610. The second holes done on Page 69 are in # 3550 and 3597. The third holes done on Page 69 are in # 3562, 3574, 3592, 3593 and 3594. The fourth holes done on Page 69 are in # 3558, 3604 and 3605. The fifth holes done on Page 69 are in # 3572, 3584, 3585 and 3586.

The smallest new factor reported on Page 69 has 24 digits. See # 3567. It comes from the extension. The smallest new factor of a number not from the extension has 25 digits and is in # 3609. The base 5 and base 11 tables will be extended at Update 2.8 in 1994.

Only 13 numbers smaller than 100 digits remain in Appendix C. A c92 and a c95 were added in # 3603 and # 3564. In addition, there remain five c97's, two c98's and four c99's. A c97 was added when the base 5 table was extended from 270 to 280.

There is a lot of news about Fermat numbers. Using his Cruncher, H. Dubner found six new Fermat factors: $763 \cdot 2^{6210} + 1$ divides F_{6208}, $303 \cdot 2^{6393} + 1$ divides F_{6390}, $645 \cdot 2^{8557} + 1$ divides F_{8555}, $81 \cdot 2^{12189} + 1$ divides F_{12185}, $55 \cdot 2^{15164} + 1$ divides F_{15161} and $33 \cdot 2^{18766} + 1$ divides F_{18757}. Also, F_{22} was shown composite in October 1993 by R. Crandall, J. Doenias, C. Norrie, and J. Young. They also found that the cofactors of F_{19} and F_{21} are composite.

I have corrected several of your addresses recently. If you move, please tell me.

Keep the factors coming!

Sam Wagstaff