December 28, 1994

Even though it is not quite full, Page 71 is being mailed now to beat the U.S. Postal rate increase.

Three 'Most Wanted' numbers were factored on Page 71. From the old list mailed with Page 69, the group CWI factored 3,319− c119 and Bob Silverman factored 10,149+ c123. From the same 'Most Wanted' list (and repeated on the list in Update 2.8) Silverman factored 5,206+ c143. The Number Field Sieve was used for all three of the factorizations.

Five 'More Wanted' numbers were factored on Page 71. I factored 2,548+ c157 with the Elliptic Curve Method. Arjen Lenstra and Bruce Dodson factored 6,187− c107, 2,898L c107 and 5,209+ c108 using the Quadratic Sieve. Silverman factored 11,131+ c129 by NFS. New wanted lists appear on the 'Champions' page. One number which appeared on the 'Most Wanted' list of Update 2.8 has been removed because it is in progress: Silverman did the NFS sieving for 3,307+ c137 and CWI is finishing it now.

Five of the 'Smaller but Needed' numbers were done on Page 71, all by QS. Boender, Lioen and te Riele finished the c99 of 2,914M which Peter Montgomery left on Page 70. The group MullFac factored 2,588+ c97 and 6,217− c97. Alec Muffett, Paul Leyland and Michael Graff factored 3,314+ c106 and 5,218+ c106. 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 the book. Seven of these numbers were factored on Page 71. Silverman factored 5,206+ c143, 10,149+ c123, and 11,131+ c129, all by NFS. CWI factored 3,319− c119 by NFS. Muffett, Leyland and Graff factored 3,314+ c106 by QS. Arjen Lenstra and Dodson factored 5,209+ c108 and 6,187− c107 by QS. At this writing, four of these numbers remain to be factored. (One of the four, 3,307+ c137, is nearly done. The other three are the base 3 numbers on the 'Most Wanted' list.)

There were no new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. A list of recent champions and the first holes in each table is given on another sheet.

The abbreviation BLtR means Henk Boender, Walter Lioen and Herman te Riele. MullFac means Isle of Mull Factoring Group; it includes George Sassoon, Vivian Stevens and Richard Edwards. CWI means Henk Boender, Marije Huizing, Walter Lioen, Peter Montgomery, Herman te Riele and Dik Winter at the Centrum voor Wiskunde en Informatica in Amsterdam. AKL+BAD means Arjen Lenstra and Bruce Dodson. M+L+G means Alec Muffett, Paul Leyland and Michael Graff. 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 71 are in # 3680, 3693, 3694, 3695, 3696, 3697, 3704 and 3725. The only second hole done on Page 71 is in # 3676. The third holes done on Page 71 are in # 3682, 3683, 3688, 3706 and 3731. The fourth holes done on Page 71 are in # 3681, 3713, 3720, 3721 and 3723. The fifth holes done on Page 71 are in # 3684, 3690, 3692 and 3728.

The smallest new factor reported on Page 71 has 24 digits. See # 3679. The largest number factored on Page 71 was 2,1181− c349. See # 3702. Not since 24 October 1990 has a larger number (2,1187+ c357) been factored.

The last Cunningham number with b^n smaller than 10^{140} has been factored. It is 11,131+ c129. See # 3704. Only four Cunningham numbers with b^n smaller than 10^{150} remain.

MullFac factored the last number printed in Appendix C of the Second Edition. It was 2,588+ c97. Only one number smaller than 100 digits remains in Appendix C. It is 2,1446L c97 and MullFac is doing it now.

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

Keep the factors coming!

Sam Wagstaff