May 22, 1995

One 'Most Wanted' number was factored on Page 72. From the old list mailed with Page 70, Bob Silverman and the group CWI factored 3,307+ c137 using the Number Field Sieve.

One 'More Wanted' number was factored on Page 72. Peter Montgomery and CWI factored 7,182+ by NFS. We will issue new Wanted lists with Update 2.9 later this summer.

All four of the 'Smaller but Needed' numbers were done on Page 72. Peter Montgomery factored 2,597+ c104 and 11,275M c105 by NFS. Paul Leyland factored 11,177− c104 by ppmpqs. I factored 7,203− c104 by ppmpqs. 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. One of these numbers was factored on Page 72. Bob Silverman and the group CWI factored 3,307+ c137 using the Number Field Sieve. At this writing, three of these numbers remain to be factored. They are the first three holes in the 3+ table.

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. Marije Huizing factored 6,223+ c107 by the General Number Field Sieve. A list of recent champions and the first holes in each table is given on another sheet.

MullFac means Isle of Mull Factoring Group; it includes George Sassoon, Vivian Stevens and Richard Edwards. 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 Huizing, Walter Lioen, Peter Montgomery, Herman te Riele and Dik Winter at the Centrum voor Wiskunde en Informatica in Amsterdam. BAD means Bruce Dodson. We use mpecm to refer to an Elliptic Curve program for the MasPar computer written by Arjen Lenstra and Brandon Dixon.

The only first hole done on Page 72 is in # 3746. The only second hole done on Page 72 is in # 3793. The third holes done on Page 72 are in # 3748, 3776. The fourth holes done on Page 72 are in # 3752, 3775, 3787, 3789. The fifth holes done on Page 72 are in # 3742, 3750.

The smallest new factor reported on Page 72 has 25 digits. See # 3757. The largest number factored on Page 72 was 2,1187− c344. See # 3756.

Only three Cunningham numbers with b^n smaller than 10^{150} remain to be done. They are 3,313+ c129, 11,142+ c141 and 12,137− c123.

Peter Montgomery factored the last base 11 Aurifeuillian from the second edition of the book, namely 11,275M c105. MullFac factored the last c97, 2,1446L. Georg Wambach and I each factored c101's which were left recently when larger numbers were factored. With the temporary exception of 7,371M, the smallest composite numbers left in the table have 104 digits, and there are but two of them: 3,385− and 5,280+.

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

Keep the factors coming!

Sam Wagstaff