June 21, 1994

This mailing includes Page 70 and Update 2.8. Several tables have been lengthened.

Two 'Most Wanted' numbers were factored on Page 70. The group 'CWI' factored 2,511− c123 using the Number Field Sieve. Bob Silverman factored 7,178+ using the same method.

Six 'More Wanted' numbers were factored on Page 70. From the old wanted lists in Update 2.7, Silverman factored 7,173− c146 using NFS. and Arjen Lenstra and Mark Manasse and the network factored 7,172+ c114 with the Quadratic Sieve. From the wanted lists mailed with Page 69, M. Huizing used the Elliptic Curve Method to factor 2,902M c111. Silverman factored 7,173+ by NFS. Peter Montgomery found a factor of 2,914M c133 by ECMFFT, leaving a 99-digit composite cofactor which is being finished by Boender, Lioen and te Riele. CWI factored 2,543− by NFS. New wanted lists appear in Update 2.8. Two numbers which appeared on the 'Most Wanted' list mailed with Page 69 have been removed because they are in progress: CWI is doing 3,319− c119 and Silverman is doing 10,149+ c123.

Contini and Peralta factored five of the 'Smaller but Needed' numbers, 2,519+ c104, 2,535+ c101, 2,854M c102, 2,874M c102 and 2,926L c103, all by QS. The group 'MullFac' factored 2,958L c92 by QS. Arjen Lenstra factored 2,575+ c101 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. Four of these numbers were factored on Page 70. Silverman factored 7,173− c146, 7,173+ c123, and 7,178+ c146, all by NFS. Arjen Lenstra, Mark Manasse and the network factored 7,172+ c114 by QS. At this writing, 11 of these numbers remain to be factored. (Two of them are in progress.)

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

There are three 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 Elliptic Curve factorization is the p42 of 2,603−. The new champion Special Number Field Sieve factorization is the c162 of 12,151−. A new category of champion was created when someone finally factored a Cunningham number with the General Number Field Sieve. The champion is the c105 of 3,367−. 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. C+P means Scott Contini and René Peralta. The abbreviation 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. 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. DHW means Frank Damm, F. P. Heider and G. Wambach. 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 70 are in # 3612, 3621, 3623, 3632, 3646, 3653, 3661 and 3671. The second holes done on Page 70 are in # 3633, 3636 and 3650. The third holes done on Page 70 are in # 3618, 3635, 3660 and 3673. The fourth holes done on Page 70 are in # 3613, 3616, 3651, 3662 and 3664. The fifth holes done on Page 70 are in # 3649, 3665 and 3669.

The smallest new factor reported on Page 70 has 25 digits. See # 3614 and # 3647. Several tables have been extended in Update 2.8.

Only five numbers smaller than 100 digits remain in Appendix C. They are four c97's (two of them from the extension) and the c99 of 2,914M. Most numbers between c98 and c103 have been done.

There is a new Mersenne prime. David Slowinski and Paul Gage found that $2^{859433} - 1$ is prime. They used a C90 at Cray Research.

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

Keep the factors coming!

Sam Wagstaff