

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907
November 23, 1998

Many “Wanted” numbers were factored on Page 80. From the wanted lists mailed with Page 76 in July, 1997, Bob Silverman and CWI factored the “More Wanted” number 5,242+. From the wanted lists mailed with Page 79 in July, 1998, Bob Silverman and CWI factored the “More Wanted” number 6,218+. From the wanted lists mailed with Update 2.B in February, 1998, the group CWI factored the “More Wanted” number 2,1138L. From the wanted lists mailed with Update 2.C in August, 1998, Bob Silverman factored the “Most Wanted” number 3,349+ and CWI factored the “More Wanted” numbers 3,358+, 3,361+, 3,362+ and 3,373-. All of the factorizations mentioned so far were done with the Number Field Sieve. The Elliptic Curve Method was used by Paul Zimmermann of ECMNET to factor the “More Wanted” number 7,211+, leaving a 128-digit composite cofactor which is still “Wanted”. Torbjörn Granlund factored the “More Wanted” number 10,197+ by ECM.

New wanted lists will be issued with Page 81.

On Page 80, Table 3+ joined Tables 3-, 5-, 6±, 7±, 11± and 12± in being completed up to the second edition limit. Only eight numbers remain from the higher base tables in the second edition. They include two, one and five numbers from Tables 5+, 10- and 10+, respectively.

Tables 3-, 5-, 6-, 7±, 10±, 11± and 12± were extended at Update 2.C to insure that every table has at least five holes.

CWI means Henk Boender, Stefania Cavallar, Marije Elkenbracht-Huizing, Walter Lioen, Peter Montgomery, Herman te Riele and Dik Winter at the Centrum voor Wiskunde en Informatica in Amsterdam. ECMNET means Paul Zimmermann, Torbjörn Granlund, Michel Quercia, Witold Grabysz, Vilmar Trevisan and many helpers who use Granlund’s GMP-ECM program.

There were four new champions for factoring Cunningham numbers on this page. Recall that a champion is one of the best two records in its class. The 53-digit factor of 2,677-, found by Conrad Curry of ECMNET, set a new record for factoring a Cunningham number by ECM. The 79-digit penultimate factor of 3,362+ found by CWI set a new record (second place) for penultimate prime factor of a Cunningham number. The factorization of the C178 cofactor of 3,373- by CWI set a new record (second place) for SNFS factorization by size. The factorization of the C176 cofactor of 3,376+ by CWI set a new record (second place) for SNFS factorization by difficulty. A list of recent champions and the first holes in each table is given on another sheet.

The first holes done on Page 80 are in # 4231, # 4233, # 4240, # 4243, # 4247, # 4265, # 4266, # 4267, # 4268, # 4269, # 4285, # 4286 and # 4287. No second holes were done on Page 80. The only third hole done on Page 80 is in # 4252. The fourth holes done on Page 80 are in # 4230, # 4250, # 4258, # 4259 and # 4270. The fifth holes done on Page 80 are in # 4239 and # 4257.

The smallest new factor reported on Page 80 has 30 digits. See # 4273. The largest number factored on Page 80 has 337 digits. See # 4255.

If your address changes, please tell me.

Keep the factors coming!

Sam Wagstaff