Factorising

For many years I have had an interest in finding the factors of large integers, especially Mersenne and Fermat numbers. When pressed to justify the relevance of this pursuit, I have usually replied that it is "only a hobby", although occasionally I have mentioned the connection between factorization and public key cryptosystems.

In the days before electronic computers or public-key cryptosystems, factorization was a good hobby to occupy wet Sunday afternoons. At least one famous factorization is said to have taken "a month of Sundays". An example of what can easily be done by hand is Euler's factorization of the Fermat number $F_5 = 2^{2^5} + 1 = 641 \cdot 6400417$. To verify this, consider the computation modulo 641:

$$5 \cdot 2^7 = -1 \Rightarrow 5^4 \cdot 2^{28} = 1 \Rightarrow (-16) \cdot 2^{28} = 1 \Rightarrow 2^{32} + 1 = 0.$$

Of the Fermat numbers $F_n = 2^{2^n} + 1$, only F_1 to F_4 are known to be prime; certainly F_5 to F_{21} are composite. However, the only complete factorizations known until recently were those of F_5 (Euler), F_6 (Landry), and F_7 (Morrison and Brillhart).

It is not difficult to show that any factor of F_n must be of the form $2^{n+2}k + 1$ (e.g. for $n = 5$ we have factors for $k = 5$ and $k = 52347$). In 1980 John Pollard and I realised how to take advantage of this to speed up the search for factors of F_n by a variant of Pollard's "rho" algorithm. This enabled us to find the factorization

$$F_8 = 1238926361552897 \cdot p_{62},$$

where p_{62} is a 62-decimal digit prime number. Pollard constructed a mnemonic

"I am now entirely persuaded to employ the method,
a handy trick, on gigantic composite numbers"

to advertise our method and enable us to remember the smaller factor of F_8.

Almost ten years later, much to my surprise, I succeeded in factorizing the 617-digit Fermat number $F_{11} = 2^{2^{11}} + 1$. In fact

$$F_{11} = 319489 \cdot 974849 \cdot p_{21} \cdot p_{22} \cdot p_{564}$$

where the two 6-digit factors were already known (Cunningham, 1899), the 21-digit and 22-digit prime factors

$$p_{21} = 167988556341760475137$$

and

$$p_{22} = 3560841906445833920513$$

Appeared (slightly abbreviated) in the "Hobbies and Mathematics" section of *Australian Math. Soc. Gazette* 16 (1989), 154-155.

E-mail address: rpb@cslab.anu.edu.au rpb118 typeset using TEX

were found using the two-phase elliptic curve method, and p_{564} is a 564-decimal digit prime. (How to prove its primality is another story.)

As an "application" of factorization, Graeme Cohen, Herman te Riele and I have recently proved that there is no odd perfect number less than 10^{300}. The main part of the proof was generated by computer, has about 13,000 lines, and involves many thousands of nontrivial factorizations.

References to the results mentioned above are available from the author.

The following problems may appeal to readers interested in verbal or numerical puzzles:

Problem 1: Find elegant mnemonics to describe the factors p_{21} and p_{22} of F_{11}. A zero digit could be encoded by a word of ten letters, or alternatively the digit n could be encoded by a word of $n+1$ letters ($n = 0, 1, \ldots, 9$).

Problem 2: Complete the factorizations of

$$F_9 = 2424833 \cdot c_{148}$$

and

$$F_{10} = 45592577 \cdot 6487031809 \cdot c_{291},$$

where c_k denotes a composite number of k decimal digits.

Richard P. Brent
Computer Sciences Laboratory
Australian National University

References

1. R. P. Brent, "Some integer factorization algorithms using elliptic curves", *Australian Computer Science Communications* 8 (1986), 149-163.
2. R. P. Brent, "Factorization of the eleventh Fermat number (preliminary report)", *AMS Abstracts* 10 (1989), 89T-11-73.
3. R. P. Brent, G. L. Cohen and H. J. J. te Riele, "Improved techniques for lower bounds for odd perfect numbers", Technical Report, Computer Sciences Laboratory, Australian National University, 1989, to appear.
4. R. P. Brent and J. M. Pollard, "Factorization of the eighth Fermat number", *Mathematics of Computation* 36 (1981), 627-630.
5. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., "Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers", *Contemporary Mathematics*, Vol. 22 (2nd edition), American Math. Soc., Providence, Rhode Island, 1988.
6. H. W. Lenstra, Jr., "Factoring integers with elliptic curves", *Ann. of Math.* 126 (1987), 649-673.
7. M. A. Morrison and J. Brillhart, "A method of factoring and the factorization of F_7", *Mathematics of Computation* 29 (1975), 183-208.
8. R. L. Rivest, A. Shamir and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystems", *Comm. ACM* 21 (1978), 120-126.