On Factoring $2^k \pm 1$

Peter Hilton and Jean Pedersen

The cover of the October, 1990 issue of the excellent South African student journal *Mathematical Digest*, founded and edited by our good friend John Webb, showed the factorization of the ninth Fermat number, $F_9 = 2^{29} + 1$. In particular, it showed that the smallest prime factor of F_9 is 2,424,833. John Webb stated that the factorization of the ninth Fermat number took six weeks of computation on 1,000 linked computers.

We thought it might be of interest to show how the fact that 2,424,833 is a factor of F_9 could be *verified* in just over an hour and a half using a hand calculator.[1] We first need to describe our notion of a *symbol*, and state our *Binary Quasi-order Theorem* concerning the symbol. After that we will show how executing the algorithm which produces the symbol and using the theorem can provide a verification that 641 is a factor of $F_5 = 2^{25} + 1$. The reader should then have no difficulty duplicating the process to verify factorizations of other F_n (where at least one factor is known). The implications are obvious–if it is suspected that a certain number, say b, is a factor of F_n, then there is an easy way to check the suspect. The difficulties are also obvious–there are lots of suspects and very few culprits! Nevertheless, it may be satisfying to be able to "check" such apparently inaccessible facts as those stated in our opening paragraph by (i) using only relatively small numbers (no number occurring in our algorithm is larger than the number b in the symbol below, so that verifying that 2,424,833 is a factor of $2^{29} + 1$ involves no number bigger than 2,424,833), and (ii) using only simple arithmetic (which may be carried out on a hand calculator). Let us proceed.

The symbol we will construct is this:

$$b \left| \begin{matrix} a_1 & a_2 & . & . & . & a_r \\ k_1 & k_2 & . & . & . & k_r \end{matrix} \right| \quad (*)$$

where a_i, b are odd, $a_i < b/2$, and $b = a_i + 2^{k_i} a_{i+1}$, $i = 1, 2, \ldots, r$ ($a_{r+1} = a_1$). We have shown (Hilton & Pedersen, 1985, 1987a) that such a symbol always exists for a given b and $a = a_1$, and it is plainly uniquely determined by b and a if we insist that the a_i are all distinct. In the same articles we have proved the following theorem.

> **The Binary Quasi-order Theorem**: If the symbol (*) is reduced (i.e., $\gcd(b, a_1) = 1$) and contracted (i.e., the symbol involves no repeated a_i), then the quasi-order[2] of 2 mod b is $k = \sum_{i=1}^{r} k_i$ and, in fact, $2^k \equiv (-1)^r \bmod b$.

The theorem has the consequence that b is a factor of $2^k - (-1)^r$. Notice, however, that we *start* with the factor b and find the smallest k such that b is a factor of $2^k \pm 1$ (of course determining whether we should take +1 or –1). This is not at all the procedure taught in the traditional study of factorization, which is typically approached merely as an arithmetical exercise. Notice, too, that we read k and r off the symbol (*), but that k and the parity (odd or even) of r depend only on b, although the symbol depends on b and a. This independence of a is so remarkable a feature of our theorem that we feel we should illustrate it with an example.

Example 1: We have the following reduced and contracted symbols (we will explain the construction of such a symbol, in some detail, below):

$$41 \left| \begin{matrix} 1 & 5 & 9 \\ 3 & 2 & 5 \end{matrix} \right|$$

and

$$41 \left| \begin{matrix} 3 & 19 & 11 & 15 & 13 & 7 & 17 \\ 1 & 1 & 1 & 1 & 2 & 1 & 3 \end{matrix} \right| .$$

In both cases $k = 10$; in the first case $r = 3$, in the second $r = 7$. Thus *either* symbol tells us that the quasi-order of 2 mod 41 is 10, and further, that $2^{10} \equiv -1 \bmod 41$, so that $41 \mid 2^{10} + 1$.

To justify our description of the quasi-order algorithm as a means of factorizing $2^k \pm 1$, we should show how to find the complementary factor. This is already available

Peter Hilton is Distinguished Professor of Mathematics at the State University of New York at Binghamton. He is well known for his research in algebraic topology, homological algebra, and group theory.
Jean Pedersen is an Associate Professor of Mathematics at Santa Clara University in California. She has published articles on polyhedral geometry, combinatorics, and number theory.
Professors Hilton and Pedersen recently visited the University of Otago, New Zealand, where they worked with Professor Derek Holton on a book designed to attract bright high school students and undergraduates to mathematics.

from the symbol, as the following theorem shows (see Hilton & Pedersen, 1987a, 1987b).

> **The Complementary Factor Theorem**: If the symbol (*) is reduced and contracted, then $aB = Ab$, where $B = 2^k - (-1)^r$ and
> $A = 2^{k-k_r} - 2^{k-k_r-k_{r-1}} + 2^{k-k_r-k_{r-1}-k_{r-2}} -$
> $\ldots + (-1)^r 2^{k_1} - (-1)^r$.
> In particular, $2^k - (-1)^r = bc$, where $c = A/a$, which is an integer.

Let us return to our example.

Example 1 (revisited): The first symbol has $a = 1$ and $A = 2^5 - 2^3 + 1 = 25$, so that $c = 25$. The second symbol has $a = 3$ and $A = 2^7 - 2^6 + 2^4 - 2^3 + 2^2 - 2 + 1 = 75$, so that, again, $c = 25$. Thus, either symbol tells us that $2^{10} + 1 = 41 \times 25$.

Notice that this factorization (like all of the factorizations in this article) is established without ever expressing $2^{10} + 1$ in base 10. Indeed, our arithmetic involves only dividing numbers less than or equal to 40 by 2, taking powers of 2 up to at most 2^9 (actually, only up to 2^7 in this case), and simple addition and subtraction.

We now go into greater detail on how to use our theorems, especially in connection with factorizations of Fermat numbers. Suppose we want to find the quasi-order of 2 mod 641. In other words, we wish to find the smallest positive integer k such that $2^k \equiv \pm 1 \bmod 641$. We begin by constructing a symbol (*) with $b = 641$, choosing $a_1 = 1$. Begin by writing

$$641 \left| \begin{array}{c} 1 \\ \\ \end{array} \right. .$$

Then calculate as follows (using a hand calculator is convenient, but not necessary): $641 - 1 = 640$, $640/2 = 320$, $320/2 = 160$, $160/2 = 80$, $80/2 = 40$, $40/2 = 20$, $20/2 = 10$, $10/2 = 5$ (and STOP, because 5 is odd). These calculations show that $641 = 1 + 2^7(5)$, and hence $k_1 = 7$ and $a_2 = 5$. Now record $k_1 = 7$ (the number of times we divided by 2) directly below $a_1 = 1$, and record $a_2 = 5$ (the last quotient) to the immediate right of $a_1 = 1$. The symbol is then extended to

$$641 \left| \begin{array}{cc} 1 & 5 \\ & \\ 7 & \end{array} \right. .$$

Next, repeat the algorithm by calculating as follows: $641 - 5 = 636$, $636/2 = 318$, $318/2 = 159$ (stop here because 159 is odd). These calculations show that $641 = 5 + 2^2(159)$, and hence $k_2 = 2$ and $a_3 = 159$. Now record $k_2 = 2$ directly below $a_2 = 5$ and $a_3 = 159$ to the immediate right of $a_2 = 5$, so that the symbol grows to

$$641 \left| \begin{array}{ccc} 1 & 5 & 159 \\ & & \\ 7 & 2 & \end{array} \right. .$$

The algorithm is continued until the a_i's begin to repeat; thus, in this example, we stop when the quotient, after repeated division by 2, is 1. The reader may wish to carry out the algorithm until this happens to verify that the completed symbol will be

$$641 \left| \begin{array}{ccccccccc} 1 & 5 & 159 & 241 & 25 & 77 & 141 & 125 & 129 \\ & & & & & & & & \\ 7 & 2 & 1 & 4 & 3 & 2 & 2 & 2 & 9 \end{array} \right. . \qquad (**)$$

From (**) we see that $\sum_{i=1}^{9} k_i = 7 + 2 + 1 + 4 + 3 + 2 + 2 + 2 + 9 = 32$ and that $r = 9$, which is odd. Hence, by the Binary Quasi-Order Theorem, we conclude that 32 is the smallest positive integer k such that $2^k \equiv \pm 1 \bmod 641$, and that , in fact, $2^{32} \equiv -1 \bmod 641$. Thus, $641 \mid 2^{32} + 1 = 2^{25} + 1$, and so, as promised, we have shown that 641 is a factor of F_5.

It is natural to ask what would have happened if we had started our symbol with one of the other suitable numbers for a_i. We know we would have obtained the same information as above, but could we ever obtain a shorter symbol? To illustrate part of the answer, observe that if we had started our symbol with any of the numbers in the top row of (**), say $a_1 = 5$, we would have obtained essentially the same symbol with the position of the entries permuted cyclically, as shown in (***) below.

$$641 \left| \begin{array}{ccccccccc} 5 & 159 & 241 & 25 & 77 & 141 & 125 & 129 & 1 \\ & & & & & & & & \\ 2 & 1 & 4 & 3 & 2 & 2 & 2 & 9 & 7 \end{array} \right. . \qquad (***)$$

Of course, the information contained in (**) and (***) is exactly the same. However, if we had started with $a_1 = 3$, then the symbol would have been very different and, as the reader may verify, would actually have contained 15 entries. If we regard (**) and (***) as the same symbol (think of the numbers to the right of 641 as written around a cylinder), then, as a matter of fact, for $b = 641$ there are just 10 different contracted symbols, each with an odd number of entries varying in length between 9 and 23. But in each case the sum of the entries of the bottom row is 32.

The reader may now check his or her understanding of how to construct a symbol by actually constructing the symbols presented in Example 1. Next, the more ambitious reader may wish to construct a symbol and use our theorem to show that 274,177 is a factor of F_6–or that

2,424,833 is a factor of F_9. The symbol with $b = 274,177$ that begins with $a_1 = 1$ has 19 entries, and we have not found any symbol with $b = 274,177$ having fewer entries. Further, with $b = 2,424,833$, the symbol beginning $a_1 = 1$ has 237 entries, but the symbol beginning with $a_1 = 65,537$ has only 213 entries. We do not know whether or not the symbols we have found verifying the factors of F_6 and F_9 are the shortest possible or not. Can any reader do better? (Notice that $65,537 = F_4$!.)

We now show how our second theorem enables us to obtain the complementary factor for our factorization of F_5 using the symbol (**). We repeat the calculation with the symbol (***) to give the reader experience.

Example 2–referring to (**)

$A = 2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^{10} + 2^9 - 2^7 + 2^0 = 6,700,417$, where

23 = 32 - 9
21 = 32 - 9 - 2
19 = 32 - 9 - 2 - 2
.
.
.
0 = 32 - 9 - 2 - 2 - 2 - 3 - 4 - 1 - 2 - 7

(Hint: Derive these exponents from the numbers in the bottom row of (**) read backwards.) Thus $F_5 = 641 \times 6,700,417$. (Notice that the calculation is, to some extent, self-checking, as the last exponent in the expression for A must be 0.)

Example 3–referring to (***)

$A = 2^{25} - 2^{16} + 2^{14} - 2^{12} + 2^{10} - 2^7 + 2^3 - 2^2 + 2^0 = 33,502,085$, where

25 = 32 - 7
16 = 32 - 7 - 9
14 = 32 - 7 - 9 - 2
.
.
.
0 = 32 - 7 - 9 - 2 - 2 - 2 - 3 - 4 - 1 - 2

(Hint: Look at the numbers in the bottom row of (***).) Since $a = 5$ in (***), we find that the complementary factor is $33,502,085/5 = 6,700,417$. Thus, again, $F_5 = 641 \times 6,700,417$.

We close with one final point about the Binary Quasi-Order Theorem. We have stressed that it gives us a means of obtaining, for a given odd number b, a positive integer k and a parity r such that $2^k \equiv (-1)^r \bmod b$. However, as we have also said, it does more because the k we obtain from our algorithm is the *smallest* positive integer such that $2^k \equiv \pm 1 \bmod b$. For example, with $b = 7$ we find $k = 3$ and $2^3 \equiv 1 \bmod 7$; but of course it is also true that $2^6 \equiv 1 \bmod 7$. Again, with $b = 9$ we find $k = 3$ and $2^3 \equiv -1 \bmod 9$; but $2^6 \equiv 1 \bmod 9$, and $2^9 \equiv -1 \bmod 9$.

However, in the case of the Fermat numbers, it is natural not to stress the minimality of k. For if $2^{2^n} \equiv -1 \bmod b$, then 2^n must be minimal! This follows from the observations (i) that if *any* power 2^l is congruent to $-1 \bmod b$, then the minimal power of 2 congruent to $\pm 1 \bmod b$ is, in fact, congruent to $-1 \bmod b$; and (ii) if the minimal power of 2 congruent to $-1 \bmod b$ is 2^s then *any* power 2^l congruent to $-1 \bmod b$ has $l = st$, *with t odd*. Thus if $2^{2n} \equiv -1 \bmod b$ and the quasi-order of 2 mod b is s, then $2^n = st$, with t odd. But this forces $t = 1$ and $2^n = s$, so 2^n is itself the quasi-order of 2 mod b.

Readers may be intrigued to know that our algorithm arose in designing a systematic way to fold straight strips of paper into regular convex and star polygons. For details see Hilton and Pedersen, 1987a and 1988. Ambitious readers eager to know more about the relation of Fermat numbers and symbols might like to consult Hilton and Pedersen, in press.

Thoughts on Mathematics Education

What implications might our article have for the teaching of mathematics? First and foremost, it shows that a little mathematical thought can avoid a huge amount of machine time. Thus the availability of machines certainly does not render the mathematical analysis of a problem unnecessary–on the contrary, it stimulates it. The proper mathematical use of machines is not to crunch numbers but to conduct mathematical experiments, on the basis of which hypotheses may be formulated and theorems proved. We would also like to think that our article shows that mathematics can be fun and can contain the element of surprise. We are glad to be able to report that elementary students who had thought themselves to possess no mathematical talent whatsoever have derived great pleasure, even excitement, from calculating quasi-orders by our algorithm, and then verifying the resulting factorizations on their calculators.

Notes

[1]When the numbers were large, or we were tired, we used a Casio fx-7000 graphics calculator to carry out the computations. We found that scrolling the screen was an advantage because we could easily see the previous entries, but any hand calculator could be used. With only pencil and paper, the necessary calculation could be done in less than three hours.

[2]Here we understand the *quasi-order* of 2 mod b, where b is odd, to be the smallest integer k such that

$2^k \equiv \pm 1 \bmod b$. Of course, there is a corresponding definition for the quasi-order of t mod b, where t is an integer relatively prime to b. Our algorithm may be generalized also (see Hilton & Pedersen, 1986, 1987a), to give a Quasi-order Theorem for a general $t \geq 2$.

References

Hilton, P., & Pedersen, J. (1985). Folding regular star polygons and number theory. *Mathematical Intelligencer, 7*(1) 15-26.

Hilton, P., & Pedersen, J. (1986). The general quasi-order algorithm in number theory. *International Journal of Mathematics and Mathematical Sciences, 9*(2), 245-251.

Hilton, P., & Pedersen, J. (1987a). Geometry in practice and numbers in theory. *Monographs in Undergraduate Mathematics, 16*. Greensboro, NC: Department of Mathematics, Guilford College.

Hilton, P., & Pedersen, J. (1987b). On the complementary factor in a new congruence algorithm. *International Journal of Mathematics and Mathematical Sciences*, *10*(1), 113-123.

Hilton, P., & Pedersen, J. (1988). *Build your own polyhedra*. Menlo Park, CA: Addison-Wesley.

Hilton, P., & Pedersen, J. (in press). On folding instructions for products of Fermat numbers. Preprint available from the authors.

Editorial *(continued from p. 2)*

in teaching must be presented, but documentation is difficult and it is nearly impossible to make the case for promotion based primarily on excellence in teaching. Further, at many places, scholarly productivity in teaching means writing articles about teaching for refereed journals. Materials (e.g. articles, books, computer programs, videos, multimedia) provide the tangible record.

Third, there is a continuous problem of communicating the nature of scholarly productivity in mathematics education to our peers who are not in mathematics education (but who serve on review committees). This is as much a problem whether our peers are generalists in education, specialists in some other area of education, or in some other field. It is particularly a problem when our peers are in mathematics since many mathematics educators are housed in mathematics departments and judged by colleagues who are not always supportive of work in mathematics education.

Sadly, the promotion and tenure review process can be difficult and impersonal while it is intended to be impartial. It often takes most of a year to run its course, the committees are usually anonymous, and candidates seldom have any opportunity for input into the process other than by formal written procedures. The JPBM Report (1994) offers six guiding principles to assist faculty in the mathematical sciences to work on each institution's definition of the reward structure (pp. 28-38).

Anticipating the process of promotion and tenure review is one aspect of career planning and is best viewed in that light. The supporting evidence in a file or dossier does not come together just in the months before it is submitted but rather it is accumulated and assessed from the start of one's appointment. If the items of evidence for a dossier are prepared and accumulated continuously, a lot of the unnecessary pressure of the promotion year can be alleviated. Some institutions will have mentors or administrators who facilitate and assist in this long-term preparation. If such assistance is not provided, a young faculty member is well advised to informally seek out mentors.

Another advantage of long term planning is that it provides a framework for deciding whether assignments and activities might add to the evidence in support of promotion. One might still decide to follow an activity of interest for some other reason, but at least the decision is made within a framework.

Generally, the promotion and tenure process serves the university and its faculty well. It continues to be driven by faculty input and it facilitates one's career development. It is our "quality control" mechanism and despite anxiety for meeting the requirements and procedures, most of us would not want it any other way.

Reference

Joint Policy Board for Mathematics. (1994). Recognition and Rewards in the Mathematical Sciences. Report of the Committee on Professional Recognitions and Rewards. *Providence, RI: American Mathematics Society.*