MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 463-474

HOW WAS F_6 FACTORED?

H. C. WILLIAMS

Dedicated to the memory of my friend, D. H. Lehmer

ABSTRACT. In 1880 at the age of 82 Fortuné Landry factored the 20 digit number $F_6 = 2^{64} + 1$. How did he do it? Landry himself never described how he factored F_6; however, he did leave enough clues in his work and letters to provide some indication of the ideas with which he was working. In this paper we present a likely reconstruction of Landry's technique.

1. INTRODUCTION

On July 12, 1880 Fortuné Landry [8] published the following short announcement:

> "I have just factored the number
>
> $$2^{64} + 1 = 18446744073709551617.$$
>
> This number is the product of two factors 274177 which is prime, and 67280421310721. I do not currently know if this last factor is a prime."

This remarkable achievement, made even more so when one considers that Landry was 82 at the time, has unfortunately not received the attention that it deserves. There are two reasons for this: first, the factor 274177 is so small that many would tend to regard it as having been found by the simple process of trial division. This was *not*, however, the way Landry factored F_6. This brings us to the second reason that his work has been largely ignored: he never published any account of how he did factor F_6. Nevertheless, he did leave several clues as to how he did it, and the purpose of this paper is to use these clues to reconstruct the probable method that he used.

It should be mentioned that according to Lucas [17] both Landry and LeLasseur succeeded later in proving that the larger factor of F_6 is a prime. This seems to be the only contribution that LeLasseur made to the problem of factoring F_6.

In 1869 Landry [7] published a pamphlet containing the complete factorization of each integer of the form $2^n \pm 1$ for $n \leq 64$, with the exception of four numbers that he was unable to factor: $2^{59} - 1$, $2^{61} - 1$, $(2^{61} + 1)/3$, $2^{64} + 1$.

Received by the editor November 23, 1991.
1991 *Mathematics Subject Classification*. Primary 11A51, 01A55.
Research supported by NSERC of Canada Grant #A7649.

In [15, pp. 238–240] Lucas states that Landry later factored $2^{59} - 1$ and that Landry thought (probably because they were difficult to factor) that the remaining three were prime. In fact, in 1877 Lucas [13] knew that $F_6 = 2^{64} + 1$ is composite, but his technique (see [15, p. 238, p. 313]) did not reveal the factors. He [14] also proved the following

Theorem. *The prime divisors of* $2^{4q} + 1$ *are of the form* $16hq + 1$. □

In 1891 Lucas [17] stated that by using this result for simplifying the search for factors of F_6, Landry was able to factor F_6 after a labor of several months. Landry, however, said very little indeed about how he did this. One of the few explicit references in print that Landry made to his technique is in a letter to Lucas, which, fortunately, Gérardin published in *Sphinx-Oedipe* [9]. Because of its importance in this investigation, we reproduce it in full here. It should be mentioned that all the work reported on in this paper was originally written in French; thus, all quotes are translations of this French into English.

> Paris, 7 July 80
>
> Sir
>
> The number $2^{64} + 1$ or 18446744073709551617 is the product of two factors 67280421310721 and 274177, the latter being prime.
>
> Notice of the result has been sent to the Academy today.
>
> Your advice proved to be ever the wiser, considering that the smaller factor is relatively small and would require only about 1000 operations to discover by using the standard method of successive divisions.
>
> I had set up my calculations with the intention of taking the process to its end and thus I would be able to announce a result. There was not much left to do when I unexpectedly came upon the factor 274177. After such a lengthy process, I could hardly believe it. The procedure I use first considers the largest divisors, less than $\sqrt{N}$ of course, of the number to be factored.
>
> One could very well conclude from this that the other factor is a prime, but besides the possibility that I could have erred during the course of such a lengthy process, in order to facilitate my work, I purposely left out divisors of particular forms which would be easy to deal with separately.
>
> I thank you very much for your interest in this work. This last 14-digit number will allow me to describe the methods that I use. I hope to arrive for the Congress quite early. Could you please let me know where I would be able to obtain the pamphlet where you will mention my work.
>
> My thanks to you.
>
> Landry

According to Lucas's theorem, any prime factor of F_6 must be of the form $256k+1$. Since $274177 = 256 \cdot 1071 + 1$, we see what Landry was talking about in his third paragraph. Also, in [16] Lucas points out that the smallest factor for each of the Fermat numbers $F_n = 2^{2^n} + 1$ of (then) known factorization is the smallest prime of the form $k2^{n+2} + 1$. Thus, he was likely of the belief that one factor of a composite Fermat number might tend to be small. This, undoubtedly, was the advice that he gave to Landry. It appears, however, that Landry did not take Lucas's advice because he states in his next paragraph that he wanted to set up his technique in order to test for all possibilities. Since $\sqrt{F_6}/256 \approx 1\cdot 7 \times 10^7$ is so large, trial division just wouldn't do the job. Indeed, in 1867 he [6] had estimated that attempting to prove F_6 a prime by trial division (using the then-known form of the factors as $128k+1$ instead of $256k+1$) could take up to 3000 years. We will explain certain other features of this letter as they become relevant to our discussion.

2. Landry's early factoring ideas

In order to get some familiarity with how Landry approached the factoring problem, it is of some value to discuss his work prior to 1869. Apart from some simple tables of primes and factors, Landry's first significant work on factoring is his 1859 pamphlet [5] in which he proved that $2^{31}-1$ is a prime. This had also been done in 1772 by Euler, but Landry's interest in the problem was in reducing the amount of work to be done.

Euler had realized that any prime factor p of $N = 2^{31}-1$ must have the form $1+31k$. He also was aware that since $(2/p) = 1$, p must be congruent to ± 1 modulo 8. Thus, $p = 248k+1$ or $248k+63$ for some integer k. Since $[\sqrt{N}/248] = 186$, this means that after 372 trial divisions (or fewer if one excludes composite values of $248k+1$ and $248k+63$), N can be shown prime.

Landry approached this problem as follows. If N is composite, then

$$N = (62x+1)(62x'+1),$$

where $x, x' \in \mathbf{Z}$, and with no loss of generality $62x+1$ is a prime such that $62x+1 < \sqrt{N}$, i.e., $x < 748$. Since

$$N = 62^2 \cdot 558658 + 62 \cdot 37 + 1,$$

we get

$$x + x' = 62h + 37, \tag{2.1}$$

$$xx' = 558658 - h \tag{2.2}$$

for some $h \in \mathbf{Z}^+$. It follows from (2.1) and (2.2) that $2|h$, $h \equiv 3$ or $4 \pmod 5$, and $h \equiv 1$ or $6 \pmod 9$. Hence,

$$h = 90h' + k,$$

where $k \in \{24, 28, 64, 78\}$. If we solve (2.1) and (2.2) for x and x', we get

$$2x,\, 2x' = 62h + 37 \pm \sqrt{62^2h^2 + 4592h - 2233263}. \tag{2.3}$$

If we eliminate x' from (2.1) and (2.2), we get

$$h = \frac{558658 - x(37-x)}{62x+1} \in \mathbf{Z}^+. \tag{2.4}$$

Substitute $90h'+k$ for h and we find

$$h' = \frac{558658 - k - x(62k - 137 - x)}{90(62x+1)} \in \mathbf{Z}^{\geq 0}. \tag{2.5}$$

Now we may assume that $x < 748$; but, if $x \geq 80$, then from (2.5) we see that $h' < 1$ and therefore $h' = 0$. If, however, $h' = 0$, then from (2.3)

$$62^2k^2 + 4592k - 2233263 = t^2 \qquad (t \in \mathbf{Z})$$

for some $k \in \{24, 28, 64, 78\}$. As this is not the case, we must have $x < 80$. In fact, if $x \geq 60$, then from (2.5) one has $h < 2$. Since

$$62^2(k+90)^2 + 4592(k+90) - 2233263 \neq t^2 \qquad (t \in \mathbf{Z})$$

for any $k \in \{24, 28, 64, 78\}$, we must have $x < 60$.

Consider now $62x+1$. We know from Euler's observation that $62x+1 \equiv \pm 1 \pmod 8$. Also, $62x+1 \not\equiv 0 \pmod{3, 5, 7}$. It follows that since $x < 60$, we can only have

$$x \in \{5, 9, 20, 21, 24, 33, 41, 44, 45, 48, 53, 56\}.$$

However, (2.4) is not satisfied for any of these 12 values of x; hence, N must be a prime. Notice that with just 12 trial divisions (with the dividend much smaller than N) and 8 perfect square tests, Landry was able to show that N is a prime.

Later in 1867 Landry [6] announced that he had discovered a very simple principle which he had used to obtain a number of factorizations of numbers of the form $2^n \pm 1$. He did not reveal this method, however; instead he presented several of his more impressive factorizations. This work was followed by the table in [7]. What was this new method? Landry finally described it in a letter [10] that he wrote to Charles Henry.

Let $N = ab$, where a, b are odd and $a > b$. Put $x = (a+b)/2$, $y = (a-b)/2$, and we get

$$x^2 - N = y^2. \tag{2.6}$$

Determine for $x = [\sqrt{N}]+1, [\sqrt{N}]+2, \ldots$ a value for y such that (2.6) holds. Certain values of x can be easily eliminated by making use of moduli m such that for these values of x we cannot have

$$x^2 - N \equiv y^2 \pmod{m}.$$

For example, if $m = 5$ and $N \equiv 2 \pmod 5$, then $x \not\equiv 0, 4 \pmod 5$. Today, we call such moduli *exclusion moduli.*

This method of factoring, which is particularly effective if the two factors a and $b = N/a$ are close in value, had been discovered many years earlier by Fermat [3]. Landry, however, remained unaware of Fermat's work until Henry, one of the people involved in publishing Fermat's complete works, put it in print in his *Recherches sur les Manuscrits de Fermat.* It was the similarity of Fermat's idea to that of Landry that particularly struck Landry and caused him to write his letter to Henry.

Landry also noted in this letter that if $N = 2^n \pm 1$, then for "certain" values of n the process can be accelerated because we know that

$$a = 2nu + 1, \qquad b = 2nv + 1 \qquad (u, v, \in \mathbf{Z}).$$

Hence, $x = 1 + ns$, $y = nt$ $(s, t \in \mathbf{Z})$. Although he did not say so, he must have been aware that from (2.6) these latter results allow us to restrict the value of x to a single residue class modulo n^2, a result first put in print by Pepin

[18]. He went on to say that one could (by using other moduli) accelerate the course of the calculations, but that it is then necessary to follow up each series of possible values of x separately.

Is this the method that Landry used to factor F_6? No, for he mentioned that it was found to be insufficient for the larger numbers that he turned to after 1867. In fact, he said that he had to find another method, and it was by this new method that he had recently factored F_6. Also, at the time of writing this letter (July or August of 1880) he stated that he was busy writing up this new method.

3. Landry's later factoring ideas

It appears that Landry published most of this new method in the Proceedings of the Congress that he referred to at the end of his letter to Lucas. This annual conference was sponsored by the French Association for the Advancement of Science, and Landry's paper [11] was presented at the session devoted to mathematics on August 16, 1880. Unfortunately, this discussion of his techniques gives the impression that they are almost trivial; this is certainly well illustrated by the synopsis of the paper given in Dickson [2, p. 371]. In fact, however, if one reads the paper carefully, it is clear that the new method is a further development of the idea presented in [5]. In view of this, we will rearrange the order of topics in this paper and modify them somewhat for our presentation here. Also, in order to aid us in showing what is going on, we use upper case letters to refer to quantities that are either known or easily calculated and lower case letters to represent those quantities that are difficult to evaluate.

Suppose we wish to factor $N = f_1 f_2$, where we know in advance that

$$f_1 = Pn_1 + A, \quad f_2 = Pn_2 + A \qquad (n_1, n_2 \geq 1).$$

Landry referred to factors f_1, f_2 such that $f_1 \equiv f_2 \pmod{P}$ as being "similar" modulo P. By substitution we get

$$Pn_1n_2 + A(n_1 + n_2) = (N - A^2)/P = PQ + R; \tag{3.1}$$

hence,

$$A(n_1 + n_2) \equiv R \pmod{P}$$

and

$$n_1 + n_2 = R' + Ph, \tag{3.2}$$

where $R' \equiv A^{-1}R \pmod{P}$ $(0 \leq R' < P)$. Putting (3.2) into (3.1) and using

$$Q' = Q - (AR' - R)/P,$$

we get

$$n_1n_2 = Q' - Ah. \tag{3.3}$$

Solving (3.2) and (3.3) for h, we find that

$$h = \frac{Q' - n_1(R' - n_1)}{Pn_1 + A} \in \mathbf{Z}^{\geq 0}. \tag{3.4}$$

With regard to the simultaneous equations (3.2), (3.3), Landry was aware of the following

Theorem. *If p is an odd prime and $p \nmid PN$, then there are exactly $(p+(N/p))/2$ values of h* (mod p) *such that* (3.2) *and* (3.3) *can hold simultaneously modulo p.* □

Furthermore, if $(N/p) = 1$, we can get a case of similar factors modulo p, i.e., $n_1 \equiv n_2 \pmod{p}$. To a single value of $h \pmod{p}$, there correspond two possible forms $n_1 \equiv a$, $n_1 \equiv b \pmod{p}$. These forms of n_1 Landry called the "conjugate" values to that of h modulo p.

Landry preferred the use of (3.4) to the usual trial division process because the numerator was less than N. Also, we can assume that $n_1 < \sqrt{N}/P$. Landry states that "when the values of N become large, it becomes necessary, in order to avoid numerous operations, to resort to forms of h and n, for moduli $2, 3, 6, 5, \ldots$ and to put aside for separate treatment the similar factors of N which result when $n_1 \equiv n_2$ for any of these moduli." That is, we attempt to restrict h by using certain moduli and (3.2), (3.3) with respect to these moduli. With the exception of the number[1] 6, Landry's moduli were intended to be the small primes.

Suppose G is a product of certain moduli and K a possible value of h modulo G. We have

$$h = Gh' + K \qquad (h' \geq 0,\ 0 \leq K < G),$$

and

$$h' = \frac{Q' - n_1(R' - n_1)}{G(Pn_1 + A)} - \frac{K}{G}.$$

Notice that if n_1 exceeds some bound B ($\approx Q'/(PG)$), we must get $h' < 1$. Since this forces $h' = 0$, we must have

$$(3.5) \qquad \begin{cases} n_1 + n_2 = R' + PK, \\ n_1 n_2 = Q' - AK \end{cases}$$

when $n_1 > B$; but, if (3.5) has no solution in integers, then this possible value of $h \pmod{G}$ can be eliminated. On the other hand, if (3.5) has a solution (n_1, n_2), then $N = f_1 f_2$, where $f_1 = Pn_1 + A$, $f_2 = Pn_2 + A$.

Notice that there are two problems here: (1) find a convenient value of G in order to get B small, (2) determine a fast method of resolving (3.5). With respect to the first of these problems, Landry suggested the use of several moduli, but pointed out that "it becomes necessary to adopt for the work a particular setup which allows us to conveniently group together the residues of the forms of h and then those of the n_1 values which are conjugate to them." He hoped to show how this could be done "soon", but never did. With respect to the second problem, he said that he "would give a method", but none appears in [11]. Fortunately, he does provide us with his method in a later paper [12]. Indeed, he even states in [12] that he used this idea in his work on factoring F_6. (Actually, he does not mention F_6 explicitly, but refers to [1], which is an announcement of his factorization of F_6.)

The idea is very simple and rather neat. Suppose, for a given pair of integers

[1] Landry singled 6 out as a special modulus in his treatment in [11], but it is not really necessary to do this.

P, $Q \geq 0$, we want to find positive integers x', x such that $x' \leq x$ and

$$x' + x = P,$$
$$x'x = Q.$$

Suppose further that

$$x' = d_0 10^k + d_1 10^{k-1} + \cdots + d_k \qquad (0 \leq d_i \leq 9,\ d_0 \neq 0),$$

and put $a = d_0 10^k$. If

$$\begin{aligned} x_1 &= x - a \ (\geq 0), \\ x_1' &= x' - a \ (\geq 0), \\ P_1 &= P - 2a \ (\geq 0), \\ Q_1 &= Q - (P - a)a \ (\geq 0), \end{aligned}$$

then

$$\begin{aligned} x_1 + x_1' &= P_1, \\ x_1 x_1' &= Q_1. \end{aligned}$$

Notice that a is the largest possible multiple of 10^k such that the four inequalities above can hold. Also, since $x' = Q/(P - x')$ and $0 < x'/P \leq 1/2$, we get

$$Q/P < x' \leq 2Q/P;$$

thus not many trials are needed to find a. Indeed, as Landry notes, we have

$$\frac{P}{P - x'} = 1 + \frac{x'}{x},$$
$$\frac{P_1}{P_1 - x_1'} = \frac{P_1}{x_1} = \frac{x_1 + x_1'}{x_1} = 1 + \frac{x_1'}{x_1} = 1 + \frac{x' - a}{x - a};$$

thus, $P_1/(P_1 - x_1')$ is closer to 1 than $P/(P - x')$. It follows that the values for successive values of a_n are closer to Q_n/P_n as n increases. Thus, the value of x' can be computed very simply, one digit at a time. If there are no possible values for x, x', this will become clear when no value for an a_n can be determined, i.e., no $Q_n = 0$.

Consider the following example:

$$x + x' = 3842 = P,$$
$$xx' = 1330945 = Q.$$

Since $[Q/P] = 346$, try $a = 300$.

$$\begin{array}{rr} P = 3842 & 1330945 = Q \\ 2a = 600 & 1062600 = a(P - a) \\ \hline P_1 = P - 2a = 3242 & 268345 = Q_1 \\ 2a_1 = 160 & 259360 = a_1(P_1 - a_1) \\ \hline P_2 = P_1 - 2a_1 = 3082 & 15385 = Q_2 \\ 2a_2 = 10 & 15385 = a_2(P_2 - a_2) \\ \hline P_3 = P_2 - 2a_2 = 3072 & 0 = Q_3. \end{array}$$

Hence, $x' = 385$ and $x = 3457$.

In the large, then, Landry's factoring idea is the following: (1) Test for all possible values of K whether or not (3.5) has a solution. If it does, we have a factor of N. If not, (2) test (3.4) for all possible values of $n_1 \leq B$. We either find a factor of N, or N is a prime.

4. A possible setup for factoring F_6

Since Landry seems never to have published anything more on the factorization problem than what we have mentioned above, the remainder of this paper must be somewhat speculative. We can only describe a technique for factoring F_6 which is consistent with all of Landry's work that has been published. Whatever method he did use would most likely not differ significantly from what we shall now describe.

We can (in view of Lucas [17] and Landry [9]) use $P = 256$ and $A = 1$; hence, $R = R' = 0$, $Q = Q' = 2^{48}$, and we get

$$n_1 + n_2 = 256h, \tag{4.1}$$

$$n_1 n_2 = 2^{48} - h, \tag{4.2}$$

$$h = \frac{2^{48} + n_1^2}{256n_1 + 1} \in \mathbf{Z}. \tag{4.3}$$

Also, in order for (4.1) and (4.2) to hold, we require that

$$2^{14}h^2 + h - 2^{48} = t^2 \qquad (t \in \mathbf{Z}). \tag{4.4}$$

If we use

$$G = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 77597520,$$

we find from (4.3) that if $n_1 > 14170$, then $h' = 0$ for $h = Gh' + K$ $(K > 0)$. If $h' = 0$, we get $h = K$ and

$$2^{14}K^2 + K - 2^{48} = t^2 \qquad (t \in \mathbf{Z}) \tag{4.5}$$

from (4.4). We also get

$$n_1 + n_2 = 256K, \tag{4.6}$$

$$n_1 n_2 = 2^{48} - K \tag{4.7}$$

from (4.1) and (4.2).

We next investigate the possible values of h. By using (4.4), we see that the only possible values of h are given by

$$h \equiv 0^*, 4^*, 1, 9 \pmod{16},$$
$$h \equiv 1 \pmod{3},$$
$$h \equiv 0, 1 \pmod{5},$$
$$h \equiv 1, 4, 6 \pmod{7},$$
$$h \equiv 1, 3, 4, 9, 10 \pmod{11},$$
$$h \equiv 0, 1, 2, 3, 5^*, 8, 11^* \pmod{13},$$
$$h \equiv 0, 1, 2, 3^*, 10^*, 11, 12, 13, 15 \pmod{17},$$
$$h \equiv 5, 7, 8, 9, 11, 13, 14, 15, 17 \pmod{19}.$$

Residues with an asterisk (*) lead to similar factors with respect to the given modulus or in the case of 16 a divisor of that modulus. In his letter to Lucas, Landry said that he left certain forms aside; in view of [11], these would likely be those types of forms. This is simply because for these forms the corresponding modulus (or a divisor of it) can be absorbed into the P value; and, as this increases the P value, the resulting calculations can be accomplished more quickly. Thus, if we eliminate these forms from consideration, we find that the total number of possible values of $h \bmod G$ is

$$2 \times 1 \times 2 \times 3 \times 5 \times 5 \times 7 \times 9 = 18900.$$

We must now deal with the problem of the values of n_1 which are conjugate to the h-values. We first point out that if $h \equiv 1 \pmod{16}$, then $n_1 \equiv 1, 7 \pmod{8}$; if $h \equiv 9 \pmod{16}$, then $n_1 \equiv 3, 5 \pmod{8}$. The other conjugate values modulo p, where $p|G$, are given in the tables below.

p	h	1
3	n_l	0, 1

p	h	0	1
5	n_l	2,3	1,0

p	h	1	4	6
7	n_l	4,0	3,6	1,2

p	h	1	3	4	9	10
11	n_l	1,2	0,9	4,8	6,10	3,5

p	h	0	1	2	3	8
13	n_l	5,8	0,9	7,11	2,12	1,6

p	h	0	1	2	11	12	13	15
17	n_l	4,13	0,1	7,12	3,8	14,15	2,11	6,9

p	h	5	7	8	9	11	13	14	15	17
19	n_l	1,6	12,13	16,18	9,15	0,4	8,14	5,7	10,11	3,17

Notice that if $n_1 \leq 141170$, we *cannot* have $n_1 \equiv 0 \pmod{2}$, $n_1 \equiv 2 \pmod{3}$, $n_1 \equiv 4 \pmod{5}$, $n_1 \equiv 5 \pmod{7}$, $n_1 \equiv 7 \pmod{11}$, $n_1 \equiv 3, 4, 10 \pmod{13}$, $n_1 \equiv 5, 10, 16 \pmod{17}$, or $n_1 \equiv 2 \pmod{19}$. Up to 14170 we would expect, then, to find about

$$14170 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times \frac{10}{11} \times \frac{10}{13} \times \frac{14}{17} \times \frac{18}{19} \approx 1767$$

values of n_1 which could be admissible. In fact there are exactly 1773 such values.

We now turn to the algorithm for factoring F_6.

5. The algorithm

One of the difficulties one encounters on using Landry's ideas to factor F_6 is keeping track of the large number (18900 here) of possible values of K. Landry may have just done this in a very ordinary (and tedious) fashion, but it is possible that he might have done this as we describe here. We first note that if $G = G_1 G_2$, where $\gcd(G_1, G_2) = 1$ and

$$K \equiv K_1 \pmod{G_1}, \qquad K \equiv K_2 \pmod{G_2},$$

then

$$K \equiv W_1 + W_2 \pmod{G},$$

where

$$W_1 \equiv G_2 Z_2 K_1, \quad W_2 \equiv G_1 Z_1 K_2 \pmod{G}$$

and

$$G_1 Z_1 \equiv 1 \pmod{G_2}, \qquad G_2 Z_2 \equiv 1 \pmod{G_1}.$$

This is just a simple case of what today is called the Chinese Remainder Theorem. In its more general form it can be found in Gauss [4, art. 36]. Since Landry had read [4] (see [6]), it is entirely possible that he was aware of this and that he utilized it in his calculations. We will show how below.

We also know that Landry was aware of the idea of using exclusion moduli to eliminate possible candidates as solutions for certain equations. Thus he might very well have used this technique to eliminate values of K which fail to satisfy (4.5). Suppose that $\mathscr{E} = \{23, 29, \dots\}$ (no prime in $\mathscr{E}$ can divide G) is the set of prime exclusion moduli which Landry used. Note that $|\mathscr{E}|$ need not be very large and could have even been 0.

A simple idea for keeping track of the K-values (and for eliminating many of them) can now be implemented by making use of three relatively short lists: $\mathscr{L}_1, \mathscr{L}_2, \mathscr{L}_3$. We point out that there are 135 possible values of $K \pmod{G_1}$ when $G_1 = 1463 = 7 \cdot 11 \cdot 19$. For each of these compute a list made of the corresponding W_1-values given above, together with a sequence of the values of each W_1 modulo the exclusion moduli in $\mathscr{E}$. There are 140 possible values of $K \pmod{G_2}$ when $G_2 = 53040 = 16 \cdot 3 \cdot 5 \cdot 13 \cdot 17$. For each of these compute a list of $\mathscr{L}_2$ made up of the corresponding W_2-values, together with a sequence of the values of each W_2 modulo the elements in $\mathscr{E}$. Finally, compute a list $\mathscr{L}_3$ of all values of $Y \pmod{E}$ such that

$$\left(\frac{2^{14}Y^2 + Y - 2^{48}}{E}\right) = -1$$

for $E \in \mathscr{E}$.

We now have the following

Algorithm.

(1) To each $W_1 \in \mathscr{L}_1$ add every element $W_2 \in \mathscr{L}_2$ (and reduce mod G). Check if the resulting value of K can be excluded from satisfying (4.5) by using the easily computed value of K modulo E for $E \in \mathscr{E}$ and $\mathscr{L}_3$. If this does not exclude the K-value, use the method of [12] to solve the simultaneous equations (4.6), (4.7).

(2) Test if any of the 1773 possible values for $n_1 \leq 14170$ is such that (4.3) holds.

Even if $|\mathscr{E}| = 0$, this algorithm could probably have been executed by hand in the several months that Lucas said that Landry required. However, it is useful to see how effective the use of exclusion moduli is in this problem. The total number of K-values here is 18900. In the table below we give the number of K-values remaining in this problem as various exclusion moduli are used.

$\lvert\mathscr{E}\rvert$	new modulus	number of K-values remaining
0	–	18900
1	23	9041
2	29	4656
3	31	2259
4	37	1126
5	41	542
6	43	268
7	47	140
8	53	67
9	59	37
10	61	19
11	67	11
12	71	6
13	73	2
14	79	1

In view of this rapid rate of decrease (a decrease rate with which Landry would have to have been familiar after doing the work reported in [6] and [7]), it is difficult to accept that he would not have made use of at least a few exclusion moduli in order to lessen his work load.

Note that this algorithm would find the factor 274177 toward the end of all the work, as most of the work is done in Step (1) of the algorithm and $n_1 = 1071$ is the 137th value in the list (in ascending order) of the 1773 possible values for $n_1 \leq 14170$ in Step (2).

In summary, then, Landry seems to have been most unlucky in his attempts to factor F_6. He first tried to use Fermat's difference of squares method; but, as the factors of F_6 are not at all close in value, he failed. This failure seems to have left him for awhile with the impression that F_6 is prime. When Lucas later stated that it is composite, Landry decided to try again. As simple trial division would (possibly) be very time-consuming, he elected (contrary to Lucas's advice, it appears) to use a more sophisticated technique, which grew out of his early primality testing ideas. This method would, after a large but manageable amount of labor, ultimately yield the factorization. When, after a great deal of work, Landry finally discovered the factorization, one of the factors turned out to be so small that it could have been found considerably more quickly by the simple trial division process. It must, however, be emphasized that his ingenious method would still have worked with about the same amount of effort even if the small factor had been much larger. Unfortunately for Landry, it was not.

Acknowledgments

The author would like to thank Hendrik W. Lenstra, Jr. for suggesting this problem to him. He also would like to express his gratitude to Sunil Rottoo for helping him to read Landry's rather difficult (for the author) French and to Mike Jacobson for some computer work. Also, permission to use the excellent mathematical library at Brown University was very much appreciated.

BIBLIOGRAPHY

1. Anonymous, *Décomposition de* $2^{64} + 1$, Nouv. Corresp. Math. **6** (1880), 417.
2. L. E. Dickson, *History of the theory of numbers*, Vol. 1: *Divisibility and primality*, Carnegie Inst. of Washington, Publ. No. 256 (1919); reprinted by Chelsea Books, New York, 1971.
3. P. Fermat, *Fragment d'une lettre de Fermat*, Oeuvres de Fermat **2** (1894), 256–258.
4. C. F. Gauss, *Disquisitiones arithmeticae*, English transl. by A. A. Clarke, Springer-Verlag, New York, 1986.
5. F. Landry, *Procédés nouveaux pour démontrer que le nombre* 2147483647 *est premier*, Librarie Hachette, Paris, 1859; partially reprinted Sphinx-Oedipe **4** (1909), 6–9.
6. ——, *Aux mathematiciens de toutes les parties du monde. Communication sur la décomposition des nombres en leurs facteurs simples*, Librairie Hachette, Paris, 1867.
7. ——, *Décompositions des nombres* $2^n \pm 1$ *en leurs facteurs premiers de* $n = 1$ *à* $n = 64$ (*moins quatre*), Librairie Hachette, Paris, 1869.
8. ——, *Sur la décomposition du nombre* $2^{64} + 1$, C. R. Acad. Sci. Paris **91** (1880), 138.
9. ——, Letter addressed to Lucas dated July 7, 1880, Sphinx-Oedipe **18** (1923), 70–71.
10. ——, Letter to Charles Henry, Boll. di Biblio. Storia Sci. Mat. Fis. **13** (1880), 469–470.
11. ——, *Méthode de décomposition des nombres en facteurs premiers*, Assoc. Français Avance. Sci. Comptes Rendus **9** (1880), 185–189.
12. ——, *Note d'algèbre*, J. Math. Élémentaires et Spéciales **5** (1881), 3–9.
13. E. Lucas, *Considérations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonférence en parties égales*, Assoc. Français Avanc. Sci. Comptes Rendus **6** (1877), 159–167.
14. ——, *Théorème d'arithmétique*, Atti Reale Accad. Sci. Torino **13** (1877-8), 271–284.
15. ——, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
16. ——, *Remarque*, Nouv. Corresp. Math. **4** (1878), 285.
17. ——, *Récreations mathématiques*, vol. 2, 2nd ed., Paris, 1891, pp. 230–235.
18. T. Pepin, *Sur la décomposition des grands nombres en facteurs premiers*, Atti Accad. Pontificia dei Nuovi Lincei **43** (1889-90), 163–191.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA, CANADA R3T 2N2

E-mail address: Hugh_Williams@csmail.cs.umanitoba.ca