Objekttyp: **Group**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **46 (2000)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.03.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

by (3) and (4). This implies that the ratios (z/x) and (w/y) must both be very close to g. We therefore try to set

$$z = gx - s\,, \qquad w = gy - t\,, \tag{7}$$

with integers s, t expected to be small. Then (5) will hold, provided that

$$x^2 + y^2 = q\,, \qquad xs + yt = a\,, \qquad ys - xt = 1\,. \tag{8}$$

From (8) it follows that

$$a^2 + 1 = qu\,, \qquad u = s^2 + t^2. \tag{9}$$

Since the integers q and a are known and comparatively small, it is not difficult to find an integer solution of (8) and (9) by trial and error, namely $x = 516$, $y = 89$, $s = 29$, $t = 5$, $u = 866$. The solution of (8) and (9), with z and w given by (7), provides a solution of (5). This completes the verification of the factorization of the sixth Fermat number. The factorization (4) of $2^{24} - 1$ leads directly to the factorization (5) of $2^{64} + 1$.

Instead of using trial and error to solve (8) and (9), we can obtain a solution more elegantly by using an old theorem of Serret [Serret, 1848; Perron, 1954] on continued fractions. In the statement of the theorem, q and a are any pair of coprime integers with $0 < a < q$. The ratio q/a may be expressed as a continued fraction with partial quotients $(a_j,\ j = 1, \ldots, n)$ in precisely two ways, one with n even and one with n odd. In one way, the last two quotients are $[j, 1]$, where j may be any integer. In the other way these two quotients are replaced by the single quotient $[j + 1]$, all other quotients remaining the same. We say that the continued fraction q/a with n quotients is a palindrome if

$$a_j = a_{n+1-j}\,, \qquad j = 1, \ldots, n\,. \tag{10}$$

SERRET'S THEOREM. *Suppose that the continued fraction q/a with n partial quotients is given. It will be a palindrome if and only if an integer u exists with*

$$qu = a^2 + (-1)^n. \tag{11}$$

Proof of theorem. Let A be any finite ordered set of positive integers, and let $S(A)$ be the numerator of the continued fraction whose partial quotients are the members of A. Euler discovered the explicit formula for $S(A)$ [Euler, 1764; Perron, 1954],

(12) $$S(A) = \sum_B P(B),$$

where the sum extends over certain ordered subsets B of A, and $P(B)$ is the product of the members of B. The subsets included in the sum (12) are A itself, and those B for which the complement $A - B$ is a union of non-overlapping pairs, each pair consisting of two consecutive members of A. The empty set E will appear in the sum (12) if and only if the number of members of A is even. Thus, for example, $S(E) = 1$, $S(a) = a$, $S(a,b) = 1 + ab$, $S(a,b,c) = a + c + abc$, $S(a,b,c,d) = 1 + ab + ad + cd + abcd$. For a lucid and accessible explanation of Euler's formula, see [Davenport, 1982], chapter 4, pp. 82–84.

Let now A be the set $(a_j,\ j = 1,\dots,n)$ of partial quotients of one of the two continued fractions q/a. We write

(13) $$N(k,m) = S(a_k,\dots,a_m),$$

so that

(14) $$q = N(1,n), \qquad a = N(2,n).$$

Euler's formula (12) implies the symmetry relation

(15) $$S(a_1,\dots,a_n) = S(a_n,\dots,a_1),$$

and the recurrence relations

(16) $$N(1,n) = N(1,k)N(k+1,n) + N(1,k-1)N(k+2,n),$$

(17) $$N(1,n)N(2,n-1) - N(1,n-1)N(2,n) = (-1)^n.$$

Suppose that (11) holds. Define

(18) $$b = N(1,n-1), \qquad v = N(2,n-1).$$

The symmetry (15) implies

(19) $$q/b = S(a_n,\dots,a_1)/S(a_{n-1},\dots,a_1),$$

so that one of the two continued fractions for q/b has the same partial quotients as the continued fraction for q/a, in reversed order. Then (11), (17) and (18) imply

(20) $$qv = ab + (-1)^n, \qquad q(u-v) = a(a-b).$$

Now $q > a > 0$ by hypothesis, and $q > b > 0$ by (19), so that $q > |a-b|$. If $a \neq b$, the fraction $(u-v)/(a-b)$ is equal to a/q, which is impossible because a and q are coprime and $|a-b| < q$. Therefore $a = b, u = v$, and the continued fractions for q/a and q/b are identical, so that (10) holds and the continued fraction is a palindrome. Conversely, if (10) holds, (13) and (18) imply $a = b$, and then (17) implies (11) with $u = v$ defined by (18). □

Applying the theorem to q and a given by (3) and (9), we deduce that the continued fraction q/a with n even must be a palindrome. The partial quotients are easily calculated, with the result

$$(21) \quad q = S(17,1,3,1,5,5,1,3,1,17)\,, \qquad a = S(1,3,1,5,5,1,3,1,17)\,.$$

We now apply the recurrence relation (16) to (21) with $k = n/2 = 5$. As a result of the symmetry (15) and the palindrome property of q, (16) gives a solution of (8) with

$$(22) \quad \begin{aligned} x &= S(17,1,3,1,5) = 516\,, & y &= S(17,1,3,1) = 89\,, \\ s &= S(1,3,1,5) = 29\,, & t &= S(1,3,1) = 5\,. \end{aligned}$$

In this way Serret's theorem leads to a solution of (8), following a deductive route rather than trial and error.

The same method leads to the factorization of the fifth Fermat number, starting from

$$(23) \quad q = 1 + 2^7 f\,, \quad 2(2^8 - 1) = fg\,, \quad f = 2^2 + 1\,, \quad g = 2(2^2 - 1)(2^4 + 1)\,.$$

The palindromic continued fraction q/a has numerator $q = S(4,6,6,4)$, and the factorization of $2^{32} + 1$ results with $x = S(4,6) = 25$, $y = S(4) = 4$, $s = S(6) = 6$, $t = S(E) = 1$, $x^2 + y^2 = 641$. But in this case the argument using (1) and (2) gives the same result more quickly. It would be more interesting if we could understand in a similar way the factorizations of the seventh and higher Fermat numbers. For a summary of the known factorizations, see [Brent, 1999]. The seventh Fermat number has two prime factors with 17 and 22 decimal digits.

According to (21), the partial quotients of q/a in the case of the sixth Fermat number are all odd, while in the case of the fifth Fermat number the partial quotients are all even. To decide whether this unexpected behavior of the partial quotients is a numerical accident or a general rule, we need to find more examples.

The factorization of the sixth Fermat number was originally published in [Landry, 1880], without any explanation of how it was found. For a conjectured reconstruction of Landry's method see [Williams, 1993]. Landry worked for several months to find the factorization. The argument presented in this note only verifies the factorization after the factors are known.

ACKNOWLEDGMENT. The author is grateful to a referee for informing him of the existence of Serret's theorem and providing the references to Perron, Serret and Davenport.