MATHEMATICS OF COMPUTATION, VOLUME 26, NUMBER 120, OCTOBER 1972

Note on Representing a Prime as a Sum of Two Squares

By John Brillhart

Abstract. An improvement is given to the method of Hermite for finding a and b in $p = a^2 + b^2$, where p is a prime $\equiv 1 \pmod 4$.

In a one-page note, Hermite [1] published the following efficient method for representing a given prime $p \equiv 1 \pmod 4$ as a sum of squares (see Lehmer [2]):

(i) Find the solution x_0 of $x^2 \equiv -1 \pmod p$, where $0 < x_0 < p/2$.

(ii) Expand x_0/p into a simple continued fraction to the point where the denominators of its convergents A'_n/B'_n satisfy the inequality $B'_{k+1} < \sqrt{p} < B'_{k+2}$. Then

$$p = (x_0 B'_{k+1} - p A'_{k+1})^2 + (B'_{k+1})^2.$$

This method, which was the best method known for computing a and b (see Shanks [5]), appeared simultaneously with a paper of Serret [4] on the same subject. Hermite's method, however, is superior, in that it contains a criterion for ending the algorithm at the right place, while Serret's does not.

It is the purpose of this note to point out that the calculation of the convergents in (ii) can be dispensed with, since the values needed for the representation are already at hand in the continued fraction expansion itself. Thus, the shortened algorithm is:

(i) The same.

(ii) Carry out the Euclidean algorithm on p/x_0 (not x_0/p), producing the sequence of remainders $R_1, R_2, \cdots$, to the point where R_k is first less than $\sqrt{p}$. Then

$$\begin{aligned} p &= R_k^2 + R_{k+1}^2, \quad &\text{if} \quad R_1 > 1, \\ &= x_0^2 + 1, \quad &\text{if} \quad R_1 = 1. \end{aligned}$$

Proof. Assume $R_1 > 1$. Since $0 < x_0 < p/2$ and $p \mid (x_0^2 + 1)$, then, from Perron [3], the following properties hold:

(1) The continued fraction expansion of p/x_0 has an even number of partial quotients and is palindromic, i.e.,

$$p/x_0 = [q_0, q_1, \cdots, q_k, q_k, \cdots, q_1, q_0] = A_{2k+1}/B_{2k+1},$$

$k \geqq 0$. (Observe that the convergents A'_{n+1}/B'_{n+1} for the expansion of x_0/p are the reciprocals of the convergents A_n/B_n for p/x_0.)

(2) $A_{2k+1} = p$ and $A_{2k} = x_0$.

(3) $p = A_k^2 + A_{k-1}^2$.

Received February 17, 1972.

AMS 1969 *subject classifications.* Primary 1003, 1009.

Key words and phrases. Algorithm, sum of two squares.

(4) From (2), the recursion formula for the numerators A_n gives the following set of equations:

$$p = q_0 x_0 + A_{2k-1}, \qquad x_0 = q_1 A_{2k-1} + A_{2k-2}, \cdots .$$

The equations in (4) are clearly identical with those in the Euclidean algorithm for p/x_0. Hence, $A_{2k-1} = R_1$, $A_{2k-2} = R_2$, $\cdots$, $A_{k+1} = R_{k-1}$, $A_k = R_k$, $A_{k-1} = R_{k+1}$, $\cdots$. Using these equations with (3), gives $p = R_k^2 + R_{k+1}^2$. Certainly, then, $R_k < \sqrt{p}$. If $k = 1$, then R_k *is* the first $R_k < \sqrt{p}$. If $k > 1$, then from the observation in (1), $R_{k-1} = A_{k+1} = B'_{k+2}$. But, from Hermite's development, $B'_{k+2} > \sqrt{p}$, so R_k is the first remainder less than $\sqrt{p}$.

If $R_1 = 1$, then $p = q_0 x_0 + 1$ and $p/x_0 = [q_0, q_0]$. Together, these imply $q_0 = x_0$, so $p = x_0^2 + 1$. Q.E.D.

Remark. The solution x_0 of $x^2 \equiv -1 \pmod p$ can be obtained by computing $x_0 \equiv c^{(p-1)/4} \pmod p$, where c is a quadratic nonresidue of p. (Observe that $c = 2$ and $c = 3$ can be used when $p \equiv 5 \pmod 8$ and $p \equiv 17 \pmod{24}$, respectively. In the remaining case, $p \equiv 1 \pmod{24}$, c can be found by using the quadratic reciprocity law.)

Example. Let $p = 10006721 \equiv 17 \pmod{24}$. Then $c = 3$ and $x_0 \equiv 3^{2501680} \equiv 2555926 \pmod p$. Then

$$\begin{aligned}
10006721 &= 3\cdot 2555926 + 2338943\\
2555926 &= 1\cdot 2338943 + 216983\\
2338943 &= 10\cdot 216983 + 169113\\
216983 &= 1\cdot 169113 + 47870\\
169113 &= 3\cdot 47870 + 25503\\
47870 &= 1\cdot 25503 + 22367\\
&\text{- - - - - - - - - - - - - - - -}\\
25503 &= 1\cdot 22367 + 3136\\
22367 &= 7\cdot 3136 + 415
\end{aligned}$$

Hence, since $22367^2 > p$ and $3136^2 < p$,

$$p = 3136^2 + 415^2.$$

Remark. Some primes of special form can be expressed as a sum of two squares without much calculation. For example, the number $N = (2^{691} - 2^{346} + 1)/5$ has recently been shown to be prime by the author and J. L. Selfridge. Hence, we can write $N = [(3\cdot 2^{345} - 1)/5]^2 + [(2^{345} - 2)/5]^2$. Also, the identity $U_{2k+1} = U_k^2 + U_{k+1}^2$, where U_n is the nth Fibonacci number, provides such a representation for Fibonacci primes in terms of the Fibonacci numbers themselves.

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

1. C. HERMITE, "Note au sujet de l'article précédent," *J. Math. Pures Appl.*, v. 1848, p. 15; also: "Note sur un théorème rélatif aux nombres entières," *Oevres.* Vol. 1, p. 264.

2. D. H. LEHMER, "Computer technology applied to the theory of numbers," *Studies in Number Theory,* Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N.J.), 1969, pp. 117–151. MR **40** #84.

3. O. PERRON, *Die Lehre von den Kettenbrüchen*, 2nd ed., Chelsea, New York, 1950, pp. 32–34. MR **12,** 254.

4. J. A. SERRET, "Sur un théorème rélatif aux nombres entières," *J. Math. Pures Appl.*, v. 1848, pp. 12–14.

5. D. SHANKS, Review of "A table of Gaussian primes," by L. G. Diehl and J. H. Jordan, *Math. Comp.*, v. 21, 1967, pp. 260–262.