ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 43, Number 3, 2013

THE COMPLETION OF EULER'S FACTORING FORMULA

RICHARD BLECKSMITH, JOHN BRILLHART AND MICHAEL DECARO

Dedicated to William Blair, Chair of the Department of Mathematical Sciences at Northern Illinois University (1990–2010)

ABSTRACT. In this paper we derive a formula for a nontrivial factorization of an odd, composite integer N that has been expressed in two different ways as $mx^2 + ny^2$. This derivation is based on an approach that Euler used in a special case in 1778. We also modify this formula to handle the case when N is expressed in two different ways as $mx^2 - ny^2$. This latter factorization, however, may sometimes be trivial.

1. Introduction. Among the classical factoring methods, there are two that depend on first expressing the number N to be factored as binary quadratic forms. The earliest such method (1643) is Fermat's method [**2**, page 357 (1)] in which an odd, nonsquare integer N is expressed as

$$N = x^2 - y^2 = (x - y) \cdot (x + y). \tag{1}$$

That such a representation always exists follows from the identity $N = [(N + 1)/2)]^2 - [(N - 1)/2]^2$. This representation, however, only proves existence, since it gives the trivial factorization $N = 1 \cdot N$. It remains then to determine the values of x for which (1) gives a nontrivial factorization of a composite N:

Let $N = a \cdot b$, where $1 < a < \sqrt{N}$. Then, since $x - y = a$ and $x + y = b$, we see that $x = (a + b)/2 = (a + (N/a))/2$. It follows that the factorization in (1) is nontrivial only when $\sqrt{N} < x < (N + 1)/2$.

The second factoring method, which was initiated by Euler, is based on a solution of the following problem:

Main factoring problem. Suppose an odd integer $N > 1$ is expressed in two different ways as

$$N = ma^2 + nb^2 = mc^2 + nd^2, \tag{2}$$

Received by the editors on October 26, 2010.
DOI:10.1216/RMJ-2013-43-3-755