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

where $a, b, c, d, m, n \in Z^+$ and $(ma, nb) = (mc, nd) = 1$. Then, using (2), find a formula that expresses N as a product of two nontrivial factors.

Euler actually never dealt with this problem in its full generality. Instead, he only solved it in two special cases of interest to him.

In Case 1, where $m = n = 1$, he obtained a formula that always gives a nontrivial factorization [**1**, page 929, (3)]. In Case 2, he considered a slightly more general problem with $m = 1$ and $n \geq 1$ satisfying a side condition. We give Euler's approach to solving Case 2, where he derives his formula (7). From (2), he interestingly employs only the single equation

$$a^2 + nb^2 = c^2 + nd^2. \tag{3}$$

Note that N itself is not involved here.

In Section 3, we derive formula (12) that solves the Main factoring problem. In Section 4, we prove that this factorization is never trivial.

In Section 5, we modify (12) to obtain formula (16) for the related factoring problem of an odd $N > 1$ that is expressed in two different ways as $N = mx^2 - ny^2$. This section ends with a discussion of the possible triviality of this factorization.

2. Euler's formula.

In 1778, when Euler had become blind, his mathematical secretary, Nicholas Fuss, wrote a letter to A. Beguelin [**3**, page 11, Section 1] that contained a brief and poorly argued version of Euler's solution to Case 2 above.

In what follows, we give a more fully argued version of Fuss's account in that we insert two important omitted steps, viz., the GCD condition following (5) and the splitting formula in (6).

To begin, note that (3) implies the equation $a^2 - c^2 = n\,(d^2 - b^2)$ which can be written as

$$\frac{a+c}{n(d+b)} = \frac{d-b}{a-c}. \tag{4}$$

If the fraction on the right side is reduced to its lowest terms p/q, we then have

$$\frac{a+c}{d+b} = \frac{np}{q}, \quad \text{and} \quad \frac{d-b}{a-c} = \frac{p}{q}, \quad (p, q) = 1. \tag{5}$$

Assuming that $(n, q) = 1$, then $(np, q) = 1$ follows, so (5) implies that $a + c = npr$, $d + b = qr$ and $d - b = ps$, $a - c = qs$ for some r, $s \in Z^+$. Thus, $2a = npr + qs$ and $2b = qr - ps$.

Next consider the double-sign version of Euler's "splitting formula" for the irreducible polynomial $F(x, y) \doteq mx^2 + ny^2$, where $m, n \in Z^+$ are given. (Compare with [**4**, Part II, Chapter XI, page 178]): If $p, q, r, s \in Z^+$, we have that

$$F\left(npr \pm qs,\, mqr \mp ps\right) = \left(np^2 + mq^2\right) \cdot \left(s^2 + mnr^2\right). \tag{6}$$

Thus, Euler's factorization formula [**2**, page 362, (39)] immediately follows:

$$N = F(2a, 2b)/4 = (np^2 + q^2) \cdot (s^2 + nr^2)/4. \qquad \square \tag{7}$$

Since Euler's result has never been extended beyond the case when $(n, q) = 1$, we will derive the complete formula in the next section (cf. [**5**, page 222]).

3. The general factoring formula.

In proving the general formula (12), we will follow the three steps we used in the preceding section: (i) Manipulate the equation $ma^2 + nb^2 = mc^2 + nd^2$ so as to solve for $2a$ and $2b$; (ii) Give a relevant splitting formula for $mx^2 + ny^2$; (iii) Use this splitting formula to express N as a product of two factors.

We begin by first deriving formula (12), which is comparable to (7) in Section 2. From (2), we obtain that

$$m(a - c)(a + c) = n(d - b)(d + b). \tag{8}$$

With $r = (a + c,\, d + b)$, we can write $a + c = ru$ and $d + b = rv$, where $(u, v) = 1$. Substituting these results into (8) gives

$$mu(a - c) = nv(d - b). \tag{9}$$

Now let $(m, v) = m_1$, so we can write $v = m_1\widehat{v}$, and set $m_2 = m/m_1$. Putting these results into (9) gives

$$m_2u(a - c) = n\widehat{v}(d - b), \tag{10}$$

from which we conclude that $\widehat{v} \mid m_2\,(a-c)$. But $(m_2,\widehat{v}) = (m/m_1, v/m_1) = 1$, so $\widehat{v} \mid (a-c)$. Thus, we can write $a-c = s\widehat{v}$.

Substituting this result into (10) gives

$$m_2 s\, u = n(d-b). \tag{11}$$

Now let $(n,s) = n_1$, put $s = n_1\widehat{s}$, and let $n_2 = n/n_1$. Substituting these results into (11), we find that $n_2 \mid \widehat{s}u$. But $(n_2,\widehat{s}) = (n/n_1, s/n_1) = 1$, so $n_2 \mid u$. Putting $u = n_2\widehat{u}$ into (11), it follows that $d-b = m_2\widehat{s}\widehat{u}$. We can now give the factorization:

$$N = \big(m_2 n_2 \widehat{u}^2 + m_1 n_1 \widehat{v}^2\big)\cdot\big(m_1 n_2 r^2 + m_2 n_1 \widehat{s}^2\big)/4. \tag{12}$$

Proof. (i) From the above development, we see that $a+c = ru = n_2 r\widehat{u}$, $d+b = rv = m_1 r\widehat{v}$, and $a-c = s\widehat{v} = n_1\widehat{s}\widehat{v}$, $d-b = m_2\widehat{s}\widehat{u}$. Combining the pairs of these equations, we obtain

$$2a = n_2\widehat{u}r + n_1\widehat{v}\widehat{s} \qquad 2b = m_1\widehat{v}r - m_2\widehat{u}\widehat{s}; \tag{13}$$

(ii) Let $F(x,y) = mx^2 + ny^2$, where $m,n \in Z^+$ are given. Also, consider the "refinements" $m = m_1m_2$ and $n = n_1n_2$ for any possible choices of $m_1, m_2, n_1, n_2 \in Z^+$. Then,

$$\begin{aligned} &F(n_2pr \pm n_1qs,\ m_1qr \mp m_2ps) \\ &\qquad\qquad = (m_2n_2p^2 + m_1n_1q^2)\cdot(m_1n_2r^2 + m_2n_1s^2); \end{aligned} \tag{14}$$

(iii) From (13) and (14), we obtain

$$\begin{aligned} N = F(2a,2b)/4 &= F(n_2\widehat{u}r + n_1\widehat{v}\widehat{s},\ m_1\widehat{v}r - m_2\widehat{u}\widehat{s})/4 \\ &= \big(m_2n_2\widehat{u}^2 + m_1n_1\widehat{v}^2\big)\cdot\big(m_1n_2r^2 + m_2n_1\widehat{s}^2\big)/4. \qquad \square \end{aligned}$$

Question. Is there a relationship between the quadratic factors in (12) and the classical quadratic form theory related to $mx^2 + ny^2$?

Example 1. The Mersenne number $M_{11} = 2^{11} - 1$ can be written as $2047 = 6\cdot 2^2 + 7\cdot 17^2 = 6\cdot 12^2 + 7\cdot 13^2$, so $2047 = (2\cdot 7\cdot 1^2 + 3\cdot 5^2)\cdot(3\cdot 7\cdot 2^2 + 2\cdot(-2)^2)/4 = 89\cdot(92/4) = 89\cdot 23$.

Example 2. For the Fermat number $F_5 = 2^{32} + 1 = 4394967297 = 69{\cdot}7389^2 + 77{\cdot}2618^2 = 69{\cdot}6674^2 + 77{\cdot}3983^2$, we have $F_5 = (3{\cdot}7{\cdot}7^2 + 23{\cdot}11{\cdot}1^2){\cdot}(23{\cdot}7{\cdot}287^2 + 3{\cdot}11{\cdot}65^2)/4 = (1282/2){\cdot}(13400834/2) = 641{\cdot}6700417$.

4. Nontriviality. To complete our discussion of the factorization in (12), we will establish the following result:

Theorem 1. *The factorization in* (12) *is never trivial.*

Proof. For convenience, write $A = m_2 n_2 \widehat{u}^2 + m_1 n_1 \widehat{v}^2$ and $B = m_1 n_2 r^2 + m_2 n_1 \widehat{s}^2$. Since all the variables in A and B are positive integers, then A and B exceed 1, which means that "triviality" amounts to one or the other of them being 2 or 4. Since $(m, n) = 1$, we can assume without loss of generality that m is odd. The proof is divided into four parts.

Subpart 1. $[A = 2,\ B = 2\cdot$ odd$]$. Here $A = m_2 n_2 \widehat{u}^2 + m_1 n_1 \widehat{v}^2 = 2$, so $m_2 n_2 \widehat{u}^2 = m_1 n_1 \widehat{v}^2 = 1 \Rightarrow m_2 = n_2 = \widehat{u} = m_1 = n_1 = \widehat{v} = 1$. Then $a + c = ru = r(n_2 \widehat{u}) = r(m_1 \widehat{v}) = rv = d + b$ and $a - c = s\widehat{v} = (n_1 \widehat{s})\widehat{v} = m_2 \widehat{s}\widehat{u} = d - b$. Combining these two equations gives $c = b$ and $d = a$. Also, since $m = m_1 m_2 = 1$ and $n = n_1 n_2 = 1$, equation (8) becomes $N = a^2 + b^2 = b^2 + a^2$. But these are not different representations. Contradiction.

Subpart 2. $[A = 4,\ B$ is odd$]$. Then $A = m_2 n_2 \widehat{u}^2 + m_1 n_1 \widehat{v}^2 = 4$. There are 3 possibilities. In each of the following subcases we will show that 2 divides B, contradicting that B is odd.

(a) $[m_2 n_2 \widehat{u}^2 = 3,\ m_1 n_1 \widehat{v}^2 = 1]$. Then $\widehat{u} = m_1 = n_1 = \widehat{v} = 1$. Also, $a + c = ru = r(n_2 \widehat{u}) = n_2 r$, $a - c = s\widehat{v} = s = (n_1 \widehat{v})\widehat{s} = \widehat{s}$ and $B = n_2 r^2 + m_2 \widehat{s}^2$. There are two possibilities: If $m_2 = 3$, $n_2 = 1$, then we have $a + c = r$, $a - c = \widehat{s}$, and $B = r^2 + 3\widehat{s}^2 = (a + c)^2 + 3(a - c)^2 = 4(a^2 - ac + c^2)$, contradicting that B is odd. If $m_2 = 1$, $n_2 = 3$. then $a + c = 3r$, $a - c = \widehat{s}$ and $B = 3r^2 + \widehat{s}^2 = 3[(a + c)/3]^2 + (a - c)^2$, which implies that $3B = 4(a^2 - ac + c^2)$. Contradiction.

(b) $[m_2 n_2 \widehat{u}^2 = m_1 n_1 \widehat{v}^2 = 2]$. Since m is odd, $m_2 = \widehat{u} = m_1 = \widehat{v} = 1$ and $n_2 = n_1 = 2$. Thus, $B = 2r^2 + 2\widehat{s}^2$. Contradiction.

(c) $[m_2 n_2 \widehat{u}^2 = 1,\ m_1 n_1 \widehat{v}^2 = 3]$. Then $m_2 = n_2 = \widehat{u} = \widehat{v} = 1$. Also, $a + c = ru = r(n_2 \widehat{u}) = r$, $a - c = s\widehat{v} = (n_1 \widehat{s})\widehat{v} = n_1 \widehat{s}$, and

$B = m_1 r^2 + n_1 \widehat{s}^2$. There are two possibilities: If $m_1 = 1, n_1 = 3$, then $a + c = r$, $a - c = 3\widehat{s}$ and $B = r^2 + 3\hat{s}^2 = (a+c)^2 + 3[(a-c)/3]^2$, which implies $3B = 3(a+c)^2 + (a-c)^2 = 4(a^2 + ac + c^2)$, a contradiction. If $m_1 = 3$, $n_1 = 1$, then $a + c = r$, $a - c = \widehat{s}$ and $B = 3\,r^2 + \widehat{s}^2 = 3(a+c)^2 + (a-c)^2 = 4(a^2 + ac + c^2)$. Contradiction.

Subpart 3. [$B = 2$, $A = 2\cdot$ odd]. Here $B = m_1 n_2 r^2 + m_2 n_1 \widehat{s}^2 = 2$, so $m_1 n_2 r^2 = m_2 n_1 \widehat{s}^2 = 1$ and $m_1 = n_2 = r = m_2 = n_1 = \widehat{s} = 1$. Then, $a + c = ru = r(n_2 \widehat{u}) = m_2 \widehat{s}\widehat{u} = d - b$ and $a - c = s\widehat{v} = (n_1 \widehat{s})\widehat{v} = r(m_1 \widehat{v}) = rv = d + b$. Combining these two equations, we obtain $d = a$ and $c = -b$, from which (8) becomes $N = a^2 + b^2 = b^2 + a^2$, which are not different representations. Contradiction.

Subpart 4. [$B = 4$, A is odd]. Here $B = m_1 n_2 r^2 + m_2 n_1 \widehat{s}^2 = 4$. There are 3 possibilities: (a) $m_1 n_2 r^2 = 3$, $m_2 n_1 \widehat{s}^2 = 1$; (b) $m_1 n_2 r^2 = m_2 n_1 \widehat{s}^2 = 2$; (c) $m_1 n_2 r^2 = 1$, $m_2 n_1 \widehat{s}^2 = 3$. In each case, we obtain a contradiction by showing that 2 or 4 divides A. Case (a) splits into two subcases: (i) $m_1 = 1$, $n_2 = 3$ and (ii) $m_1 = 3$, $n_2 = 1$. Also, Case (c) splits into the subcases: (i) $m_2 = 1$, $n_1 = 3$ and (ii) $m_2 = 3$, $n_1 = 1$. The argument here is very similar to the one given in Subpart 2, where the contradiction arose by showing that the odd B was even. This is left to the reader to complete. □

Corollary 1. *If m and n are positive integers, then a prime can be represented as $mx^2 + ny^2$ in at most one way.*

Remark. We should mention that there is a second factorization formula derived from (2), viz.,

$$(15) \qquad N = (N, ad - bc) \cdot (N, ad + bc) = (N, ad - bc) \cdot \frac{N}{(N, ad - bc)},$$

where this factorization is always nontrivial.

This elegant formula was obtained in [**1**, pages 930–931] by rewriting Mathews' argument which combined the pair of *equations* $N = ma^2 + nb^2$ and $N = mc^2 + nd^2$ to show that $(N,\ ad + bc)$ is a factor of N (cf. (3)). Note that (15) also implies Corollary 1.

5. The factoring formula when $N = mx^2 - ny^2$. It is simple to see in the proof of (12) that changing the sign of n in (2) leads to changing the sign of n_2 in (12). (See also [**4**, Part II, Chapter XI, page 176]). Thus, if N is expressed in two different ways as $N = ma^2 - nb^2 = mc^2 - nd^2$, we have the factorization formula

$$N = \big(m_1 n_1 \widehat{v}^2 - m_2 n_2 \widehat{u}^2\big) \cdot \big(m_2 n_1 \widehat{s}^2 - m_1 n_2 r^2\big)/4. \tag{16}$$

The situation with (16), however, is different from that in (12), since (16) sometimes gives a trivial factorization.

Example 3. $N = 2^{11} - 1 = 2047 = 63^2 - 2 \cdot 31^2 = 47^2 - 2 \cdot 9^2 = 65^2 - 2 \cdot 33^2$. Using the first two representations, (16) gives $2047 = (1 \cdot 2 \cdot 4^2 - 1 \cdot 1 \cdot 11^2) \cdot (1 \cdot 2 \cdot 2^2 - 1 \cdot 1 \cdot 10^2)/4 = (-89) \cdot (-92)/4 = 89 \cdot 23$. By way of contrast, if we use the first and third representations, we get a trivial factorization:

$$2047 = (1 \cdot 2 \cdot 1^2 - 1 \cdot 1 \cdot 2^2) \cdot (1 \cdot 2 \cdot (-1)^2 - 1 \cdot 1 \cdot 64^2)/4 = 1 \cdot 2047. \tag{17}$$

In the next example we show that (17) is readily generalized to give an infinite sequence of trivial factorizations.

Example 4. Let $N = 2^{2n+1} - 1$. Then we have the representations: $N = (2^{n+1} - 1)^2 - 2(2^n - 1)^2 = (2^{n+1} + 1)^2 - 2(2^n + 1)^2$. Then (16) gives $N = (1 \cdot 2 \cdot 1^2 - 1 \cdot 1 \cdot 2^2) \cdot (1 \cdot 2 \cdot (-1)^2 - 1 \cdot 1 \cdot (2^{n+1})^2)/4 = 1 \cdot N$. Trivial.

Acknowledgments. We would like to thank Professor Dominic Klyve of Central Washington University, Director of the Euler Archive, for his assistance in using the Archive. See URL: `http://www.math.eulerarchive.org`.

REFERENCES

1. J. Brillhart, *A note on Euler's factoring problem*, Amer. Math. Monthly **116** (2009), 928–931.

2. L.E. Dickson, *History of the theory of numbers*, Vol. 1, Chelsea, New York, 1952.

3. L. Euler, *Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne?*, Nova Acta Acad. Sci. Imperial. Petropol. **14**, (1805) 11–51; Euler Archive, E719.

4. L. Euler, *Elements of algebra*, 5th ed., Springer-Verlag, New York. Originally published in 1770. (Translation by John Hewlett 1972); Euler Archive, E388.

5. A. Weil, *Number theory*, Birkhäuser, Boston, 1984.

Department of Mathematics, Northern Illinois University, Dekalb, IL 60115
Email address: richard@math.niu.edu

Department of Mathematics, University of Arizona, Tucson, AZs 85721
Email address: jdb@math.arizona.edu

Department of Mathematics, Northern Illinois University, Dekalb, IL 60115
Email address: decaro@math.niu.edu