Using Conic Sections to Factor Integers

Richard Blecksmith, John Brillhart, and Michael Decaro

Dedicated to our friend Richard Guy

Abstract. This paper explores the factorization of an odd, composite integer N that has been expressed in two different ways as $mx^2 \pm ny^2$. The negative case $mx^2 - ny^2 = N$ turns out to be quite different from the positive case $mx^2 + ny^2 = N$ because it deals with a hyperbola instead of an ellipse. Of particular interest in the negative case is that Pell-connected representations produce trivial factorizations.

1. INTRODUCTION. In about 1643, Fermat devised an effective sieving method for representing an odd, composite integer N as an integer point (a, b) on the hyperbola $x^2 - y^2 = N$, which yields the nontrivial factorization $N = (a - b)(a + b)$ [**5**, Ch. XIV, p. 357]; [**7**, pp. 55–58]. The importance of Fermat's new factoring method was threefold: (1) It represented a number as a quadratic form for the first time. (2) It improved the ancient practical factoring method, where N is trial-divided by the successive primes $\leq \sqrt{N}$ generated by the progressively more-complicated Eratosthenes sieve. (3) It used a new kind of sieve, a *quadratic* sieve, where about half the possibilities are excluded for each modulus used in the sieving.

About a century later, Euler used similar ideas to derive a formula to express N as a product of two nontrivial factors by finding two representations of N by the ellipse $E : mx^2 + ny^2 = N$ for certain given positive integers m, n. A discussion of Euler's method can be found in [**1**] and [**4**, Chapters 3–5].

About a century after Euler, Lucas, and Mathews developed an elegant factorization formula for numbers with double representations by the ellipse E, discussed in the recent work [**2**, eq. (7)]. The present paper extends the investigation to the hyperbola $H : mx^2 - ny^2 = N$. Historically, all we know about the hyperbolic case is Fermat's method with $m = n = 1$, where we do not need to find a second integer point on the hyperbola because $x^2 - y^2$ is already reducible. To our knowledge, the general case $mx^2 - ny^2 = N$ was never considered in its own right because we suppose no one thought of doing so due to the apparent sufficiency of that method.

In Sec. 2, we discuss the Lucas–Mathews factorization formula in both the elliptic and hyperbolic cases. Interestingly, in the latter case, a complication arises when certain pairs of representations of N lead to the trivial factorization $N = N \cdot 1$. Our analysis of this curious anomaly in Sec. 3 shows that the trivial factorization occurs only when the two points belong to the same "Pell family," an infinite set of integer points on H, based on the equation $x^2 - mny^2 = 1$. Section 4 contains a commentary on an approach to factoring Mersenne numbers using double hyperbolic representations. The paper concludes with a discussion of applications of the method.

2. THE LUCAS–MATHEWS FORMULA.

Factoring using an ellipse. [**2**, Thm. 2]

http://dx.doi.org/10.4169/amer.math.monthly.123.2.168
MSC: Primary 11A51

Theorem 1 (Lucas–Mathews formula for an ellipse.). *If an odd integer N is represented in two different ways as*

$$N = ma^2 + nb^2 = mc^2 + nd^2, \tag{1}$$

where

$$m, n, a, b, c, d \in \mathbb{Z}^+ \quad \text{and} \quad (ma, nb) = (mc, nd) = 1, \tag{2}$$

then N factors nontrivially as

$$N = (N, ad - bc)\,(N, ad + bc). \tag{3}$$

Remark. In general, if N divides a product $u \cdot v$, we cannot conclude that $N = (N, u)(N, v)$. This equation does hold, however, if (N, u) and (N, v) are relatively prime, which is the case in equation (3), as the following argument shows. Let p be a prime divisor of $(N, ad - bc)$ and $(N, ad + bc)$. Then p divides N, $2ad$, and $2bc$. Since N is odd, p cannot be 2, so either $p|a$ or $p|d$. If $p|a$, then $p|N - ma^2 = nb^2$, which violates the gcd condition $(ma, nb) = 1$ in (2). A similar contradiction is reached if $p|d$.

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

$$\begin{aligned} 2047 &= (2047, 2 \cdot 13 - 17 \cdot 12)(2047, 2 \cdot 13 + 17 \cdot 12) \\ &= (2047, -178)(2047, 230) = 89 \cdot 23. \end{aligned}$$

Example 2. The Fermat number $F_5 = 2^{32} + 1 = 4394967297$ is represented as $69 \cdot 7389^2 + 77 \cdot 2618^2 = 69 \cdot 6674^2 + 77 \cdot 3983^2$, so

$$\begin{aligned} F_5 &= (F_5, 7389 \cdot 3983 - 2618 \cdot 6674)(F_5, 7389 \cdot 3983 + 2618 \cdot 6674) \\ &= (F_5, 11957855)(F_5, 46902919) = 641 \cdot 6700417. \end{aligned}$$

The proof of the Lucas–Mathews formula makes use of the next two equations that readily follow from (1).

Proposition 2. *If $N = ma^2 + nb^2 = mc^2 + nd^2$, then*

$$(d^2 - b^2)N = m(ad - bc)(ad + bc) \tag{4}$$

and

$$\big(mac \mp nbd\big)^2 + mn\big(ad \pm bc\big)^2 = N^2. \tag{5}$$

Because of (1) and the gcd condition $(am, bn) = 1$ in (2), the integer N in Theorem 1 is relatively prime to m. It follows from (4) that N divides $(ad - bc)(ad + bc)$, so factors of N are found by taking gcd's. The Lucas–Mathews formula (3)

follows from the further observation that the gcd conditions in (2) imply that the two factors $(N, ad - bc)$ and $(N, ad + bc)$ are relatively prime. Finally, equation (5) is instrumental in showing that $1 < ad + bc < N$, from which we deduce the nontriviality of the two factors in (3). (Cf. [**2**, (9) et seq.])

Factoring using a hyperbola. All we need to do in going from the ellipse $E : mx^2 + ny^2 = N$ to the hyperbola $H : N = mx^2 - ny^2$ is replace n by $-n$. Equation (4) continues to hold using this replacement as that equation has no n on its right-hand side. Since $(N, m) = 1$, N again divides $(ad - bc)(ad + bc)$ as in the elliptical case. Hence, the Lucas–Mathews formula (3) also holds in the case of a double hyperbolic representation. A question remains, however: Is this factorization nontrivial?

Example 3. From the double representation

$$M_{11} = 2^{11} - 1 = 2047 = 1 \cdot 63^2 - 2 \cdot 31^2 = 1 \cdot 47^2 - 2 \cdot 9^2,$$

(3) becomes

$$\begin{aligned} M_{11} &= (M_{11}, ad - bc)(M_{11}, ad + bc) \\ &= (2047, 63 \cdot 9 - 31 \cdot 47)\,(2047, 63 \cdot 9 + 31 \cdot 47) \\ &= (2047, -890)\,(2047, 2024) = 89 \cdot 23. \end{aligned}$$

Example 4. Now consider another double representation for the same number: $M_{11} = 2^{11} - 1 = 1 \cdot 63^2 - 2 \cdot 31^2 = 1 \cdot 65^2 - 2 \cdot 33^2$. We then have that

$$\begin{aligned} (M_{11}, ad - bc) &= (2047, 63 \cdot 33 - 65 \cdot 31) = (2047, 64) = 1 \quad \text{and} \\ (M_{11}, ad + bc) &= (2047, 4094) = (M_{11}, 2M_{11}) = M_{11}, \quad \text{so} \end{aligned}$$

the factorization in (3) is trivial: $M_{11} = 1 \cdot M_{11}$.

Thus, the situation for a hyperbola is more complicated than for an ellipse: Example 3 shows that the two representations do lead to a nontrivial factorization of N, while Example 4 produces only a trivial factorization. (Cf. [**1**, Sec. 5].) We investigate the cause of this factorization failure in the next section.

To see why the nontriviality proof in the elliptical case, based on (5), fails in the case of a hyperbola, it is helpful to replace n by $-n$ in (5), which gives the following equation.

Proposition 3. *If $N = ma^2 - nb^2 = mc^2 - nd^2$, then*

$$\big(mac \pm nbd\big)^2 - mn\big(ad \pm bc\big)^2 = N^2. \tag{6}$$

Equation (6), whose analogue (5) was so basic in proving that the factors $(N, ad \pm bc)$ in Theorem 1 are nontrivial, fails to ensure nontriviality in the hyperbolic case. In fact, we cannot deduce any information about the relative size of $ad \pm bc$ and N from (6) because it involves a difference instead of a sum.

3. PELL FAMILIES AND NONTRIVIALITY. Consider the integer points (a, b) and (c, d) on the hyperbola $H : mx^2 - ny^2 = N$. We will show that there exist certain families of points on H that always produce a trivial factorization when (a, b) and

(c, d) belong to one of these families, as in Example 4. The key mathematical element in the construction of such families is the Pell equation [**3**, pp. 31–34]

$$x^2 - mny^2 = 1. \tag{7}$$

Consider the two rational points defined by

$$\begin{bmatrix} \alpha^{\pm} \\ \beta^{\pm} \end{bmatrix} = \frac{1}{N} \begin{bmatrix} mac \pm nbd \\ ad \pm bc \end{bmatrix}. \tag{8}$$

By equation (6), these points satisfy (7). We say that (a, b) and (c, d) are *Pell-related* if and only if (α^+, β^+) or (α^-, β^-) in (8) is an integer point on (7).

In Example 3, with $(a, b) = (63, 31)$ and $(c, d) = (47, 9)$ that gave the nontrivial factorization of 2047, the two rational points in (8) are $(\alpha^+, \beta^+) = \left(\frac{153}{89}, \frac{88}{89}\right)$ and $(\alpha^-, \beta^-) = \left(\frac{27}{23}, -\frac{10}{23}\right)$, neither of which is an integer solution to $x^2 - 2y^2 = 1$. Thus, the pairs (a, b) and (c, d) are not Pell related.

On the other hand, in Example 4, when we use $(a, b) = (63, 31)$ and $(c, d) = (65, 33)$ in (8), we see that

$$\begin{bmatrix} \alpha^+ \\ \beta^+ \end{bmatrix} = \frac{1}{2047} \begin{bmatrix} 63 \cdot 65 + 2 \cdot 31 \cdot 33 \\ 63 \cdot 33 + 31 \cdot 65 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

is an integer point satisfying the Pell equation $x^2 - 2y^2 = 1$, thus demonstrating that (a, b) and (c, d) are Pell related.

Looking at the situation differently, given a point (a, b) on the hyperbola, and a Pell solution $\alpha^2 - mn\beta^2 = 1$, we can write

$$N \cdot 1 = (ma^2 - nb^2)(\alpha^2 - mn\beta^2) = m(\alpha a + n\beta b)^2 - n(m\beta a + \alpha b)^2,$$

so the second Pell-related point (c, d) on H is obtained from

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} \alpha & n\beta \\ m\beta & \alpha \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \tag{9}$$

Using the fundamental Pell solution (α_0, β_0) of (7), we can create an infinite family of solutions of $mx^2 - ny^2 = N$ by multiplying one solution (a, b) by any integral power of the matrix in (9). (A negative power comes from the inverse matrix.)

One suspects that two Pell-related points will always produce a trivial factorization. Giving a second representation using a Pell equation is like obtaining a second equation in a linear system by multiplying one of the equations by a constant. It adds no new information.

Theorem 4. *If an odd, positive integer N is represented in two different ways as $N = ma^2 - nb^2 = mc^2 - nd^2$, where $m, n, a, b, c, d \in \mathbb{Z}^+$ and $(ma, nb) = (mc, md) = 1$, then the factorization*

$$N = (N, ad - bc)\,(N, ad + bc) \tag{10}$$

is trivial if and only if (a, b) and (c, d) are Pell related.

Proof. ($\Longrightarrow$) If the factorization in (10) is trivial, then, since $N \mid (ad - bc)(ad + bc)$, either $N \mid ad - bc$ or $N \mid ad + bc$. In the first case, we can take $\alpha = \dfrac{mac - nbd}{N}$ and $\beta = \dfrac{ad - bc}{N}$ and, in the latter, $\alpha = \dfrac{mac + nbd}{N}$ and $\beta = \dfrac{ad + bc}{N}$. Either way, β is an integer and by (6), α and β are rational numbers satisfying $\alpha^2 - mn\beta^2 = 1$. Since α is a rational whose square, $mn\beta^2 + 1$, is an integer, it follows that α is also an integer and hence (a, b) and (c, d) are Pell related.

($\Longleftarrow$) Suppose (a, b) and (c, d) are Pell related. Then there is an integral solution (α, β) of (7) given by (8). Moreover, $\beta = \dfrac{1}{N}(ad \pm bc)$, so N divides $ad \pm bc$, and hence either $(N, ad - bc) = N$ or $(N, ad + bc) = N$. ∎

Representations of N as $mx^2 - ny^2$ can be viewed as binary quadratic forms of discriminant 4mn. (In general, the discriminant of the form $ax^2 + bxy + cy^2$ is $b^2 - 4ac$.) The issue of Pell-related representations has a natural interpretation in terms of such forms, which correspond to solutions of the Pell equation. Powering of the fundamental solution yields the other Pell-related integer solutions.

4. FACTORING MERSENNE NUMBERS. The Mersenne numbers $M_p = 2^p - 1$, where p is prime, go back to the time of Euclid and the idea of a perfect number. The search for Mersenne primes has been a continuing preoccupation for centuries [**5**, Ch. 1], especially in the age of high-speed computers. Most notable is GIMPS [**6**], an acronym for Great Internet Mersenne Prime Search. Currently, less than 50 Mersenne primes are known, the largest being $M_{57885161}$, a number with over 17 million digits. No one has been able to prove that there are infinitely many Mersenne primes. More surprising, however, is the fact that no one has shown that infinitely many Mersenne numbers M_p are composite [**8**, p. 29].

In this section, we bring our method to bear on the Mersenne numbers M_p. The idea is simple. Find a hyperbola $mx^2 - ny^2$ that represents M_p and then look for a second representation, using the same m and n. The hyperbola $x^2 - 2y^2$ is a natural form for representing numbers $M_p = 2^p - 1$ for any odd number p:

$$M_p = 2^p - 1 = (2^{(p+1)/2} - 1)^2 - 2(2^{(p-1)/2} - 1)^2. \tag{11}$$

Thus, one way to factor M_p is to find a second, non-Pell-related representation of the form $x^2 - 2y^2$. We present a small table below showing the minimum values of c and d for such a second representation (when it exists) for odd primes $p < 50$. Note that there are no second representations when $p = 3, 5, 7, 13, 17, 19, 31$ since M_p is prime for these exponents. The values of c and d, together with $a = 2^{(p+1)/2} - 1$ and $b = 2^{(p-1)/2} - 1$, give the Lucas–Mathews factors $f = (M_p, ad - bc)$ and $g = (M_p, ad + bc)$ in the following table.

p	$M_p = 2^p - 1$	c	d	f	g
11	2047	47	9	89	23
23	8388607	3225	1003	47	178481
29	536870911	23231	1185	2089	256999
37	137438953471	463161	196315	223	616318177
41	2199023255551	1890999	829715	13367	164511353
43	8796093022207	2968127	82719	431	20408568497
47	140737488355327	11911223	754899	10610063	13264529

Figuring out a pattern for the second representations could be a first step in settling the long-standing conjecture that there are infinitely many primes p for which M_p is composite. Considering the scarcity of Mersenne primes, it would be a rare mathematician who would doubt the truth of this conjecture.

5. APPLICATIONS. The method presented in this paper extends Fermat's method of expressing a number N to be factored as a difference of squares $x^2 - y^2$ to the problem of finding a double representation of the general form $mx^2 - ny^2$. Just how the theory may end up being used to design new schemes to factor numbers of various forms in the era of standard or quantum computers remains to be seen. One would hope that this new basic method would be useful in giving flexibility to some of the excellent computer factoring methods. On its own, however, finding a double representation seems an impractical way to factor a large number N, say, of 50 or more digits. The obvious difficulty lies in choosing the appropriate values of m, n, a, b, c, and d. We had hoped that the Lucas–Mathews method might have applied to certain classes of numbers, such as Mersenne or Fermat numbers, but our limited experience suggests that more work is needed.

We conclude by considering the following question. What odd positive integers N have double representations satisfying (2) that allow them to be factored? By the remark at the end of Theorem 1, N must have at least two prime factors. In the elliptic case, not all composite values of N have double representations of the form $mx^2 + ny^2$. For example, it is easy to check by exhaustion that double representations do not exist for $N = 15$, 39, 95, and 105. The situation is different when using hyperbolas, however, as the following surprising, but elementary, theorem asserts.

Theorem 5. *Let $N = xy$, where x and y are relatively prime odd integers ≥ 3. Then there exist positive integers m, n, a, b, c, and d satisfying $N = ma^2 - nb^2 = mc^2 - nd^2$ and the conditions* (2) *such that*

$$(N, ad - bc) = x \quad \text{and} \quad (N, ad + bc) = y. \tag{12}$$

Proof. Assume without loss of generality that $x > y$. Take $m = n = 1$, and define

$$a = \frac{x+y}{2}, \quad b = \frac{x-y}{2}, \quad c = \frac{xy+1}{2}, \quad d = \frac{xy-1}{2}. \quad \blacksquare \tag{13}$$

ACKNOWLEDGMENT. We would like to thank the referees for their comments and suggestions.

REFERENCES

1. R. Blecksmith, J. Brillhart, M. Decaro, The completion of Euler's factoring formula, *Rocky Mountain J. of Math* **43** (2013) 755–762.
2. J. Brillhart, Note on Euler's factoring problem, *Amer. Math. Monthly* **116** (2009) 928–931.
3. D. A. Buell, *Binary Quadratic Forms*. Springer Verlag, New York, 1989.
4. M. Decaro, *On Representations of the Forms $mx^2 \pm ny^2$*. Ph.D. dissertation, Northern Illinois University, DeKalb, IL, 2012.
5. L. E. Dickson, *History of the Theory of Numbers*. Vol. 1, Chelsea, New York, 1952.
6. GIMPS, Great Internet Prime Search, www.mersenne.org.
7. O. Ore, *Number Theory and Its History*. McGraw Hill, New York, 1948.
8. D. Shanks, *Solved and Unsolved Problems in Number Theory*. AMS Chelsea, New York, 2002.

JOHN BRILLHART was born in Berkeley in 1930 where he received his education. He obtained his Ph. D. in mathematics at UC Berkeley in 1967 as a student of D. H. Lehmer. As a computational number theorist, he became one of the group of mathematicians at Berkeley who for decades had been dedicated to the development of effective methods for factoring integers or testing them for primality. In 1970, he and Mike Morrison made a breakthrough in factoring huge, composite integers N by devising an efficient method for computing pairs of integers (x, y) that satisfy the congruence $x^2 \equiv y^2 \pmod{N}$.
University of Arizona, Tucson, AZ 85721
jdb@math.arizona.edu

RICHARD BLECKSMITH is a student of John Brillhart and obtained his Ph. D. from the University of Arizona in 1983. His interests are number theory and computation. He has been a professor at Northern Illinois University since 1984. He is now retired, a victim of "pension reform."
Northern Illinois University, DeKalb, IL 60115
richard@math.niu.edu

MIKE DECARO is a student of Richard Blecksmith and obtained his Ph. D. from Northern Illinois University in 2012 in the area of analytic and computational number theory, with a focus on hunting for patterns in very interesting places. Postprofessorial career, he is currently running the department of Data Sciences for Intelligent Medical Objects Inc., a leading company in healthcare terminology.
Intelligent Medical Objects, Inc., Northbrook, IL 60062
mdecaro@imo-online.com