THE AMERICAN MATHEMATICAL MONTHLY

Volume 116, Number 10 December 2009

AN OFFICIAL PUBLICATION OF THE MATHEMATICAL ASSOCIATION OF AMERICA

Taylor & Francis
Taylor & Francis Group

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

A Note on Euler's Factoring Problem

John Brillhart

To cite this article: John Brillhart (2009) A Note on Euler's Factoring Problem, The American Mathematical Monthly, 116:10, 928-931

To link to this article: https://doi.org/10.4169/000298909X477050

Published online: 13 Dec 2017.

Submit your article to this journal

Article views: 7

Citing articles: 1 View citing articles

order $\preceq$ of Ω and define the function

$$X(\omega) := \begin{cases} \Delta & \text{if } \omega \text{ is periodic;} \\ \text{the unique } x \text{ minimizing } \tau^{-x}\omega \text{ under } \preceq & \text{otherwise.} \end{cases}$$

(We may think of $\tau^{-x}\omega$ as ω viewed from location x, in which case X is the location from which ω appears least.) Clearly, X is shift-equivariant. It is almost-everywhere defined since Ω contains only countably many periodic elements. ■

ACKNOWLEDGMENTS. Alexander E. Holroyd is funded in part by an NSERC (Canada) Discovery Grant. Terry Soo is funded in part by an NSERC PGS D and a UBC Graduate fellowship.

REFERENCES

1. D. Blackwell and P. Diaconis, A non-measurable tail set, in *Statistics, Probability and Game Theory*, IMS Lecture Notes-Monograph Series, vol. 30, Institute of Mathematical Statistics, Hayward, CA, 1996, 1–5.
2. R. M. Burton and M. Keane, Density and uniqueness in percolation, *Comm. Math. Phys.* **121** (1989) 501–505. doi:10.1007/BF01217735
3. M. Keane and M. Smorodinsky, A class of finitary codes, *Israel J. Math.* **26** (1977) 352–371. doi:10.1007/BF03007652
4. ———, Bernoulli schemes of the same entropy are finitarily isomorphic, *Ann. of Math. (2)* **109** (1979) 397–406. doi:10.2307/1971117
5. J. C. Oxtoby, *Measure and Category*, 2nd ed., Graduate Texts in Mathematics, vol. 2, Springer-Verlag, New York, 1980.
6. H. L. Royden, *Real Analysis*, 3rd ed., Macmillan, New York, 1988.
7. R. M. Solovay, A model of set-theory in which every set of reals is Lebesgue measurable, *Ann. of Math. (2)* **92** (1970) 1–56. doi:10.2307/1970696
8. G. Vitali, Sul problema della misura dei gruppi di punti di una retta, Gamberini and Parmeggiani, Bologna, 1905.
9. E. Zermelo, Beweis, daß jede Menge wohlgeordnet werden kann, *Math. Ann.* **59** (1904) 514–516. doi:10.1007/BF01445300

Department of Mathematics, University of British Columbia, 121–1984 Mathematics Rd,
Vancouver, BC V6T 1Z2, Canada
holroyd@math.ubc.ca; tsoo@math.ubc.ca

A Note on Euler's Factoring Problem

John Brillhart

1. THE INITIAL PROBLEM. In 1640 Fermat communicated the following result to Mersenne [**5**, p. 67]: A prime of the form $4n + 1$ can be expressed as a sum of two squares in just one way.

About a century later, Euler became interested in the following immediate consequence of this result: An odd integer N that can be expressed as a sum of two squares in two different ways is composite. (That N has the form $4n + 1$ is clear from reducing the sum of two squares mod 4). The factoring problem associated with this

doi:10.4169/000298909X477050

compositeness is, of course, how to find factors of N using the two representations. Here "factoring" means splitting a composite integer N into a product of two factors.

Euler gave a simple solution to this problem that appears as equation (2) in the next theorem.

Theorem 1 [1, p. 360]. *Let N be an odd integer, expressible in two different ways as*

$$N = a^2 + b^2 = c^2 + d^2, \tag{1}$$

where $a, b, c, d \in Z^+$. Then

$$N = \frac{1}{4(d-b)^2}\big[(a-c)^2 + (d-b)^2\big] \cdot \big[(a+c)^2 + (d-b)^2\big]. \tag{2}$$

Proof. Using (1) and the equation $a^2 - c^2 = d^2 - b^2$, we have that

$$\begin{aligned}
&\big[(a-c)^2 + (d-b)^2\big] \cdot \big[(a+c)^2 + (d-b)^2\big] \\
&\quad = (a^2-c^2)^2 + (d-b)^2\big[(a-c)^2 + (a+c)^2\big] + (d-b)^4 \\
&\quad = (d-b)^2\big[(d+b)^2 + 2(a^2+c^2) + (d-b)^2\big] \\
&\quad = 2(d-b)^2(a^2+b^2+c^2+d^2) = 4(d-b)^2 N. \qquad \blacksquare
\end{aligned}$$

Somewhat later Euler gave an improved solution in which the formula had no canceling and the two factors were nontrivial [**1**, p. 360, footnote 27*]. The version of his later formula we give here, viz., (5) in the following development, is taken from Ore's elegant book [**4**, p. 61, (4–12)].

Let $N = a^2 + b^2 = c^2 + d^2$ be an odd integer, where $b < d$, a and c are odd, and b and d are even. Then

$$(a-c)\,(a+c) = (d-b)\,(d+b). \tag{3}$$

Next, set $r = (a-c, d-b)$, where r is even. We can then write $a - c = rs$ and $d - b = rt$, where $(s, t) = 1$. Substituting these results into (3) gives

$$s(a+c) = t(d+b). \tag{4}$$

Since $(s, t) = 1$, we see that $t \mid (a+c)$, so we can write $a + c = tu$. Putting this result into (4), we find that $d + b = su$, which implies that $(a+c, d+b) = u$, where u is even. We can now give the factorization formula:

$$N = \left[\left(\frac{r}{2}\right)^2 + \left(\frac{u}{2}\right)^2\right] \cdot (s^2 + t^2), \tag{5}$$

where the factors are clearly nontrivial.

Proof.

$$\begin{aligned}
\left[\left(\frac{r}{2}\right)^2 + \left(\frac{u}{2}\right)^2\right] \cdot (s^2+t^2) &= \frac{1}{4}\Big[(rs)^2 + (rt)^2 + (su)^2 + (tu)^2\Big] \\
&= \frac{1}{4}\Big[(a-c)^2 + (d-b)^2 + (d+b)^2 + (a+c)^2\Big] \\
&= \frac{1}{2}\big(a^2+b^2+c^2+d^2\big) = N. \qquad \blacksquare
\end{aligned}$$

2. THE GENERAL PROBLEM. Following this investigation, Euler considered the general problem in which an odd integer N is expressed in two different ways as $mx^2 + ny^2$ for fixed positive integers m and n.

He first gave a factorization formula similar to (5) in the case $m = 1$ [**1**, p. 362]. The general problem was later addressed by his mathematical assistants who aided Euler when he became blind. Unfortunately, their writing was lacking, or as Weil puts it [**5**, p. 222], it was "clumsy" and "hardly convincing." This state of affairs seems to have continued until the end of the next century when Lucas reconsidered these questions.

In 1891 Lucas published in volume 1 of his remarkable number theory book a neat proof that a prime cannot be expressed in two different ways as $mx^2 + ny^2$, $m, n \in Z^+$ [**1**, p. 364] [**2**, pp. 356–357]. He also stated that his proof was not a particular case of the theory of quadratic forms which had been used previously.

He mentioned further that he would wait until later (presumably in volume 2 of his book) to publish his associated factoring method. This, however, was not to be, since he tragically died of a virulent infection in 1891, shortly after a freak accident at a banquet when a fragment of a broken dish cut his cheek.

The following year Mathews published a factoring algorithm based on the identities that Lucas had used in proving his theorem [**1**, p. 364] [**3**, Sec. 215]. Since it is unnecessary to prove a number is composite when a formula is to be given for its factorization, we will not present Lucas' proof here. Instead, we will rewrite Mathews' algorithm as the proof of the next theorem in which formula (7) expresses N as the product of two nontrivial factors. This formula clearly shows that he (and no doubt Lucas) had solved Euler's general factoring problem.

Theorem 2. *Let $N > 1$ be an odd integer expressed in two different ways as*

$$N = ma^2 + nb^2 = mc^2 + nd^2, \tag{6}$$

where $a, b, c, d, m, n \in Z^+$, $b < d$, and $(ma, nb) = (mc, nd) = 1$. Then

$$N = (N, ad - bc) \cdot \frac{N}{(N, ad - bc)}, \tag{7}$$

where the factors are nontrivial.

Proof. From (6) we readily obtain the two identities

$$(d^2 - b^2)N = m(ad - bc)(ad + bc) \tag{8}$$

and

$$N^2 = (mac - nbd)^2 + mn(ad + bc)^2. \tag{9}$$

Since $(m, N) = 1$ by (6), it follows from (8) that

$$N \mid (ad - bc)(ad + bc). \tag{10}$$

Note in (9) that if $mn > 1$, then $ad + bc < N$. However, if $mn = 1$, i.e., $m = n = 1$, then (9) becomes

$$N^2 = (ac - bd)^2 + (ad + bc)^2. \tag{11}$$

Further, if $ac - bd = 0$, it follows that $d/c = a/b$. Since $(a, b) = (c, d) = 1$, then $d = a$ and $c = b$, so (6) becomes

$$N = a^2 + b^2 = b^2 + a^2,$$

which are not different representations of N. Thus, $ac - bd \neq 0$ and by (11) we conclude again that $ad + bc < N$.

On the other hand, since $b < d$, (8) implies that $ad - bc \geq 1$. However, using (10) and $ad + bc < N$, we see that $ad - bc > 1$. Thus,

$$1 < ad - bc < ad + bc < N,$$

from which the nontriviality of the factorization in (7) follows from (10). ■

From a computational point of view, (7) can hardly be improved on since it contains only a little arithmetic and the computation of a single GCD. Interestingly, this formula does not contain m or n.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, vol. 1, Chelsea, New York, 1952.
2. E. Lucas, *Théorie des Nombres*, Tome Premier, Librairie Scientifique et Technique, Albert Blanchard, Paris, 1961.
3. G. B. Mathews, *Theory of Numbers*, 2nd ed., Chelsea, New York, 1961.
4. O. Ore, *Number Theory and Its History*, McGraw Hill, New York, 1948.
5. A. Weil, *Number Theory*, Birkhäuser, Boston, 1984.

Department of mathematics, University of Arizona, Tucson, AZ 85721
jdb@math.arizona.edu

π_p, the Value of π in ℓ_p

Joseph B. Keller and Ravi Vakil

The two-dimensional space ℓ_p is the set of points in the plane, with the distance between two points (x, y) and (x', y') defined by $(|x - x'|^p + |y - y'|^p)^{1/p}$, $1 \leq p \leq \infty$. The distance from (x, y) to the origin is then $(|x|^p + |y|^p)^{1/p}$. The equation of the unit circle C_p, i.e., the circle with its center at the origin and radius 1, is

$$(|x|^p + |y|^p)^{1/p} = 1. \tag{1}$$

Figure 1 shows C_p for $p = 1$, $3/2$, 2, 3, and ∞. Equation (1) is unchanged when x is replaced by $-x$, when y is replaced by $-y$, and when x and y are interchanged. Therefore C_p is symmetric about the y-axis, about the x-axis, and about the line $x = y$.

It is natural to define π_p as the ratio of the circumference of C_p (in the p-metric) to two times its radius (also in the p-metric), which is its "diameter," 2. This definition has

doi:10.4169/000298909X477069