Leonhard Euler's Convenient Numbers

Günther Frei

To my dear friend Paulo Ribenboim
on the occasion of the 200th anniversary
of Leonhard Euler's death

1. Introduction

Leonhard Euler, the great Swiss mathematician, died in St. Petersburg (now Leningrad) 200 years ago, on the 18th of September, 1783. Euler was the most eminent and influential mathematician of the 18th century and he was by far the most prolific mathematician of all time. His discoveries in mathematics and in many fields of science are so numerous that his collected work will eventually fill about 80 quarto volumes.

All his life Euler worked intensively on problems in number theory. He was already 70 years old and almost blind when he discovered the *convenient numbers* in connection with his search for large prime numbers. There is a close relationship of these numbers with class field theory, and there remain many interesting open questions relating to them.

2. Sums of Squares

Effectively opening up class field theory, Fermat, Euler and Lagrange made the fundamental observation that the prime numbers represented by certain integral binary quadratic forms are all in the same arithmetical progressions, that is that they can be characterized by congruence conditions and hence are representable by *linear* forms. This means that there is a class field (that is, an abelian extension) L over the rationals $\mathbf{Q}$ such that all primes represented by that same form have the same decomposition law in L.

A first such observation was made by Fermat in a letter to his friend Mersenne on the 25th of December, 1640.

THEOREM 1: *An odd prime number p is the sum of two squares of natural numbers, $p = x^2 + y^2$, $x,y \in \mathbf{N} = \{1,2,3, \ldots\}$, if and only if $p \equiv 1$ modulo 4.*

Furthermore, this representation is unique and x and y are relatively prime, $(x,y) = 1$.

Euler proved this theorem more than a century later, in 1750. In 1758, Euler noticed and proved that the converse is also true.

THEOREM 2: *If an odd natural number $n > 1$ is representable as a sum of two non-negative integers in exactly one way $n = x^2 + y^2$, $x,y \in \mathbf{N}$ ($\mathbf{N}$ stands for the non-negative integers) and if, in addition, x and y are relatively prime, then n is a prime number.*

Hence a criterion is obtained that allows us to test whether a given number n is prime or not. It suffices to subtract from n all squares x^2 less than $n/2$ and to check whether a square y^2 is left over exactly once and whether $(x,y) = 1$ for this pair x,y.

In view of Theorem 1 this method can only be applied to numbers $n \equiv 1$ modulo 4. In order to extend it also to numbers n of the form $n \equiv 3$ modulo 4 Euler examined the representations $n = x^2 + 2y^2$ and $n = x^2 + 3y^2$, which had already been studied by Fermat, and, more generally, $n = ax^2 + by^2$ where a and b are any natural numbers with $(a,b) = 1$. Euler's results, published in 1774 and 1763, are these:

THEOREM 3: (a) *An odd prime number p is representable by the form $x^2 + 2y^2$, $p = x^2 + 2y^2$, with $x,y \in \mathbf{N}$, if and only if $p \equiv 1,3$ modulo 8. This representation is unique and x and y are relatively prime.*

(b) *Conversely, if $n > 1$ is an odd natural number which is representable in exactly one way as $n = x^2 + 2y^2$ with $x,y \in \mathbf{N}$, and if x and y are relatively prime, then n is a prime.*

THEOREM 4: (a) *A prime $p \neq 2,3$ is representable by the form $x^2 + 3y^2$, $p = x^2 + 3y^2$, with $x,y \in \mathbf{N}$ if and only if $p \equiv 1$ modulo 3. This representation is unique and x and y are relatively prime.*

(b) *Conversely, if $n > 1$ is an odd natural number which is representable in exactly one way as $n = x^2 + 3y^2$, with $x,y \in \mathbf{N}$, and if x and $3y$ are relatively prime, then n is a prime.*

Euler proved all parts of Theorem 3 except the one that says that if $p \equiv 3$ modulo 8 then p is representable as $p = x^2 + 2y^2$. As to Theorem 4, Euler proved only the first half of the theorem. Complete proofs of Theorems 3 and 4 were first given by Lagrange in 1775. With the help of the last theorem Euler was able to show, for instance, that $n = 1{,}000{,}003 = 1000^2 + 3 \cdot 1^2$ is prime, whereas $n = 10{,}003 = 100^2 + 3 \cdot 1^2 = 16^2 + 3 \cdot 57^2$ is not. In fact $10{,}003 = 7 \cdot 1429$, whereby the two factors can be found by means of the two different representations.

3. Convenient Numbers

Unfortunately it is not possible to get theorems analogous to Theorems 2, 3, and 4 for the general form $ax^2 + by^2$. This is shown by the example $x^2 + 11y^2$. For, $15 = 2^2 + 11 \cdot 1^2$ is the only representation of 15 by the form $x^2 + 11y^2$, but 15 is not prime. Euler was thus led to pose the following question. Which natural numbers m satisfy the following criterion (C)?

(C) *If $n > 1$ is an odd natural number which is representable as $n = x^2 + my^2$ with non-negative numbers $x,y \in \mathbf{N}$ in exactly one way, and if in addition, $(x,my) = 1$, then n is a prime.*

If a natural number m satisfies criterion (C) then it is called a *convenient number* (*numerus idoneus*).

More precisely, Euler introduced convenient numbers in 1778 in the following way.

DEFINITION 5: *A form $ax^2 + by^2$, with $a,b \in \mathbf{N}$ and $(a,b) = 1$, is called a* convenient form *if it satisfies the following condition:*

> Any natural number $n > 1$ that is representable in exactly one way as $n = ax^2 + by^2$, with $x,y \in \mathbf{N}$ such that $(x,y) = 1$, is necessarily of the form
>
> $n = tp$ or $n = 2tp$ or $n = t2^s$,
>
> where t is a divisor of $a \cdot b$, p is an odd prime, and s is a natural number.

In his definition Euler did not explicitly mention the possibility $n = t \cdot 2^s$, with $t \neq 1$, but this case has to be included.

Notice that a convenient form $x^2 + my^2$ satisfies condition (C). For, if $n > 1$ is required to be odd, then $n = t \cdot p$, and the condition $(x,my) = 1$ implies that $t = 1$ since t is a divisor of m and of n and hence any prime factor of t is a divisor of x and of my.

Next Euler established the following result.

THEOREM 6: *Let $a,b \in \mathbf{N}$ with $(a,b) = 1$. Then the form $ax^2 + by^2$ is convenient if and only if the form $x^2 + aby^2$ is convenient.*

In his proof Euler assumed that a and b are not divisible by squares, but we shall see later that this assumption is not necessary (see Theorem 13).

This last theorem suggests the following definition.

DEFINITION 7: *A number $m \in \mathbf{N}$ is called* convenient (*Latin:* idoneus, *French:* convenable) *if the form $x^2 + my^2$ is convenient.*

Such a number m is indeed convenient (in the everyday sense) for searching for large prime numbers and for testing whether a given number n is prime or not.

Euler gave several illustrations of his method of searching for prime numbers (see Sections 2 and 8).

4. Euler's Criterion

Next Euler set out to determine all convenient numbers and he noted in 1778 the following empirical result:

THEOREM 8: *The following 65 numbers are convenient*

1	2	3	4	5	6	7	8	9	10
12	13	15	16	18	21	22	24	25	28
30	33	37	40	42	45	48	57	58	60
70	72	78	85	88	93	102	105	112	120
130	133	165	168	177	190	210	232	240	253
273	280	312	330	345	357	385	408	462	520
760	840	1320	1365	1848					

He added that he obtained this table "quite easily" by applying the following criterion, which we will refer to as "Euler's criterion."

THEOREM 9: *A number $m \in \mathbf{N}$ is convenient if and only if every natural number n of the form*

$n = m + x^2 < 4m$ *with* $x \in \mathbf{N}$, $(x,m) = 1$

is necessarily of one of the four forms

$n = p$, $n = 2p$, $n = p^2$, or $n = 2^s$,

where p is an odd prime number and $s \in \mathbf{N}$.

This criterion was, in its turn, obtained by Euler from the following result, which has no overt reference to convenient numbers.

THEOREM 10: *If a composite number $r \cdot s$ $(r > s)$ is representable by the form $x^2 + my^2$ in a single way with $x,y \in \mathbf{N}$ and with $(x,my) = 1$ and $(rs,mxy) = 1$, then there exist infinitely many other composite numbers with the same property. In particular, if the hypothesis is satisfied, then there is always such a composite number rs with $rs < 4m$.*

Euler himself illustrated the criterion embodied in Theorem 9 for the numbers $m = 11, 13, 14, 15, 60$.

For $m = 13$ we have, for instance,

$$13 + 1^2 = 14 = 2p$$
$$13 + 2^2 = 17 = p$$
$$13 + 3^2 = 22 = 2p$$
$$13 + 4^2 = 29 = p$$
$$13 + 5^2 = 38 = 2p$$
$$13 + 6^2 = 49 = p^2$$

hence $m = 13$ must be convenient. Again, with $m = 15$ we have

$$15 + 1^2 = 16 = 2^4$$
$$15 + 2^2 = 19 = p$$
$$15 + 4^2 = 31 = p$$

and we conclude that 15 is convenient. On the other hand, 14 is not convenient, since

$$14 + 1^2 = 15 = 3 \cdot 5$$

Euler's proof of Theorem 9 contains some serious gaps as Grube noticed in 1874. Grube was, however, able to show that the criterion is indeed necessary; but whether it is also sufficient is still an open problem, in spite of the remark made by Gauss in his "Disquisitiones arithmeticae" (Art. 303) that this is easy to prove. Thus, we should regard as incomplete the proof just given that 13 and 15 are convenient. On the other hand, Grube could derive from Gauss's theory of quadratic forms a criterion which comes close to Euler's criterion (see Theorem 15).

Euler was surprised to discover that he did not find any more convenient numbers beyond 1848 in spite of his efforts to extend the calculations up to 3000 and later up to 10,000. In order to understand this phenomenon, he studied the distribution of the convenient numbers and found the following ten properties.

THEOREM 11: 1. *If m is convenient and $m = t^2$, then $t = 1, 2, 3, 4, 5$.*

2. *If m is convenient and $m \equiv 3$ modulo 4, then $4m$ is convenient.*

3. *If m is convenient and $m \equiv 4$ modulo 8, then $4m$ is convenient.*

4. *If k^2m is convenient, then m is convenient.*

5. *If m is convenient and $m \equiv 2$ modulo 3, then $9m$ is convenient.*

6. *If $m > 1$ is convenient and $m \equiv 1$ modulo 4, then $4m$ is not convenient.*

7. *If m is convenient and $m \equiv 2$ modulo 4, then $4m$ is convenient.*

8. *If m is convenient and $m \equiv 8$ modulo 16, then $4m$ is not convenient.*

9. *If m is convenient and $m \equiv 16$ modulo 32, then $4m$ is not convenient.*

10. *If m is convenient and $m + a^2 = p^2 < 4m$ for a prime p, then $4m$ is not convenient.*

Euler's proofs of the properties 4, 6, 8 and 9 above were not quite rigorous, but Grube was able to give a complete proof of Theorem 11 in 1874. Grube, who, in fact, gave proofs of generalized versions of several of these properties, showed that they are all easy consequences of Gauss's theory of quadratic forms.

5. Gauss's Criterion and Grube's Criterion

The principal theorem of Gauss concerning convenient numbers, on which Grube's paper is based, is the following (see [8], Art. 303).

THEOREM 12: (a) *A number $m \in \mathbf{N}$ is convenient if and only if every genus of properly primitive integral binary quadratic forms of determinant $d = -m$ contains precisely one proper class of properly primitive forms;*

or alternatively,

(b) *A number $m \in \mathbf{N}$ is convenient if and only if every proper class of properly primitive integral binary quadratic forms with determinant $d = -m$ is a proper ambiguous class of properly primitive forms.*

For the definition of these notions and for more details see [6] or the forthcoming publication [7].

Gauss certainly has a proof of this theorem, but the credit for having first published a proof must go to Grube (1874).

From the criterion of Theorem 12 one immediately derives the next theorem, of which Theorem 6 is a special case.

THEOREM 13: *If a, b, a', b' are natural numbers with $(a,b) = 1$, $(a',b') = 1$ and $ab = a'b'$, then the form $F = ax^2 + by^2$ is convenient if and only if the form $F' = a'x^2 + b'y^2$ is convenient.*

This follows from Gauss's criterion (Theorem 12), since F and F' are properly primitive forms, because $(a,b) = 1$ and $(a',b') = 1$, and have the same determinant $d = -ab = -a'b'$.

Gauss's criterion, together with the reduction theory of quadratic forms, is at the basis of the following criterion, attributable to Grube.

THEOREM 14: *A number $m \in \mathbf{N}$ is convenient if and only if every natural number n of the form*

$$n = m + x^2 \text{ with } x \in \mathbf{N} \text{ and } x < \sqrt{\frac{m}{3}}$$

admits no factorizations

$$n = rs \text{ with } s \geq r \geq 2x,\ r, s \in \mathbf{N}$$

except those of the form

$$r = s \text{ or } r = 2x.$$

Notice that Grube's criterion reinstates 13 and 15 as convenient numbers.

Now let us look at some further examples. For $m = 48$, one has the factorizations

$$\begin{aligned} 48 + 1^2 &= 49 = 7 \cdot 7 \;: r = s \\ 48 + 2^2 &= 52 = 4 \cdot 13 : r = 2x \\ 48 + 3^2 &= 57 \\ 48 + 4^2 &= 64 = 8 \cdot 8 \;: r = s \end{aligned}$$

(there are no other factorizations $n = rs$ with $s \geq r \geq 2x$). Hence $m = 48$ is convenient. Similarly $m = 60$ is convenient, since

$$\begin{aligned} 60 + 1^2 &= 61 \\ 60 + 2^2 &= 64 = 8 \cdot 8 : r = s \\ 60 + 3^2 &= 69 \\ 60 + 4^2 &= 76 \end{aligned}$$

but $m = 11$ is not convenient, because

$$11 + 1^2 = 12 = 3 \cdot 4 \text{ with } s > r > 2x.$$

Grube determined all convenient numbers which are divisible by a square $k^2 \neq 1$. For the others, he derived the following criterion which comes close to the still unproven criterion of Euler.

THEOREM 15: *Suppose $m \in \mathbf{N}$ is not divisible by a square and suppose $m \neq 3, 7, 15$.*

Then m is convenient if and only if every natural number n of the form

$$n = m + x^2 \text{ with } n \in \mathbf{N} \text{ and } x < \sqrt{\frac{m}{3}}$$

is also of the form

$$n = tp,\ n = 2tp \text{ or } n = p^2$$

where t is a divisor of m, and p is an odd prime number.

As an example let us examine $m = 120$. From Theorem 11, properties 4 and 7, we deduce that $m = 4(4k + 2)$, $k \in \mathbf{N}$, is convenient if and only if $4k + 2$ is convenient. Hence 120 is convenient if and only if 30 is convenient. By applying Theorem 15, as we may since 30 is not divisible by a square, we find

$$\begin{aligned} 30 + 1^2 &= 31 = p \\ 30 + 2^2 &= 34 = 2 \cdot 17 = 2p \\ 30 + 3^2 &= 39 = 3 \cdot 13 = tp \end{aligned}$$

and therefore that $m = 30$ is convenient. Thus $m = 120$ is also convenient.

6. The Problem of the Completeness of Euler's Table

Euler's guess that his table (Theorem 8) contains all convenient numbers is still an unproven conjecture, although this problem seems to be close to a solution. Initial progress was made by S. Chowla who showed in 1934 that there are only finitely many convenient numbers. His proof rests on a paper by Heilbronn and on the property that

$$\lim_{d \to \infty} \frac{h(d)}{g(d)} = \infty$$

where $h(d)$ denotes the number of proper classes and $g(d)$ the number of genera of binary quadratic forms with determinant d. By using Siegel's asymptotic formula and the analytic class number formula, Briggs and Chowla (1954), and later E. Grosswald (1963), and P. J. Weinberger (1973) made further progress on the problem. The result which emerges from this work is that the table is, in fact, complete, *except for possibly one more number!*

7. Applications

Euler applied the convenient numbers effectively in order to search for prime numbers or test given numbers for primality. In addition to the examples already mentioned in Section 2 he determined, by means of the convenient number $m = 232$, all prime numbers p of the form

$$p = 1 + 232y^2 \text{ with } 1 \leq y \leq 300,\ y \in \mathbf{N}.$$

He further studied primes of the form

$$p = 40x^2 + 13y^2$$

and of the form

$$p = x^2 + 1848y^2.$$

In particular, he found all primes p of the form

$$p = 197^2 + 1848y^2 \text{ with } 1 \leq y \leq 100,\ y \in \mathbf{N}.$$

There are, in fact, 22 such prime numbers and the largest among them is

$$p = 197^2 + 1848 \cdot 100^2 = 18{,}518{,}809.$$

This was by far the largest prime known at that time, except for the Mersenne prime $p = 2^{31} - 1$, also discovered by Euler.

From class field theory and from Gauss's criterion, one can deduce another important property of con-

continued on page 64

sibly with the aid of the Mathematics Education Department; and an evening for the local mathematics teachers is also under consideration. Time is of course the major problem.

Events of this kind have to be rather carefully organized. We had an advisory committee including teachers, Local Authority representatives, and people from the University and GEC. While this did not have to meet very often, it did keep a careful eye on the preparations over a long period: about six months prior to the classes themselves. Without this kind of preparation, we doubt the classes would have been a success. In fact we found that the classes involved as much preparation as an undergraduate lecture course, and were more exhausting to give, but very rewarding.

It was important that the lecturers and tutors were on familiar ground both geographically and mathematically (except in the case of the gyroscope class, when the tutors refused to descend from their balcony for coffee in case their ignorance was revealed). The informal atmosphere, the (at least partial) blurring of the hierarchical teacher/pupil relationship, was absolutely crucial. The children were sacrificing a large part of their weekends for ten solid weeks: they had to do this voluntarily, and because they enjoyed it. If it had been "an extra day of school" they wouldn't have kept coming. There was clearly some strong pressure on them from schools and parents, to keep attending, but this alone would not have sustained the kind of interest we observed; and the children themselves commented favourably on the atmosphere.

It was very satisfying to work on a project that involved not just the University, but the community: schools, and above all local industry. The GEC representative, John Lorriman, took a great interest in the way the classes developed.

Whether the classes made any impact that will amount to much in the long run is unclear: ten weeks is a very short time. But they do show that it is possible to capture the interest of the most able young mathematicians at a crucial stage in their development. We hope that other institutions, with similar concerns, may take up the masterclass idea, or use it as a basis for their own efforts; and we'd like to think that we've made a small but significant contribution to the future of mathematics in this country.

Mathematics Institute
University of Warwick
Coventry CV4 7AL
England

Euler's Convenient Numbers
continued from page 58

venient numbers, which we now describe.

THEOREM 16: *Let* $m \in \mathbf{N}$. *Then all prime numbers* p *of the form*

$$p = x^2 + my^2 \text{ with } x,y \in \mathbf{N}$$

can be characterized by congruence conditions with respect to a single *modulus* f *if and only if* m *is convenient.*

The number f is called the *conductor* of m. Recall that, for $m = 1, 2, 3$ we found $f = 4, 8, 3$ respectively (see Theorems 1, 3 and 4).

These directions of research and these results, however, by no means exhaust the possibilities inherent in Euler's concept of convenient numbers. To name but one totally different type of application, we refer to the work of Hilf who showed in 1963 (see [1], p. 57) the relation of convenient numbers to eigenvalue problems in physics. The mathematical legacy of Euler seems truly a cornucopia.

References

1. Baltes, H. P. and Hilf, E. R.: Spectra of Finite Systems. Bibliographisches Institut, Zürich, 1976
2. Chowla, S.: An Extension of Heilbronn's Class Number Theorem. Quarterly J. Math. (Oxford) 5 (1934), 304–307
3. Chowla, S. and Briggs, W. E.: On discriminants of binary quadratic forms with a single class in each genus. Canadian J. Math. 6 (1954), 463–470
4. Euler, L.: Opera Omnia. Series Prima. Teubner, Leipzig, 1911–
5. Fermat, P.: Oeuvres. Tome 2, 212–217, Gauthier-Villars, Paris, 1894
6. Frei, G.: On the Development of the Genus of Quadratic Forms. Ann. Sci. Math. Québec 3 (1979), 5–62
7. Frei, G.: Les nombres convenables de Leonhard Euler. (To appear)
8. Gauss, C. F.: Disquisitiones arithmeticae. Leipzig, 1801 (or: Untersuchungen über höhere Mathematik. Herausgegeben von H. Maser, Springer, Berlin, 1889)
9. Grosswald, E.: Negative discriminants of binary quadratic forms with one class in each genus. Acta Arithmetica 8 (1963), 295–306
10. Grube, F.: Ueber einige Eulersche Sätze aus der Theorie der quadratischen Formen. Zeitschrift für Mathematik und Physik 19 (1874), 492–519
11. Lagrange, J.-L.: Recherches d'arithmétique, 1773 et 1775. Oeuvres, Tome 3, Gauthier-Villars, Paris, 1867
12. Steinig, J.: On Euler's Idoenal Numbers. Elemente der Mathematik 21 (1966), 73–88
13. Weinberger, P. J.: Exponents of the class groups of complex quadratic fields. Acta Arithmetica 22 (1973), 117–124

Département de mathématiques
Université Laval
Ste-Foy, Québec
Canada GIK 7P4

Mathematik
ETH
CH-8092 Zürich
Switzerland