Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 21 (1966)
Heft: 4

Artikel: On Euler's idoneal numbers
Autor: Steinig, J.
DOI: https://doi.org/10.5169/seals-24651

ELEMENTE DER MATHEMATIK
Revue de mathématiques élémentaires – Rivista di matematica elementare
Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts
Publiziert mit Unterstützung des Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung

El. Math. Band XXI Heft 4 Seiten 73–96 10. Juli 1966

On Euler's Idoneal Numbers

1. Introduction

In his 1621 edition of the Arithmetic of DIOPHANTUS [1], BACHET DE MÉZIRIAC cautiously observed that 'almost all' primes of the form $4k + 1$ are representable as a sum of two integral squares[1]). ALBERT GIRARD went a step further and stated[2]) without proof in 1625 and 1634, in commentaries to his edition of SIMON STEVIN's mathematical works ([2] and [3]) that all such primes are thus representable.

In 1641 FERMAT communicated[3]) the same theorem to FRENICLE DE BESSY [4], while a stronger formulation affirming the uniqueness of this representation for a given prime is enunciated[4]) in a letter [5] to MERSENNE dated 1640, and also appears as a marginal note[5]) in FERMAT's copy of BACHET's *Diophantus* [6].

FRENICLE probably discovered independently that a prime can have at most one representation, for in his reply [7] to FERMAT's letter he proposes[6]) the problem of factoring some integer which has several expressions as a sum of two squares; in particular he asks FERMAT to deduce from $221 = 10^2 + 11^2 = 5^2 + 14^2$ that $221 = 13 \cdot 17$.

FERMAT's proof of GIRARD's theorem is outlined in a very interesting letter [8] sent to CARCAVI in 1659, which contains an account of his principal methods and dis-

---

[1]) '...quandoquidem omnes fere huiusmodi numeri componuntur ex duobus quadratis, quales sunt 5. 13. 17. 29. 41. aliique primi numeri qui sublata unitate relinquunt numerum pariter parem'.

[2]) 'Determinaison d'un nombre qui se peut diviser en deux quarrez entiers:
I. Tout nombre quarré.
II. Tout nombre premier qui excede un nombre quaternaire de l'unité.
III. Le produict de ceux qui sont tels.
IV. Et le double de chascun d'iceux.'

[3]) 'La proposition fondamentale des triangles rectangles est que tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés'.

[4]) 'Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle'.

[5]) 'Numerus primus, qui superat unitate quaternarii multiplicem, semel tantum est hypotenusa trianguli rectanguli'.

[6]) 'Sur le sujet des triangles, voici ce que je vous proposerai encore: Une hypoténuse composée étant donnée avec les quarrés premiers entre eux qui la composent par leur addition, trouver ses parties. Que 221 soit l'hypoténuse donnée avec les quarrés qui la composent, savoir: 100, 121 et 196, 25, il faut trouver par le moyen d'iceux que 221 a 13 et 17 pour parties'.

coveries in number theory. He writes[7]) that after several unsuccessful attempts he has obtained a proof by 'descente infinie'.

A natural question to ask is whether a prime $4k + 3$ is representable as a sum of two squares; it is very simple to show that this is impossible, and indeed that no integer of this form can be thus represented. This result was known to FERMAT, who mentioned it in a letter [9] to ROBERVAL[8]).

It is evident that if a prime is a sum of two natural numbers they must be relatively prime. Bearing this in mind, the results of GIRARD, FERMAT, and FRENICLE yield the following theorem:

An odd prime is representable as a sum of two squares if and only if it is of the form $4k + 1$. *This representation is unique, and the two squares are relatively prime*[9]).

This in turn provides two criteria for primality; it follows that an odd integer is composite in either of the following cases: a) it is of the form $4k + 1$ but is not representable as a sum of two squares, thus 21; b) it has several such representations, as 221.

FERMAT died in 1665, and no further progress was made for about a century, until EULER published the first recorded proof of GIRARD's theorem[10]) in 1760 and then sought to obtain another criterion for primality by proving a converse of the sharper theorem of FERMAT. We know that an odd integer which is a sum of two squares must be of the form $4k + 1$; may one affirm that an odd integer which is uniquely representable as $x^2 + y^2$ is a prime it $(x, y) = 1$? EULER proved that this is indeed true (except for the trivial case $x = 1, y = 0$); his discovery can be expressed as follows: *An odd integer greater than 1 which is a sum of two squares in only one way is a prime if these squares are relatively prime.*

Unfortunately he twice gave an erroneous formulation of this result. The first occurs in a letter [10] to GOLDBACH, dated 1745, where EULER writes '*Si numerus* $4n + 1$ *unico modo in duo quadrata resolvi possit, tum certe erit numerus primus*', which is obviously wrong since 45, although composite, has the unique representation $45 = 3^2 + 6^2$.

Then in 1758 he published [11] a proof of his converse, which he enunciated in the following manner: '*Si numerus formae* $4n + 1$ *unico modo in duo quadrata inter se prima resolvi queat, tum certe est numerus primus*'. This is also incorrect; he should have written '*Si numerus major quam unitas et formae* $4n + 1$ *unico modo in duo quadrata resolvi queat, ac ea quadrata inter se prima sint, tum certe est numerus primus*'.

Indeed, it is one thing to say that an integer has a unique representation as a sum of two relatively prime squares, and quite a different one to say that an integer has a unique representation as a sum of two squares and that these are relatively prime.

---

[7]) '...si un nombre premier pris à discretion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y aura un nombre premier de même nature, moindre que le donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés'.

[8]) '...j'ai autrefois démontré qu'un nombre moindre de l'unité qu'un multiple du quaternaire n'est ni un quarré, ni composé de deux quarrés, ni en entiers ni en fractions'.

[9]) In saying that an integer is a sum of two squares, I mean two squares of nonnegative integers. Further, two representations which differ only in the order of the summands are considered to be identical; thus 49 is uniquely representable as a sum of two squares (but these are not relatively prime).

[10]) EULER attributed [32] the theorem to FERMAT.

For instance, although 125 is not a prime, it is a sum of two relatively prime squares in only one way: $125 = 2^2 + 11^2 = 5^2 + 10^2$. EULER himself undoubtedly had an accurate idea of what he had proved, for he knew that an integer with several representations as a sum of two squares must be composite. In fact, he correctly wrote [12] some twenty-five years later that '*...iam rigorose est demonstratum omnes numeros, qui unico tantum modo sunt summae duorum quadratorum, semper etiam esse primos, dummodo fuerint impares, atque numeri x et y primi inter se, quae levis limitatio sponte sua patet*'.

A contemporary of EULER's, BEGUELIN, probably noticed his error, and gave [13] a formulation which is both correct (apart from the trivial case noted above) and extremely elegant: '*...M. Euler a démontré ... que tout nombre impair qui est la somme de deux quarrés premiers entr'eux, est un nombre premier lorsqu'il ne peut pas être décomposé en deux autres quarrés*'.

However, EULER's unfortunate lapses were the origin of errors which have persisted up to our day. For example, F. RUDIO wrote in his preface [14] to Volume I of EULER's *Commentationes Arithmeticae* that '*Wenn sich eine Zahl* $4n + 1$ *nur auf eine einzige Art als Summe von zwei Quadraten, die unter sich prim sind, darstellen lässt, dann ist sie sicher eine Primzahl*', which contains the same syntactic error as EULER's article. Then, in RUDIO's preface [15] to Volume II we find the passage '*...Zahlen der Form* $4n + 1$. *Von diesen hatte er ... bewiesen, dass sie prim sind, falls sie sich nur auf eine einzige Weise in der Form* $a^2 + b^2$ *darstellen lassen*', which repeats the mistake of EULER's letter to GOLDBACH. Finally R. FUETER, who prefaced [16] Volume III, gives EULER's result as '*Ist nämlich eine Zahl nur auf eine Weise als Summe von zwei Quadraten darstellbar, so muss sie Primzahl sein*', to which we can object that $10 = 1^2 + 3^2$ without being a prime.

In his search for further criteria of primality, EULER then discovered that certain other forms can be put to the same use as $x^2 + y^2$: some natural numbers D have the interesting property that any odd integer greater than unity which is representable as $\alpha x^2 + \beta y^2$ in a single manner is a prime if $\alpha\beta = D$ and $(\alpha x, \beta y) = 1$. These particular values D he named 'congruent' or (more frequently) 'idoneal' numbers.

Most of his theorems concerning idoneal numbers are stated without proof, and he admits that they are based on induction, by which he means that he has not encountered any counterexample[11]). Also, many of his statements are unclear or incomplete and several of his errors have been transmitted by later authors, thus creating a somewhat confused state of affairs.

After this situation had come to light during a seminar, Professor H. HOPF suggested that I attempt a historical and critical appraisal[12]) of the subject; I would like to seize this opportunity to express my gratitude for his constant interest and unfailing kindness.

2. A Property of Binary Quadratic Forms

In 1778 EULER announced [12] the following property of binary quadratic forms, which is an extension of the result obtained by FERMAT and FRENICLE for the form

[11]) In the summary introducing EULER's *Specimen de usu observationum in mathesi pura* [17] we find the passage 'Talis cognitio solis observationibus innixa, quamdiu quidem demonstratione destituitur, a veritate sollicite est discernenda atque ad inductionem referri solet' (for a translation of relevant extracts of this summary and comments on EULER's use of induction, see G. PÓLYA [18]).

[12]) Another essay on this subject has recently been written by I. G. MELNIKOV [19].

$x^2 + y^2$: '*...constat omnes numeros, qui in tali forma* $m\,x\,x + n\,y\,y$ *duplici modo continentur, certe non esse primos, siquidem numeri* m *et* n *ambo fuerint positivi...*'. The condition that the coefficients m and n be positive is essential, as EULER himself points out with the example $2\,x^2 - y^2$, which represents the prime 7 for infinitely many pairs of natural numbers x, y. This important restriction is unfortunately omitted[13]) in other articles ([20], [21]). EULER gave two proofs of this theorem; both consist in showing how an integer with several representations can be factored, and both are incomplete.

His first proof ([20], [21]) is as follows: let the integer N have two different representations by the form $\alpha\,x^2 + \beta\,y^2$:

$$N = \alpha\,a^2 + \beta\,b^2 = \alpha\,A^2 + \beta\,B^2. \tag{1}$$

By eliminating β we get

$$N\,(B - b)\,(B + b) = \alpha\,(a\,B + A\,b)\,(a\,B - A\,b), \tag{2}$$

and EULER [20] concludes '*unde satis patet numerum* N *primum esse non posse, sed certe communem factorem habere, tam cum formula* $a\,B + A\,b$ *quam cum formula* $a\,B - A\,b$, *quandoquidem istae formulae diversae sunt a prioribus* $B + b$ *et* $B - b$' [14]). This is not very convincing; it makes no use of the fact that α and β are positive, and conceivably one of the parentheses $(a\,B + A\,b)$ or $(a\,B - A\,b)$ could be a multiple of N, thus reducing (2) to a trivial identity. To complete EULER's proof, we remark first that there is no loss of generality in assuming $\alpha\,a^2$ and $\beta\,b^2$ to be relatively prime, for any common factor of these two integers divides N. Clearly, the condition $(\alpha\,a^2, \beta\,b^2) = 1$ implies that $(N, \alpha) = 1$, and this together with (2) shows that N divides the product $(a\,B + A\,b)\,(a\,B - A\,b)$. Therefore it is sufficient to prove the inequality $N > |\,a\,B \pm A\,b\,|$ in order to show that both parentheses have a non-trivial common factor with N. This can be done by multiplying the two representations in (1) to obtain the relation[15])

$$N^2 = (\alpha\,a\,A \pm \beta\,b\,B)^2 + \alpha\,\beta\,(a\,B \mp A\,b)^2, \tag{3}$$

whence $N^2 \geqslant \alpha\,\beta\,(a\,B \pm A\,b)^2$; since $\alpha\,\beta \geqslant 1$, it follows that

$$N^2 \geqslant (a\,B \pm A\,b)^2,$$

and therefore $N \geqslant a\,B + A\,b > |\,a\,B - A\,b\,|$. It is easily seen that equality cannot occur, since this would imply $\alpha = \beta = 1$ and $a\,A = b\,B$, thus giving two identical representations in (1)[16]).

---

[13]) For example in [20] we read: 'Si numerus N duplici modo contineatur in tali formula: $\alpha\,x\,x + \beta\,y\,y$, ubi α et β sunt numeri dati quicunque, tum certum est illum numerum N non esse primum, atque adeo eius divisores facile investigari poterunt'.

[14]) This was translated [21] by EULER's assistant NICOLAS FUSS for BEGUELIN as follows: '...par conséquent le nombre proposé N aura dans ce cas-ci toujours un facteur commun tant avec $a\,B + A\,b$ qu'avec $a\,B - A\,b$, parce que ces formules sont toutes différentes des formules $B + b$ & $B - b$...'.

[15]) EULER applied this relation in [20] to prove that the product of two numbers of the form $\alpha\,x^2 + \beta\,y^2$ is of the form $x^2 + \alpha\,\beta\,y^2$.

[16]) NAGELL [22] and TROST [23] prove EULER's theorem by using (2) and (3) to show that if N is a prime, the two representations in (1) must be identical.

EULER's second proof rested on another method for factoring an integer N which has several representations. In [24] he explains it for the particular case $\alpha = 1$; let

$$N = a^2 + \lambda b^2 = x^2 + \lambda y^2, \tag{4}$$

and write this as $(a + x)/(b + y) = \lambda (y - b)/(a - x)$. Then simplify the fraction on the right until numerator and denominator are relatively prime: $(y - b)/(a - x) = p/q$ with $(p, q) = 1$, so that $y - b = n p$ and $a - x = n q$ for some integer n. Thus $(a + x)/(y + b) = \lambda p/q$ and EULER sets $a + x = \lambda m p$, $y + b = m q$. From the four equations

$$y - b = n p \qquad y + b = m q$$
$$a - x = n q \qquad a + x = \lambda m p$$

one obtains $a = (n q + \lambda m p)/2$ and $b = (m q - n p)/2$, whence by replacing in (4),

$$N = \frac{1}{4} (\lambda m^2 + n^2) (\lambda p^2 + q^2). \tag{5}$$

EULER then asserts '*... unde patet formulam $\lambda p p + q q$ vel ipsam vel eius semissem vel quadrantem esse factorem numeri propositi N*', which is not always correct; if $(\lambda, q) > 1$, m is not an integer, and then EULER's conclusion is erroneous[17]). However, his mistake is easily repaired by setting $(\lambda, q) = t$ and $\lambda = t \lambda'$, $q = t q'$. We then get $y + b = m' q'$ and $a + x = \lambda' m' p$, where m' is an integer. As above we obtain

$$N = \frac{1}{4} (\lambda' m'^2 + t n^2) (\lambda' p^2 + t q'^2), \tag{6}$$

and it is not difficult to show that (6) yields two non-trivial factors of N[18]).

EULER indicated ([12], [20], [21]) a similar method for obtaining factors of an integer which has several representations when $1 < \alpha < \beta$, but his account contains the same type of error as for the case $\alpha = 1$.

A rather well-known illustration of EULER's method for factoring large integers concerns the number 1000009. After proving his converse to FERMAT's theorem for the form $x^2 + y^2$, EULER concluded his article [11] of 1758 with several examples, one of which consisted in showing that 1000009 is expressible as a sum of two squares in two different manners and is therefore not a prime. Then in 1774 he discussed the problem of constructing a table of primes, and gave a list [26] allegedly containing all primes between 10^6 and 1002000, but which in fact omitted one prime and included several composite numbers[19]), in particular 1000009. A correction to this effect appeared [27] in the Proceedings of the St. Petersburg Academy of Sciences for 1777, and in 1778[20]) EULER again showed [28] that

$$1\,000\,009 = 1000^2 + 3^2 = 235^2 + 972^2,$$

whence he inferred that this integer is composite and has the factors 293 and 3413, both primes[21]).

---

[17]) A similar mistake occurs in TROST [23], and was pointed out by L. SCHOENFELD in his review [25] of this book.

[18]) This depends on the fact that λ, and hence λ', are positive.

[19]) See F. RUDIO's footnote to page 403 of [26].

[20]) Although written in 1778, [28] was not published until 1797, for the reasons set out in §5.

[21]) L. E. DICKSON mistakenly writes [29]: 'L. EULER proved that $1000^2 + 3^2$ is a prime since not expressible as a sum of two squares in another way'.

3. The Form $x^2 + y^2$

a) EULER's Proof of GIRARD's Theorem

Let us now briefly examine EULER's proof of GIRARD's theorem. He enters upon this subject for the first time in his *Theoremata circa divisores numerorum in hac forma* $p\,a\,a \pm q\,b\,b$ *contentorum* [30], published in 1751 but probably written between 1744 and 1746[22]). In this article he formulates fifty-nine theorems, which may be separated into two categories. The first type of theorem states that all prime divisors of a certain binary quadratic form must also be contained in certain linear forms. For example, if $(a, b) = 1$ we have '*Numerorum in hac forma* $a\,a + b\,b$ *contentorum divisores primi omnes sunt vel 2 vel huius formae* $4\,m + 1$ *numeri*'[23]).

The second category contains theorems stating that if a prime has a prescribed linear form, then it is also representable by a certain binary quadratic form. For instance, '*Omnes numeri primi huius formae* $4\,m + 1$ *vicissim in hac numerorum formula* $a\,a + b\,b$ *continentur*'; this is GIRARD's theorem. None of the theorems stated in this article are proved, but EULER came very near to proving GIRARD's theorem in his *De numeris qui sunt aggregata duorum quadratorum* [11], written about 1752 and published in 1758; several of its results were already communicated by EULER to GOLDBACH in 1745 [10] and 1747 [31]. This paper contains the following proposition: '*Summa duorum quadratorum inter se primorum dividi nequit per ullum numerum, qui ipse non sit summa duorum quadratorum*', which EULER establishes by a method of descent.

He then reasons as follows: since each divisor of a sum of two relatively prime squares is itself a sum of two squares, GIRARD's theorem would be proved if one could show that every prime $4\,n + 1$ divides some sum of two relatively prime squares. In a paragraph entitled *Tentamen demonstrationis*, he attempts to show that this is indeed the case: let $p = 4\,n + 1$ and $(a, b) = (a, p) = (b, p) = 1$. Then we have

$$a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p},$$

whence $p \mid a^{p-1} - b^{p-1}$, which is the same as $p \mid a^{4n} - b^{4n}$ or $p \mid (a^{2n} - b^{2n})\,(a^{2n} + b^{2n})$. Since p is a prime, it must divide at least one of the two parentheses. It remains to show that, for each prime p of the form $4\,n + 1$, it is possible to choose a and b in such a manner that $p \nmid a^{2n} - b^{2n}$. Then we would have

$$p \mid (a^n)^2 + (b^n)^2 \quad \text{with } (a^n, b^n) = 1,$$

so that p would be a sum of two squares.

This last difficulty was overcome in *Demonstratio theorematis Fermatiani, omnem numerum primum formae* $4\,n + 1$ *esse summam duorum quadratorum* [32], published in 1760. There he actually shows how to find a and b: if $p = 4\,n + 1$, consider the sequence $1, 2^{2n}, 3^{2n}, \ldots, (4\,n)^{2n}$, and construct its first differences: $2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4\,n)^{2n} - (4\,n - 1)^{2n}$. Now at least one of these terms is not divisible by p, for otherwise p would also divide all the second differences, and so on for the third, fourth and

---

[22]) The article appeared in the *Commentarii academiae scientiarum Petropolitanae* for the years 1744–46, which were printed in 1751.

[23]) This theorem already appears in FERMAT's letter [9] of 1640 to ROBERVAL ('Si un nombre est composé de deux quarrés premiers entre eux, je dis qu'il ne peut être divisé par aucun nombre premier moindre de l'unité qu'un multiple du quaternaire').

following differences. But the differences of order $2n$ are constant and all equal to $(2n)!$ Since p is a prime greater than $2n$, it cannot divide $(2n)!$ Hence,

$$p \nmid c^{2n} - (c-1)^{2n} \text{ for some } c,\ 2 \leqslant c \leqslant 4n.$$

Further, $4n+1$ is a prime and $c < 4n+1$, so that $(c-1, 4n+1) = (c, 4n+1) = 1$. Also, $(c, c-1) = 1$ and therefore

$$p \mid c^{2n} + (c-1)^{2n}, \text{ with } (c^n, (c-1)^n) = 1.$$

This is EULER's proof; extremely ingenious, but also rather complicated. He later used similar devices for the forms $x^2 + 2y^2$, which represents primes $8k+1$ and $8k+3$, and $x^2 + 3y^2$, which represents primes $6k+1$.

b) EULER's Converse of FERMAT's Theorem

The second article [11] mentioned above also contains the theorem '*Si p et q sint duo numeri, quorum uterque est summa duorum quadratorum, erit etiam eorum productum p q summa duorum quadratorum*'; EULER proves this with the identity

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 = (ac-bd)^2 + (ad+bc)^2,$$

which was already known to DIOPHANTUS.

If $b > 0$ and $d > 0$ we have $ac + bd > ac - bd$, so that the two representations are identical only if $ac + bd = ad + bc$. But this is the same as $(a-b)(c-d) = 0$, which implies that $a = b$ or $c = d$, and hence that pq is even.

Therefore, the product of two odd integers, each of which is a sum of two squares of natural numbers, is a sum of two squares in at least two different ways.

Now let N be odd and $N = x^2 + y^2$ in only one way, and that with $(x, y) = 1$. We know that all divisors of N are also sums of two squares. If N is greater than 1, it is either prime or composite. But if N were composite, it follows that N would have several representations as a sum of two squares. Therefore N must be a prime. This completes the proof of the following proposition: '*An odd integer greater than 1 which is a sum of two coprime squares is a prime if it has no other representation as a sum of two squares*', which is a correct formulation of EULER's converse to FERMAT's theorem for the form $x^2 + y^2$.

EULER then briefly remarks that certain even integers have only one representation as a sum of two squares, as $10 = 1 + 9$. Some twenty years later he mentioned[24]) that if the two squares are relatively prime, such integers are always the double of a prime. He never set down his proof, but his article contains enough hints to permit us to reconstruct it: let $N = 2N' = x^2 + y^2$ in only one way, and that with $(x, y) = 1$. Since N is even and $(x, y) = 1$, x^2 and y^2 must both be of the form $4k+1$. This indicates that $4 \nmid N$, and hence that N' is odd. Now $2N' = x^2 + y^2$ implies $N' = a^2 + b^2$, where $a = (x-y)/2$ and $b = (x+y)/2$ are integers; conversely, $N' = a^2 + b^2$ implies $N = 2N' = (a-b)^2 + (a+b)^2$, so that there are as many representations of N' as of N as a sum of two squares. Finally, we must have $x = a - b$ and $y = a + b$, whence $(a-b, a+b) = (x, y) = 1$, and therefore $(a, b) = 1$.

Thus N' is odd, uniquely representable as a sum of two squares, and these are relatively prime. Therefore N' must be a prime if $N' > 1$, and we have the following

[24]) See the quotation from EULER's letter [40] to BEGUELIN reproduced in §5.

theorem: *An even integer $N > 2$ which is a sum of two squares in only one way is the double of a prime if these squares are relatively prime.*

In 1769 EULER published the essay *Quomodo numeri praemagni sint explorandi, utrum sint primi necne* [33], where he applied the results which we have just discussed to test several large integers of the form $4k + 1$ for primality. He showed that the representations

$$3\,861\,317 = 961^2 + 1714^2 \quad \text{and} \quad 10\,091\,401 = 1251^2 + 2920^2$$

are unique, and concluded that these two integers are primes.

4. The Forms $x^2 + 2y^2$ and $x^2 + 3y^2$

In 1654 FERMAT affirmed in a letter [34] to PASCAL that all primes of the form $8k + 1$ or $8k + 3$ are (uniquely) representable as $x^2 + 2y^2$ in natural numbers x and y[25]). There is also a letter from FERMAT to KENNELM DIGBY [35] dated 1658 which mentions the same result.

Then in 1756 EULER wrote in his *Specimen de usu observationum in mathesi pura* [17] that he had attempted without success to prove this theorem, and that he was also incapable of proving several similar theorems which he believed to be true[26]), such as '*Omnes numeri primi in aliqua harum formularum contenti* $24n + 1$, $24n + 7$ *simul quoque sunt formae* $6aa + bb$', or '*Omnes numeri primi in alterutra harum formularum contenti* $24n + 5$ *et* $24n + 11$ *simul sunt numeri formae* $3aa + 2bb$'.

It was only in 1774 that EULER published [36] a proof of FERMAT's theorem for $x^2 + 2y^2$. However, in his article [17] of 1756 he established a converse to this theorem by reasoning as for $x^2 + y^2$: if $(x, 2y) = 1$, each divisor of $x^2 + 2y^2$ is of the same form, and since

$$(2a^2 + b^2)(2c^2 + d^2) = (2ac \pm bd)^2 + 2(ad \mp bc)^2,$$

a product of two odd primes of the form $x^2 + 2y^2$ is expressible in this same form in two different ways. He comes to the following conclusion: '*Si numerus formae* $2aa + bb$ *unico modo in hanc formam fuerit resolubilis atque a et b fuerint primi inter se, tum ille numerus certe est primus*'. This is not quite correct, as shown by the example $38 = 6^2 + 2 \cdot 1^2$. What EULER should have written (and what he in fact proved) is '*Si numerus impar formae* $2aa + bb$ *et maior quam unitas unico modo in hanc formam fuerit resolubilis atque a et b fuerint primi inter se, tum ille numerus certe est primus*'.

EULER then conveniently albeit not quite correctly expressed FERMAT's theorem, his own converse and the particular case of the theorem discussed in §2 which concerns the form $x^2 + 2y^2$ as a single proposition: '*Si numerus quicunque in alterutra harum formularum* $8n + 1$ *vel* $8n + 3$ *contentus nullo modo in formam* $2aa + bb$ *resolvi possit, tum non erit primus; at si unico modo in hanc formam possit resolvi, tum erit primus; sin autem plus uno modo haec resolutio succedat, tum pariter non erit primus, sed compositus*'. If we correct it by adding the restriction 'atque *a* et *b* inter se primi sint' after the verb 'resolvi', then the second and third parts of this statement are respec-

---

[25]) 'Tout nombre premier, qui surpasse de 1 ou de 3 un multiple de 8, est composé d'un quarré et du double d'un autre quarré, comme 11, 17, 19, 41, 43, etc.'

[26]) The theory of binary quadratic forms can be applied to show that all of EULER's theorems of this type enunciated in [17] are correct.

tively EULER's converse and a particular case of the theorem of §2, while FERMAT's result follows from the third part and the contraposition of the first.

It is interesting to note that EULER had already applied [37] this criterion for primality in 1750, six years before publishing a proof, to show that 198899 is a prime. He indicated that the representation $198899 = 441^2 + 2 \cdot 47^2$ is unique, and added the incorrect statement *'Certum autem est, si quis numerus unico modo in forma 2 a a + b b contineatur, tum eum esse primum, sin autem duplici vel pluribus modis ad formam 2 a a + b b redigi queat, tum eum esse compositum'*, whence he deduced that 198899 is a prime (which is correct, since 47 and 441 are relatively prime).

In his letters to PASCAL[27]) and DIGBY, FERMAT further asserted that all primes of the form $6k + 1$ are also of the form $x^2 + 3y^2$. EULER proved [38] this in 1760 by essentially the same method as he had used for $x^2 + y^2$, first showing that if $(x, 3y) = 1$, every odd prime divisor of $x^2 + 3y^2$ is again of the same form. Surprisingly, he did not proceed to prove a converse to FERMAT's theorem for this form, as he had done with $x^2 + y^2$ and $x^2 + 2y^2$, but applied this property of the divisors of $x^2 + 3y^2$ to obtain solutions for the Diophantine equation $x^3 + y^3 + z^3 = v^3$.

5. Euler's Discovery of the Idoneal Numbers

We have seen in the preceeding sections how EULER, in considering theorems of FERMAT on the forms $x^2 + dy^2$ for $d = 1, 2$ and 3, noticed that these three forms provide necessary and sufficient conditions for the primality of certain classes of integers.

Then in 1777 BEGUELIN published an article[28]) [13] concerned with the form $x^2 + y^2$. EULER, who had been blind for the past eleven years[29]), had it read to him and in May 1778 sent BEGUELIN a letter [40] in which, after recalling *'...cette belle propriété, que tous les nombres qui ne sont contenus qu'une seule fois dans la formule x x + y y, sont ou premiers, ou doubles de premiers, en prenant les nombres x et y premiers entr'eux'*, he announced the discovery of several other forms with a similar property: *'Or j'ai remarqué que plusieurs autres formules semblables de la forme n x x + y y sont douées de la même propriété, et que, pourvu qu'on donne à la lettre n des valeurs convenables, telles que, par exemple, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13 etc. on en tire toujours des nombres premiers...'*. Although it is not immediately clear what EULER means by 'on en tire toujours des nombres premiers', his idea is that for certain forms $m x^2 + n y^2$ a uniquely representable odd integer greater than one is a prime if $m x$ and $n y$ are relatively prime. The main reason for the vagueness of EULER's statement is a rather unusual acceptation of the word 'prime' in several of his texts; another reason is that he probably considered his meaning sufficiently clear, and trusted that BEGUELIN would provide a more precise enunciation if he found it necessary.

This second explanation is suggested by a more detailed letter [21] on the same subject, written to BEGUELIN on EULER's behalf by his assistant NICOLAS FUSS. There we read *'Il y a des formules de cette forme, par exemple $x^2 + y^2$, $2x^2 + y^2$, $3x^2 + y^2$, $3x^2 + 2y^2$, $5x^2 + y^2$, $5x^2 + 2y^2$ etc. dont il est démontré que tout nombre qui*

[27]) 'Tout nombre premier, qui surpasse de l'unité un multiple de 3, est composé d'un quarré et du triple d'un autre quarré, comme 7, 13, 19, 31, 37, etc.'

[28]) I have already quoted from this article in my introduction.

[29]) An interesting account of EULER's progressive loss of eyesight may be found in FUETER [39].

n'y est contenu que d'une seule façon, est premier, excepté quelques cas qui sont évidens par eux-mêmes...' [30]). (We remark in passing that FUSS exaggerates somewhat in writing 'il est démontré', since EULER could only prove this for the first three forms).

The first reason is indicated by FUSS and also by EULER himself. EULER points out in one of his articles [12] that in considering the form $m\,x^2 + n\,y^2$ he uses the word 'prime' in a more general sense than usual: '*...non solum numeri primi ipsi p, sed etiam 2 p et δ p instar primorum spectari queant, denotante δ divisorem quempiam numeri m n, quibus adeo certis casibus etiam potestates binarii annumerare licet*'; all other natural numbers he calls 'truly composite': '*... omnes reliquos numeros, quos revera compositos vocemus...*'. In a later text [20] he added that squares of primes must also be considered as primes: '*...hinc si p sit numerus primus, in hac investigatione, praeter ipsum numerum p, etiam eius quadratum p p simulque eius duplum 2 p ut primi spectari debebunt; praeterea etiam omnes potestates binarii pro primis spectari debent*'.

FUSS wrote in his letter to BEGUELIN that '*...tout nombre de la forme m x x + y y n'est censé être composé que lorsque outre le facteur de 2 m il contient encore deux ou plusieurs autres facteurs premiers entr'eux*'; for him a number is a 'prime' when it is of the form $t\,p^r$, where $t \mid 2\,m$. However, EULER's class of 'primes' is too small (for instance it does not include integers of the form $2\,\delta\,p$, such as $30 = 5^2 + 5 \cdot 1^2$), while FUSS' may be reduced somewhat; in order to interpret EULER's theorems and definitions correctly, it is sufficient to call an integer 'prime' with respect to the form $m\,x^2 + n\,y^2$ when it is of one of the forms $t\,p$, $t\,p^2$ or $t\,2^\lambda$, where $t \mid 2\,m\,n$.

These two letters contain the substance of a series of five articles which EULER had presented to the St. Petersburg Academy of Sciences in March 1778, some two months before communicating his results to BEGUELIN. They were only published in the years 1801 to 1806, a delay which EULER certainly anticipated since FUSS prefaced his letter to BEGUELIN by explaining that '*Mr. Euler...m'a chargé de vous en faire le petit Extrait que vous trouverez ci-joint, considérant que la publication des Mémoires qu'il a composés depuis peu de tems sur ce sujet, pourroit bien être différée trop longtems*'.

This delay is best explained by the following passage from the eulogy [41] which FUSS pronounced on EULER in 1783: '*M. Euler s'était engagé plus d'une fois envers le Comte Orlof, de fournir à l'Académie assez de mémoires, pour remplir les Actes jusqu'à vingt ans après sa mort; il était homme à tenir sa parole*'.

The most important of these five articles is *De formulis speciei m x x + n y y ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus* [12], which appeared in 1801. In the opening section EULER states the theorem which we have already encountered in §2: '*...constat omnes numeros, qui in tali forma m x x + n y y duplici modo continentur, certe non esse primos, siquidem numeri m et n ambo fuerint positivi...*'. He then raises the following question: since primes have at most one representation, may one affirm that an integer with exactly one representation is a 'prime' in the sense explained above? This is generally untrue, as evinced by the form $7x^2 + 2y^2$ which represents 15 in a single manner and with $(x, y) = 1$. Thus, as EULER writes, '*Ex quo manifesto apparet istam propositionem inversam, quod numeri unico tantum modo in tali formula m x x + n y y contenti etiam sint numeri primi, in genere veritate non esse consentaneam*'. But the fact that this proposition is true for the forms $x^2 + y^2$

[30]) It was EULER's custom to write $m\,x^2 + n\,y^2$ with $m \geqslant n$; the notation $m \leqslant n$ was introduced by GAUSS.

and $x^2 + 2y^2$ suggests the possibility of finding other values of m and n for which the form $m x^2 + n y^2$ has the property that an odd, uniquely representable integer greater than unity is a prime if $(m x, n y) = 1$. Examples of such forms are $3x^2 + y^2$, $3x^2 + 2y^2$, $5x^2 + 3y^2$ and so on, of which EULER writes '*... iam demonstratum, vel saltem observatum est, quod omnes numeri in quapiam earum unico tantum modo contenti etiam certe sint primi, si modo paucissimi casus, per se perspicui, excipiantur; scilicet quando numeri vel sunt pares, vel cum numeris m et n communem divisorem recipiunt. Quin etiam in certis formulis evenire potest, ut adeo potestates binarii unico modo contineantur, veluti numerus 8 in formula 5 x x + 3 y y ... quibus ergo casibus potestates binarii numeris primis aequivalere sunt censendae...*'.

EULER calls such forms 'congruent', and gives the following definition: '*Quando numeri m et n ita sunt comparati, ut omnes numeri unico modo in formula m x x + n y y contenti sint vel ipsi primi vel tantum binarium vel quempiam factorem numerorum m et n involvant, vel etiam certis casibus sint potestates binarii, tales formulas in sequentibus formulas congruas appellabimus; ubi quidem per se perspicuum est ambos numeros x et y inter se primos accipi debere*'.

The latin 'vel' is not exclusive, so that EULER calls a form $m x^2 + n y^2$ congruent (or later idoneal) when every positive integer representable by it in exactly one way, and that with $(x, y) = 1$, is one of p, $2p$, δp, $2\delta p$ (where $\delta \mid m n$) or 2^λ. It must be noted that EULER forgets to mention integers of the form $\delta 2^\lambda$, such as $56 = 7^2 + 7 \cdot 1^2$ or $24 = 3^2 + 15 \cdot 1^2$. Thus, if we exclude even numbers and the integer 1[31]), the only integers uniquely representable and with $(m x, n y) = 1$ are primes. He similarly defines congruent or idoneal numbers: '*Omnes numeros, quos loco producti m n assumere licet, ut formulae m x x + n y y evadant congruae, in posterum appellabimus numeros idoneos vel etiam congruos, dum reliquos omnes incongruos vocabimus*'.

Then EULER lists the sixty-five integers which he knows to be idoneal: this list was also included in his letter to BEGUELIN but contained a misprint (44 instead of 45). These numbers are 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.

At first he had imagined the sequence of idoneals to be infinite, and he registers his surprise at not finding more than sixty-five: '*... hoc phaenomenon maxime mirandum se obtulit, quod multitudo istorum numerorum neutiquam in infinitum excrescat, verum adeo non plures quam 65 huiusmodi numeros complectatur*'.

How did EULER determine whether a given positive integer is idoneal or not? In this article he explains his criterion, which consists in examining all integers of the form $m n + y^2$ and smaller than $4 m n$ (i.e. with $y^2 < 3 m n$). If they are all 'primes', that is to say of one of the forms $t p$, $t p^2$ or $t 2^\lambda$ with $t \mid 2 m n$, then $m n$ is idoneal: '*Si numerus m n ita fuerit comparatus, ut omnes numeri in formula m n + y y contenti et minores quam 4 m n sint vel primi vel primis aequipollentes, tum iste numerus certe erit idoneus et formula m n x x + y y congrua*'.

In his letter to BEGUELIN, EULER had given a slightly different version of his criterion (which he later repeated in another article [20]), by adding the restriction

[31]) EULER apparently forgets the trivial case $1^2 + m n \cdot 0^2 = 1$, but this can be included among the integers of the form 2^λ, with $\lambda = 0$.

that y and $m\,n$ be relatively prime. He illustrated his method for BEGUELIN with $m\,n = 60$: one must test all integers $60 + y^2$ with $y^2 < 180$ and $(y, 60) = 1$. The only natural numbers y satisfying both conditions are $y = 1$, 7, 11 and 13, and since $60 + 1^2 = 61$, $60 + 7^2 = 109$, $60 + 11^2 = 181$ and $60 + 13^2 = 229$ are all primes, EULER concluded that 60 must be an idoneal number. Thus, although he correctly listed sixty-five idoneal numbers, his method for obtaining them is not quite clear and no proof is known for his criterion in either form.

EULER continues his article by formulating ten theorems concerning idoneal numbers and forms; they are all correct, but several of his proofs are insufficient and were later corrected by GRUBE [42], who also proved a criterion very similar to EULER's. These ten theorems are the following:

1) The form $m\,x^2 + n\,y^2$ is congruent if and only if $x^2 + m\,n\,y^2$ is congruent.
2) The only idoneal numbers which are squares are 1, 4, 9, 16, and 25.
3) If an integer $4\,k - 1$ is idoneal, so is $4\,(4\,k - 1)$.
4) If $4\,i$ is idoneal and i is odd, then $16\,i$ is also idoneal.
5) If λ is some integer and $\lambda^2\,i$ is idoneal, then i is also idoneal.
6) When an integer $3\,k - 1$ is idoneal, so is $9\,(3\,k - 1)$.
7) When an integer $4\,k + 1$ $(k \geqslant 1)$ is idoneal, then $4\,(4\,k + 1)$ is not idoneal.
8) If $4\,k + 2$ is idoneal, so is $4\,(4\,k + 2)$.
9) If i is odd and $8\,i$ idoneal, $32\,i$ is not idoneal.
10) If i is odd and $16\,i$ is idoneal, $64\,i$ is not.

EULER was clearly disturbed by the fact that there appears to be no greater idoneal number than 1848; his aim in proving these ten theorems was probably to render this more plausible by showing that when searching for idoneals, certain classes of integers (such as squares greater than 25) may be excluded right away.

He concludes this important essay by indicating that he has examined the positive integers up to 10000 without encountering any new idoneals: '*Quia autem usque ad decies mille nulli alii se mihi obtulerunt, multo magis verisimillimum videtur, post hunc terminum nullos praeterea existere...*'.

The next article to be printed [20] was *De variis modis numeros praegrandes examinandi, utrum sint primi necne*, in 1802. Here EULER repeats his list of idoneal numbers and gives a proof of his criterion; unfortunately this proof contains several important errors. He then determines several arithmetical progressions which contain only a few idoneal numbers. The following example is typical: the only idoneals of the form $3\,k + 2$ are 2, 5, and 8. Indeed, according to EULER's criterion a necessary condition for the integer $3\,k + 2$ to be idoneal is that $3\,(k + 1)$ be of one of the forms $t\,p$, $t\,p^2$ or $t\,2^\lambda$, with $t \mid 2\,(3\,k + 2)$. But it is readily seen that these cases occur only when $k = 0$, 1 or 2, and we know that for these values $3\,k + 2$ is idoneal. The same result can be established with GRUBE's criterion.

Two of the articles submitted by EULER in March 1778 appeared together in 1805 and are devoted to the search for large primes by means of idoneal forms.

In *Facillima methodus plurimos numeros primos praemagnos inveniendi* [43] he uses the idoneal number 232 to find all primes of the form $232\,a^2 + 1$ with $a \leqslant 300$ by excluding all values of a for which $232\,a^2 + 1 = 232\,x^2 + y^2$ with $y > 1$.

In *Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne* [24] EULER shows that 100003 is a prime, since it is uniquely expressible by the

idoneal form $10x^2 + 3y^2$ as $100003 = 10 \cdot 100^2 + 3 \cdot 1^2$. This integer is also (uniquely) representable by the idoneal form $40x^2 + 3y^2$: $100003 = 40 \cdot 50^2 + 3 \cdot 1^2$, and EULER remarks that the larger the idoneal number $\alpha\beta$, the easier it is to see whether there is more than one representation by the form $\alpha x^2 + \beta y^2$: *'Ex posteriori autem huius numeri examine intelligere licet in genere eo maius lucrum expectari posse, quo maiores numeros pro α et β accipere liceat'*; hence his disappointment at not finding any idoneals beyond 1848. Similarly, 1000003 is a prime since it has only one decomposition by the idoneal form $19x^2 + 3y^2$, namely $1000003 = 19 \cdot 8^2 + 3 \cdot 577^2$, and $(19 \cdot 8, 3 \cdot 577) = 1$.

He discovers a very large prime by using the idoneal form $1848x^2 + y^2$: the integer $N = 18518809 = 197^2 + 1848 \cdot 100^2$ is a prime since it has no other representation by this form and $(197, 1848 \cdot 100) = 1$.

In a final section to this article, EULER gives a list of the 22 primes of the form $1848a^2 + 197^2$ in the range $1 \leqslant a \leqslant 100$.

EULER's last article on idoneal numbers appeared only in 1806, twenty-three years after his death. It is entitled *Illustratio paradoxi circa progressionem numerorum idoneorum sive congruorum* [44]; in it he again attempts to give some plausible reasons for the finite number of idoneals.

6. The Idoneal Numbers in Mathematical Literature

As we have noticed in examining EULER's various papers on binary quadratic forms and idoneal numbers, his definitions and the formulation of his theorems vary slightly from one article to the next. This is probably due to the blindness from which he suffered during the last sixteen years of his life. His proofs are not all correct, and indeed the greater part of his discovery is presented without proof, since the only forms which he could show to be idoneal were $x^2 + y^2$, $x^2 + 2y^2$ and $x^2 + 3y^2$ [32]).

Erroneous versions of EULER's theorems abound in mathematical literature. There are roughly two types of mistake, the one deriving from his unusual meaning for the word 'prime', and the other resembling the error of syntax in his article [11] of 1758 devoted to the form $x^2 + y^2$. However, all sorts of combinations of these and other errors can be found by a diligent searcher. For instance, many authors seem to believe that EULER's articles contain proofs for the idoneity of all his sixty-five numbers.

One of the earliest examples of the first sort of mistake appears in the summary preceding EULER's last article [44] concerned with idoneal numbers; mentioning his previous *Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne* [24], the author of this résumé writes *'Ce mémoire renferme une table de tous les nombres $\alpha\beta$ tels que tous les nombres contenus d'une seule manière dans la forme $\alpha x^2 + \beta y^2$ soyent premiers'*. This not only omits the important condition $(\alpha x, \beta y) = 1$, but also neglects the particular meaning which must be read into the expression 'nombre premier' in several of EULER's texts. The same error occurs in [23] and in texts [45] through [47].

[32]) Although EULER did not mention the fact, the idoneity of $x^2 + y^2$ implies that of $x^2 + 4y^2$. EULER's methods can also be applied to the form $x^2 + 7y^2$, which has the property that if $(x, 7y) = 1$, all its odd divisors are expressible in the same manner. To prove the idoneity of the sixty remaining numbers requires the theory of binary quadratic forms.

A. FERRIER committed an error of the second sort when he wrote [48] that '*Pour qu'un nombre* $4n + 1$, *non carré, soit premier, il faut et il suffit qu'il soit, et d'une seule manière, somme de deux carrés premiers entre eux*' [33]).

L. E. DICKSON gave a rather confused account in Volume I of his *History of the Theory of Numbers* [29] and in his *Introduction to the Theory of Numbers* ([50] or [51]): '*In 1778 Euler found that these 65 idoneal numbers D are the only ones* < 10000 *having the property that if* $a\,b = D$, *every number represented by* $f = a\,x^2 + b\,y^2$ (*with* $a\,x$ *prime to* $b\,y$) *is a prime, the square of a prime, the double of a prime, or a power of two. If a number is represented by f in a single way, it is a prime*'.

This is quite wrong; the qualification 'in a single way' should also be included in the first sentence, while the second sentence should read 'If an *odd* number *greater than one*...'. Finally, it can be shown [34]) that if $a\,b = D$, the only idoneal form $a\,x^2 + b\,y^2$ which represents squares of primes is $x^2 + D\,y^2$, so that if p is a prime and p^2 is representable as $x^2 + D\,y^2$ with $x > 0$ and $y > 0$, this representation is unique only if we exclude the case $y = 0$. Otherwise we may omit the phrase 'the square of a prime'. A corrected version of DICKSON's statement would accordingly be: *In 1778 Euler found that these 65 idoneal numbers D are the only ones* < 10000 *having the property that if* $a\,b = D$, *every number represented in a single way by* $a\,x^2 + b\,y^2$ *in nonnegative integers x and y, and that with* $(a\,x, b\,y) = 1$, *is a prime, the double of a prime or a power of two. Thus, if the number is odd and greater than one, it is a prime.*

A. AUBRY gave an interpretation [52] which betrays a complete incomprehension of EULER's results: '...*Euler parle pour la première fois de ses fameux numeri idonei, qu'il caractérise par cette propriété qu'un nombre premier quelconque ne peut être représenté que d'une seule manière par la forme* $x^2 + k\,y^2$, *si k est un numerus idoneus*'; this property is the one expressed by EULER's theorem of §2, and in no way characterizes idoneal numbers.

Many other references to false interpretations of EULER's discovery are mentioned in MELNIKOV's article [19].

In concluding, we observe that EULER's results find their natural setting in GAUSS' theory of binary quadratic forms (*Disquisitiones Arithmeticae*, 1801). In the language of this theory, an idoneal number is a positive integer D such that for the discriminant $-4D$ there is a single class of forms in each genus. By applying this theory, GRUBE [42] was able to prove almost all of EULER's propositions. Only one of his conjectures concerning idoneal numbers has never been verified: although S. CHOWLA proved [53] that there are only finitely many, it is not yet known whether 1848 is the largest. Results of J. D. SWIFT [54] indicate that there is none between 1848 and 2500000, while W. E. BRIGGS and S. CHOWLA have shown [55] that there is at most one idoneal number beyond 10^{65}.

J. STEINIG, Zürich

BIBLIOGRAPHY

[1] *Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Nunc primum Graece et Latine editi, atque absolutissimis commentariis illustrati. Auctore Claudio Gaspare Bacheto. Lutetiae Parisiorum. Sumptibus Hieronymi Drouart,*

[33]) In [49] W. SIERPIŃSKI corrected this by proving that an odd integer is the sum of two squares of relatively prime positive integers in a single manner if and only if it is of the form p^k, where k is a natural number and $p \equiv 1 \pmod 4$, a prime. Similar results can be obtained for all the other idoneal forms.

[34]) Briefly, this follows from the fact that if D is idoneal, $x^2 + Dy^2$ is the only reduced, positive, primitive form of discriminant $-4D$ all of whose characters are equal to $+1$.

1621, particularly pages 301–302. (There is another edition, *sumptibus Sebastiani Cramoisy*, of the same year, which differs from the above only by the illustration of the title-page.)

[2] *L'Arithmetique de Simon Stevin de Bruges, Reueuë, corrigee et augmentee de plusieurs traictez et annotations par Albert Girard Samielois Mathematicien. A Leide, de l'Imprimerie des Elzeviers, 1625*, in particular page 622.

[3] *Les Œuvres Mathématiques de Simon Stevin de Bruges. Ou sont insérées les Memoires Mathématiques, Esquelles s'est exercé le Tres-haut et Tres-illustre Prince Maurice de Nassau, Prince d'Aurenge, Gouverneur des Provinces des Païs-bas unis, General par Mer et par Terre, etc. Le tout reveu, corrigé et augmenté par Albert Girard Samielois, Mathematicien. A Leyde, chez Bonaventure et Abraham Elsevier, Imprimeurs ordinaires de l'Université, 1634*, in particular page 156.

[4] *Œuvres de Fermat*, Tome II (Gauthier-Villars, Paris, 1894), 221–226 (FERMAT à FRENICLE, 15 juin 1641).

[5] *Œuvres de Fermat*, Tome II, 212–217 (FERMAT à MERSENNE, 25 décembre 1640).

[6] *Œuvres de Fermat*, Tome I (Gauthier-Villars, Paris, 1891), 293–297 (Observation VII sur Diophante).

[7] *Œuvres de Fermat*, Tome II, 226–232 (FRENICLE à FERMAT, 2 août 1641).

[8] *Œuvres de Fermat*, Tome II, 431–436 (FERMAT à CARCAVI, août 1659).

[9] *Œuvres de Fermat*, Tome II, 202–205 (FERMAT à ROBERVAL, août 1640).

[10] P. H. FUSS, *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIIIe siècle* (St. Pétersbourg, 1843), Tome I, 311–314 (L. EULER to CHR. GOLDBACH, 16 February 1745).

[11] *De numeris qui sunt aggregata duorum quadratorum*, L. EULERI Opera Omnia, Series I, Vol. 2 (= Commentationes Arithmeticae I), 295–327.

[12] *De formulis speciei m x x + n y y ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus*, L. EULERI Opera Omnia, Series I, Vol. 4 (= Comm. Arith. III), 269–289.

[13] N. BEGUELIN, *Solution particulière du problème sur les nombres premiers*, Nouveaux Mémoires de l'académie Royale des Sciences et Belles-Lettres de Berlin pour l'année 1775 (published in 1777), 300–322.

[14] L. EULERI Opera Omnia, Series I, Vol. 2 (= Comm. Arith. I), *Vorwort des Herausgebers*, particularly page XXV.

[15] L. EULERI Opera Omnia, Series I, Vol. 3 (= Comm. Arith. II), *Vorwort des Herausgebers*, in particular page IX.

[16] L. EULERI Opera Omnia, Series I, Vol. 4 (= Comm. Arith. III), *Vorwort des Herausgebers*, particularly page XV.

[17] L. EULERI Opera Omnia, Series I, Vol. 2, 459–492.

[18] G. PÓLYA, *Mathematics and Plausible Reasoning*, Vol. I (*Induction and Analogy in Mathematics*), Princeton University Press 1954, on page 3.

[19] I. G. MELNIKOV, *La découverte des «nombres commodes» par L. Euler* (in Russian), Istor.-Mat. Issled. *13*, 187–216 (1960).

[20] *De variis modis numeros praegrandes examinandi utrum sint primi necne*, L. EULERI Opera Omnia, Series I, Vol. 4, 303–328.

[21] *Extrait d'une lettre de M. Fuss à M. Beguelin, écrite de Pétersbourg le 19/30 juin 1778*[35]), L. EULERI Opera Omnia, Series I, Vol. 3, 421–428 (also in Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin pour l'année 1776, 340–346).

[22] T. NAGELL, *Introduction to Number Theory*, John Wiley & Sons, Inc. (New York); Almqvist & Winksell (Stockholm), 1951; in particular page 100.

[23] E. TROST, *Primzahlen*, Verlag Birkhäuser, Basel und Stuttgart, 1953, particularly pages 28 to 33.

[24] *Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne*, L. EULERI Opera Omnia, Series I, Vol. 4, 360–394.

[35]) The first date is that of the julian calendar (in use in Russia until 1918) and the second, that of the gregorian calendar.

[25] LOWELL SCHOENFELD, Bull. Amer. Math. Soc. *62*, 54–57 (1956).
[26] *De tabula numerorum primorum usque ad millionem et ultra continuanda in qua simul omnium numerorum non primorum minimi divisores exprimantur*, L. EULERI Opera Omnia, Series I, Vol. 3, 359–403.
[27] L. EULERI Opera Omnia, Series I, Vol. 3, 404.
[28] *Utrum hic numerus 1000009 sit primus necne inquiritur*, L. EULERI Opera Omnia, Series I, Vol. 4, 245–254.
[29] L. E. DICKSON, *History of the Theory of Numbers*, Vol. I, Washington, 1919 (reprinted by Chelsea, New York, 1952), page 361.
[30] L. EULERI Opera Omnia, Series I, Vol. 2, 194–222 (particularly pages 194 and 195).
[31] L. EULER, letter to CHR. GOLDBACH of 6 May 1747 (contained in the same vol. as [10]).
[32] *Demonstratio theorematis Fermatiani, omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum*, L. EULERI Opera Omnia, Series I, Vol. 2, 328–337.
[33] L. EULERI Opera Omnia, Series I, Vol. 3, 112–130.
[34] *Œuvres de Fermat*, Tome II, 310–314 (FERMAT à PASCAL, 25 septembre 1654).
[35] *Œuvres de Fermat*, Tome III (Gauthier-Villars, Paris, 1896), 314–319 (FERMAT à DIGBY, juin 1658). This letter is reproduced in the original Latin in *Œuvres de Fermat*, Tome II, 402–408.
[36] *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, L. EULERI Opera Omnia, Series I, Vol. 3, 240–281.
[37] *De numeris amicabilibus*, L. EULERI Opera Omnia, Series I, Vol. 2, 86–162, particularly page 115.
[38] *Supplementum quorumdam theorematum arithmeticorum quae in nonnullis demonstrationibus supponuntur*, L. EULERI Opera Omnia, Series I, Vol. 2, 556–575.
[39] R. FUETER, *Über eine Eulersche Beweismethode in der Zahlentheorie*, Festschrift Prof. Dr. Alfred Vogt, Basel 1939, 103–111.
[40] *Extrait d'une lettre de M. Euler à M. Beguelin, en mai 1778*, L. EULERI Opera Omnia, Series I, Vol. 3, 418–420 (also with [21] in Nouveaux Mémoires ... pour l'année 1776, 337–339).
[41] NICOLAS FUSS, *Eloge de Monsieur Léonard Euler, lu à l'Académie Impériale des Sciences, dans son Assemblée du 23 octobre 1783*, St. Pétersbourg, 1783.
[42] F. GRUBE, *Über einige Eulersche Sätze aus der Theorie der quadratischen Formen*, Zeitschrift Math. Phys. *19*, 492–519 (1874).
[43] L. EULERI Opera Omnia, Series I, Vol. 4, 352–359.
[44] L. EULERI Opera Omnia, Series I, Vol. 4, 395–398.
[45] E. BOREL, *Les nombres premiers*, Presses Universitaires de France (Collection «Que sais-je ?»), Paris 1958, particularly page 34.
[46] G. PALAMÀ, *Numeri primi e composti contenuti nella forma* $1848\,x^2 + y^2$ *dell'intervallo* $11000000 - 11100000$, Boll. Un. Mat. Ital., Serie III, *7*, 168–171 (1952).
[47] *Mathematisches Wörterbuch*, Akademie-Verlag GmbH (Berlin) und B. G. Teubner Verlagsgesellschaft (Stuttgart), 1961.
[48] A. FERRIER, *Les nombres premiers*, Librairie Vuibert, Paris (1947).
[49] W. SIERPIŃSKI, *Sur les nombres impairs admettant une seule décomposition en une somme de deux carrés de nombres naturels premiers entre eux*, El. Math. *16*, 27–30 (1961).
[50] L. E. DICKSON, *Introduction to the Theory of Numbers*, Chicago University Press, 1929 – also as Dover reprint S342, 1957; particularly page 89.
[51] German translation of [50] by E. BODEWIG: *Einführung in die Zahlentheorie*, B. G. Teubner (Leipzig und Berlin), 1931.
[52] A. AUBRY, *L'œuvre arithmétique d'Euler*, L'enseignement math. *11* (1909), particularly page 346.
[53] S. CHOWLA, *An Extension of Heilbronn's Class-Number Theorem*, Quart. J. Math. Oxf. Ser. *5*, 304–307 (1934).
[54] J. D. SWIFT, *Note on Discriminants of Binary Quadratic Forms With a Single Class in Each Genus*, Bull. Amer. Math. Soc. *54*, 560–561 (1948).
[55] W. E. BRIGGS and S. CHOWLA, *On Discriminants of Binary Quadratic Forms With a Single Class in Each Genus*, Canadian J. Math. *6*, 463–470 (1954).