

The Hermite–Serret Algorithm and $12^2 + 33^2$

Alf van der Poorten

Abstract. Musing on the cute observation that $12^2 + 33^2 = 1233$ led me to remind myself of well known techniques for writing a given integer n as a sum of two squares, given (or having already found) a square root z , say, of -1 modulo n . In brief, one applies the Euclidean algorithm to n and z , stopping at the first pair x and y of remainders that are smaller than \sqrt{n} . Then, lo! it happens that $n = x^2 + y^2$. Naturally, square roots of -1 properly different from z lead to different representations of n as sum of two squares. Obviously, so simple an algorithm must have an elegant and near trivial explanation, yet the literature contains some rather turgid proofs. I briefly point out that, in general, a representation of n by a reduced definite binary quadratic form can readily be found by symmetric decomposition of a symmetric matrix, a process well known as *reduction*; and that this does give insight into why certain remainders in the Euclidean algorithm applied to n and some square root mod n yield the representation. My story is for our mild amusement, and provides a nice and easily comprehended story to tell our students.

1. 1233 and All That

The pleasing observation that $1233 = 12^2 + 33^2$ apparently emanates from Hendrik Lenstra. It came to me by way of the text [1]. Happily, it is more than just a numerical curiosity, being the augur of infinitely many such cute decompositions.

Lemma 1.1. *The identity $a^2 + b^2 = 10^u a + b$ is equivalent to the representation $10^{2u} + 1 = (10^u - 2a)^2 + (2b - 1)^2$.*

Proof. Multiplying $a^2 + b^2 - 10^u a - b = 0$ by 4 and completing squares readily yields $(10^{2u} - 4 \cdot 10^u a + 4a^2) + (4b^2 - 4b + 1) = 10^{2u} + 1$. \square

It's enough, therefore, to look for representations of $10^{2u} + 1$ as a sum $x^2 + y^2$ with $x = 10^u - 2a$ even, and $y = 2b - 1$ odd.

Example 1.2. Because 101 is prime, its only representation as sum of squares is $10^2 + 1^2$, yielding $a = 0$ and $b = 1$ and so the boring decomposition $1 = 1^2$. However, $10^4 + 1 = 73 \cdot 137$ and so has a second potentially interesting decomposition given by $(8^2 + 3^2)(4^2 + 11^2) = (8 \cdot 11 - 3 \cdot 4)^2 + (8 \cdot 4 + 3 \cdot 11)^2 = 76^2 + 65^2$. That is

$a = 12$ and $b = 33$, as in our motivating example. Similarly, $10^6 + 1 = 101 \cdot 9901$ yields the possibly interesting decomposition $10^6 + 1 = 980^2 + 199^2$. But that is $a = 10$ and $b = 100$ and provides only the quite dull $10100 = 10^2 + 100^2$.

It is easy to see that there are plenty of u so that $10^{2u} + 1$ has lots of prime factors, but it's not entirely obvious that seemingly interesting sums of squares yield amusing decompositions. Indeed, the example $10^{10} + 1 = 101 \cdot 3541 \cdot 27961$ has an encouraging three prime factors but the $4 - 1 = 3$ possibly amusing decompositions are $2584043776 = 25840^2 + 43776^2$, $1765038125 = 17650^2 + 38125^2$, which are pretty interesting, but also the unacceptable $99009901 = 990^2 + 09901^2$. In all, the claim there are infinitely many 'cute' decompositions is not totally convincing.

Example 1.3. The following brief selection¹ possibly is more compelling

$$\begin{aligned} 116788^2 + 321168^2 &= 116788321168 & 768180^2 + 2663025^2 &= 7681802663025 \\ 1675455088^2 + 3734621953^2 &= 16754550883734621953. \end{aligned}$$

I take it as known that 2, and each prime p congruent to 1 modulo 4 has an essentially unique presentation as a sum of two positive integer squares. Then the identity $(a^2 + b^2)(c^2 + d^2) = (ad \pm bc)^2 + (ac \mp bd)^2$ readily shows by induction that a product of s distinct odd primes $\equiv 1$ modulo 4 has 2^{s-1} essentially different representations as a sum of squares.

However, we had best first discuss just how one finds the decomposition of an integer as a sum of two squares.

2. Representation of Integers in the Form $ax^2 + 2bxy + cy^2$

It seems more convincing to discuss the more general problem of representation by arbitrary quadratic forms of negative discriminant. The matter of representation of integers by binary quadratic forms is one of the oldest problems of number theory. Of course, the real issue is to explain just which integers are represented, and why, but it certainly is also of interest actually to find representations.

2.1. Symmetric Decomposition.

My following remarks are a minor variant on known algorithms for determining representations by definite forms. The idea is conveniently illustrated by a toy example.

Consider the problem of finding nonnegative integers x and y so that

$$173 = 2x^2 + 3y^2.$$

We first solve the congruence $z^2 \equiv -3 \cdot 2 \pmod{173}$. Indeed $72^2 = 30 \cdot 173 - 6$. Accordingly we study the matrix

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}.$$

¹From a complete list up to $u = 10$ for which I thank Michael Volpato.

Here I have effected the decomposition by the Euclidean algorithm *on the rows* of M , with the details given by the array

$$\begin{array}{r} 173 \quad 72 \\ 2 \quad 72 \quad 30 \\ 2 \quad 29 \quad 12 \\ 2 \quad 14 \quad 6 \\ 14 \quad 1 \quad 0 \\ \quad 0 \quad 6 \end{array}$$

Dually, we might have performed the Euclidean algorithm *on the columns* of M , obtaining

$$\begin{array}{r} 2 \quad 2 \quad 2 \quad 14 \\ 173 \quad 72 \quad 29 \quad 14 \quad 1 \quad 0 \\ 72 \quad 30 \quad 12 \quad 6 \quad 0 \quad 6 \end{array}$$

This dual decomposition is particularly friendly to left-handed mathematicians. But it yields the transpose of the previous decomposition, namely

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}.$$

Something is clearly wrong here. M is a symmetric matrix, yet our methods of decomposition destroy that symmetry. So we try again, working symmetrically both by row and by column. Our working begins with the two steps, one *row operation*, then one *column operation*,

$$\begin{array}{r} 2 \\ 173 \quad 72 \\ 2 \quad 72 \quad 30 \quad 12 \\ \quad 29 \quad 12 \quad 5 \end{array}$$

reporting that

$$M = \begin{pmatrix} 173 & 72 \\ 72 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 30 & 12 \\ 12 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ultimately, we have

$$\begin{array}{r} 2 \quad 2 \quad 1 \\ 173 \quad 72 \\ 2 \quad 72 \quad 30 \quad 12 \\ 2 \quad 29 \quad 12 \quad 5 \quad 2 \\ 1 \quad \quad 6 \quad 2 \quad 2 \quad 0 \\ \quad \quad \quad 3 \quad 0 \quad 3 \end{array}$$

4. Remarks

The educated reader will already have recognised that ‘symmetric decomposition’ is no more than reduction of a quadratic form. Set (a, b, c) to denote the form $aX^2 + 2bXY + cY^2$. Then the opening example of §2 amounts to the reduction

$$(173, 72, 30) \xrightarrow{2} (30, 12, 5) \xrightarrow{2} (5, 2, 2) \xrightarrow{1} (2, 0, 3).$$

Note that these forms correspond precisely to the residual matrices left after each double step of the symmetric decomposition. Further, we have kept track of the translations involved and can thus readily compute

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 3 & 2 \end{pmatrix},$$

obtaining $173 = 2 \cdot 7^2 + 3 \cdot 5^2$. In all, the algorithm I point to of course is well known and is reasonably efficient. By the way, although I was not obliged to say anything at all about representation by indefinite forms, the present reformulation of symmetric decomposition in terms of reduction of quadratic forms makes it clear how one will proceed in that case. A version of §2 appears as a section in [7].

4.1. Cornacchia’s Algorithm

Detailed proof of the algorithm is given variously in [4] and [6]. Let me briefly hint why my remarks can lead to a proof of a generalised result. First, suppose that $n/z = [a_0, a_1, \dots, a_s]$ with $\gcd(n, z) = 1$. Then it’s not dead obvious, but not too difficult to see, that the remainders appearing in the Euclidean algorithm applied to n and z are the numerators of the quantities $[a_i, \dots, a_s]$. Now let me illustrate what the Principal Remark says on an example from [6]. With $n = 1938758870912466947228$, take $z = 1838519813993681402789$ so that $z^2 \equiv -4755 = -15 \cdot 317 \pmod{n}$. Here $k = 1743463386375897354317$, and my symmetric decomposition yields $\begin{pmatrix} n & z \\ z & k \end{pmatrix} = N^t \begin{pmatrix} 15 & 0 \\ 0 & 317 \end{pmatrix} N$, where the first half of the continued fraction expansion of n/z is

$$[1, 18, 2, 1, 13, 5, 3, 1, 5, 1, 1, 6, 2, 40, 1, 91] \longleftrightarrow N^t = \begin{pmatrix} 11354668973 & 123452677 \\ 10767601996 & 117069841 \end{pmatrix}$$

and provides the transpose of N . By the Principal Remark we have

$$n = 15 \cdot 11354668973^2 + 317 \cdot 123452677^2.$$

But, seemingly, we’ve done that without even looking at the second half of the expansion and meeting remainders from the Euclidean algorithm on n and z .

However, first note that if the matrix N^t corresponds to a certain continued fraction expansion, then N corresponds to that same expansion in reverse order. Set $M = \begin{pmatrix} 15 & 0 \\ 0 & 317 \end{pmatrix}$, and note that, of course, MN sort of corresponds to the second half of the continued fraction expansion of n/z . Thus N^tM , recall that M is symmetric, similarly corresponds to that second half in reverse order. Precisely when M is of the shape $\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$, which is the case of representations $x^2 + my^2$ with which Cornacchia’s algorithm concerns itself in the first instance, one finds that

the entry in the $(1, 1)$ position of $N^t M$, which is a remainder, coincides with that entry of N^t , to wit x . In our example we get $15x$ as that entry in $N^t M$.

There's a number of not altogether trivial details I gloss over, signalled in part by such words as 'half' and 'sort of', or hidden by particularities of the example. So these remarks just hint at an explanation, with a justification for Cornacchia's algorithm *inter alia* requiring a considerably more detailed introduction to the correspondence between continued fraction expansions and two by two matrices.

5. Acknowledgements

I am grateful to Frits Beukers for treating me as an honorary Dutchman and sending me [1], among other things provoking the remarks reported here. I also acknowledge with thanks useful advice from the referee inducing me to sketch a relation between my first principles remarks and methods directly relying on the Euclidean algorithm.

This work was supported in part by a grant from the Australian Research Council.

References

- [1] Frits Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, Utrecht, 1999.
- [2] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993, xii+534 pp.
- [3] Michel Dekking, Michel Mendès France and Alfred J. van der Poorten, *FOLDS! II: Symmetry disturbed*, The Mathematical Intelligencer **4** (1982), 173–181.
- [4] Kenneth Hardy, Joseph B. Muskat and Kenneth S. Williams, *A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v* , Math. Comp. **55** (1990), 327–343.
- [5] Kenneth Hardy, Joseph B. Muskat and Kenneth S. Williams, *Solving $n = au^2 + buv + cv^2$ using the Euclidean algorithm*, Util. Math. **38** (1990), 225–236.
- [6] Abderrahmane Nitaj, *L'algorithmme de Cornacchia*, Exposition. Math. **13** (1995), 358–365.
- [7] A. J. van der Poorten, *On Number Theory and Kustaa Inkeri*, to appear in Proc. Turku Symposium on Number Theory in Memory of Kustaa Inkeri (Turku, May 31–June 4, 1999), Matti Jutila and Tauno Metsänkylä eds., Walter de Gruyter, Berlin 2000, 13pp.
- [8] H. J. S. Smith, *De compositione numerorum primorum formae $4\lambda + 1$ ex duobus quadratis*, J. für Math. (Crelle), **50** (1855), 91–92.

ceNTRe for Number Theory Research
 Macquarie University, Sydney,
 NSW 2109, Australia
E-mail address: alf@math.mq.edu.au (Alf van der Poorten)