

A CURIOUS CUBIC IDENTITY AND SELF-SIMILAR SUMS OF SQUARES

ALF VAN DER POORTEN, KURT THOMSEN, AND MARK WIEBE

To Richard K. Guy on his 90th birthday

INTRODUCTORY QUOTE. “There are just four numbers (after 1) which are the sums of the cubes of their digits, viz. $153 = 1^3 + 5^3 + 3^3$, $370 = 3^3 + 7^3 + 0^3$, $371 = 3^3 + 7^3 + 1^3$, and $407 = 4^3 + 0^3 + 7^3$.

This is an odd fact, very suitable for puzzle columns and likely to amuse amateurs, but there is nothing in it which appeals much to a mathematician. The proof is neither difficult nor interesting—merely a little tiresome. The theorem is not serious; and it is plain that one reason (though perhaps not the most important) is the extreme speciality of both the enunciation and the proof, which is not capable of any significant generalization.”

see G. H. Hardy, *A Mathematician's Apology*

Hendrik Lenstra's cute observation that $12^2 + 33^2 = 1233$, is readily generalised. If $a^2 + b^2 = 10^k a + b$ then $10^{2k} + 1 = (2a - 10^k)^2 + (2b - 1)^2$, so to discover the example it suffices to decompose $10^4 + 1$ as the sum of two squares. Noting that $10001 = 137 \cdot 73$ one readily finds the trivial $10^4 + 1 = 100^2 + 1^2$, and $10^4 + 1 = 76^2 + 33^2$. The latter yields the opening remark, and also $88^2 + 33^2 = 8833$. Quite as readily, see [3], one finds decompositions of all lengths $2k$, helped by the fact that if n is a divisor of $10^{2k} + 1$, then $10^k \equiv -1 \pmod{n}$. A striking special case is the sequence of integers $(10^{8(4u+1)} + 1)/17$, $u = 0, 1, \dots$. Thus

$$588^2 + 2353^2 = 5882353 = (10^8 + 1)/17,$$

$$\begin{aligned} &5\ 882\ 352\ 941\ 176\ 470\ 588^2 + 23\ 529\ 411\ 764\ 705\ 882\ 353^2 \\ &= 588\ 235\ 294\ 117\ 647\ 058\ 823\ 529\ 411\ 764\ 705\ 882\ 353 = (10^{24} + 1)/17, \end{aligned}$$

and so on. By the way

$$58823529412^2 + 235294117648^2 = 58823529412235294117648$$

commences a not quite so well behaved sequence for $k = 12, 28, \dots$.

Corresponding decompositions in cubes are far less natural, so one expects the example $1^3 + 5^3 + 3^3 = 153$ to be no more than an isolated curiosity. Surprisingly, however, also

$$\begin{aligned} 16^3 + 50^3 + 33^3 &= 165033 \\ 166^3 + 500^3 + 333^3 &= 166500333 \\ 1666^3 + 5000^3 + 3333^3 &= 166650003333 \end{aligned}$$

⋮

This is so surprising that it must be trivial. Indeed, both sides of

$$a^3 + b^3 + c^3 = 10^{2k}a + 10^k b + c \quad k = 1, 2, \dots,$$

are $36a^3 + 66a^2 + 42a + 9$, whenever $10^k = 1 + a + b + c$, with $b = 3a + 2$, and $c = 2a + 1$.

We are indebted to Gery Myerson for several helpful remarks, particularly for reminding us that we should immediately have recognised the number 153.

1. INTRODUCTION

I report here on work done some years ago with Kurt Thomsen and Mark Wiebe, at the time undergraduate students at the University of Manitoba. I had promised that I would convert that work into possibly publishable form, but the priority I gave my commitment turned out to be too low. Happily, the topic promised a suitable talk for a celebration of Richard Guy's 90th birthday at the Summer Meeting of the Canadian Mathematical Society, 2006 in Calgary. I narrate that talk below.

AlfvdP

The visit by Kurt and Mark to the ceNTRe for Number Theory Research, then at Macquarie University, Sydney, was in part supported by an Australian Research Council international research exchange grant.

2. A VERY NICE OBSERVATION

In his fine text *Getaltheorie voor beginners*, Frits Beukers quotes Hendrik Lenstra, at §10.4 *Kunstjes met decimalen*, as making the 'heel fraaie observatie'

$$12^2 + 33^2 = 1233$$

and remarks that such examples may be generated systematically, citing

$$1826147812^2 + 3863503888^2 = 18261478123863503888.$$

as 'een indrukwekkend voorbeeld'.

I had received the book direct from the author as 'one of the few foreigners who speak Dutch and may be able to appreciate some elementary number theory' and was indeed appreciative, both of Hendrik's very nice observation and the impressive example.

Frits points out in the text that of course

$$a^2 + b^2 = 10^k a + b$$

entails

$$(10^{2k} - 4 \cdot 10^k a + 4a^2) + (4b^2 - 4b + 1) = (10^k - 2a)^2 + (2b - 1)^2 = 10^{2k} + 1.$$

So finding examples is a matter of representing $10^{2k} + 1$ as a sum of two other squares, with the even other square providing a and the odd one b . We all know, in any case I knew, that finding such representations is a matter of factorising $10^{2k} + 1$, representing the factors as a sum of two squares, and hoping that the subtlety of consequent representations of $10^{2k} + 1$ is not spoiled by trailing zeros in a or b , let alone leading zeros in b (a and b , have to be of the same, k digits, length).

Specifically, for $k = 2$ it is easy to see that

$$105^2 - 2^{10} = 11025 - 1024 = 10^4 + 1 = 73 \cdot 137,$$

readily providing

$$10^4 + 1 = (10^2 - 2a)^2 + (2b - 1)^2 = 76^2 + 65^2$$

by way of $73 = 8^2 + 3^2$ and $137 = 4^2 + 11^2$. Thus we know that $a = 12$ and $b = 33$ must give $12^2 + 33^2 = 1233$ (all this, without our having to be able to compute $33^2 = 2500 - 1700 + 17^2 = 1089$).

I was provoked [3] to compute other interesting examples, not so much concentrating on the issue of factorising $10^{2k} + 1$, but rather on that of representing its factors as sums of two squares; and ‘composing’ such sums: here I recalled that

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

details composition of the quadratic form $X^2 + Y^2$ with itself.

In very brief, one uses: if -1 is a square modulo f , say $m^2 = -1 \pmod f$, then the Euclidean algorithm applied to m and f efficiently writes f as a sum of two squares. The key notions are Cornacchia’s algorithm [2] (in this special case, Hermite-Serret), or reduction of a definite quadratic form. If f divides $10^{2k} + 1$, then $m = 10^k$ will do. For example

$$5\,882\,353 = 588 \cdot 10\,000 + 2\,353$$

$$10\,000 = 4 \cdot 2\,353 + 588$$

⋮

and we have already obtained the first two remainders less than $\sqrt{5882353}$.

It turned out not to be entirely evident 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 $2^{3-1} - 1 = 3$ possibly amusing decompositions are

$$2584043776 = 25840^2 + 43776^2, \quad 1765038125 = 17650^2 + 38125^2,$$

which are pretty interesting, but also the unacceptable $99009901 = 990^2 + 09901^2$. In all, it is not immediately completely compelling that there are infinitely many delightful decompositions.

2.1. The curious case 17. However, I did feel a *frisson* of excitement on noticing that $10^8 + 1 = 17 \cdot 5882353$ and, without *any* fuss,

$$5882353 = 588^2 + 2353^2.$$

The numbers $(10^{8(2u+1)} + 1)/17$ all have analogous *automatic* decompositions.

2.2. An embarrassment. The preceding remarks were the sort of thing that I showed Kurt Thomsen and Mark Wiebe back in 2001. They immediately embarrassed me by remarking that, of course, also $88^2 + 33^2 = 8833$.

I had failed to see actively that, if $a + a' = 10^k$,

$$a^2 + b^2 = 10^k a + b \quad \text{immediately entails} \quad a'^2 + b^2 = 10^k a' + b.$$

Notwithstanding my protests, Kurt and Mark then proceeded to play with cubic identities, silencing me by making the useful remark already quoted in my opening summary. We then drifted on to quite different topics and I only became aware that Kurt and Mark had politely returned to the subtle sums of squares when they reported on their work at the end of their visit.

Kurt and Mark avoid representing integers as sums of squares and the like. They favour a viewpoint closer to their cubic diversion. By the way, further results for cubes seem to call for merely tiresome activity.

3. SEQUENCES OF SELF-SIMILAR SUMS OF SQUARES

3.1. **Examples.** As first example, consider integers t so that

$$\begin{aligned} a &= 3(3t + 1) & b &= 3(8t + 3) \\ a' &= 8(8t + 3) & 10^k &= a + a' = 73t + 27. \end{aligned}$$

The choices $k = 2, 10, 18, \dots$ all are admissible and after $12^2 + 33^2 = 1233$ yield $1\ 232\ 876\ 712^2 + 3\ 287\ 671\ 233^2 = 12\ 328\ 767\ 123\ 287\ 671\ 233, \dots$

What we have here is a not all that curious property of $73 = 3^2 + 8^2$. Indeed, $3^2 \cdot 137 = (3 \cdot 4)^2 + (3 \cdot 11)^2$. The curious matter is just how much more curious such an identity seems to be when 3 is replaced by 1.

Compare the examples

$$\begin{aligned} a &= t & b &= 4t + 1 & \text{and} & a &= t & b &= 4t \\ a' &= 4(4t + 1) & 10^k &= 17t + 4 & & a' &= 4(4t - 1) & 10^k &= 17t - 4 \end{aligned}$$

which are admissible respectively for $k = 4, 20, \dots$, and $k = 12, 28, \dots$, and provide sequences associated with 17 already mentioned above.

3.2. **Analysis.** To see what's going on here, suppose that

$$\begin{aligned} a &= u_1 t + u_2 & b &= b_1 t + b_2 \\ a' &= u'_1 t + u'_2 & 10^k &= (u_1 + u'_1)t + (u_2 + u'_2) = n_1 t + n_2 \end{aligned}$$

and $a^2 + b^2 = 10^k a + b$; here the coefficients all are integers.

Viewing that last equation as equating the coefficients of polynomials in t yields $b_1^2 = u_1 u'_1$ and, oBdA*, both u_1 and u'_1 are squares, say $u_1 = a_1^2$, $u'_1 = a'_1{}^2$, with $b_1 = a_1 a'_1$. It follows that $a_1 | u_2$ and, just so, that $a'_1 | u'_2$.

A re-examination of the equations next shows that b_2 must be either $a_1 a'_2$ or $a'_1 a_2$; and a second's thought shows such an ambiguity is necessary. The cases entail $a_1 a'_2 - a'_1 a_2 = 1$, respectively $a'_1 a_2 - a_1 a'_2 = 1$.

One readily confirms — a critical step — that $n_1 = a_1^2 + a'_1{}^2$ divides $10^{2k} + 1$, for example by noticing that $n_2^2 + 1 = (a_1 a_2 + a'_1 a'_2)^2 + (a_1 a'_2 - a'_1 a_2)^2 = n_1 (a_2^2 + a'_2{}^2)$.

3.3. **Summary.** To sum up,

$$\begin{aligned} a &= a_1(a_1 t + a_2) & b &= a_1(a'_1 t + a'_2) \\ a' &= a'_1(a'_1 t + a'_2) & 10^k &= (a_1^2 + a'_1{}^2)t + (a_1 a_2 + a'_1 a'_2), \end{aligned}$$

and, mind you, $a_1^2 + a'_1{}^2$ divides $10^{2k} + 1$; equivalently, $a_1 a'_2 - a'_1 a_2 = 1$. Those with negative inclinations can readily ring changes on this summary, say by both changing the sign of t and of a, a' , and 10^k , and, say a_1 .

*When lecturing, many of us use the abbreviation 'wlog', confusing our students by suddenly introducing a logarithm, and not recognising that 'with loss of generality' is similarly denoted. The german version plainly is an abbreviation of something, and unambiguously alleges *no* Beschränkung of the Allgemeinheit.

By the way, complaints of decimalism are baseless. The number 10 appearing here may be replaced by any other base. Computers may prefer 16, some of us will like 64; 90 might be considered peculiarly suitable to the present occasion.

3.4. Conclusion. The upshot of all this is that one can construct all examples of sequences of self-similar sums of squares at will.

- (1) Select a_1 and a'_1 so that $a_1^2 + a_1'^2$ divides one and therefore lots of $10^{2k} + 1$.
- (2) Compute a_2 and a'_2 so that $a_1 a_2' - a_1' a_2 = 1$.
- (3) Write the four equations and compute pairs (k, t) .

Conversely, given a self-similar sum of squares one easily identifies sequences to which it belongs. In all, the boring completeness of this solution removes all subtlety. To make up for that, I've left several cute asides for readers to discover for themselves.

4. ARITHMETIC

Rather than end on this downbeat note, let me quickly tell you about some fine advice John Conway once gave me on instant factorisation of three-digit numbers. The difficulty is that doing it seems to require one to memorise the 168 primes less than a thousand. "Surely you're not saying that's a problem, Alf?" John said askance to me. However, not to worry. There are only, and indeed exactly, one hundred (100) *nontrivial composites* less than a thousand.

4.1. Nontrivial Composites. Usually one thinks of positive integers as being one of 1, prime, or composite. John recommends the more refined partition: 1, prime, trivially composite, or nontrivially composite.

Here, a composite integer is *trivially* composite if it is divisible by 2, 3, or 5.

4.2. Exercises.

- (a) List the nontrivial composites less than a thousand. Learn them. Annoy your friends by factorising every three digit number that comes your way.
- (b) Let S denote the set $\{1, 2, 3, \dots, 100\}$. As usual $|S|$ denotes $\#S$, the number of elements in the set (in this case $\#S = 100$, of course). Let $S_n = \{a \in S : n|a \text{ (} n \text{ divides } a)\}$. Compute

$$|S| - (|S_2| + |S_3| + |S_5|) + (|S_6| + |S_{15}| + |S_{10}|) - |S_{30}|,$$

and, noting that there are just three nontrivial composites, namely $49 = 7^2$, $77 = 7 \cdot 11$, and $91 = 7 \cdot 13$, less than one hundred, find the number of primes less than 100.

- (c) Similarly, now take $S = \{1, 2, 3, \dots, 1000\}$. Given that there are exactly one hundred nontrivial composites less than a thousand, find the number of primes less than 1000.

John Conway was saddened to find at the Guy 90 meeting that I had not recently redone exercise (a) and could not instantly report $871 = 13 \cdot 67$. He points out that exceeding our grasp by aiming to factorise not just three digit but four digit integers is the best way to internalise the first hundred nontrivial composites; the three bonus factorisations below[†] promote that cause.

[†]The table was T_EXed at the time by Mark and Kurt not just as Exercise (a) but also as part proof that I had successfully taught them to L^AT_EX.

REFERENCES

- [1] Frits Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, Utrecht, 1999.
 [2] Abderrahmane Nitaj, 'L'algorithm de Cornacchia', *Exposition. Math.* **13** (1995), 358–365.
 [3] Alfred J. van der Poorten, 'The Hermite-Serret algorithm and $12^2 + 33^2$ ', Proc. Workshop on *Cryptography and Computational Number Theory* (CCNT'99), (National University of Singapore, 22-26 November, 1999), K.-Y. Lam, I. E. Shparlinski, H. Wang and C. Xing eds., Birkhäuser 2001, 129–136.

The First Hundred Nontrivial Composites

49 = 7 ²	301 = 7 × 43	497 = 7 × 71	679 = 7 × 97	841 = 29 ²
77 = 7 × 11	319 = 11 × 29	511 = 7 × 73	689 = 13 × 53	847 = 7 × 11 ²
91 = 7 × 13	323 = 17 × 19	517 = 11 × 47	697 = 17 × 41	851 = 23 × 37
119 = 7 × 17	329 = 7 × 47	527 = 17 × 31	703 = 19 × 37	869 = 11 × 79
121 = 11 ²	341 = 11 × 31	529 = 23 ²	707 = 7 × 101	871 = 13 × 67
133 = 7 × 19	343 = 7 ³	533 = 13 × 41	713 = 23 × 31	889 = 7 × 127
143 = 11 × 13	361 = 19 ²	539 = 7 ² × 11	721 = 7 × 103	893 = 19 × 47
161 = 7 × 23	371 = 7 × 53	551 = 19 × 29	731 = 17 × 43	899 = 29 × 31
169 = 13 ²	377 = 13 × 29	553 = 7 × 79	737 = 11 × 67	901 = 17 × 53
187 = 11 × 17	391 = 17 × 23	559 = 13 × 43	749 = 7 × 107	913 = 11 × 83
203 = 7 × 29	403 = 13 × 31	581 = 7 × 83	763 = 7 × 109	917 = 7 × 131
209 = 11 × 19	407 = 11 × 37	583 = 11 × 53	767 = 13 × 59	923 = 13 × 71
217 = 7 × 31	413 = 7 × 59	589 = 19 × 31	779 = 19 × 41	931 = 7 ² × 19
221 = 13 × 17	427 = 7 × 61	611 = 13 × 47	781 = 11 × 71	943 = 23 × 41
247 = 13 × 19	437 = 19 × 23	623 = 7 × 89	791 = 7 × 113	949 = 13 × 73
253 = 11 × 23	451 = 11 × 41	629 = 17 × 37	793 = 13 × 61	959 = 7 × 137
259 = 7 × 37	469 = 7 × 67	637 = 7 ² × 13	799 = 17 × 47	961 = 31 ²
287 = 7 × 41	473 = 11 × 43	649 = 11 × 59	803 = 11 × 73	973 = 7 × 139
289 = 17 ²	481 = 13 × 37	667 = 23 × 29	817 = 19 × 43	979 = 11 × 89
299 = 13 × 23	493 = 17 × 29	671 = 11 × 61	833 = 7 ² × 17	989 = 23 × 43

1001 = 7 × 11 × 13	1003 = 17 × 59	1007 = 19 × 53
--------------------	----------------	----------------

CENTRE FOR NUMBER THEORY RESEARCH, SYDNEY, 1 BIBIL PLACE, KILLARA NSW 2071, AUSTRALIA
E-mail address: alf@maths.usyd.edu.au (Alf van der Poorten)

E-mail address: kurt_thomsen@hotmail.com (Kurt Thomsen)

FRANTIC FILMS, RESEARCH AND DEVELOPMENT, <http://software.franticfilms.com/>
E-mail address: mwiebe@franticfilms.com (Mark Wiebe)