105.39 The Eureka theorem of Gauss

Introduction

In 1796, Gauss proved that every positive integer is a sum of at most three triangular numbers [1]. The result has received its catchy name because Gauss noted his breakthrough by writing

$$\text{EYPHKA! Num} = \Delta + \Delta + \Delta$$

in his diary.

To prove Gauss's result it is sufficient to prove that every positive integer of the form $8k + 3$ can be expressed as a sum of three squares. Considering such an expression modulo 8 shows that the squares must all be odd and we then have

$$8k + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2$$

$$\Rightarrow k = \frac{x(x + 1)}{2} + \frac{y(y + 1)}{2} + \frac{z(z + 1)}{2}.$$

Various proofs of Gauss's result and the equivalent result for three squares have been published but few are accessible without a prior study of such matters as the quasi-reduction of positive-definite ternary quadratic forms; a relatively easy-to-understand version of such a proof is given in [2]. Another relatively easy-to-understand proof is given in [3] and the proof below owes much to a prior reading of Ankeny's proof.

Preliminary ideas

Most proofs of the Eureka theorem assume Dirichlet's theorem that for any two relatively prime positive integers a and b there are infinitely many primes of the form $a + rb$ with $r \in \mathbb{Z}$. We shall follow suit since this result is much easier to state than to prove.

We shall also require an elementary use of the law of quadratic reciprocity. An especially straightforward proof is given in [4]. For m and n coprime positive odd integers, the Jacobi symbol notation for quadratic reciprocity and its supplements are

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{((m-1)(n-1))/4}$$

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

Our proof will produce a number which contains no prime of the form $4k + 3$ to an odd power. Fermat's result that the number is then a sum of two squares is then applied. This result is well-known and very short proofs of the basic result are given in [5, 6].

A crucial result used in the proof is Minkowski's theorem [7]. This 19th

https://doi.org/10.1017/mag.2021.121 Published online by Cambridge University Press

century result was a major breakthrough of the day, enabling some deep number theoretic results to be proved by surprisingly simple geometric means.

The theorem can be stated and proved as follows.

If an object S is convex, symmetric about the origin and has volume greater than 8, then it contains a point with integer coefficients other than the origin.

Proof: Each point (x, y, z) of S can be mapped to a point (X, Y, Z), $-1 \leqslant X, Y, Z \leqslant 1$, where $X \equiv x, Y \equiv y, Z \equiv z \pmod 2$. This translates disjoint pieces of S to subsets of the cube F defined by $-1 \leqslant X, Y, Z \leqslant 1$ with the same volume. Since F has volume 8, the translated pieces must overlap. At least two points of S, $\mathbf{u} \neq \mathbf{v}$ say, must therefore be mapped to the same point in the cube.

Then there are integers a, b, c such that $\mathbf{v} - \mathbf{u} = (2a, 2b, 2c)$. By symmetry $-\mathbf{u} \in S$ and then, by convexity, $\frac{1}{2}(\mathbf{v} - \mathbf{u}) = (a, b, c) \in S$.

Eureka!

It is sufficient to prove that a square-free integer m of the form $8k + 3$ is always a sum of three squares.

Choose a prime $q = 4k + 1 + 4l(8k + 3)$, for $l = 0, 1, 2, \ldots$. Then

$$q \equiv 1 \pmod 4 \text{ and } -2q \equiv 1 \pmod m. \tag{1}$$

Using Jacobi symbols,

$$\left(\frac{-m}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{q}\right) = \left(\frac{q}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right)\left(\frac{-2q}{m}\right) = +1$$

and so there is an integer p such that $p^2 + m$ is a multiple of q. Replacing p by $q - p$ if necessary, we can assume p is odd and then

$$m + p^2 \text{ is a multiple of } 4q. \tag{2}$$

Now consider the transformation, with volume scale factor $2qm$, defined by

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ p & 2q & 0 \\ p & 2q & m \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

In (X, Y, Z) space, the region $mX^2 + Y^2 + 2qZ^2 < 4qm$ has volume $\frac{4}{3}\pi\sqrt{32q^2m^2}$. In (x, y, z) space, this corresponds to a convex region, symmetric about the origin, of volume $\frac{4}{3}\pi\sqrt{8}$. This volume is greater than 8 and so there are integers x, y, z not all zero such that

$$mX^2 + Y^2 + 2qZ^2 < 4qm.$$

https://doi.org/10.1017/mag.2021.121 Published online by Cambridge University Press

From (1) and (2) we then have

$$mX^2 + Y^2 + 2qZ^2 \equiv (1 + 2q)(px + 2qy)^2 \equiv 0 \pmod{m}$$

$$mX^2 + Y^2 + 2qZ^2 \equiv (m + p^2)x^2 \equiv 0 \pmod{2q}.$$

Since $2q$ and m are relatively prime, $mX^2 + Y^2 + 2qZ^2 \equiv 0 \pmod{2qm}$ and so

$$mX^2 + Y^2 + 2qZ^2 = 2qm. \tag{3}$$

Now suppose the prime power factorisation of $mX^2 + Y^2$ contained a prime r to an odd power, where $r \equiv 3 \pmod 4$. Let $X = gX_1$ and $Y = gY_1$ where g is the g.c.d. of X and Y. Then

$$r \neq q,\ mX_1^2 + Y_1^2 \equiv 0 \pmod{r},\ Z^2 \equiv m \pmod{r}. \tag{4}$$

If r is not a factor of m then $\left(\frac{-m}{r}\right) = \left(\frac{m}{r}\right) = +1$ and $r \equiv 1 \pmod 4$, a contradiction. If r is a factor of m then it is also a factor of Y and Z. Since m is square-free, (1) and (3) give $X^2 \equiv 2q \equiv -1 \pmod{r}$ and, again, $r \equiv 1 \pmod 4$.

Hence $m - Z^2 = \dfrac{mX^2 + Y^2}{2q}$ is a sum of two integer squares, as required.

References

1. C. F. Gauss, *Disquisitiones arithmeticae*, Yale Univ. Press, New Haven, Conn., and London (1966).
2. P. Pollack and P. Schorn, Dirichlet's proof of the three-square theorem, http://pollack.uga.edu/finding3squares-6.pdf
3. N. C. Ankeny, Sums of three squares, *Proc. Amer. Math. Soc.* **8** (1957) pp. 316-319.
4. S. W. Dolan, Nint reciprocity, *Math. Gaz.* **98** (July 2014), pp. 317-319.
5. S. W. Dolan, Primes of the form $x^2 + z^2$, *Math. Gaz.* **101** (November 2017) p. 465.
6. S. W. Dolan, A very simple proof of the two-squares theorem, Math. Gaz. 105 (November 2021) p. 511.
7. H. Davenport, The geometry of numbers, *Math. Gaz.* **31** (October 1947) pp. 206-210.

STAN DOLAN
4 Orchard Close, Charmouth DT6 6RS
e-mail: *stan@standolan.co.uk*

10.1017/mag.2021.121
© The Mathematical Association 2021

105.40 A tale of two cubics

While dealing with quadratics one observes that if $x^2 + ax + b$ factorises into linear polynomials with integer coefficients for some choice of integers a and b then so does $x^2 - ax + b$ because

$$x^2 - ax + b = (-x)^2 + a(-x) + b$$

https://doi.org/10.1017/mag.2021.121 Published online by Cambridge University Press