The Eureka theorem of Gauss

STAN DOLAN

1. *Introduction*

On 10th July 1796, when he was still a teenager, Gauss famously wrote *EYPHKA*! in his diary when recording the completion of a proof that every positive integer is the sum of at most three triangular numbers.

Gauss's proof is included in his book, *Disquisitiones Arithmeticae* [1], which was published in 1801. No short exposition of Gauss's proof appears to be extant but [2] is an excellent guide to understanding Gauss's work.

The purpose of this Article is to give a relatively short algebraic proof of the Eureka theorem using Gauss's approach and without recourse to results which were not available to Gauss, for example Dirichlet's theorem on primes in arithmetic progressions. The notations of group theory and of matrix algebra will be employed to simplify the algebra. These concepts are implicit in Gauss's development of the underlying theory but not explicitly used by him. Quadratic reciprocity, with standard Jacobi symbols, will be used and modern proofs can readily be found, for example in [3].

The difficulty that Gauss faced in expressing his arguments without using the notation of matrix algebra should not be underestimated. A good example of this is given in Section 235 of [1]. There, after seven pages of calculations using 23 numbered equations, Gauss ends by saying:

'The calculation, which would be too long to include here, we leave to the reader.'

The matrix algebra that we will require is relatively elementary. The following results about cofactors will prove especially useful.

For any 3×3 matrix $\boldsymbol{A}$, let $\overline{\boldsymbol{A}}$ denote its cofactor matrix. Then for any 3×3 matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ we have

$$\overline{\boldsymbol{AB}} = \overline{\boldsymbol{A}}\,\overline{\boldsymbol{B}}, \overline{\boldsymbol{A}^{\boldsymbol{T}}} = \overline{\boldsymbol{A}}^{\boldsymbol{T}} \text{ and } \overline{\overline{\boldsymbol{A}}} = \det(\boldsymbol{A})\boldsymbol{A}.$$

In particular, for a symmetric matrix $\boldsymbol{M}$,

$$\overline{\boldsymbol{UMU}^{\boldsymbol{T}}} = \overline{\boldsymbol{U}}\,\overline{\boldsymbol{M}}\,\overline{\boldsymbol{U}}^{\boldsymbol{T}}.$$

A transformation of $\boldsymbol{M}$ by $\boldsymbol{U}$ is therefore the same as a transformation of $\overline{\boldsymbol{M}}$ by $\overline{\boldsymbol{U}}$. We shall denote the element in row i and column j of a matrix $\boldsymbol{A}$ by $\boldsymbol{A}_{ij}$.

2. *Equivalent forms and matrices*

Gauss's proof of the Eureka theorem was based upon his analysis of the representation of integers as quadratic polynomials $ax^2 + bxy + cy^2$.

We will make the following definitions.

- If $a > 0$ and $\gcd(a, b, c) = 1$, then $f(x, y) = ax^2 + bxy + cy^2$ will be termed a *form*. The quantity $\Delta = b^2 - 4ac$ is termed the *discriminant* of the form.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

- Although much of what we shall prove is true more generally, we will assume throughout that all forms have a given discriminant $\Delta \equiv 5 \pmod 8$, such that $\Delta < 0$ and $|\Delta|$ is the product of r distinct primes, $p_1 p_2 \ldots p_r$.
- The notation $[a, b, c]$ will sometimes be used for f. For non-zero a, we can write $[a, b, -]$, since the value of c is determined by a, b and Δ.

It will prove useful to think of $ax^2 + bxy + cy^2$ as the matrix product

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

If $\boldsymbol{R}$ and $\boldsymbol{S}$ are symmetric matrices of the same dimension, we define them to be *equivalent* if there is a matrix $\boldsymbol{U}$ such that

$$\boldsymbol{U R U^T = S},$$

where $\boldsymbol{U}$ has integer coefficients and $\det(\boldsymbol{U}) = 1$. Since the inverse of $\boldsymbol{U}$ has integer coefficients this is clearly an equivalence relation.

Matrix equivalence corresponds to a change of variables $\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \boldsymbol{U}$ since

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

where $\begin{pmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{pmatrix} = \boldsymbol{U} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \boldsymbol{U^T}$. In this case, we shall now prove that $[A, B, C]$ is a form if $[a, b, c]$ is a form. We can then define them to be equivalent forms.

Lemma 1: Let a form $[a, b, c]$ be transformed into $[A, B, C]$ by $\boldsymbol{U} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ where $\boldsymbol{U}$ is an integer matrix of determinant 1.

(i) $A = f(p, q) > 0$.

(ii) $[A, B, C]$ is a form which represents precisely the same integers as $[a, b, c]$.

Proof:

(i) Multiplying out: $A = ap^2 + bpq + cq^2 = f(p, q)$. Then
$4af(p, q) = (2ap + bq)^2 - \Delta q^2 > 0$, and so $f(p, q) > 0$.

(ii) The transformation multiplies the discriminant by $|\boldsymbol{U}|^2 = 1$ and so the discriminant is unaltered. Since the inverse of $\boldsymbol{U}$ is also a matrix with integer coefficients, $\gcd(A, B, C)$ is a factor of $\gcd(a, b, c) = 1$. Thus $[A, B, C]$ is a form.

Since the change of variables is invertible, the equivalent forms $[a, b, c]$ and $[A, B, C]$ represent precisely the same integers.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

The next two lemmas enable us to replace forms by simpler equivalent forms.

Lemma 2:

(i) A matrix $\begin{pmatrix} a & b \\ b & - \end{pmatrix}$, $a \neq 0$ is equivalent to a matrix $\begin{pmatrix} a & b + am \\ b + am & - \end{pmatrix}$, for any integer m. Note that by a suitable choice of m we can suppose $|b + am| \leqslant \frac{1}{2}|a|$.

(ii) A 2×2 symmetric matrix with rational coefficients and determinant D is equivalent to a matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with $|a| \leqslant \sqrt{\frac{4}{3}|D|}$.

(iii) There is only a finite number of equivalence classes of forms of a given discriminant.

Proof:

(i) $\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\begin{pmatrix} a & b \\ b & - \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b + am \\ b + am & - \end{pmatrix}$, as required.

(ii) By multiplying the symmetric matrix by a suitable integer, we can suppose without loss of generality that it has integer coefficients. Let $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ be the matrix of an equivalent form with the smallest possible absolute value of a diagonal element. Transforming by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ if necessary, we can assume $|a| \leqslant |c|$.

If $a = 0$, then there is nothing to prove. Otherwise, by Lemma 2(i), we can suppose $|b| \leqslant \frac{1}{2}|a|$. Then

$$a^2 \leqslant |ac| = |D + b^2| \leqslant |D| + \tfrac{1}{4}a^2 \Rightarrow a^2 \leqslant \tfrac{4}{3}|D|.$$

(iii) By parts (i) and (ii), a given form is equivalent to a form $[a, b, c]$ with $|b| \leqslant a$ and $a^2 \leqslant \frac{1}{3}|\Delta|$. Thus there is only a finite number of possibilities for a and b and each such choice determines the value of c.

Lemma 3:

(i) Let $f = [a, b, c]$ be a form. For any non-zero integer m, f is equivalent to a form $[a', -, -]$ where a' is coprime to m.

(ii) Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \ldots$ be a finite sequence of (not necessarily distinct) classes of forms. Then, for each i and some integer b, there is a form $[a_i, b, -] \in \mathcal{F}_i$, such that the a_i are pairwise coprime and coprime to Δ.

Proof:

(i) We can suppose m is square-free. Let $m = \alpha\beta\gamma\delta$, where

$$\gcd(m, a, b) = \beta, \gcd(m, a, c) = \gamma, \gcd(m, a) = \alpha\beta\gamma.$$

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

Then $f(\alpha, \delta)$ is coprime to m. Let ε and μ be integers such that $\alpha\mu - \delta\varepsilon = 1$. Then f is equivalent to a form with matrix

$$\begin{pmatrix} \alpha & \delta \\ \varepsilon & \mu \end{pmatrix}\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}\begin{pmatrix} \alpha & \varepsilon \\ \delta & \mu \end{pmatrix} = \begin{pmatrix} f(\alpha, \delta) & - \\ - & - \end{pmatrix}, \text{ as required.}$$

(ii) By part (i), we can choose forms $[a_i, b_i, -] \in \mathcal{F}_i$ such that each a_{i+1} is coprime to $a_1 \ldots a_i\Delta$. Then all the b_i are odd and we can solve the equations

$$b \equiv b_i \pmod{2a_i}.$$

Applying the method of Lemma 2(i) then completes the proof.

3. *The class group*

Gauss's proof of the Eureka Theorem depended upon his theory of the composition of forms. This idea is important in its own right and is a fundamental concept in algebraic number theory. However, the algebra of Gauss's discovery is so involved that many details were not included in *Disquisitiones Arithmeticae*. Thus, in article 240, Gauss says:

> It would take too much time to derive all 37 of these equations. We will be satisfied with establishing some of them as a pattern for the rest.

We will write $f \sim g$ to denote the equivalence of forms f and g. The equivalence class of f will be denoted by (f). We shall adopt an approach based upon the following simple idea given in [2].

> If two forms are $[a, b, -]$ and $[a', b, -]$, where $4aa'$ is a divisor of $b^2 - \Delta$ then $[aa', b, -]$ is a form and we can define a composition, $*$, by $[a, b, -] * [a', b, -] = [aa', b, -]$.

Now let $\mathcal{F}$ and $\mathcal{F}'$ be any two, not necessarily distinct, equivalence classes of forms. By Lemma 3(ii) we can find forms $f = [a, b, -]$ and $f' = [a', b, -]$ in $\mathcal{F}$ and $\mathcal{F}'$ respectively, where a and a' are coprime. Then $\frac{1}{4}(b^2 - \Delta)$ is a multiple of both a and a' and therefore of aa'. It is therefore natural to try to define $\mathcal{F} * \mathcal{F}'$ to be $\langle aa', b, - \rangle$ but we can only do this if we can prove that all possible choices of f and f' lead to the same equivalence class.

Lemma 4:

Let $[a, b, -] \sim [A, B, -]$ and $[a', b, -] \sim [A', B, -]$, where $b^2 - \Delta$ is a multiple of $4aa'$ and $B^2 - \Delta$ is a multiple of $4AA'$. Then $[aa', b, -] \sim [AA', B, -]$.

Proof:

By Lemma 3(ii), there are forms $[\alpha, \beta, -] \sim [a, b, -]$ and $[\alpha', \beta, -] \sim [a', b, -]$ such that α, α' and $aa'AA'$ are pairwise coprime. It is sufficient to prove that $[aa', b, -]$ and $[AA', B, -]$ are (separately)

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

equivalent to $[\alpha\alpha', \beta, -]$ and so there is no loss of generality in just considering the case when $\gcd(aa', AA') = 1$.

We can solve the equations

$$\mathcal{B} \equiv 1 \pmod 2, \ \mathcal{B} \equiv b \pmod{aa'}, \ \mathcal{B} \equiv B \pmod{AA'}.$$

Then, by Lemma 2(iii), $[x, b, -] \sim [x, \mathcal{B}, -]$ and $[x, B, -] \sim [x, \mathcal{B}, -]$ for x any divisor of aa' or AA'. Therefore there is no loss of generality in just considering the case $B = b$.

Since $[a, b, -]$ and $[A, b, -]$ are equivalent there are integers c and C and an integral matrix of determinant 1, $U = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ such that

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} = \begin{pmatrix} A & \frac{1}{2}b \\ \frac{1}{2}b & C \end{pmatrix}\begin{pmatrix} u & -t \\ -s & r \end{pmatrix},$$

where a' divides c and C.

Then $\frac{1}{2}rb + sc = \frac{1}{2}rb - tA$ and so a' divides t. Therefore

$$\begin{pmatrix} r & sa' \\ \frac{t}{a'} & u \end{pmatrix}\begin{pmatrix} aa' & \frac{1}{2}b \\ \frac{1}{2}b & \frac{c}{a'} \end{pmatrix} = \begin{pmatrix} Aa' & \frac{1}{2}b \\ \frac{1}{2}b & \frac{C}{a'} \end{pmatrix}\begin{pmatrix} u & -\frac{t}{a'} \\ -sa' & r \end{pmatrix},$$

and so $[aa', b, -] \sim [Aa', b, -]$. Similarly, $[Aa', b, -] \sim [AA', b, -]$ and so, as required, $[aa', b, -] \sim [AA', b, -]$.

We can therefore define the composition of equivalence classes in the manner described just before Lemma 4. It is now straightforward to establish a group structure for the composition of equivalence classes.

The class group theorem

Let $CL(\Delta)$ be the set of equivalence classes of forms of discriminant Δ. Under composition of classes, $CL(\Delta)$ is an abelian group, called the *class group*.

Proof:

Let $\mathcal{F}_0 = \langle 1, 1, - \rangle$. Then $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & - \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} - & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$ and so $[1, 1, -] \sim [-, 1, 1]$. Then, by Lemma 2(i), $\mathcal{F}_0 = \langle 1, b, - \rangle = \langle -, b, 1 \rangle$ for any odd integer b. Let $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{F}_3$ be any three, not necessarily distinct, classes of forms. By Lemma 3, we can find integers A_i and B, with the A_i pairwise coprime, such that $\mathcal{F}_i = \langle A_i, B, - \rangle$. Then:

$\mathcal{F}_1 * \mathcal{F}_2 = \langle A_1A_2, B, - \rangle = \langle A_2A_1, B, - \rangle$ and so we have closure and commutativity, $(\mathcal{F}_1 * \mathcal{F}_2) * \mathcal{F}_3 = \mathcal{F}_1 * (\mathcal{F}_2 * \mathcal{F}_3) = [A_1A_2A_3, B, -]$ and so $*$ is associative, $\mathcal{F}_0 * \mathcal{F}_1 = \langle [1, B, -] * [A_1, B, -] \rangle = \langle A_1, B, - \rangle = \mathcal{F}_0$ and so $\mathcal{F}_1$ is the identity, $\mathcal{F}_1 * \langle -, B, A_1 \rangle = \langle [A_1, B, -] * [-, B, A_1] \rangle = \langle \frac{1}{4}(B^2 - \Delta), B, 1 \rangle = \mathcal{F}_0$ and so $CL(\Delta)$ contains inverses.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

Let $S(\Delta) = \{\mathcal{F}^2 \mid \mathcal{F} \in CL(\Delta)\}$. Then the map $\mathcal{F} \to \mathcal{F}^2$ is a group homomorphism from $CL(\Delta)$ onto the subgroup $S(\Delta)$. The kernel is $T(\Delta) = \{\mathcal{F} \in CL(\Delta) \mid \mathcal{F}^2 = \mathcal{F}_0\}$ and so $|CL(\Delta)| = |S(\Delta)||T(\Delta)|$. The next theorem will give us a useful bound on the number of elements in $T(\Delta)$.

The counting theorem

$[CL(\Delta) : S(\Delta)] \geqslant 2^{r-1}$.

Proof:

Let a be a positive divisor of $\Delta = -p_1p_2\ldots p_r$. Then a is odd and $\left[a, a, \frac{a^2 - \Delta}{4a}\right]$ is a form. Let $\mathcal{F}(a) = \left\langle a, a, \frac{a^2 - \Delta}{4a}\right\rangle$.

Let $c = \frac{1}{4a}(a^2 - \Delta)$. The matrix $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ transforms $[a, a, c]$ into $[c, a, a]$ and so

$$[a, a, c] * [a, a, c] = [a, a, c] * [c, a, a] = [ac, a, 1].$$

Therefore $\mathcal{F}(a)^2 = \mathcal{F}_0$ and $\mathcal{F}(a) \in T(\Delta)$.

There are 2^r positive divisors of Δ. However some of these may produce forms in the same class. So suppose that $\mathcal{F}(a) = \mathcal{F}(A)$. Since $-\Delta$ is a square-free positive multiple of both a and A we can write

$$a = PQ, A = PR, -\Delta = PQRS,$$

where P, Q, R, S are pairwise coprime positive integers. Since $[a, a, c]$ must represent A, there are integers x and y such that

$$ax^2 + axy + \frac{a^2 - \Delta}{4a}y^2 = A$$

$$\Rightarrow \quad a^2(2x + y)^2 - \Delta y^2 = 4aA$$

$$\Rightarrow \quad PQ(2x + y)^2 + RSy^2 = 4PR.$$

Then R is a factor of $2x + y$ and P is a factor of y. Let $2x + y = RX$ and $y = PY$, then

$$QRX^2 + PSY^2 = 4.$$

Either $QR = 1$, in which case $a = A$, or $PS = 1$, in which case $aA = -\Delta$. Hence each equivalence class of forms contains at most 2 forms of the type $\left[a, a, \frac{a^2 - \Delta}{4a}\right]$ and so $[CL(\Delta) : S(\Delta)] = |T(\Delta)| \geqslant 2^{r-1}$.

4. *The representation theorem*

Modern mathematical interest in the representation of integers as $ax^2 + bxy + cy^2$ for given integers a, b and c probably started with

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

Fermat's proof that *any prime of the form* $4k + 1$ *can be expressed as the sum of two squares*.

The general representation of integers by a form is still the subject of active research. Some of the deep mathematical ideas involved are explained extremely well in [4]. We shall avoid some of the difficulties by considering representations modulo the discriminant Δ of the form. First, we will extend Lemma 2(ii) to 3×3 matrices.

Lemma 5:

Let $\boldsymbol{M}$ be a 3×3 symmetric matrix with rational coefficients and determinant D. Then $\boldsymbol{M}$ is equivalent to a matrix $\begin{pmatrix} a & b & * \\ b & c & * \\ * & * & * \end{pmatrix}$ with $a^2 \leqslant \dfrac{4|ac - b^2|}{3} \leqslant \sqrt{\dfrac{64|aD|}{27}}$.

Proof:

As in Lemma 2(ii) we can assume that $\boldsymbol{M}$ has integer coefficients. We can further assume that $|M_{11}| + |\overline{M}_{33}|$ is the minimum possible for all matrices equivalent to $\boldsymbol{M}$. Then $M_{11}^2 \leqslant \frac{4}{3}|\overline{M}_{33}|$ since, otherwise, we could use Lemma 2(ii) to apply a transformation of the form $\begin{pmatrix} \boldsymbol{L} & \boldsymbol{O} \\ \boldsymbol{O} & 1 \end{pmatrix}$ which leaves $\overline{M}_{33}$ unchanged and reduces $|M_{11}|$.

Similarly, suppose it is not the case that $\overline{M}_{33}^2 \leqslant \frac{4}{3}|\overline{\overline{M}}_{11}| = \frac{4}{3}|M_{11}D|$. Applying Lemma 2(ii) again, there is a transformation of $\overline{\boldsymbol{M}}$ of the form $\begin{pmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & \overline{\boldsymbol{K}} \end{pmatrix}$ which leaves $\overline{\overline{M}}_{11}$ unchanged and reduces $|\overline{M}_{33}|$. We therefore obtain the contradiction that the transformation $\begin{pmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{K} \end{pmatrix}$ leaves M_{11} unchanged and reduces $|\overline{M}_{33}|$.

Hence $M_{11}^2 \leqslant \frac{4}{3}|\overline{M}_{33}| \leqslant \sqrt{\frac{64}{27}|M_{11}D|}$, as required.

Lemma 6:

Let $a + bx + cx^2$ be an integer quadratic with $\gcd(a, b, c) = 1$ and let M be any odd integer. Then there is an integer value of x such that $a + bx + cx^2$ and M are coprime.

Proof:

Let p be any prime divisor of M.

If p does not divide a then choose $x \equiv 0 \pmod{p}$.

If p divides a and bc then choose $x \equiv 1 \pmod{p}$.

If p divides only a then choose $x \equiv \frac{b}{c} \pmod{p}$.

Then $a + bx + cx^2$ is coprime to p and, by the Chinese Remainder Theorem, we can choose an x which works for all prime divisors of M.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

The representation theorem for squares

If the forms in equivalence class $\mathcal{F}$ represent, modulo Δ, a square coprime to Δ then $\mathcal{F} \in S(\Delta)$.

Proof:

From Lemma 3(i) we can suppose that $f = [a, b, c] \in \mathcal{F}$. with a odd and coprime to Δ. Then there are integers L, M, N with N coprime to Δ, such that

$$aL^2 + bLM + cM^2 \equiv N^2 \pmod{\Delta}.$$

Multiplying throughout by the inverse of N, modulo Δ, we have integers l, m, n such that

$$al^2 + blm + cm^2 = 1 + n\Delta.$$

Let $\boldsymbol{A} = \begin{pmatrix} a & \frac{1}{2}b & -\frac{1}{2}m \\ \frac{1}{2}b & c & \frac{1}{2}l \\ -\frac{1}{2}m & \frac{1}{2}l & -n \end{pmatrix}$ then $|A| = -\frac{1}{4}$. Any matrix M equivalent to $\boldsymbol{A}$ has integral $\boldsymbol{M_{11}}$ and then, from Lemma 5, $\boldsymbol{A}$ is equivalent to a matrix $\begin{pmatrix} 0 & 0 & E \\ 0 & F & G \\ E & G & H \end{pmatrix}$ with $2E$, F,$2G$, H integers and $E^2F = \frac{1}{4}$. Then $E = \pm\frac{1}{2}$, $F = 1$ and

$$\begin{pmatrix} 1 & 0 & 0 \\ -4EG & 1 & 0 \\ H & 0 & -2E \end{pmatrix}\begin{pmatrix} 0 & 0 & E \\ 0 & 1 & G \\ E & G & H \end{pmatrix}\begin{pmatrix} 1 & -4EG & H \\ 0 & 1 & 0 \\ 0 & 0 & -2E \end{pmatrix} = \begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}.$$

Hence there is an integral matrix $\boldsymbol{U}$ of determinant ± 1 such that

$$\boldsymbol{A} = \boldsymbol{U}\begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}\boldsymbol{U^T}.$$

In this equation, $\boldsymbol{U}$ can be replaced by $\boldsymbol{U}(x) = \boldsymbol{U}\begin{pmatrix} 1 & 0 & 0 \\ 2x & 1 & 0 \\ x^2 & x & 1 \end{pmatrix}$ for any integer x.

By considering the determinant of $\boldsymbol{U}$, we have

$$\overline{\boldsymbol{U}}_{31}\boldsymbol{U}_{31} + \overline{\boldsymbol{U}}_{32}\boldsymbol{U}_{31} + \overline{\boldsymbol{U}}_{33}\boldsymbol{U}_{31} = \pm 1$$

and therefore $\gcd\left(\overline{\boldsymbol{U}}_{31}, \overline{\boldsymbol{U}}_{32}, \overline{\boldsymbol{U}}_{33}\right) = 1$.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

$$\text{Now } \overline{\boldsymbol{U}(x)}_{33} = \begin{pmatrix} \overline{\boldsymbol{U}}_{31} & \overline{\boldsymbol{U}}_{32} & \overline{\boldsymbol{U}}_{33} \end{pmatrix} \overline{\begin{pmatrix} 1 & 0 & 0 \\ 2x & 1 & 0 \\ x^2 & x & 1 \end{pmatrix}} = x^2\overline{\boldsymbol{U}}_{31} - x\,\overline{\boldsymbol{U}}_{32} + \overline{\boldsymbol{U}}_{33}.$$

By Lemma 6 we can therefore choose a value of x such that $\overline{\boldsymbol{U}}_{33}$ is coprime to Δ. For this value of x let

$$\boldsymbol{U}(x) = \begin{pmatrix} p & q & - \\ r & s & - \\ - & - & - \end{pmatrix}.$$

Then $\begin{pmatrix} r & -p & 0 \end{pmatrix}\boldsymbol{U}(x) = \begin{pmatrix} 0 & u & - \end{pmatrix}$, where $u = qr - ps$ is coprime to Δ. Therefore

$$f(r, -p) = \begin{pmatrix} r & -p & 0 \end{pmatrix}\boldsymbol{A}\begin{pmatrix} -r \\ p \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & u & - \end{pmatrix}\begin{pmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ u \\ - \end{pmatrix} = u^2.$$

If p and r have a common factor t, then t is also a factor of u. By cancelling, we can therefore suppose that p and r are coprime integers such that $f(r, -p) = u^2$.

Let α and β be integers such that $\beta r + \alpha p = 1$. Then

$$\begin{pmatrix} r & -p \\ \alpha & \beta \end{pmatrix}\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}\begin{pmatrix} r & \alpha \\ -p & \beta \end{pmatrix} = \begin{pmatrix} u^2 & * \\ * & * \end{pmatrix}.$$

Then there are integers v, w such that $f \sim [u^2, v, w]$, where u is coprime to Δ and therefore to v. Then $[|u|, v, w|u|]$ is a form and $[u^2, v, w] = [|u|, v, w|u|]^2$.

Let G be the multiplicative group of integers modulo $|\Delta| = p_1p_2\ldots p_r$ and let S be the subgroup of squares. Two elements x and y of G are in the same coset of S in G if, and only if,

$$\left(\frac{x}{p_i}\right) = \left(\frac{y}{p_i}\right), \text{ for } 1 \leqslant i \leqslant r.$$

Hence there are 2^r cosets of S in G. Furthermore, precisely 2^{r-1} of these cosets contain the elements such that $\left(\frac{x}{|\Delta|}\right) = 1$, i.e. such that an even number of $\left(\frac{x}{p_i}\right)$ are -1.

We are now in position to determine which integers can be represented modulo Δ by establishing a close connection between $CL(\Delta)/S(\Delta)$ and G/S.

The representation theorem

- A form represents, modulo Δ, all the integers in a particular coset of S and no integer of G in any other coset.
- An integer m of G is represented by a form modulo Δ if, and only if, $\left(\frac{m}{|\Delta|}\right) = 1$.

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

Proof:

Let f be any form of discriminant Δ. By Lemma 3(i) we can suppose that f is a form $[a, b, c]$ with a odd and coprime with Δ. Since $\Delta = b^2 - 4ac$ we have $\left(\frac{\Delta}{a}\right) = 1$. By quadratic reciprocity, since $|\Delta| \equiv 3 \pmod 4$, we have $\left(\frac{a}{|\Delta|}\right) = \left(\frac{|\Delta|}{a}\right)\left(\frac{-1}{a}\right) = \left(\frac{\Delta}{a}\right) = 1$. Let $m = ar^2 + brs + cs^2$. Then

$$m = a\left(r + \frac{bs}{2a}\right)^2 + \frac{4ac - b^2}{2a}s^2 \in aS \text{ and } \left(\frac{m}{|\Delta|}\right) = \left(\frac{a}{|\Delta|}\right) = 1.$$

Conversely, let $\mathcal{F}$ and $\mathcal{F}'$ be classes of forms in distinct cosets of $S(\Delta)$ in $CL(\Delta)$. By Lemma 3 we can suppose $\mathcal{F} = \langle a, b, c\rangle$ and $\mathcal{F}' = \langle a', b', c'\rangle$, where a, a' and Δ are pairwise coprime. If a and a' are in the same coset of S in G, then $aa' \in S$ and, by the representation of squares theorem, $\mathcal{F}\mathcal{F}' \in S(\Delta)$, a contradiction. Thus, by the counting theorem, we have at least 2^{r-1} cosets of S in G (and therefore precisely 2^{r-1} cosets) containing elements which are represented by forms modulo Δ.

We can now prove the Eureka theorem by applying the method used in [2].

5. *A proof of the Eureka theorem*

Theorem:

Every positive integer is the sum of at most three triangular numbers.

Proof:

Let n be a positive integer and define u to be the square-free part of $8n + 3$. Let $\Delta = -u$, then $\Delta \equiv 5 \pmod 8$ and

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

So, by the representation theorem and Lemma 3(i), there is a form $[a, b, c]$ such that $\gcd(a, \Delta) = 1$, $b^2 - 4ac = \Delta$ and $ax^2 + bxy + cy^2 \equiv -2 \pmod \Delta$.

Let $A = 2a$, $C = 2c$ and $u = -\Delta$ then A and u are coprime, $AC \equiv b^2 \pmod u$ and $A > 0$. Also, $(2ax + by)^2 + (4ac - b^2)y^2 \equiv -8a \pmod \Delta$ and so there is an integer X such that $-A \equiv X^2 \pmod u$.

Then X and u are coprime and so there is an integer Y such that $b \equiv XY \pmod u$ and $C \equiv -Y^2 \pmod u$.

Now consider the symmetric matrix

$$\boldsymbol{M} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{Y}{u} & -\frac{X}{u} & 1 \end{pmatrix}\begin{pmatrix} A & b & 0 \\ b & C & 0 \\ 0 & 0 & \frac{1}{u} \end{pmatrix}\begin{pmatrix} 1 & 0 & -\frac{Y}{u} \\ 0 & 1 & -\frac{X}{u} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} A & b & * \\ b & C & * \\ * & * & * \end{pmatrix}.$$

$|\boldsymbol{M}| = 1$ and the coefficients of $\boldsymbol{M}$ are the integers

$$A,\ b,\ C,\ -\frac{AY + bX}{u},\ -\frac{bY + CX}{u},\ \frac{(A + X^2)(C + Y^2) - (b - XY)^2}{u^2}.$$

https://doi.org/10.1017/mag.2024.15 Published online by Cambridge University Press

Note that $\begin{pmatrix} x & y & z \end{pmatrix}\begin{pmatrix} A & b & 0 \\ b & C & 0 \\ 0 & 0 & \frac{1}{u} \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \dfrac{(Ax+by)^2+uy^2}{A} + \dfrac{z^2}{u} \geqslant 0$, with equality if, and only if, $x = y = z = 0$. This property is called *positive-definiteness* and both $\boldsymbol{M}$ and any equivalent matrix will also be positive-definite.

By Lemma 5, $\boldsymbol{M}$ is equivalent to an integer matrix $\begin{pmatrix} r & s & t \\ s & * & * \\ t & * & * \end{pmatrix}$ with $r^2 \leqslant \sqrt{\frac{64|r|}{27}}$ and so $|r| = 0$ or 1. By positive definiteness, $r = 1$ and then

$$\begin{pmatrix} 1 & 0 & 0 \\ -s & 1 & 0 \\ -t & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & s & t \\ s & * & * \\ t & * & * \end{pmatrix}\begin{pmatrix} 1 & -s & -t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{N} \end{pmatrix}.$$

By similarly applying Lemma 2(ii) to $\boldsymbol{N}$ we see that $\boldsymbol{M}$ is equivalent to the identity matrix. Then $\boldsymbol{M^{-1}}$ is also equivalent to the identity matrix and so $\boldsymbol{M^{-1}} = \boldsymbol{YY^T}$ for some integer matrix $\boldsymbol{Y}$.

Let $\begin{pmatrix} \alpha & \beta & \gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}\boldsymbol{Y}$. Then, applying cofactors,

$$u = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}\boldsymbol{M^{-1}}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \alpha^2 + \beta^2 + \gamma^2.$$

Then $8n + 3$ is also the sum of three squares. Working modulo 8 these squares must all be odd, and so we have

$$8n + 3 = (2A + 1)^2 + (2B + 1)^2 + (2C + 1)^2$$
$$\Rightarrow n = \frac{A(A+1)}{2} + \frac{B(B+1)}{2} + \frac{C(C+1)}{2}.$$

'*EYPHKA*! *num*=Δ+Δ+Δ'; a truly astonishing result for a 19-year old to have proved.

References

1. C. F. Gauss, *Disquisitiones arithmeticae*, Yale Univ Press (1966).
2. D. E. Flath, *Introduction to number theory*, Wiley (1988).
3. S. W. Dolan, Nint reciprocity, *Math. Gaz.* **98** (July 2014), pp. 317-319.
4. D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley (2013).

10.1017/mag.2024.15 © The Authors, 2024
Published by Cambridge University Press
on behalf of The Mathematical Association

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