The three squares theorem & enchanted walks, w$^{\text{th}}$ various (mostly trivial) ruminations

France Dacar, Jožef Stefan Institute
France.Dacar@ijs.si

August 4, 2012
August 23, 2012 (corrected, slightly expanded)

We know that Fermat's two square theorem for integers can be retold, almost verbatim, as the corresponding theorem for rationals.[1] How about the sums of three squares?

Theorem 1 (The three squares theorem)**.** *An integer is a sum of three squares of integers if and only if it is non-negative and is not of the form $4^m(8k+7)$ for some natural numbers m and k.*

In particular, twice an odd natural number is always a sum of three integer squares. The four squares theorem is a straightforward consequence of Theorem 1:

Theorem 2 (Lagrange's four squares theorem)**.** *Every natural number is a sum of four squares of integers.*

Proof. Let $n \in \mathbb{N}$. If n is not of the form $4^m(8k+7)$, then it is a sum of three squares, hence a sum of four squares. If n is of the form $4^m(8k+7)$, then $n = (2^m)^2\big((8k+6)+1\big)$, where $8k+6 = 2\cdot(4k+3)$ is a sum of three squares, thus n is a sum of four squares. □

How can we use Theorem 1 to derive a characterization of sums of three squares of rational numbers? In its present form we can't. First we have to reformulate the theorem in terms of the prime factorization of a natural number that is not a sum of three squares of integers. Let $n = 4^m(8k+7)$ for some $m, k \in \mathbb{N}$, and let $n = \prod_p p^{e_p}$ be its prime factorization.[2] The condition on the number of prime factors 2 is clear: e_2 must be even. If on top of that the product of the odd primes in the factorization is $\equiv 7 \pmod 8$, we have a necessary and sufficient condition. Each odd prime is of the form $p = 8k + j$, where $j \in \{1, 3, 5, 7\}$. The set $J := \{1, 3, 5, 7\}$, regarded as a subset of $\mathbb{Z}/8\mathbb{Z}$, is the group $(\mathbb{Z}/8\mathbb{Z})^\times$ of invertible elements of the ring $\mathbb{Z}/8\mathbb{Z}$. The group J is an instance of the four-group: $3^2 = 5^2 = 7^2 = 1$, $3\cdot5 = 7$, $3\cdot7 = 5$, and $5\cdot7 = 3$. The product $3^{i_3}\cdot5^{i_5}\cdot7^{i_7}$, where $i_3, i_5, i_7 \in \{0, 1\}$, equals 7 if and only if $i_3 = i_5 = 1$ and $i_7 = 0$, or $i_3 = i_5 = 0$ and $i_7 = 1$.

[1] We know this from the essay [2].

[2] By convention, an index p will always run through the set of all primes.

For each $j \in J$ and every non-zero natural number n set $h_j(n) := \sum_{p \equiv j \pmod 8} e_p(n)$. Then we have the following characterization of (non)sums of three integral squares:

Theorem 3 (The three squares theorem, reformulated)**.** *A positive integer n is not a sum of three squares of integers if and only if $e_2(n)$ is even, and either (i) $h_3(n)$ and $h_5(n)$ are odd and $h_7(n)$ is even, or (ii) $h_3(n)$ and $h_5(n)$ are even and $h_7(n)$ is odd.*

We have omitted from the formulation of the theorem the trivial observations that a negative integer is not, while the integer 0 is, a sum of three squares of integers.

Since the condition in Theorem 3 depends only on the parities of the exponents in the prime factorization, it can be reused for rational numbers, provided that for every positive rational number $r = \prod_p p^{e_p(r)}$ and each $j \in J$ we define $h_j(r) := \sum_{p \equiv j \pmod 8} e_p(r)$.

Theorem 4 (The three squares theorem for rationals)**.** *A positive rational number r is not a sum of three squares of rational numbers if and only if $e_2(r)$ is even, and either (i) $h_3(r)$ and $h_5(r)$ are odd and $h_7(r)$ is even, or (ii) $h_3(r)$ and $h_5(r)$ are even and $h_7(r)$ is odd.*

We don't give the proof, which runs along the same lines as the proof of the Fermat's two square theorem for rationals. The following corollary of Theorems 3 an 4 is obvious:

Corollary 5. *If an integer is expressible as a sum of three squares of rational numbers, then it is expressible as a sum of three squares of integers.*

---*---*---*---

But we are doing this arse-forward. The well-known proof of the three squares theorem establishes the sufficiency of the condition stated in the theorem in two stages: first it shows that a positive integer n that is not of the form $4^m(8k+7)$ for some natural numbers m and k can be represented as a sum of three squares of rational numbers,[3] and then proceeds to show that n is actually a sum of three squares of integers. The story of how the latter is achieved is told at the beginning of the MathOverflow discussion [3]:

> Serre's *A Course in Arithmetic* gives essentially the following proof of the three-squares theorem, which says that an integer a is the sum of three squares if and only if it is not of the form $4^m(8n+7)$: first one shows that the condition is necessary, which is straightforward. To show it is sufficient, a lemma of Davenport and Cassels, using Hasse-Minkowski, shows that a is the sum of three rational squares. Then something magical happens:
>
> Let C denote the circle $x^2+y^2+z^2 = a$. We are given a rational point p on this circle. Round the coordinates of p to the closest integer point q, then draw

[3] This can be proved using the theory of Hasse-Minkowski, about which we won't have anything to say, not in this essay.

> the line through p and q, which intersects C at a rational point p'. Round the coordinates of p' to the closest integer point q', and repeat this process. A straightforward calculation shows that the least common multiples of the denominators of the points p, p', p'', ... are strictly decreasing, so this process terminates at an integer point on C.
>
> Bjorn Poonen, after presenting this proof in class, remarked that he had no intuition for why this should work. Does anyone have a reply?
>
> [Asked by Qiaochu Yuan Oct 29 2009 at 15:12]

That is, starting at a rational point of the sphere $x^2 + y^2 + z^2 = n$, we take an enchanted walk on the sphere, which reliably leads us to an integral point of the sphere. The "magic" underlying the walk is explained later on in the discussion:

> A few days ago Serre told me about some modest improvements to the proof, based on Weil's book *Number theory: an approach through history from Hammurapi to Legendre* and on a 1998 letter from Deligne to Serre; I will paraphrase these below.
>
> According to Weil (p. 292), the "magical" argument is due to an amateur mathematican: L. Aubry, *Sphinx-Œdipe* **7** (1912), 81–84. Here is a generalization that allows for a clearer proof.
>
> **Lemma:** Let $f = f_2 + f_1 + f_0 \in \mathbb{Z}[x_1, \ldots, x_n]$, where f_i is homogenous of degree i. Suppose that for every $\boldsymbol{x} \in \mathbb{Q}^n \smallsetminus \mathbb{Z}^n$ there exists $\boldsymbol{y} \in \mathbb{Z}^n$ such that $0 < |f_2(\boldsymbol{x} - \boldsymbol{y})| < 1$. If f has a zero in $\mathbb{Q}^n$, then it has a zero in $\mathbb{Z}^n$.
>
> Proof: If $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{Q}^n$, let $\operatorname{den}(\boldsymbol{x})$ denote the lcm of the denominators of the x_i. By iteration, the following claim suffices: If $\boldsymbol{x} \in \mathbb{Q}^n \smallsetminus \mathbb{Z}^n$ and $\boldsymbol{y} \in \mathbb{Z}^n$ satisfy $0 < |f_2(\boldsymbol{x} - \boldsymbol{y})| < 1$, and the line L through $\boldsymbol{x}$ and $\boldsymbol{y}$ intersects $f = 0$ in $\boldsymbol{x}$, $\boldsymbol{x}'$, then $\operatorname{den}(\boldsymbol{x}') < \operatorname{den}(\boldsymbol{x})$. By restricting to L and choosing a coordinate t on it taking the value 0 at $\boldsymbol{y}$ and integer values exactly on $L \cap \mathbb{Z}^n$, we reduce to proving the following: given $f(t) = At^2 + Bt + C \in Z[t]$ with zeros $x, x' \in \mathbb{Q}$ such that $0 < \left|Ax^2\right| < 1$, we have $\operatorname{den}(x') < \operatorname{den}(x)$. Proof: $0 < \left|Ax^2\right| < 1$ implies $0 < |A| < \operatorname{den}(x)^2$, and we have $xx' = C/A$, so $\operatorname{den}(x)\operatorname{den}(x') \leqslant |A| < \operatorname{den}(x)^2$, so $\operatorname{den}(x') < \operatorname{den}(x)$.
>
> [Bjorn Poonen Dec 31 2009 at 23:08]

(Note the time stamp... it's the mark of a true mathematician.) This is just a sketch of a proof, so let us expand it, working out the details. There is an error towards the end of the above proof sketch: if x and x' are rational numbers such that $xx' = C/A$, then it does not follow that $\operatorname{den}(x)\operatorname{den}(x') \leqslant |A|$, as demonstrated by $\frac{2}{3}\frac{3}{4} = \frac{1}{2}$. Our first undertaking will be the elimination of this glitch (quite possibly introduced by a too hasty paraphrasing — it *was* a New Year's Eve); we shall show that if x and x' are the two zeros of $At^2 + Bt + C$, then the product $\operatorname{den}(x)\operatorname{den}(x')$ divides $|A|$, so it is $\leqslant |A|$.

Every rational number has a unique representation as a reduced fraction $x = m/n$, where m and n are integers, $n > 0$, and $\gcd(m, n) = 1$; we write $\operatorname{den}(x) := n$.

Lemma 6. *Let a, b, c be integers, where $a \neq 0$. If the polynomial $at^2 + bt + c$ in t has a rational zero x, then the other zero x' is rational, and $|a| = \gcd(a, b, c)\operatorname{den}(x)\operatorname{den}(x')$.*

Proof. Clearly $x' = -b/a - x$ is rational. Let $x = m/n$, $x' = m'/n'$ be the reduced representations. Then x and x' are the zeros of the quadratic polynomial

$$nn'(t-x)(t-x') \;=\; nn't^2 - (mn'+nm')t + mm' \;\in\; \mathbb{Z}[t]\;. \tag{1}$$

We claim that the gcd of the coefficients of this polynomial is 1. Let p be any prime dividing both nn' and mm'. Supposing p divides n (the other case, with p dividing n', is treated similarly), then p does not divide m, hence divides m', hence does not divide n', and we see that p does not divide $mn' + nm'$.

It follows that, writing $k := \operatorname{sgn}(a)\gcd(a,b,c)$, we have $a = knn'$, $b = -k(mn'+nm')$, and $c = kmm'$. □

In the last step of the proof we silently used the following simple fact:

Lemma 7. *If $a_1, \ldots, a_d$ are integers with $\gcd(a_1,\ldots,a_d) = 1$, and $b_1, \ldots, b_d$ are integers such that $(b_1,\ldots,b_d) = \lambda\cdot(a_1,\ldots,a_d)$, then $|\lambda| = \gcd(b_1,\ldots,b_d)$.*

Proof. Since at least one of the integers a_i is not zero, λ is rational; let $\lambda = m/n$ be its reduced representation. For every index i the product $\lambda a_i = ma_i/n$ is an integer, thus n divides a_i; we conclude that $n = 1$ and hence $\lambda = m \in \mathbb{Z}$. But then $\gcd(b_1,\ldots,b_d) = |\lambda|\gcd(a_1,\ldots,a_d) = |\lambda|$. □

One consequence of this lemma is that every point $\boldsymbol{x} = (x_1,\ldots,x_d) \in \mathbb{Q}^d$ has a unique reduced representation $(x_1,\ldots,x_d) = (m_1/n,\ldots,m_d/n)$ (all denominators are n), where $m_1, \ldots, m_d$, n are integers, $n > 0$, and $\gcd(m_1,\ldots,m_d,n) = 1$; we write $\operatorname{den}(\boldsymbol{x}) := n$. It is clear that $\operatorname{den}(\boldsymbol{x}) = 1$ if and only if $\boldsymbol{x} \in \mathbb{Z}^d$, and that for all $\boldsymbol{x} \in \mathbb{Q}^d$ and all $\boldsymbol{z} \in \mathbb{Z}^d$ we have $\operatorname{den}(\boldsymbol{x}+\boldsymbol{z}) = \operatorname{den}(\boldsymbol{x})$. If $r \in \mathbb{Q}$ and $\boldsymbol{x} \in \mathbb{Q}^d$, then $\operatorname{den}(r\boldsymbol{x})$ divides $\operatorname{den}(r)\operatorname{den}(\boldsymbol{x})$.

We are ready to prove the lemma presented in the MathOverflow discussion.

Lemma 8 (Aubry-Davenport-Cassels-Weil-Deligne-Serre)**.** *Let $d > 0$ be a natural number, and let $f = f_2 + f_1 + f_0 \in \mathbb{Z}[x_1,\ldots,x_d]$, where f_i is homogenous of degree i. Suppose that for every $\boldsymbol{x} \in \mathbb{Q}^d \smallsetminus \mathbb{Z}^d$ there exists $\boldsymbol{y} \in \mathbb{Z}^d$ such that $0 < \big|f_2(\boldsymbol{x}-\boldsymbol{y})\big| < 1$. If f has a zero in $\mathbb{Q}^d$, then it has a zero in $\mathbb{Z}^d$.*

Proof. Let $\boldsymbol{x} \in \mathbb{Q}^d$ be a zero of f. If $\boldsymbol{x} \in \mathbb{Z}^d$, we are done, so suppose that $\boldsymbol{x} \notin \mathbb{Z}^d$. We shall prove that f has a zero $\boldsymbol{x}' \in \mathbb{Q}^d$ with $\operatorname{den}(\boldsymbol{x}') < \operatorname{den}(\boldsymbol{x})$; through iteration, this will also prove the lemma.

Write $n := \operatorname{den}(\boldsymbol{x})$. There exists $\boldsymbol{y} \in \mathbb{Z}^d$ such that $0 < \big|f_2(\boldsymbol{x}-\boldsymbol{y})\big| < 1$. Setting $\boldsymbol{u} := \boldsymbol{x} - \boldsymbol{y}$, we have $\operatorname{den}(\boldsymbol{u}) = \operatorname{den}(\boldsymbol{x}) = n$, hence $\boldsymbol{u} = \boldsymbol{r}/n$ for some $\boldsymbol{r} \in \mathbb{Z}^d$. The line in $\mathbb{R}^d$ through the points $\boldsymbol{x}$ and $\boldsymbol{y}$ has a parameterization $\boldsymbol{z}(t) := \boldsymbol{y} + t\boldsymbol{r}$, $t \in \mathbb{R}$, where $\boldsymbol{z}(0) = \boldsymbol{y}$ and $\boldsymbol{z}(1/n) = \boldsymbol{x}$. The function $F(t) := f\big(\boldsymbol{z}(t)\big)$ is a quadratic polynomial in the real variable t with integer coefficients: $F(t) = At^2 + Bt + C$ with $A, B, C \in \mathbb{Z}$. Since

$$z_i(t)z_j(t) \;=\; (y_i + tr_i)(y_j + tr_j) \;=\; r_ir_jt^2 + (y_ir_j + y_jr_i)t + y_iy_j\;,$$

we see that $A = f_2(\boldsymbol{r}) = n^2 f_2(\boldsymbol{u}) \neq 0$. The polynomial F has the rational zero $\tau := 1/n$,

so its other zero τ' is likewise rational and $\operatorname{den}(\tau)\operatorname{den}(\tau')$ divides A, whence $\operatorname{den}(\tau') \leqslant |A| / \operatorname{den}(\tau) = |A|/n$. Since $|A| = n^2\big|f_2(\boldsymbol{u})\big| < n^2$, we have $\operatorname{den}(\tau') \leqslant |A|/n < n$. The point $\boldsymbol{x}' := \boldsymbol{y} + \tau'\boldsymbol{r}$ is a zero of f, and $\operatorname{den}(\boldsymbol{x}') = \operatorname{den}(\tau'\boldsymbol{r})$ divides $\operatorname{den}(\tau')$, therefore $\operatorname{den}(\boldsymbol{x}') \leqslant \operatorname{den}(\tau') < n = \operatorname{den}(\boldsymbol{x})$. □

We did not follow the reasoning of the proof's sketch in MathOverflow quite faithfully: the integral points $\boldsymbol{y} + k\boldsymbol{r}$, $k \in \mathbb{Z}$, do lie on the line L through the points $\boldsymbol{x}$ and $\boldsymbol{y}$, but they may not be *all* the integral points on L. Write $s := \gcd(r_1, \ldots, r_d)$ and $\boldsymbol{q} := \boldsymbol{r}/s \in \mathbb{Z}^d$; then $L \cap \mathbb{Z}^d = \{\boldsymbol{y} + k\boldsymbol{q} \mid k \in \mathbb{Z}\}$, thus $\{\boldsymbol{y} + k\boldsymbol{r} \mid k \in \mathbb{Z}\}$ is the set of all integral points on L if and only if $s = 1$. We used the integral vector $\boldsymbol{r}$ as the unit step along the line L because this was good enough for our purpose: the important thing was that with the parameterization $\boldsymbol{z}(t) = \boldsymbol{y} + t\boldsymbol{r}$ we had $\boldsymbol{x} = \boldsymbol{z}(1/n)$, where $\operatorname{den}(1/n) = n = \operatorname{den}(\boldsymbol{x})$.

Let us see what happens if we do use $\boldsymbol{q}$, instead of $\boldsymbol{r}$, with the parameterization $\boldsymbol{z}_1(t_1) := \boldsymbol{y} + t_1\boldsymbol{q}$ of the line L. Now we have the quadratic polynomial $F_1(t_1) := f\big(\boldsymbol{z}_1(t_1)\big) = A_1t_1^2 + B_1t_1 + C_1$ in t_1 with integer coefficients, where $A_1 = f_2(\boldsymbol{q})$. Since $\boldsymbol{z}_1(t_1) = \boldsymbol{z}(t_1/s)$, we have $F_1(t_1) = F(t_1/s) = (A/s^2)t_1^2 + (B/s)t_1 + C$, and we see that $A = A_1s^2$, $B = B_1s$, and $C = C_1$. The two zeros of F_1 are $\tau_1 = s\tau = s/n$ and $\tau_1' = s\tau'$. Write $n' := \operatorname{den}(\tau_1')$, $g := \gcd(A_1, B_1, C_1)$, and $\varphi := \big|f_2(\boldsymbol{u})\big|$ (where $\boldsymbol{u} = \tau_1\boldsymbol{q}$). Then $\varphi = |A_1|\,\tau_1^2 = |A_1|\,s^2/n^2$, hence $|A_1| = \varphi n^2/s^2$, and $|A_1| = gnn'$ (by Lemma 6), hence $n' = |A_1|\,/gn = (\varphi/gs^2)\cdot n$. Since $\gcd(q_1, \ldots, q_d) = 1$, we have $\operatorname{den}(\boldsymbol{x}') = \operatorname{den}(\boldsymbol{y} + \tau_1'\boldsymbol{q}) = \operatorname{den}(\tau_1'\boldsymbol{q}) = \operatorname{den}(\tau_1') = n'$, thus

$$\operatorname{den}(\boldsymbol{x}') \;=\; n' \;=\; \frac{\varphi}{gs^2}\cdot n \;=\; \frac{\big|f_2(\boldsymbol{x}-\boldsymbol{y})\big|}{\gcd(A_1, B_1, C_1)\,\gcd(r_1, \ldots, r_n)^2}\,\operatorname{den}(\boldsymbol{x})\;. \tag{2}$$

One piece of information we can extract from (2) is this: if $\varphi = j/k$ is the reduced representation, then from $n' = jn/kgs^2$ we see that k divides n; that is, $\operatorname{den}\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big)$ divides $\operatorname{den}(\boldsymbol{x})$. We find this slightly surprising, till we remember that $\boldsymbol{x}$ is not just any rational point, that it is a rational zero of the polynomial $f = f_2 + f_1 + f_0$. Starting from this observation, we can prove, in a less roundabout way than above, that for every zero $\boldsymbol{x} \in \mathbb{Q}^d$ of f, and for any point $\boldsymbol{y} \in \mathbb{Z}^d$ whatsoever, $\operatorname{den}\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big)$ divides $\operatorname{den}(\boldsymbol{x})$: we have the reduced representation $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{r}/n$, the parameterization $\boldsymbol{z}(t) = \boldsymbol{y} + t\boldsymbol{r}$ (of a line if $\boldsymbol{y} \neq \boldsymbol{x}$, of a single point when $\boldsymbol{y} = \boldsymbol{x}$), and the polinomial $F(t) = f\big(\boldsymbol{z}(t)\big) = At^2 + Bt + C \in \mathbb{Z}[t]$ of degree at most two, where $F(1/n) = f\big(\boldsymbol{z}(1/n)\big) = f(\boldsymbol{x}) = 0$; then $f_2(\boldsymbol{x}-\boldsymbol{y}) = A/n^2 = -B/n - C$ and hence $\operatorname{den}\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big) = \operatorname{den}(B/n)$ divides $n = \operatorname{den}(\boldsymbol{x})$.

Let us look at some examples of enchanted walks on the sphere $x^2 + y^2 + z^2 = 179$, which contains, up to permutations and sign changes of coordinates, only three essentially different integral points $(1, 3, 13)$, $(3, 7, 11)$, and $(7, 7, 9)$. Given a rational (but not integral) point $\boldsymbol{x}$ on the sphere we round its coordinates to nearest integers and obtain the integral point $\boldsymbol{y} = \operatorname{round}(\boldsymbol{x})$ with $f_2(\boldsymbol{x}-\boldsymbol{y}) \leqslant \frac{3}{4}$ (where $f_2(x, y, z) = x^2 + y^2 + z^2$). We have to produce some interesting starting rational points on the sphere, preferably with large denominators. To achieve this, we use the following trick: let $\boldsymbol{a}$ be an integral point on the sphere $x^2 + y^2 + z^2 = n$; we choose a 'random' triple $\boldsymbol{v}$ of integers, lay the line through the point $\boldsymbol{a}$ in the direction $\boldsymbol{v}$, and compute the other point

$$\boldsymbol{a}' \;:=\; \boldsymbol{a} \;-\; 2\frac{\langle \boldsymbol{a}, \boldsymbol{v}\rangle}{\langle \boldsymbol{v}, \boldsymbol{v}\rangle}\,\boldsymbol{v}$$

$\big($$\langle -,-\rangle$ is the usual scalar product of triples$\big)$ at which the line intersects the sphere. It is possible that the point $\boldsymbol{a}'$ is integral; it is even possible (though not very probable) that $\boldsymbol{a}'=\boldsymbol{a}$, if the triple $\boldsymbol{v}$ is orthogonal to the triple $\boldsymbol{a}$ $\big($so that $\langle \boldsymbol{a},\boldsymbol{v}\rangle=0\big)$. If it happens that the point $\boldsymbol{a}'$ is integral, then, well, we try again. Using the anchor point $\boldsymbol{a}=(3,7,11)$ and a vector $\boldsymbol{v}$ with independent random integer coordinates uniformly distributed through the range $[-100\,..\,100]$, I obtained many enchanted walks on the sphere, and selected three to exhibit here:

$$\begin{aligned}
&\big(\tfrac{19769}{5915},\tfrac{45867}{5915},\tfrac{61385}{5915}\big),\ \big(-\tfrac{3231}{947},\tfrac{11935}{947},\tfrac{2765}{947}\big),\ \big(-\tfrac{1017}{79},\tfrac{275}{79},\tfrac{85}{79}\big),\ (-13,3,1)\ ; \qquad (3)\\
&\big(\tfrac{68371}{8459},\tfrac{45227}{8459},\tfrac{78027}{8459}\big),\ \big(\tfrac{5701}{1499},-\tfrac{18893}{1499},-\tfrac{3573}{1499}\big),\ \big(-\tfrac{447}{257},-\tfrac{371}{257},-\tfrac{3389}{257}\big),\\
&\qquad\big(-\tfrac{489}{77},\tfrac{493}{77},-\tfrac{761}{77}\big),\ \big(\tfrac{51}{23},-\tfrac{79}{23},-\tfrac{293}{23}\big),\ \big(\tfrac{29}{7},-\tfrac{51}{7},-\tfrac{73}{7}\big),\ (-3,7,11)\ ;\\
&\big(-\tfrac{5555}{645},-\tfrac{193}{645},-\tfrac{6601}{645}\big),\ \big(-\tfrac{605}{95},-\tfrac{193}{95},-\tfrac{1101}{95}\big),\ \big(-\tfrac{349}{29},-\tfrac{73}{29},-\tfrac{153}{29}\big),\\
&\qquad\big(-\tfrac{107}{9},-\tfrac{41}{9},-\tfrac{37}{9}\big),\ (-9,7,-7)\ .
\end{aligned}$$

It is instructive to look at the the values of φ, g, and s $\big($introduced in the discussion of "den$\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big)$ divides den$(\boldsymbol{x})$" above$\big)$ associated with the steps of these three walks:

$$\begin{aligned}
&\big(\tfrac{1894}{5915},2,1\big),\ \big(\tfrac{316}{947},1,2\big),\ \big(\tfrac{20}{79},5,2\big)\ ;\\
&\big(\tfrac{1499}{8459},1,1\big),\ \big(\tfrac{514}{1499},2,1\big),\ \big(\tfrac{77}{257},1,1\big),\ \big(\tfrac{23}{77},1,1\big),\ \big(\tfrac{7}{23},1,1\big),\ \big(\tfrac{2}{7},2,1\big)\ ;\\
&\big(\tfrac{38}{129},2,1\big),\ \big(\tfrac{29}{95},1,1\big),\ \big(\tfrac{9}{29},1,1\big),\ \big(\tfrac{2}{9},2,1\big)\ ;
\end{aligned}$$

the triples are (φ,g,s). We see that there are points on the three walks at which $g>1$ and/or $s>1$. Also note that at the starting point $\boldsymbol{x}$ of the third walk, den$\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big)$ is a proper divisor of den$(\boldsymbol{x})$.

At each step of an enchanted walk, the coordinates of a rational point are rounded to nearest integers using the "banker's rounding", with which a rational number lying precisely halfway between consecutive integers is always rounded to an even integer. At a rational point on the sphere which has at least one coordinate of the form $k+\frac{1}{2}$, $k\in\mathbb{Z}$, we have at least two, possibly four or eight, different choices of rounding the point. But are there any such points? There aren't. Suppose $u^2+v^2+\big(k+\frac{1}{2}\big)^2=n$, where u and v are rational numbers while k and n are integers. Then $(2u)^2+(2v)^2=4n-(2k+1)^2\equiv 3 \pmod 4$. If x and y are integers, then x^2+y^2 is congruent to 0, 1, or 2 modulo 4; therefore, if m is an integer $\equiv 3 \pmod 4$, the equation $x^2+y^2=m$ has no integral solutions, hence has no rational solutions by (the corollary to) the Fermat's two square theorem for rationals.

Note that we are not *required* to round the coordinates of a rational point $\boldsymbol{x}$ on the sphere to nearest integers in order to obtain the integral point $\boldsymbol{y}$, since what we actually need to make a magic step is $\big|f_2(\boldsymbol{x}-\boldsymbol{y})\big|<1$; for example, if $\boldsymbol{x}=\big(i+\frac{1}{3},j+\frac{1}{3},k-\frac{1}{3}\big)$ with $i,j,k\in\mathbb{Z}$, then we have the following candidates for $\boldsymbol{y}$: $(i,j,k)=\text{round}(\boldsymbol{x})$, $(i+1,j,k)$, $(i,j+1,k)$, and $(i,j,k-1)$. We have chosen to always round the coordinates because this operation is simple to describe (and always does the job).

As I have already mentioned, I generated quite a few enchanted walks on the sphere $x^2+y^2+z^2=179$. I observed lengths of walks, trying to come up with some predictor of the expected length of a walk, knowing only the denominator of its starting point. I was surprised to find that a significant proportion — mostly between 7.5% and 8.5% — of walks had length 1, that is, they stepped directly from a rational point to an integral

point. Here are three such one-step walks (generated using an integer vector $\boldsymbol{v}$ with independent random coordinates uniformly distributed through the range $[-1000\,..\,1000]$):

$$\begin{aligned}
&\left(-\tfrac{614201}{702013}, \tfrac{1844631}{702013}, \tfrac{9188867}{702013}\right), \ \ (-1,3,13)\,;\\
&\left(\tfrac{5869209}{825257}, \tfrac{2066327}{825257}, \tfrac{9120881}{825257}\right), \ \ (7,3,11)\,;\\
&\left(\tfrac{10154653}{1509809}, \tfrac{13716531}{1509809}, \tfrac{10806223}{1509809}\right), \ \ (7,9,7)\,.
\end{aligned}$$

I was rather mystified by this strange phenomenon, until I thought of looking at details of such one-step walks, and then the mystery disappeared: I found that $\mathrm{round}(\boldsymbol{x}) = \boldsymbol{x}'$ for all such walks with large enough $\mathrm{den}(\boldsymbol{x})$. There also exist magic steps from $\boldsymbol{x}$ to $\mathrm{round}(\boldsymbol{x})$ with a not-so-large $\mathrm{den}(\boldsymbol{x})$; for example, the last step of the walk (3) is from $\boldsymbol{x} = \left(-\frac{1017}{79}, \frac{275}{79}, \frac{85}{79}\right)$ to $\mathrm{round}(\boldsymbol{x}) = (-13,3,1)$.

So, one way to finish an enchanted walk is to hit a rational point on the sphere that is close enough to an integral point on the sphere, and then to take the last step to that integral point. 'Close enough' means the following: let $Q := \left(-\frac{1}{2}\,..\,\frac{1}{2}\right)^3$ be the open unit cube centered at the origin; then a rational point $\boldsymbol{x}$ on a sphere $x^2+y^2+z^2=n$ (which is assumed to possess rational points) is 'close enough' to an integral point $\boldsymbol{y}$ on the sphere if $\boldsymbol{x} \in \boldsymbol{y} + Q$. There are $48+48+24 = 120$ integral points on the sphere $x^2+y^2+z^2=179$; the proportion α of the surface area $4\pi\cdot 179$ of the sphere that lies inside the cubes $\boldsymbol{a}+Q$ for integral points $\boldsymbol{a}$ on the sphere is small, but not extremely small: $\alpha \doteq 0.0618$. This is smaller than 0.075 (the lower end of the range from 7.5% to 8.5%), which is understandable because the procedure which 'randomly' generates rational points on the sphere does not distribute them uniformly across the sphere — far from uniformly, in fact.

The other way of making the last step of an enchanted walk is from a 'sharpshooter' point, which is a rational non-integral point $\boldsymbol{x}$ on the sphere that rounds to an integral point $\boldsymbol{y}$ *not* on the sphere such that the line through the points $\boldsymbol{x}$ and $\boldsymbol{y}$ hits the sphere at an integral point $\boldsymbol{x}'$. There are only finitely many sharpshooter points $\boldsymbol{x}$ on any sphere $x^2+y^2+z^2=n$: the distance r of the integral point $\boldsymbol{y} = \mathrm{round}(\boldsymbol{x})$ from the origin must be in the range $\sqrt{n} - \frac{1}{2}\sqrt{3} < r < \sqrt{n} + \frac{1}{2}\sqrt{3}$ (while $r \neq \sqrt{n}$), and at the same time $\boldsymbol{x}$ must lie on the line connecting the point $\boldsymbol{y}$ to an integral point on the sphere; since there are only finitely many possible integral points $\boldsymbol{y}$ satisfying the stated conditions, and also the set of integral points on the sphere is finite, there are only finitely many possibilities for $\boldsymbol{x}$. For example, our sphere $x^2+y^2+z^2=179$ possesses 207456 sharpshooter points. It would be unpractical to list all of them, but we can exhibit at least a few, together with their targets:

$$\begin{aligned}
&\left(-\tfrac{31}{3}, -\tfrac{25}{3}, \tfrac{5}{3}\right),\ \left(-\tfrac{19}{3}, \tfrac{31}{3}, \tfrac{17}{3}\right),\ \left(-\tfrac{715}{729}, -\tfrac{2867}{729}, -\tfrac{9295}{729}\right) : && (1,3,13)\,;\\
&\left(-\tfrac{5}{3}, \tfrac{35}{3}, \tfrac{19}{3}\right),\ \left(\tfrac{11}{3}, \tfrac{23}{3}, \tfrac{31}{3}\right),\ \left(-\tfrac{3565}{737}, -\tfrac{3505}{737}, -\tfrac{8499}{737}\right) : && (3,7,11)\,;\\
&\left(-\tfrac{25}{3}, -\tfrac{25}{3}, -\tfrac{19}{3}\right),\ \left(\tfrac{11}{3}, \tfrac{11}{3}, \tfrac{37}{3}\right),\ \left(-\tfrac{5005}{753}, -\tfrac{5005}{753}, -\tfrac{7169}{753}\right) : && (7,7,9)\,.
\end{aligned}$$

For each of the three target points on the right we listed the only two sharpshooter points with the least possible denominator (which is 3 in all cases) and the only sharpshooter point with the largest possible denominator. We see that if the denominator of a rational point $\boldsymbol{x}$ on the sphere is greater than 753, and a single magic step gets us from $\boldsymbol{x}$ to an integral point on the sphere, then that integral point is $\mathrm{round}(\boldsymbol{x})$.

Is 3 always the least denominator > 1 of a rational point on a sphere $x^2+y^2+z^2 = n$ (where n is a positive integer, and the sphere is assumed to contain rational points...)? The least denominator cannot be 2, because no rational point on the sphere can have any of the three coordinates of the form $k+\frac{1}{2}$, $k \in \mathbb{Z}$. (What is more, denominators of all rational points on the sphere are odd integers; indeed, if $(m_1, m_2, m_3)/n$ is the reduced representation of some rational point (x, y, z), and n is even, then the denominator of the fraction $(m_1^2+m_2^2+m_3^2)/n^2$ is divisible by 4 while the numerator isn't, thus $x^2+y^2+z^2$ is not an integer.) The answer to our question is "yes"; even more is true:

If a sphere $x^2+y^2+z^2 = n$, where n is a positive integer, contains rational points, then for every positive integer j it contains a rational point $\boldsymbol{x}$ with $\mathrm{den}(\boldsymbol{x}) = 3^j$.

I leave this as an entertaining problem for the reader, with the following hint: starting at an integral point on the sphere, take a walk around the sphere, with each step made in a direction wisely chosen from the set $\{-1, 1\}^3$.

---*---*---*---

When we tried to figure out a characterization of the sums of three rational squares, it was very obliging of the group J to turn out to be a four-group, which made possible to reformulate the condition in Theorem 1 to the one in Theorem 3, which then led to Theorem 4 and Corollary 5. Were we just lucky, or what? Actually, there was no luck involved. For any quadratic form[4] with integer coefficients the following two conditions are equivalent:

- ◇ if an integer is the form's value for some rational arguments, then it is also the form's value for some integer arguments;
- ◇ the set of all form's values for integer arguments is describable in terms of parities of exponents in the prime factorization, and of the sign, of an integer.

Moreover, when a quadratic form satisfies (either one of) these two conditions, then the set of all form's values for rational arguments has the same description in terms of prime factor parities (and the sign) as the set of all form's values for integer arguments.

This is all rather vague, so let us precisely define relevant notions[5] and then properly formulate (and prove) the above assertions.

Every non-zero rational number r has a unique prime factorization

$$r \;=\; \mathrm{sgn}(r) \prod_p p^{e_p(r)} \;,$$

where $\mathrm{sgn}(r) \in \{-1, 1\}$, and the exponents $e_p(r)$ are integers, only finitely many of them non-zero. (We have already used this factorization.) A non-zero rational number is an integer if and only if all exponents in its prime factorization non-negative.

[4] In this essay, "a form" is synonimous with "a homogenous polynomial".

[5] Be warned that some notions and notation appearing in this essay are provisional, made up on the spot solely for the needs of the essay.

We shall say that two rational numbers r and s **have the same prime factor parities**,[6] and write r *pfpar* s, if either $r = s = 0$, or both r and s are non-zero and

$$\operatorname{sgn}(r) = \operatorname{sgn}(s) \qquad \text{and} \qquad e_p(r) \equiv e_p(s) \pmod 2 \ \text{ for every prime p}\,.$$

The relation *pfpar* is an equivalence relation on $\mathbb{Q}$, and its restriction to integers is an equivalence relation on $\mathbb{Z}$. For any non-zero rational number r, the integer

$$\operatorname{core}(r) \ := \ \operatorname{sgn}(r) \prod_p p^{e_p(r) \bmod 2}$$

is called the **square-free core** of the number r; we also define $\operatorname{core}(0) := 0$. Note that for every non-zero rational number r, the integer $\operatorname{core}(r)$ is the unique square-free integer that has the same prime factor parities as r. The set $\operatorname{core}(\mathbb{Q}) = \operatorname{core}(\mathbb{Z})$, which consists of the square-free integers and the integer 0, is the set of 'canonical' representatives of equivalence classes of the equivalence relation *pfpar* (and also of the restriction of *pfpar* to integers).

The following facts are self-evident and need no proving:

Lemma 9. *Let r and s be rational numbers. The following conditions are equivalent to each other:*

- *r pfpar s;*
- *$r = t^2 s$ for some non-zero rational number t;*
- *$m^2 r = n^2 s$ for some non-zero integers m and n;*
- $\operatorname{core}(r) = \operatorname{core}(s)$.

If r is a non-zero rational number, then $r/\operatorname{core}(r)$ is a square of a rational number; if n is a non-zero integer, then $n/\operatorname{core}(n)$ is a square of an integer.

We shall say that a property ϱ of rational numbers (or, a property σ of integers) **depends only on prime factor parities** if r *pfpar* s implies $\varrho(r) \iff \varrho(s)$ for all $r, s \in \mathbb{Q}$ (resp. m *pfpar* n implies $\sigma(m) \iff \sigma(n)$ for all $m, n \in \mathbb{Z}$). We shall say that a set R of rational numbers (or, a set S of integers) is **describable in terms of prime factor parities** if the property $r \in R$ of a rational number r (resp. the property $n \in S$ of an integer n) depends only on prime factor parities.[7]

A set of rational numbers (or, of integers) is describable in terms of prime factor parities if and only if it is a union of equivalence classes of the equivalence relation *pfpar* (resp. of the restriction of *pfpar* to integers). And here are more self-evident facts:[8]

[6] This is quite a mouthful, and still it does not tell it all, since we should say "have the same prime factor parities *and the same sign*". We shall always have to add "and the same sign" under our breath. And besides that, parities are of course not of prime factors themselves but of their exponents in a prime factorization. Blech... Well, we'll somehow manage to live with it for a while.

[7] A subset of integers is of course also a subset of rationals, so we have an ambiguity here. We could remove the ambiguity by saying "$R \subseteq \mathbb{Q}$ is describable etc. in $\mathbb{Q}$" and "$S \subseteq \mathbb{Z}$ is describable etc. in $\mathbb{Z}$", or something like that. However, we let it be, since we will always know what we are talking about.

[8] I apologize for this surfeit of trivia. It is better to have these facts, however trivial, out in the open, than to implicitly use them wrong way up in some heedless "it is obvious that..." conclusion.

Lemma 10. *A set R of rational numbers is describable in terms of prime factor parities (1) if and only if for every $r \in \mathbb{Q}$ and every $t \in \mathbb{Q} \smallsetminus \{0\}$, $r \in R$ implies $t^2 r \in R$,*
(2) if and only if for every $r \in \mathbb{Q}$ and every $k \in \mathbb{Z} \smallsetminus \{0\}$, $r \in R$ is equivalent to $k^2 r \in R$.

A set S of integers is describable in terms of prime factor parities if and only if for every $n \in \mathbb{Z}$ and every $k \in \mathbb{Z} \smallsetminus \{0\}$, $n \in S$ is equivalent to $k^2 n \in S$.

One consequence of the characterization (1) is that for any subset Q of $\mathbb{Q}$ the set $\{t^2 q \mid q \in Q,\, t \in \mathbb{Q} \smallsetminus \{0\}\}$ is the least subset of $\mathbb{Q}$ that contains Q and is describable in terms of prime factor parities.

Lemma 11. *A set R of rational numbers (or, a set S of integers) is describable in terms of prime factor parities if and only if there exists a subset T of* $\mathrm{core}(\mathbb{Q})$ *(*$= \mathrm{core}(\mathbb{Z})$*) such that $R = \{r \in \mathbb{Q} \mid \mathrm{core}(r) \in T\}$ (resp. $S = \{n \in \mathbb{Z} \mid \mathrm{core}(n) \in T\}$), in which case $T = \mathrm{core}(R) \subseteq R$ (resp. $T = \mathrm{core}(S) \subseteq S$).*

Now we can precisely define what it means that a set R of rational numbers **has the same description in terms of prime factor parities** (and the sign ...) as a set S of integers: it means that there exists a subset T of $\mathrm{core}(\mathbb{Z})$ such that

$$S \;=\; \{n \in \mathbb{Z} \mid \mathrm{core}(n) \in T\} \quad \text{and} \quad R \;=\; \{r \in \mathbb{Q} \mid \mathrm{core}(r) \in T\}\ ;$$

we shall write this as $S \propto R$.[9] The set $T = \mathrm{core}(S) = \mathrm{core}(R)$ in the definition embodies the common "description in terms of prime factor parities" of the sets S and R.

To give an example, we describe the core set $T := \mathrm{core}(\mathrm{Im}_{\mathbb{Z}}\, g)$ for the three squares form $g = x^2 + y^2 + z^2$. An integer n belongs to T if and only if

- $n = 0$, or
- $n = 2m$, where m is a product of distinct odd primes, or
- n is a product of distinct odd primes, where either $h_3(n) \not\equiv h_5(n) \pmod 2$ or $h_3(n) \equiv h_5(n) \equiv h_7(n) \pmod 2$.

In the last case above $h_j(n)$ is the count of distinct primes $\equiv j \pmod 8$ that divide n.

Here comes the last installment of prime-factor-parities trivia:

Lemma 12. *Let $S \subseteq \mathbb{Z}$ and $R \subseteq \mathbb{Q}$.*

If $S \propto R$, then both S and R are describable in terms of prime factor parities, and $S = \mathbb{Z} \cap R$, $R = \{n/k^2 \mid n \in S,\, k \in \mathbb{Z} \smallsetminus \{0\}\} = \{t^2 n \mid n \in S,\, t \in \mathbb{Q} \smallsetminus \{0\}\}$.

If R is describable in terms of prime factor parities, then $\mathbb{Z} \cap R \propto R$. If S is describable in terms of prime factor parities, then $S \propto \{n/k^2 \mid n \in S,\, k \in \mathbb{Z} \smallsetminus \{0\}\}$.

If $\mathbb{Z} \cap R = S$ and $R = \{t^2 n \mid n \in S,\, t \in \mathbb{Q} \smallsetminus \{0\}\}$, then $S \propto R$.

And *now* for something completely different. (☺)

[9] Sorry, just grabbed the first remotely suitable symbol that came to hand. Some notation in this essay is provisional, remember.

Let $d \in \mathbb{N}$, $d > 0$, and let $g \in \mathbb{Z}[x_1, \ldots, x_d]$ be a quadratic form.

We shall say that g is a **$\mathbb{QZ}$-form** if every integer that is a value of g at some rational point $\boldsymbol{x} \in \mathbb{Q}^d$ is also a value of g at some integral point $\boldsymbol{y} \in \mathbb{Z}^d$.[10]

We shall write $\operatorname{Im}_{\mathbb{Z}} g := g(\mathbb{Z}^d)$ and $\operatorname{Im}_{\mathbb{Q}} g := g(\mathbb{Q}^d)$.

Since $r \in \operatorname{Im}_{\mathbb{Q}} g$ and $t \in \mathbb{Q} \smallsetminus \{0\}$ imply $t^2 r \in \operatorname{Im}_{\mathbb{Q}} g$, the set $\operatorname{Im}_{\mathbb{Q}} g$ is describable in terms of prime factor parities. Since $n \in \operatorname{Im}_{\mathbb{Z}} g$ and $k \in \mathbb{Z} \smallsetminus \{0\}$ imply $k^2 n \in \operatorname{Im}_{\mathbb{Z}} g$, the set $\operatorname{Im}_{\mathbb{Z}} g$ is describable in terms of prime factor parities if and only if it **passes the desquaring test**: for all $n \in \mathbb{Z}$ and all $k \in \mathbb{Z} \smallsetminus \{0\}$, $k^2 n \in \operatorname{Im}_{\mathbb{Z}} g$ implies $n \in \operatorname{Im}_{\mathbb{Z}} g$.

Clearly $\operatorname{Im}_{\mathbb{Z}} g \subseteq \mathbb{Z} \cap \operatorname{Im}_{\mathbb{Q}} g$. Moreover, $\operatorname{Im}_{\mathbb{Q}} g = \{n/k^2 \mid n \in \operatorname{Im}_{\mathbb{Z}} g,\, k \in \mathbb{Z} \smallsetminus \{0\}\} = \{t^2 n \mid n \in \operatorname{Im}_{\mathbb{Z}} g,\, t \in \mathbb{Q} \smallsetminus \{0\}\}$.

The folowing result relates $\mathbb{QZ}$-ness of quadratic forms with integer coefficients to describability in terms of prime factor parities.

Lemma 13. *Let $d \in \mathbb{N}$, $d > 0$. For any quadratic form $g \in \mathbb{Z}[x_1, \ldots, x_d]$ the following three properties are equivalent to each other:*

- *g is a $\mathbb{QZ}$-form;*
- *$\operatorname{Im}_{\mathbb{Z}} g$ passes the desquaring test;*
- *$\operatorname{Im}_{\mathbb{Z}} g \propto \operatorname{Im}_{\mathbb{Q}} g$.*

Proof. Each of the three properties is equivalent to $\operatorname{Im}_{\mathbb{Z}} g = \mathbb{Z} \cap \operatorname{Im}_{\mathbb{Q}} g$. □

The quadratic forms x^2, $x^2 + y^2$, and $x^2 + y^2 + z^2$ are $\mathbb{QZ}$-forms. If m is a nonzero integer, when precisely is the form mx^2, or $m(x^2 + y^2)$, or $m(x^2 + y^2 + z^2)$, a $\mathbb{QZ}$-form? The following proposition provides an answer to this kind of questions.

Proposition 14. *Suppose $S \subseteq \mathbb{Z}$ contains a non-zero integer, and let m be a non-zero integer. The set mS is describable in terms of prime factor parities if and only if the set S is describable in terms of prime factor parities and m is square-free and coprime to every non-zero integer in $\operatorname{core}(S)$, and in such a case $\operatorname{core}(mS) = m \operatorname{core}(S)$.*

Proof. The assertion of the proposition is true for the set S if and only if it is true for the set $S \smallsetminus \{0\}$, thus we can assume that $0 \notin S$ and $S \neq \varnothing$.

Suppose that mS is describable in terms of prime factor parities. Let k be any non-zero integer; for every integer n we have the chain of equivalences

$$n \in S \iff mn \in mS \iff mnk^2 \in mS \iff nk^2 \in S\ ,$$

which proves that S is describable in terms of prime factor parities. There exists in S an integer n_0 of the least absolute value among the integers in S (note that $n_0 \neq 0$); then mn_0 has the least absolute value among the integers in mS, so it must be square-free, since otherwise a desquaring of mn_0 in mS would give an integer in mS of smaller absolute value than mn_0; this proves that m is square-free. Consider any $n \in \operatorname{core}(S)$; we have to prove that m and n are coprime. Suppose, to the contrary, that a prime p

[10] $\mathbb{QZ}$: as on $\mathbb{Q}^d$ so on $\mathbb{Z}^d$. See? Pronounced same as "quiz".

divides both m and n; desquaring $mn \in mS$ in mS gives us $mn/p^2 \in mS$, which is impossible, because mn/p^2 is no longer divisible by p, so it is not divisible by m.

Now suppose that S is describable in terms of prime factor parities and that m is square-free and coprime to all integers in $\mathrm{core}(S)$. Let k be any non-zero integer. Since $k^2S \subseteq S$, we have $k^2 \cdot mS \subseteq mS$. Suppose that $k^2n \in mS$; we have to show that $n \in mS$. There exist $n' \in \mathrm{core}(S)$ and a non-zero integer j so that $k^2n = mn'j^2$. Since m and n' are square-free and coprime, it follows that $mn' = \mathrm{core}(mn'j^2) = \mathrm{core}(k^2n) = \mathrm{core}(n)$, thus $n = mn'l^2$ for some non-zero integer l, which proves that $n \in mS$ because $n'l^2 \in S$. We have proved that mS is describable in terms of prime factor parities. Elements of $m\,\mathrm{core}(S) \subseteq mS$ are fixed by $\mathrm{core}(-)$, thus $m\,\mathrm{core}(S)$ is a subset of $\mathrm{core}(mS)$. To prove the opposite inclusion, let $n \in S$; in order to show that $\mathrm{core}(mn) \in m\,\mathrm{core}(S)$, just note that $n = n'j^2$ for $n' = \mathrm{core}(n)$ and for some non-zero integer j, whence $\mathrm{core}(mn) = \mathrm{core}(mn'j^2) = mn' = m\,\mathrm{core}(n)$. □

We have excluded the trivial cases when $S \subseteq \{0\}$ or $m = 0$, because they behave differently. If $S \subseteq \{0\}$ $\big($that is, $S = \varnothing$ or $S = \{0\}\big)$, then S is certainly describable in terms of prime factor parities, and so is $mS = S$ for every integer m. If $m = 0$, then $mS \subseteq \{0\}$ for every $S \subseteq \mathbb{Z}$.

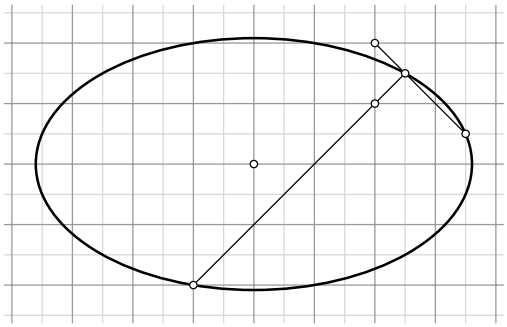
The central result of Proposition 14 can be rephrased as follows. For any set T of integers we denote by $P(T)$ the set of all prime divisors of non-zero integers in T. Suppose $S \subseteq \mathbb{Z}$ contains a non-zero integer and is describable in terms of prime factor parities, and let m be a non-zero integer; then mS is describable in terms of prime factor parities if and only if m is $\pm$ a product of distinct primes not in $P\big(\mathrm{core}(S)\big)$.

If g is a $\mathbb{QZ}$-form and m is a non-zero integer, then $\mathrm{Im}_{\mathbb{Z}}\, mg = m\,\mathrm{Im}_{\mathbb{Z}}\, g$, so we must look at $T = \mathrm{core}(\mathrm{Im}_{\mathbb{Z}}\, g)$ to determine the integers m for which mg a $\mathbb{QZ}$-form. With $g = x^2$ we have $T = \{0, 1\}$ and $P(T) = \varnothing$, and we see that mg is a $\mathbb{QZ}$-form if and only if m is square-free. When $g = x^2 + y^2$, we know from the Fermat's two square theorem that $P(T)$ consists of the prime 2 and the primes $\equiv 1 \pmod 4$, thus the form mg is $\mathbb{QZ}$ if and only if m is $\pm$ a product of distinct primes $\equiv 3 \pmod 4$. And finally, when $g = x^2 + y^2 + z^2$, the three squares theorem tells us that $2p \in T$ for every odd prime p, so $P(T)$ is the set of all primes, whence the form mg is $\mathbb{QZ}$ if and only if $m = \pm 1$.

Let us look at some more $\mathbb{QZ}$-forms.

The form $g = x^2 + 2y^2$ is $\mathbb{QZ}$ by Lemma 8 since $0 < g\big(x - \mathrm{round}(x),\, y - \mathrm{round}(y)\big) \leqslant \frac{3}{4}$ for every rational non-integral point (x, y). In order to determine $S = \mathrm{Im}_{\mathbb{Z}}\, g$ we consider the ring $R = \mathbb{Z}\big[\sqrt{-2}\,\big]$ of algebraic integers of the field $K = \mathbb{Q}\big(\sqrt{-2}\big)$. The norm of an algebraic integer $a + b\sqrt{-2}$ is $g(a, b)$, so the ring R is norm-Euclidean, hence a PID. The rational prime 2 factors in R as $2 = -\big(\sqrt{-2}\big)^2$, where $\sqrt{-2}$ is a prime of R (that is, 2 is **ramified**), every rational prime $p \equiv 1, 3 \pmod 8$ is the product $p = \pi\overline{\pi}$ of a pair of non-associated conjugate primes π and $\overline{\pi}$ of R (p **splits**), while the rational primes $\equiv 5, 7 \pmod 8$ are also primes of R (they are **inert**). From this we obtain the following description of the set S in terms of prime factor parities: an integer n belongs to S if and only if either $n = 0$, or $n > 0$ and $e_p(n)$ is even for every prime $p \equiv 5, 7 \pmod 8$. The set $P\big(\mathrm{core}(S)\big)$ consists of the prime 2 and all primes $\equiv 1, 3 \pmod 8$, therefore mg is a $\mathbb{QZ}$-form, for a non-zero integer m, if and only if m is $\pm$ a product of distinct primes $\equiv 5, 7 \pmod 8$.

The form $g = x^2 + 3y^2$ is a $\mathbb{QZ}$-form; we can show this by slightly augmenting the proof of Lemma 8. For every rational non-integral point (x, y) there exists an integral point (a, b) with $|x-a| \leqslant \frac{1}{2}$ and $|y-b| \leqslant \frac{1}{2}$ so that $0 < q(x-a, y-b) \leqslant 1$, with the equality if and only if both x and y are exactly halfway between successive integers. Starting at a rational point on an ellipse $x^2 + 3y^2 = n$ (n a positive integer), we walk an enchanted walk, which either ends in an integral point on the ellipse, or gets stuck in a point of the form $(x, y) = \big(a+\frac{1}{2}, b+\frac{1}{2}\big)$ with $a, b \in \mathbb{Z}$. In the latter case we can still step to an integral point on the ellipse, provided we make this last step with care: if the integer $a + b$ is odd, we step along the line through the points (x, y) and (a, b), and if $a + b$ is even, we step along the line through the points (x, y) and $(a, b+1)$. For example, consider the point $\big(\frac{5}{2}, \frac{3}{2}\big) = \big(2+\frac{1}{2}, 1+\frac{1}{2}\big)$ on the ellipse $x^2 + 3y^2 = 13$:



Since the sum $2+1$ is odd, we step from the point $\big(\frac{5}{2}, \frac{3}{2}\big)$ through the point $(2, 1)$ to the integral point $(-1, -2)$ on the ellipse; on the other hand, if we round the point $\big(\frac{5}{2}, \frac{3}{2}\big)$ to the integral point $(2, 2)$, the step in the direction of this other point lands us in another halfway point $\big(\frac{7}{2}, \frac{1}{2}\big)$ on the ellipse.

Why this works? We'd better begin with considering an arbitrary quadratic form $g \in \mathbb{Z}[x_1, \ldots, x_d]$. We associate with the quadratic form g the bilinear form with integer coefficients $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_g := g(\boldsymbol{x} + \boldsymbol{y}) - g(\boldsymbol{x}) - g(\boldsymbol{y})$. Suppose we have a point $\boldsymbol{x} \in \mathbb{Q}^d$ with $g(\boldsymbol{x}) = n \in \mathbb{Z}$, and let $\boldsymbol{v} \in \mathbb{Q}^d$ be a vector that is not a zero of g. For every $t \in \mathbb{Q}$ the point $\boldsymbol{z}(t) := \boldsymbol{x} + t\boldsymbol{v}$ lies on the line L laid through the point $\boldsymbol{x}$ in the direction $\boldsymbol{v}$, and

$$g\big(\boldsymbol{z}(t)\big) \;=\; g(\boldsymbol{x}) \,+\, \langle \boldsymbol{x}, \boldsymbol{v} \rangle_g \, t \,+\, g(\boldsymbol{v})\, t^2 \;.$$

The equation $g\big(\boldsymbol{z}(t)\big) = n$ has two rational roots, $t = 0$ and $t = \tau := -\langle \boldsymbol{x}, \boldsymbol{v} \rangle_g / g(\boldsymbol{v})$. There are two points (possibly identical) $\boldsymbol{y}$ on the line L that satisfy the equation $g(\boldsymbol{y}) = n$: one is $\boldsymbol{x} = \boldsymbol{z}(0)$, and the other one is

$$\boldsymbol{x}' \;:=\; \boldsymbol{z}(\tau) \;=\; \boldsymbol{x} \,-\, \frac{\langle \boldsymbol{x}, \boldsymbol{v} \rangle_g}{g(\boldsymbol{v})}\, \boldsymbol{v} \;.$$

The bilinear form associated with the quadratic form $g(x_1, x_2) = x_1^2 + 3x_2^2$ is

$$\big\langle (x_1, x_2)\,, (y_1, y_2) \big\rangle_g \;=\; 2 \cdot (x_1 y_1 + 3 x_2 y_2) \;.$$

Suppose that a point $\boldsymbol{x} \in \mathbb{Q}^2$ satisfies $g(\boldsymbol{x}) = n$, with n a positive integer, and that it has both coordinates halfway between integers. We can always choose a point $\boldsymbol{y} \in \mathbb{Z}^2$ so that $x_1 = y_1 + \frac{1}{2}$, $x_2 = y_2 + \frac{1}{2}\sigma$ with $\sigma \in \{-1, 1\}$, and the sum $y_1 + y_2$ is an odd integer. We step from the point $\boldsymbol{x}$ in the direction $\boldsymbol{v} := (1, \sigma)$ to the other point $\boldsymbol{x}'$ satisfying $g(\boldsymbol{x}') = n$, where

$$\boldsymbol{x}' \;=\; \boldsymbol{x} \,-\, 2\frac{\big(y_1+\frac{1}{2}\big) + 3\big(y_2+\frac{1}{2}\sigma\big)\sigma}{1+3\sigma^2} \cdot (1, \sigma) \;=\; \boldsymbol{x} \,-\, \Big(\tfrac{1}{2}(y_1 + 3\sigma y_2) + 1\Big) \cdot (1, \sigma) \;\;;$$

since $y_1 + 3\sigma y_2$ is an odd integer, the vector subtracted from the point $\boldsymbol{x}$ has both coordinates halfway between integers, thus the result $\boldsymbol{x}'$ is an integral point.

What is the description of the set $\mathrm{Im}_{\mathbb{Z}}\, g$ in terms of prime factor parities?

In order to answer this question we introduce the quadratic form $g_1 := x^2 + xy + y^2$, and show that $\mathrm{Im}_{\mathbb{Z}}\, g = \mathrm{Im}_{\mathbb{Z}}\, g_1$. Indeed, for all $x, y \in \mathbb{Z}$ we have

$$x^2 + 3y^2 \;=\; (x-y)^2 + (x-y)(2y) + (2y)^2 \;,$$

which proves the inclusion $\mathrm{Im}_{\mathbb{Z}}\, g \subseteq \mathrm{Im}_{\mathbb{Z}}\, g_1$. On the other hand, if at least one of the two integers x and y — say y — is even, then

$$x^2 + xy + y^2 \;=\; \big(x + \tfrac{1}{2}y\big)^2 + 3\big(\tfrac{1}{2}y\big)^2 \;,$$

while if both x and y are odd, then

$$x^2 + xy + y^2 \;=\; \big(\tfrac{1}{2}(x-y)\big)^2 + 3\big(\tfrac{1}{2}(x+y)\big)^2 \;;$$

this proves the opposite inclusion. The form g_1 satisfies the condition stated in Lemma 8, so it is a $\mathbb{QZ}$-form, hence $\mathrm{Im}_{\mathbb{Z}}\, g_1$ is describable in terms of prime factor parities. The identity $\mathrm{Im}_{\mathbb{Z}}\, g = \mathrm{Im}_{\mathbb{Z}}\, g_1$ provides an independent verification of the fact that g is a $\mathbb{QZ}$-form.

We seek the description of $S = \mathrm{Im}_{\mathbb{Z}}\, g_1 = \mathrm{Im}_{\mathbb{Z}}\, g$ in the ring $R = \mathbb{Z}[\omega]$ of algebraic integers of the field $\mathbb{Q}(\omega) = \mathbb{Q}\big(\sqrt{-3}\big)$, where $\omega = \frac{1}{2}\big(1+i\sqrt{3}\big)$ generates the multiplicative group of the six units of R. The norm of $a + b\omega \in R$ $(a, b \in \mathbb{Z})$ is $g_1(a, b)$, the ring R is norm-Euclidean, hence a PID. The rational prime 3 ramifies as $3 = -(2\omega - 1)^2$, every rational prime $\equiv 1 \pmod 6$ splits, while the rational prime 2 and all rational primes $\equiv -1 \pmod 6$ are inert. An integer n therefore belongs to S if and only if either $n = 0$, or $n > 0$ and $e_p(n)$ is even for $p = 2$ and for every prime $p \equiv -1 \pmod 6$. We have $P\big(\mathrm{core}(S)\big) = \{p \in P(\mathbb{N}) \mid p = 3 \text{ or } p \equiv 1 \pmod 6\}$, thus mg is a $\mathbb{QZ}$-form, for a non-zero integer m, if and only if m is $\pm$ a product of distinct primes from the set $\{p \in P(\mathbb{N}) \mid p = 2 \text{ or } p \equiv -1 \pmod 6\}$.

Our last example is the form $g = x^2 + y^2 + 2z^2$. We have the same problem with this form as we had with the form $x^2 + 3y^2$: an enchanted walk can get stuck in a point $\boldsymbol{x} = \big(y_1 + \frac{1}{2}, y_2 + \frac{1}{2}, y_3 + \frac{1}{2}\big)$ with $y_1, y_2, y_3 \in \mathbb{Z}$. And as before, we can still make the last step to an integral point: we step from the point $\boldsymbol{x}$ in the direction of the point (y_1, y_2, y_3) if $y_1 + y_2$ is odd, and in the direction of the point $(y_1, y_2 + 1, y_3)$ if $y_1 + y_2$ is even. The proof that this works is similar to the one for the form $x^2 + 3y^2$.

Let $g_1 = x^2 + y^2 + z^2$; we claim that $\mathrm{Im}_{\mathbb{Z}}\, g = S$, where $S := \{n \in \mathbb{Z} \mid 2n \in \mathrm{Im}_{\mathbb{Z}}\, g_1\}$. The identity

$$2\cdot(x^2 + y^2 + 2z^2) \;=\; (x-y)^2 + (x+y)^2 + (2z)^2$$

proves that $\mathrm{Im}_{\mathbb{Z}}\, g \subseteq S$. To prove the other inclusion, assume that n is an integer such that $2n = x^2 + y^2 + z^2$ for some integers x, y, and z. Either all three integers x, y, z are even, or two are odd and one is even; in either case, two are of the same parity — we can assume that these two are x and y — while the third one — that is, z — is even. But then the identity

$$x^2 + y^2 + z^2 \;=\; 2\cdot\Big(\big(\tfrac{1}{2}(x+y)\big)^2 + \big(\tfrac{1}{2}(x-y)\big)^2 + 2\big(\tfrac{1}{2}z\big)^2\Big)$$

shows that $n \in \mathrm{Im}_{\mathbb{Z}}\, g$. The relationship of the set $\mathrm{Im}_{\mathbb{Z}}\, g$ to the set $\mathrm{Im}_{\mathbb{Z}}\, g_1$ implies that $\mathrm{Im}_{\mathbb{Z}}\, g$ is describable in terms of prime factor parities, and hence that g is a $\mathbb{QZ}$-form. This is a consequence of the following simple, simply proved proposition:

Proposition 15. *If $S \subseteq \mathbb{Z}$ is describable in terms of prime factor parities and m is any integer, then $S' := \{n \in \mathbb{Z} \mid mn \in S\}$ is describable in terms of prime factor parities.*

Proof. For every integer n and every non-zero integer k we have

$$n \in S' \iff mn \in S \iff mnk^2 \in S \iff nk^2 \in S' \ . \qquad \square$$

As we did with the form x^2+3y^2, we have independently verified that $x^2+y^2+2z^2$ is a $\mathbb{QZ}$-form. Moreover, we have the following result:

Theorem 16. *An integer can be represented as $x^2+y^2+2z^2$ for some integers x, y, and z if and only if it is non-negative and is not of the form $2^{2j+1}(8k+7)$ for some natural numbers j and k.*

Since every prime is representable as $x^2+y^2+2z^2$ for some $x, y, z \in \mathbb{Z}$, the form $m\cdot(x^2+y^2+2z^2)$, where m is a non-zero integer, is $\mathbb{QZ}$ if and only if $m = \pm 1$.

Note that with the forms $g = x^2+y^2+2z^2$ and $g_1 = x^2+y^2+z^2$ we have not only $\mathrm{Im}_{\mathbb{Z}}\, g = \{n \in \mathbb{Z} \mid 2n \in \mathrm{Im}_{\mathbb{Z}}\, g_1\}$, but also $\mathrm{Im}_{\mathbb{Z}}\, g_1 = \{n \in \mathbb{Z} \mid 2n \in \mathrm{Im}_{\mathbb{Z}}\, g\}$. The identity

$$2(x^2+y^2+z^2) \ = \ (x-y)^2+(x+y)^2+2z^2$$

proves the inclusion $\mathrm{Im}_{\mathbb{Z}}\, g_1 \supseteq \{n \in \mathbb{Z} \mid 2n \in \mathrm{Im}_{\mathbb{Z}}\, g\}$; to prove the opposite inclusion, observe that if $n \in \mathbb{Z}$ and $2n = x^2+y^2+2z^2$ for some $x, y, z \in \mathbb{Z}$, then x and y are of the same parity, whence

$$n \ = \ \left(\tfrac{1}{2}(x-y)\right)^2+\left(\tfrac{1}{2}(x+y)\right)^2+z^2 \ .$$

This symmetric relationship between the forms g and g_1 is not a spurious coincidence:

Lemma 17. *Suppose $S \subseteq \mathbb{Z}$ is describable in terms of prime factor parities. Let m be a non-zero integer, and set $S' := \{n \in \mathbb{Z} \mid mn \in S\}$. Then $S = \{n \in \mathbb{Z} \mid mn \in S'\}$.*

Proof. Writing $S'' := \{n \in \mathbb{Z} \mid mn \in S'\}$, we have, for every integer n,

$$n \in S'' \iff mn \in S' \iff m^2n \in S \iff n \in S \ . \qquad \square$$

By Theorem 16 every odd natural number is representable as $x^2+y^2+2z^2$ for some integers x, y, and z. This simple observation gives us the following three-squares-double-square theorem:

Theorem 18. *Every natural number can be represented as $x_1^2+x_2^2+x_3^2+2x_4^2$ for some integers x_1, x_2, x_3, and x_4, where we can additionally require that $x_1 = 0$ or $x_1 = 1$.*

The quadratic form $g = x_1^2 + x_2^2 + x_3^2 + 2x_4^2$ is trivially a $\mathbb{QZ}$-form because $\mathrm{Im}_{\mathbb{Z}}\, g = \mathbb{N}$. The quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is $\mathbb{QZ}$ for the same reason.

---*---*---*---

In the (draft) paper [1] there is the Main Theorem, namely Theorem 4; it is a generalization of Theorem 2 in [1] which is (essentially) the same as Lemma 8 in this essay.

> **Theorem 4.** Let $(R, |\ |)$ be a normed ring not characteristic 2 and $q_{/R}$ a Euclidean quadratic form. Then q is an ADC-form.

The notions appearing in the theorem are defined in [1] as follows. Normed rings first:

> Let R be a commutative, unital ring. We write $R^\bullet$ for $R \setminus \{0\}$.
>
> A **norm** on R is a function $|\ | : R^\bullet \to \mathbb{Z}^+$ such that
>
> (N1) $\forall x \in R,\ x \in R^\times \iff |x| = 1$, and
>
> (N2) $\forall x, y \in R,\ |xy| = |x||y|$.
>
> When convenient, we extend $|\ |$ to R by putting $|0| = 0$.
>
> By a **normed ring**, we shall mean (here) a pair $(R, |\ |)$ where $|\ |$ is a norm on R. Note that a normed ring is necessarily an integral domain. We denote the fraction field by K. The norm extends uniquely to a homomorphism of groups $(K^\times, \cdot) \to \left(\mathbb{Q}^{>0}, \cdot\right)$ via $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$.

Next are Euclidean quadratic forms:

> Let $(R, |\ |)$ be a normed ring of characteristic different from 2. By a **quadratic form** over R, we mean a polynomial $q \in R[x] = R[x_1, ..., x_n]$ which is homogenous of degree 2. A quadratic form q on a normed ring $(R, |\ |)$ is **Euclidean** if for all $x \in K^n \backslash R^n$ there exists $y \in R^n$ such that $0 < |q(x - y)| < 1$.

Finally, here are ADC-forms, introduced as a special case of ADC-extensions:

> Let $R \hookrightarrow S$ be an extension of [integral] domains, and let $q_{/R}$ be a quadratic form. We say that S/R is an **ADC-extension** for q if: for all $d \in R$, if there exists $x \in S^n$ such that $q(x) = d$, there exists $y \in R^n$ such that $q(y) = d$. If R is a domain with fraction field K, we say that q is an **ADC-form** if the extension K/R is an ADC-extension for q.

The prefix ADC is the acronym for Aubry-Davenport-Cassels. ($\mathbb{QZ}$-forms of this essay are ADC-forms over the ring $R = \mathbb{Z}$.)

When I tried to undestand the proof of the Main Theorem, I found it rather messy, so I decided to tidy it up.

First of all, there are at least two typos in it: "$\frac{1}{2}\big(q(x+y) - q(x) - q(x)\big)$" should be "$\frac{1}{2}\big(q(x+y) - q(x) - q(y)\big)$", and "$x = \frac{x'}{d}$" should be "$x = \frac{x'}{t}$"; there may well be other typos — I did not look very closely at the computations in the proof, because, as it turned out, I did not need to.

Then there is this unnecessary fuss about avoiding rings of characteristic 2. The use of the factor $\frac{1}{2}$ in the definition of the bilinear form $x \cdot y := \frac{1}{2}\big(q(x+y) - q(x) - q(x)\big)$ is unavoidable if we insist on recovering the quadratic form from the bilinear form as $q(x) = x \cdot x$; but, why should we want to do this, what would it be good for? What we do need, for the purposes of the proof, is the bilinearity of $\langle x, y\rangle := q(x+y) - q(x) - q(y)$, and we need it only to show that for any x, $y \in R^n$ and t a formal variable, the expression

$$q(x+ty) \;=\; q(x) + \langle x, ty\rangle + q(ty) \;=\; q(x) + \langle x, y\rangle\, t + q(y)\, t^2$$

is a polynomial in t of degree at most 2 with coefficients in R, and, in particular, with the coefficient $q(y)$ at t^2.

The proof of the Main Theorem concludes with a contradiction. Searching back through the proof, I could not find a clear announcement of a reasoning by contradiction, and could not quite see how the contradiction proves what it is purported to prove. Musing about the missing announcement for a while, I eventually figured it out:

> We intend to prove that $|t| = 1$. Assume, to the contrary, that $|t| > 1$; then $x = \frac{x'}{t}$ does not belong to R^n, by the choice of t. Applying the Euclidean hypothesis ...

After that the proof proceeds as in the paper.

I am not a great fan of proofs by contradiction. Sometimes there is no other way to prove something, or better said, there is no *known* other way; however, most proofs by contradiction can be straightened out, so that instead of reasoning about imagined properties of an impossible situation, one that does not exist (which might be an intensely surreal experience), we reason about situations that *do* exist, about their quite real properties. So it came naturally to me to try to disentangle the proof by contradiction of the Main Theorem. Here is what I came up with:

> Let $d \in R$, and suppose that $q(x) = d$ for some $x \in K^n$. If $x \in R^n$, then we are done, so suppose that $x \notin R^n$. Represent x as a fraction $x = x'/t$ with $x' \in R^n$ and $t \in R \smallsetminus \{0\}$, where $|t|$ is as small as possible.
>
> Applying the Euclidean hypothesis with x, there exists $y \in R$ such that $0 < \big|q(x-y)\big| < 1$. [We go on from here to construct] a point $x_1 = X/T \in K^n$ with $X \in R^n$, $T \in R \smallsetminus \{0\}$, and $|T| < |t|$, which satisfies $q(x_1) = d$; if $x_1 = x_1'/t_1$ is a fraction with $x_1' \in R^n$, $t_1 \in R \smallsetminus \{0\}$, and with the least possible $|t_1|$, then $|t_1| \leqslant |T| < |t|$. If still $x_1 \notin R^d$, we go on and construct another point $x_2 \in K^n$ satisfying $q(x_2) = d$, such that for any representation $x_2 = x_2'/t_2$ with $x_2' \in R^n$, $t_2 \in R \smallsetminus \{0\}$, and the least possible $|t_2|$, we have $|t_2| < |t_1|$. And so on. The sequence x, x_1, x_2, ... of points in K^n satisfying $d = q(x) = q(x_1) = q(x_2) = \cdots$ must eventually end with a point $x_* \in R^n$ satisfying $q(x_*) = d$.

Why, but this is an enchanted walk all over again! Moreover, the straightened-up proof nowhere uses the assumed property (N1) of the norm $|\ |$.

I still had to figure out the construction of the point $x_1 = X/T$. There are two points on the line in K^d laid through the points x and y that satisfy the equation $q(z) = d$, namely the point $z = x$ and some other point (which, in general, might coincide with the point x, though in our case it does not); what else could x_1 be but that other point? I did not try to wade through calculations in the proof of the Main Theorem,

instead I attempted to reproduce the reasoning in the proof of Lemma 8 in the present more general situation. There was one obstacle to this plan: the proof of Lemma 8 uses Lemma 6, which heavily relies on existence of primes, greatest common divisors, relative primality... I somehow had to do without all this. Then I recalled the simpler of the two proofs of the fact that $\mathrm{den}\big(f_2(\boldsymbol{x}-\boldsymbol{y})\big)$ divides $\mathrm{den}(\boldsymbol{x})$ (on page 5 of this essay): this is true because $f_2(\boldsymbol{x}-\boldsymbol{y}) = A/n^2 = -B/n - C$, where $n = \mathrm{den}(\boldsymbol{x})$. Equivalently, $f_2(\boldsymbol{x}-\boldsymbol{y})\cdot n = A/n = -B - Cn$ is an integer — *and the analogous reasoning is valid in any integral domain.* With this insight, the final piece of the jigsaw puzzle clicked into place, and the reworked proof was completed.

To present the new proof, we'd better start afresh.

Let R be a commutative ring with unity $1 \neq 0$.

A **discrete multiplicative norm on** R (shorter, a **norm on** R) is a mapping $\|\mathbf{-}\| : R \to \mathbb{N}$ that satisfies the following two conditions, for all $x, y \in R$:

(i) $\|x\| = 0$ if and only if $x = 0$;

(ii) $\|xy\| = \|x\|\,\|y\|$.

(The norm is *discrete* because it takes values in $\mathbb{N}$, and it is *multiplicative* because it satisfies the condition (ii). Besides that, $\|\mathbf{-}\|$ is a *norm* — and not a *seminorm* — because it satisfies the condition (i).) Since $\|1\|\,\|1\| = \|1\cdot 1\| = \|1\| \neq 0$, we have $\|1\| = 1$, thus $\|\mathbf{-}\|$ is a homomorphism of multiplicative monoids, and as such it maps every unit of R to the only invertible element 1 of the multiplicative monoid $\mathbb{N}$. (But note that there may be also nonunits of R whose norm is 1.)

Let $\|\mathbf{-}\|$ be a discrete multiplicative norm on R.

If x and y are any non-zero elements of R, then $\|xy\| = \|x\|\,\|y\| \neq 0$, thus $xy \neq 0$; the ring R is an integral domain. Let K be the field of fractions of R. The given norm $\|\mathbf{-}\|$ on R extends in a unique way to a mapping $\|\mathbf{-}\| : K \to \mathbb{Q}^{\geqslant 0}$ satisfying the condition (ii) (which then also satisfies the condition (i)); if $x = a/b$ with $a, b \in R$ and $b \neq 0$, then $\|x\| = \|a\| \,/\, \|b\|$.

Let $d > 0$ be a natural number. Let $\boldsymbol{x} \in K^d$.

We define

$$\delta(\boldsymbol{x}) \;:=\; \min\big\{\, \|b\| \;\big|\; b \in R\smallsetminus\{0\},\, b\boldsymbol{x} \in R^d \big\}\;. \tag{4}$$

Since there exist nonzero elements b of the ring R such that $b\boldsymbol{x} \in R^d$, and since the norm $\|\mathbf{-}\|$ is discrete, the set in (4) in which the minimum is sought is a nonempty set of non-zero natural numbers, thus $\delta(\boldsymbol{x})$ is a well-defined non-zero natural number. In particular, when $d = 1$, (4) defines $\delta(x)$ for $x \in K = K^1$.

We can characterize $\delta(\boldsymbol{x})$ as follows: $\boldsymbol{x}$ can be represented as a fraction $\boldsymbol{x} = \boldsymbol{a}/b$ with $\boldsymbol{a} \in R^d$ and $b \in R\smallsetminus\{0\}$, and $\delta(\boldsymbol{x})$ is the least possible $\|b\|$ for such representations of $\boldsymbol{x}$. By the definition of $\delta(\boldsymbol{x})$, $\boldsymbol{x}$ has at least one representation with $\|b\| = \delta(\boldsymbol{x})$; any such representation of $\boldsymbol{x}$ will be said to be **reduced**.

If $\boldsymbol{x} \in R^d$, then $\delta(\boldsymbol{x}) = 1$. If $\boldsymbol{x} \in K^d$ and $\boldsymbol{y} \in R^d$, then $\delta(\boldsymbol{x}+\boldsymbol{y}) = \delta(\boldsymbol{x})$, because for every nonzero $b \in R$, the product $b\boldsymbol{x}$ is in R^d if and only if the product $b(\boldsymbol{x}+\boldsymbol{y})$ is in R^d. If $x \in K$ and $\boldsymbol{y} \in K^d$, then clearly $\delta(x\boldsymbol{y}) \leqslant \delta(x)\delta(\boldsymbol{y})$; in particular, if $x \in K$ and $\boldsymbol{y} \in R^d$, then $\delta(x\boldsymbol{y}) \leqslant \delta(x)$.

The following theorem is a bare-bones reincarnation of the Main Theorem in "ADC-Extensions", formulated as a generalization of Lemma 8:

Theorem 19. *Let R be an integral domain with a discrete multiplicative norm $\|-\|$, extended to a multiplicative norm (still denoted $\|-\|$) on K, the field of fractions of R. Let $d > 0$ be a natural number, and let $f = f_2 + f_1 + f_0 \in R[x_1, \dots, x_d]$,[11] where f_i is homogenous of degree i. Suppose that for every $\boldsymbol{x} \in K^d \setminus R^d$ there exists $\boldsymbol{y} \in R^d$ such that $0 < \big\|f_2(\boldsymbol{x}-\boldsymbol{y})\big\| < 1$. If f has a zero in K^d, then it has a zero in R^d.*

Proof. Let $\boldsymbol{x} \in K^d$ be a zero of f; if $\boldsymbol{x} \in R^d$, we are done, so assume that $\boldsymbol{x} \notin R^d$. There exists $\boldsymbol{y} \in R^d$ such that $0 < \big\|f_2(\boldsymbol{x}-\boldsymbol{y})\big\| < 1$. Let $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{v}/a$ be a reduced representation, so that $\|a\| = \delta(\boldsymbol{x}-\boldsymbol{y}) = \delta(\boldsymbol{x})$. For any $t \in K$ set $\boldsymbol{z}(t) := \boldsymbol{y}+t\boldsymbol{v}$; we have $\boldsymbol{z}(1/a) = \boldsymbol{x}$. For any $t \in K$ set $F(t) := f\big(\boldsymbol{z}(t)\big) = At^2 + Bt + C$, where the coefficients $A = f_2(\boldsymbol{v}) \neq 0$, $C = f(\boldsymbol{y})$ and $B = f(\boldsymbol{y}+\boldsymbol{v}) - A - C$ are in R; $\tau := 1/a$ is a zero of F. Let τ' be the other zero of F. Since $\tau\tau' = C/A$, we have $\tau' = C/\tau A = C/(A/a)$, where $A/a = -B - Ca \in R$ and $\|A/a\| = \big\|f_2(\boldsymbol{v}/a)\,a\big\| = \big\|f_2(\boldsymbol{x}-\boldsymbol{y})\big\|\,\|a\| < \|a\| = \delta(\boldsymbol{x})$, thus $\delta(\tau') \leqslant \|A/a\| < \delta(\boldsymbol{x})$. The point $\boldsymbol{x}' := \boldsymbol{z}(\tau')$ is a zero of f and has $\delta(\boldsymbol{x}') = \delta(\boldsymbol{y}+\tau'\boldsymbol{v}) = \delta(\tau'\boldsymbol{v}) \leqslant \delta(\tau') < \delta(\boldsymbol{x})$. If the zero $\boldsymbol{x}'$ of f is still not in R^d, we repeat the procedure and construct another zero $\boldsymbol{x}''$ of f with $\delta(\boldsymbol{x}'') < \delta(\boldsymbol{x}')$, and so on. The sequence $\boldsymbol{x}$, $\boldsymbol{x}'$, $\boldsymbol{x}''$, … of zeros of f eventually ends with a zero $\boldsymbol{x}^* \in R^d$ of f $\big($which has $\delta(\boldsymbol{x}^*) = 1\big)$. □

In the course of reworking the proof of the Main Theorem in [1] into the proof of Theorem 19, we overcame the instinctive revulsion caused by integral domains of characteristic two, we unburdened the definition of a norm on a ring of the superfluous property (N1), and we also somewhat simplified the calculations. Yet, contemplating the proof of Theorem 19, we cannot but notice that it is still wasting time doing unnecessary things — it starts with a *reduced* representation of the first point of the enchanted walk, and later on consistently replaces fractions representing further points on the walk with *reduced* representations of the points. I suspect that most mathematicians suffer from this obsessive compulsion — of always considering fractions in a reduced form — which they acquired through their dealings with integers and rationals, and later on with UFDs an their fields of fractions.[12] Let's, for once, suppress this urge (to replace every fraction in sight with a reduced one), in order to find out whether we are still able to walk an enchanted walk.

We intend to begin the proof with representing the initial zero $\boldsymbol{x} \in K^d \setminus R^d$ of f as a fraction $\boldsymbol{a}/b$ with $\boldsymbol{a} \in R^d$ and $b \in R\setminus\{0\}$ — as *any* such fraction. Then we will take a magic step to another zero $\boldsymbol{x}' = \boldsymbol{a}'/b'$ of f, where $\boldsymbol{a}' \in R^d$, $b' \in R\setminus\{0\}$, and $\|b'\| < \|b\|$. If the point $\boldsymbol{x}'$ will not be in R^d, we will take another step to a zero $\boldsymbol{x}'' = \boldsymbol{a}''/b''$ of f, where $\boldsymbol{a}'' \in R^d$, $b'' \in R \setminus \{0\}$, and $\|b''\| < \|b'\|$. And so on. At no time during this enchanted walk will we insist on reduced fractions. We will eventually arrive at a zero $\boldsymbol{x}^* \in R^d$ of f, represented as a fraction $\boldsymbol{x}^* = \boldsymbol{a}^*/b^*$ with $\boldsymbol{a}^* \in R^d$ and $b^* \in R \setminus \{0\}$, which perhaps will not *evidently* represent a point in R^d, meaning that b^* will not be a unit of R.

Ok, we have a plan; let's carry it out.

[11] Here x_1, …, x_d are formal variables.

[12] The obligatory plonking of $\frac{1}{2}$ in front of $g(\boldsymbol{x}+\boldsymbol{y}) - g(\boldsymbol{x}) - g(\boldsymbol{y})$ is another instance of such compulsive obsessive behavior.

Proof (Second proof of Theorem 19)**.** Let $\boldsymbol{x} \in K^d$ be a zero of f; if $\boldsymbol{x} \in R^d$, we are done, so assume that $\boldsymbol{x} \notin R^d$.

There exist $\boldsymbol{a} \in R^d$ and $b \in R \smallsetminus \{0\}$ such that $\boldsymbol{x} = \boldsymbol{a}/b$, and there exists $\boldsymbol{y} \in R^d$ such that $0 < \big\|f_2(\boldsymbol{x}-\boldsymbol{y})\big\| < 1$. We have $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{v}/b$, where $\boldsymbol{v} = \boldsymbol{a} - b\boldsymbol{y} \in R^d$. For any $t \in K$ set $F(t) := f(\boldsymbol{y}+t\boldsymbol{v}) = At^2 + Bt + C$, where the coefficients $A = f_2(\boldsymbol{v}) = f_2(\boldsymbol{x}-\boldsymbol{y})b^2 \neq 0$, $C = f(\boldsymbol{y})$, and $B = f(\boldsymbol{y}+\boldsymbol{v}) - A - C$ are in R; $\tau := 1/b$ is a zero of F because $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{v}/b$. Let τ' be the other zero of F. Since $\tau\tau' = C/A$, we have $\tau' = C/\tau A = C/(A/b)$, where $A/b = -B - Cb$ is in R; since also $A/b = f_2(\boldsymbol{x}-\boldsymbol{y})b$, we have $\|A/b\| = \big\|f_2(\boldsymbol{x}-\boldsymbol{y})\big\|\,\|b\| < \|b\|$. The point $\boldsymbol{x}' := \boldsymbol{y} + \tau'\boldsymbol{v}$ is a zero of f, and it can be represented as $\boldsymbol{x}' = \boldsymbol{a}'/b'$, where $b' = A/b \in R \smallsetminus \{0\}$, $\boldsymbol{a}' = b'\boldsymbol{y} + C\boldsymbol{v} \in R^d$, and $\|b'\| < \|b\|$.

If the zero $\boldsymbol{x}'$ of f is not yet in R^d, we repeat the procedure and construct another zero $\boldsymbol{x}'' = \boldsymbol{a}''/b''$ of f, where $\boldsymbol{a}'' \in R^d$, $b'' \in R \smallsetminus \{0\}$, and $\|b''\| < \|b'\|$. And so on. The sequence $\boldsymbol{x}$, $\boldsymbol{x}'$, $\boldsymbol{x}''$, … of zeros of f eventually ends with a zero $\boldsymbol{x}^* \in R^d$ of f. □

We have obtained a sequence $\boldsymbol{x} = \boldsymbol{a}/b$, $\boldsymbol{x}' = \boldsymbol{a}'/b'$, $\boldsymbol{x}'' = \boldsymbol{a}''/b''$, … of zeros of f, where $b' = f_2(\boldsymbol{x}-\boldsymbol{y}) \cdot b$, $b'' = f_2(\boldsymbol{x}'-\boldsymbol{y}') \cdot b'$, … . We can now clearly see the inner workings of the magic that guides enchanted walks.

---*---*---*---

A remark concerning the property (N1) of a norm as stated in [1].

We define an **Euclidean norm** on an integral domain R, whose field of fractions is K, to be a discrete multiplicative norm $\|\text{–}\|$ on R (extended to a multiplicative norm on K) which satisfies the additional condition

(iii) for every $x \in K$ there exists $y \in R$ such that $\|x-y\| < 1$.

An Euclidean norm on R always has the property (N1), that is, it maps non-zero non-units of R to natural numbers greater than 1. Indeed, let $\|\text{–}\|$ be an Euclidean norm on R, and let a be any non-zero non-unit of R. The inverse $a^{-1} \in K$ is not in R. There exists $b \in R$ such that $r := a^{-1} - b$ has $\|r\| < 1$. Since $a^{-1} \notin R$, r is a non-zero element of K, thus $ar = 1 - ab$ is a non-zero element of R, whence $1 \leqslant \|ar\| = \|a\|\,\|r\| < \|a\|$.

We can adapt the ploy of approximating the inverse of a non-zero non-unit of an integral domain R by an element of R, to obtain a more general result.

Let $\|\text{–}\|$ be a discrete multiplicative norm on R. Let $d > 0$ and $m > 0$ be natural numbers; a **Euclidean form** over $\big(R, \|\text{–}\|\big)$, of degree m in d variables, is a homogenous polynomial $g \in R[x_1, \ldots, x_d]$ of degree m which has the property that for every point $\boldsymbol{x}$ in $K^d \smallsetminus R^d$ there exists a point $\boldsymbol{y}$ in R^d such that $0 < \big\|g(\boldsymbol{x}-\boldsymbol{y})\big\| < 1$. Suppose there exists a Euclidean form g over $\big(R, \|\text{–}\|\big)$ (in some number d of variables, of some degree m); then the norm $\|\text{–}\|$ has the property (N1). Indeed, let a be any non-zero non-unit of R. Put $\boldsymbol{x} := \big(a^{-1}, 0, \ldots, 0\big) = a^{-1}\boldsymbol{e}_1 \in K^d \smallsetminus R^d$. Since g is Euclidean, there exists $\boldsymbol{y} \in R^d$ so that $0 < \big\|g(\boldsymbol{x}-\boldsymbol{y})\big\| < 1$, whence $0 < \big\|g(\boldsymbol{e}_1 - a\boldsymbol{y})\big\| < \|a\|^m$; since $\big\|g(\boldsymbol{e}_1 - a\boldsymbol{y})\big\|$ is an integer, we have $\|a\|^m > 1$ and therefore $\|a\| > 1$.

Though in Theorem 19 we do not explicitly assume the property (N1), the presence of the Euclidean quadratic form f_2 implies it.

References

[1] Pete L. Clark, "Euclidean quadratic forms and ADC-extensions" (draft of a paper): http://www.math.uga.edu/~pete/ADCformsv2.pdf.

[2] France Dacar, "Fermat's two square theorem for rationals" (working notes), 2012: http://dis.ijs.si/france/notes/sums-of-two-rational-squares.pdf.

[3] MathOverflow, "Intuition for the last step in Serre's proof of the three-squares theorem": http://mathoverflow.net/questions/3269.