The density of integral quadratic forms having a k-dimensional totally isotropic subspace

Lycka Drakengren and Tom Fisher

22nd January 2024

Abstract

We investigate the probability that a random quadratic form in $\mathbb{Z}[x_1, ..., x_n]$ has a totally isotropic subspace of a given dimension. We show that this global probability is a product of local probabilities. Our main result computes these local probabilities for quadratic forms over the p-adics. The formulae we obtain are rational functions in p invariant upon substituting $p \mapsto 1/p$.

1 Introduction

An integral quadratic form in n variables is a homogeneous polynomial of degree 2

$$Q(x_1, x_2, \dots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j \tag{1}$$

where the coefficients a_{ij} belong to $\mathbb{Z}$. A non-zero vector $(x_1, x_2, \dots, x_n) \in V = \mathbb{Q}^n$ is called *isotropic* (with respect to Q) if $Q(x_1, x_2, \dots, x_n) = 0$. A subspace of V is *totally isotropic* if all its non-zero vectors are isotropic. We say that Q is *k-isotropic* if V has a k-dimensional totally isotropic subspace. A quadratic form that is 1-isotropic is simply called isotropic. In Section 2 we make corresponding definitions with $\mathbb{Q}$ replaced by any field $\mathbb{F}$.

Generalising the results of [2], where only the case $k = 1$ was considered, we investigate the probability $\rho_{\mathrm{glob}}(k, n)$ that a random integral quadratic form in n variables is k-isotropic. More formally we define

$$\rho_{\mathrm{glob}}(k, n) = \lim_{H \to \infty} \frac{\# \left\{ \begin{array}{c} \text{quadratic forms } Q = \sum a_{ij} x_i x_j \in \mathbb{Z}[x_1, \dots, x_n] \\ \text{with } |a_{ij}| \leqslant H \text{ that are } k\text{-isotropic over } \mathbb{Q} \end{array} \right\}}{(2H)^{n(n+1)/2}} \tag{2}$$

if this limit exists.

Combining the Strong Hasse Principle [3, p. 75] and Witt's Cancellation Theorem (see Theorem 2.8), we know that an integral quadratic form is k-isotropic over $\mathbb{Q}$ if and only if it is k-isotropic over $\mathbb{Q}_p$ for all primes p and over $\mathbb{R}$. Applying a theorem of Poonen and Stoll [7] we deduce the following result.

Theorem 1.1. *The probability $\rho_{\mathrm{glob}}(k, n)$ that a random integral quadratic form in n variables is k-isotropic exists and is given by*

$$\rho_{\mathrm{glob}}(k, n) = \rho_\infty(k, n) \prod_p \rho_p(k, n)$$

where the product is over all primes p, and the local contributions are the probabilities of k-isotropy over $\mathbb{R}$ and over $\mathbb{Q}_p$. These local probabilities are defined as in (2), but with the numerator counting integral quadratic forms that are k-isotropic over $\mathbb{R}$ or $\mathbb{Q}_p$ as appropriate.

We fix a prime number p. The probability $\rho_p(k,n)$ may also be interpreted as the probability that a random p-adic integral quadratic form in n variables is k-isotropic over $\mathbb{Q}_p$. Here, by a random p-adic integral quadratic form, we mean a quadratic form with coefficients in $\mathbb{Z}_p$ where the coefficients are chosen independently at random according to Haar measure. Choosing the coefficient $a_{ij} \in \mathbb{Z}_p$ with respect to Haar measure means that each congruence class modulo p is equally likely, and inductively for $n > 1$, the classes

$$a,\ a + p^{n-1},\ a + 2p^{n-1},\ \ldots,\ a + (p-1)p^{n-1} \mod p^n$$

are equally likely where $0 \leqslant a \leqslant p^{n-1} - 1$ is the reduction of a_{ij} modulo p^{n-1}.

We now state our main theorem. It extends [2, Theorem 1.2] which treated the case $k = 1$.

Theorem 1.2. *The probability $\rho_p(k,n)$ that a random p-adic integral quadratic form in n variables is k-isotropic over $\mathbb{Q}_p$ is given by*

$$\rho_p(k,n) = \begin{cases} 0 & \text{if } n \leqslant 2k-1; \\ \frac{1}{4} \cdot (p^k + 1) \cdot \left(\frac{p^{k+2}-1}{(p+1)(p^{2k+1}-1)} + \prod_{i=1}^{k} \left(\frac{p^{2i-1}-1}{p^{2i}-1} \right) \right) & \text{if } n = 2k; \\ \frac{1}{2} + \frac{1}{2} \cdot (p^{k+1} + 1) \cdot \prod_{i=1}^{k+1} \left(\frac{p^{2i-1}-1}{p^{2i}-1} \right) & \text{if } n = 2k+1; \\ 1 - \frac{1}{4} \cdot (p^{k+1} + 1) \cdot \left(\frac{p^{k+3}-1}{(p+1)(p^{2k+3}-1)} - \prod_{i=1}^{k+1} \left(\frac{p^{2i-1}-1}{p^{2i}-1} \right) \right) & \text{if } n = 2k+2; \\ 1 & \text{if } n \geqslant 2k+3. \end{cases}$$

Combining Theorems 1.1 and 1.2 we deduce the following.

Corollary 1.3. *We have $\rho_{\mathrm{glob}}(k,n) = 0$ for all $n \leqslant 2k+1$,*

$$\rho_{\mathrm{glob}}(k, 2k+2) = \rho_\infty(k, 2k+2) \cdot \prod_p \left(1 - \frac{p^{k+1}+1}{4} \cdot \left(\frac{p^{k+3}-1}{(p+1)(p^{2k+3}-1)} - \prod_{r=1}^{k+1} \frac{p^{2r-1}-1}{p^{2r}-1} \right) \right)$$

and $\rho_{\mathrm{glob}}(k,n) = \rho_\infty(k,n)$ for all $n \geqslant 2k+3$.

We note two striking features of the formulae in Theorem 1.2. The first is that they are rational functions in p, where the same rational function works for all primes p including $p = 2$. The second is that the rational functions are invariant upon substituting $p \mapsto 1/p$. Exactly the same two observations were made in [1] in connection with roots of polynomials in one variable. Moreover in that paper the substitution $p \mapsto 1/p$ also related two auxiliary probabilities appearing in the recursion, denoted there by α and β. We find that an analogous statement holds in our case; see Corollary 5.8.

We employ two strategies for proving Theorem 1.2. The first is a direct generalisation of the method in [2] (which only treated the case $k = 1$), with the additional idea of splitting off hyperbolic planes (see Definition 2.5). This leads to recursive formulae that may be used to compute $\rho_p(k,n)$ for any given k and n, and also show that the answer is always a rational function in p. However further work is needed to prove Theorem 1.2 (as discussed in the next paragraph) as for this we must find formulae that hold for all k.

The second strategy is to deduce Theorem 1.2 from a theorem of Kovaleva [6], who computed the probability that a random p-adic integral quadratic form in n variables belongs to a given $\mathbb{Q}_p$-equivalence class of quadratic forms. The answers she obtained are not rational functions in p, do not exhibit the $p \leftrightarrow 1/p$ symmetries, and do not explicitly cover the case $p = 2$, where in any case it makes a difference whether we consider random quadratic forms or random symmetric matrices. However her work leads to a proof of Theorem 1.2 when p is odd. Since we already know from the first strategy that the answer is a rational function in p it follows that the theorem is also true when $p = 2$.

Both strategies work by dividing into cases according to the $\mathbb{F}_p$-equivalence class of the quadratic form reduced mod p, and from this obtaining recursive formulae for the probabilities. One difference, not already noted above, is that in the second strategy the quadratic form is diagonalised, whereas in the first we split off hyperbolic planes, and so allow 2×2 blocks on the diagonal.

In Section 2 we review some background on quadratic forms. In Section 3 we discuss the global applications of our work, and in particular explain how Theorem 1.1 and Corollary 1.3 follow from Theorem 1.2. In Section 4 we prove some results on counting quadratic forms over finite fields, in preparation for our first strategy for proving Theorem 1.2. The two strategies are explained in Sections 5 and 6 respectively. Finally in Appendix A we adapt the methods of Kovaleva to solve the recurrence relations in our first method directly.

This work originated as a summer project carried out by the first author and supervised by the second author. We thank the Trinity Summer Studentship Scheme and the Research in the CMS Programme for their support. We also thank the referee for a careful reading of our paper and some suggested improvements.

2 Background on quadratic forms

We collect together some standard definitions and results on quadratic forms. See Cassels [3] for further details. We write $\mathbb{F}$ for a general field, and V for a finite dimensional vector space over $\mathbb{F}$.

Definition 2.1. A *quadratic form* of dimension n over $\mathbb{F}$ is a polynomial

$$Q(x_1, x_2, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j, \tag{3}$$

where the coefficients a_{ij} for $1 \leqslant i \leqslant j \leqslant n$ belong to $\mathbb{F}$. We may also consider Q as a function $V \to \mathbb{F}$ where $V = \mathbb{F}^n$, and refer to the pair (V, Q) as a *quadratic space*. The corresponding symmetric bilinear form $\phi : V \times V \to \mathbb{F}$ is given by

$$\phi(x, y) = Q(x + y) - Q(x) - Q(y),$$

where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.

We refer to properties of a quadratic space (V, Q) and properties of V or Q interchangeably.

Definition 2.2. Let (V, Q) be a quadratic space and let ϕ be its associated symmetric bilinear form. The *radical* of (V, Q), when not over a field of characteristic 2, is the vector space consisting of vectors $x \in V$ such that $\phi(x, y) = 0$ for all $y \in V$. In characteristic 2, we further require that $Q(x) = 0$. A quadratic space is *regular* if its radical is zero-dimensional and *singular* otherwise. The *rank* of the quadratic form Q is $n - r$, where r is the dimension of the radical.

Definition 2.3. Quadratic spaces (V_1, Q_1) and (V_2, Q_2) over the same field $\mathbb{F}$ are *isometric* if there is a linear isomorphism $T : V_1 \to V_2$ such that $Q_1(x) = Q_2(Tx)$ for all $x \in V_1$. In this situation, the forms Q_1 and Q_2 are said to be *equivalent* over $\mathbb{F}$. In other words, quadratic forms over $\mathbb{F}$ are equivalent if they are related by a linear substitution given by a matrix $P \in \mathrm{GL}_n(\mathbb{F})$. This defines an equivalence relation on the set of quadratic forms with coefficients in $\mathbb{F}$. More generally, if $R \subset \mathbb{F}$ is a subring, then we say that quadratic forms are *equivalent over R* (or *R-equivalent*) if they are related by a matrix $P \in \mathrm{GL}_n(R)$.

The next two definitions are closely related. The first naturally extends the definitions we already gave in the introduction in the case $\mathbb{F} = \mathbb{Q}$.

Definition 2.4. Let (V, Q) be a quadratic space. A non-zero vector $x \in V$ is called *isotropic* if $Q(x) = 0$. A quadratic space (V, Q) is *isotropic* if V contains an isotropic vector, and *totally isotropic* if all its non-zero vectors are isotropic. If V has a subspace V_0 of dimension k such that the quadratic space (V_0, Q) is totally isotropic, then we say that the quadratic space (V, Q) is *k-isotropic.* In particular, a quadratic space is 1-isotropic if and only if it is isotropic.

Definition 2.5. A *hyperbolic plane* is a quadratic space (V, Q) of dimension 2 where Q is equivalent over $\mathbb{F}$ to the form $q(x_1, x_2) = x_1 x_2$.

Lemma 2.6. *A regular quadratic space (V, Q) is isotropic if and only if V has a subspace V_0 such that the quadratic space (V_0, Q) is a hyperbolic plane.*

Proof. See [3, p. 15]. ☐

We now introduce some results that will be useful for studying isotropic spaces.

Lemma 2.7. *Let Q and Q' be quadratic forms over a field $\mathbb{F}$ related by*

$$Q(x_1, \dots, x_n) = x_1 x_2 + Q'(x_3, \dots, x_n).$$

Let $k \geqslant 1$. Then Q is k-isotropic if and only if Q' is $(k-1)$-isotropic.

Proof. Let $U \subset \mathbb{F}^n$ be a k-dimensional totally isotropic subspace for Q. Let $e_1, \dots, e_n$ be the standard basis for $\mathbb{F}^n$. Since $U \cap \langle e_1, e_2 \rangle$ is a totally isotropic subspace for Q it can only be $\{0\}$, $\langle e_1 \rangle$ or $\langle e_2 \rangle$. Let $\pi : \mathbb{F}^n \to \mathbb{F}^{n-2}$ be projection onto the last $n-2$ coordinates. Then either $\pi(U \cap \{x_1 = 0\})$ or $\pi(U \cap \{x_2 = 0\})$ is a totally isotropic subspace for Q' of dimension at least $k-1$. Therefore Q' is $(k-1)$-isotropic. The converse is clear. ☐

Theorem 2.8 (Witt's Cancellation Theorem)**.** *Let (V, Q) be a quadratic space. Let V_1, V_2 be subspaces of V. Denote by $V_1^\perp$ and $V_2^\perp$ the orthogonal complements of V_1 resp. V_2 in V. If (V_1, Q) and (V_2, Q) are regular and isometric, then $(V_1^\perp, Q)$ and $(V_2^\perp, Q)$ are also isometric.*

Proof. See [5, pp. 89–92] for quadratic forms over a field of characteristic not 2, and [5, p. 118] for the case of characteristic 2. ☐

Let p be a prime. We write $\mathbb{F}_p$ for the finite field with p elements, $\mathbb{Q}_p$ for the field of p-adic numbers, and $\mathbb{Z}_p$ for the ring of p-adic integers. The following argument is one we will revisit in the proof of Lemma 5.2.

Lemma 2.9. *Let Q be a quadratic form with coefficients in $\mathbb{Z}_p$ that reduces over $\mathbb{F}_p$ to a form that is both k-isotropic and regular. Then Q is k-isotropic (and regular) over $\mathbb{Q}_p$.*

Proof. The case $k = 1$ is a consequence of Hensel's lemma. In fact if we go via Lemma 2.6 then we only need Hensel's lemma for a quadratic polynomial in one variable. For general $k > 1$ we proceed by induction on k. Once we know that Q is isotropic, we may assume via a $\mathbb{Z}_p$-equivalence, first that $Q(1, 0, \ldots, 0) = 0$, and then that

$$Q(x_1, \ldots, x_n) = x_1 x_2 + Q'(x_3, \ldots, x_n)$$

for some quadratic form Q' with coefficients in $\mathbb{Z}_p$. Note that for the latter deduction we use that $(1, 0, \ldots, 0)$ is not in the radical of Q reduced mod p. The reduction of Q' mod p is then $(k-1)$-isotropic (and regular) over $\mathbb{F}_p$ by Lemma 2.7, and the induction hypothesis applies. □

Theorem 2.10. *(i). A quadratic form over $\mathbb{F}_p$ in 3 or more variables is always isotropic.*

(ii). A quadratic form over $\mathbb{Q}_p$ in 5 or more variables is always isotropic.

Proof. (i) This is a consequence of the Chevalley-Warning theorem. See for example [8, p. 5].
(ii) This is Meyer's theorem. See for example [3, p. 41]. □

We make the following definition concerning quadratic forms over $\mathbb{F}_p$.

Definition 2.11. A quadratic form over $\mathbb{F}_p$ belongs to the class $[l, m, n]$ if it is equivalent to a form

$$Q(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{l} x_{r+2i-1} x_{r+2i} + f(x_{r+2l+1}, \ldots, x_n) \tag{4}$$

where f is a regular anisotropic form of dimension m. Note that l is the number of hyperbolic planes in the orthogonal decomposition, $m \in \{0, 1, 2\}$ by Theorem 2.10(i), n is the dimension of the form, and $r = n - 2l - m$ is the dimension of the radical.

Repeated application of Lemma 2.6 shows that every quadratic form over $\mathbb{F}_p$ belongs to the class $[l, m, n]$ for some l, m, n, and Theorem 2.8 shows that l, m, n are uniquely determined by the quadratic form.

3 Global densities

In this section we explain how Theorem 1.1 and Corollary 1.3 follow from Theorem 1.2. First we read off from Theorem 1.2 the asymptotic behaviour of $\rho_p(k, n)$ as $p \to \infty$.

Corollary 3.1. *Let $k \geqslant 1$. As $p \to \infty$, we have the following approximations.*

$$\rho_p(k, n) = \begin{cases} \frac{1}{2} + O(\frac{1}{p}) & \text{if } n = 2k; \\ 1 - \frac{1}{2p} + O(\frac{1}{p^2}) & \text{if } n = 2k+1; \\ 1 - \frac{1}{4p^3} + O(\frac{1}{p^4}) & \text{if } n = 2k+2. \end{cases}$$

Proof. In the case $n = 2k + 2$ we consider the Taylor series expansions

$$\frac{p^{k+3} - 1}{(p+1)(p^{2k+3} - 1)} = \frac{1}{p^{k+1}} \left(1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} + O\left(\frac{1}{p^4}\right)\right),$$

and

$$\prod_{i=1}^{k+1} \frac{p^{2i-1}-1}{p^{2i}-1} = \frac{1}{p^{k+1}} \left(1 - \frac{1}{p} + \frac{1}{p^2} - \frac{2}{p^3} + O\left(\frac{1}{p^4}\right) \right),$$

using the big O notation. Substituting these expansions into the formula for $\rho_p(k,n)$ in Theorem 1.2 gives the approximation for $\rho_p(k,n)$ as claimed. The other cases are similar but easier. $\square$

Fix values of k and n, and let $d = \binom{n+1}{2}$. We write U_∞ for the set of quadratic forms in $\mathbb{R}[x_1, \dots, x_n]$ that are *not* k-isotropic over $\mathbb{R}$. Likewise we write U_p for the set of quadratic forms in $\mathbb{Z}_p[x_1, \dots, x_n]$ that are *not* k-isotropic over $\mathbb{Q}_p$. Let μ_∞ denote the standard Lebesgue measure on $\mathbb{R}^d$, and let μ_p denote the Haar measure on $\mathbb{Z}_p^d$ normalised to have total volume 1.

Lemma 3.2. *Let $1 \leqslant k \leqslant n$ and $d = \binom{n+1}{2}$. Suppose that the following condition holds for all sufficiently large primes p:*

> *Every quadratic form in $\mathbb{Z}_p[x_1, \dots, x_n]$ whose reduction mod p has rank at least $n-1$ is k-isotropic over $\mathbb{Q}_p$.*

Then $\rho_{\mathrm{glob}}(k,n)$ exists and is given by

$$\rho_{\mathrm{glob}}(k,n) = \frac{\mu_\infty([-1,1]^d \setminus U_\infty)}{2^d} \cdot \prod_p (1 - \mu_p(U_p)). \tag{5}$$

Proof. As noted in the introduction, a quadratic form is k-isotropic over $\mathbb{Q}$ if and only if it is k-isotropic over $\mathbb{Q}_p$ for all primes p and over $\mathbb{R}$. We then apply [7, Lemmas 20 and 21] with U_∞ and U_p as defined above, $S = \emptyset$ and $f, g \in \mathbb{Z}[a_{11}, a_{12}, \dots, a_{nn}]$ two distinct $(n-1) \times (n-1)$ minors of the generic $n \times n$ symmetric matrix of coefficients. $\square$

It is not hard to show that, with notation as defined in the statement of Theorem 1.1, the factors on the right hand side of (5) may be written

$$\rho_\infty(k,n) = \frac{\mu_\infty([-1,1]^d \setminus U_\infty)}{2^d} \qquad \text{and} \qquad \rho_p(k,n) = 1 - \mu_p(U_p). \tag{6}$$

Proof of Theorem 1.1. Let $\rho_{\mathrm{glob}}(k,n)$ be as defined in (2), and let $\overline{\rho}_{\mathrm{glob}}(k,n)$ be the same quantity with the limit replaced by lim sup. We write $\rho_p(k,n)$ for the probabilities computed in Theorem 1.2. A standard argument (see for example [4, Proposition 3.2]) uses the local conditions at finitely many primes to show that

$$\overline{\rho}_{\mathrm{glob}}(k,n) \leqslant \prod_{p<M} \rho_p(k,n). \tag{7}$$

If $n \leqslant 2k+1$ then by Corollary 3.1 the right hand side of (7) tends to 0 as $M \to \infty$. Therefore $\rho_{\mathrm{glob}}(k,n) = 0$ and the equality claimed in Theorem 1.1 holds since both sides are zero.

If $n \geqslant 2k+2$ then we claim that the condition in Lemma 3.2 is satisfied. To see this we let $Q \in \mathbb{Z}_p[x_1, \dots, x_n]$ be a quadratic form whose reduction mod p has rank at least $n-1$. In the terminology of Definition 2.11, the reduction of Q mod p belongs to the class $[l,m,n]$ for some l,m,n with $m \in \{0,1,2\}$. Our assumptions then give $2l + m \geqslant n - 1 \geqslant 2k+1$. Since k and l are integers it follows that $l \geqslant k$. Then Q is k-isotropic over $\mathbb{Q}_p$ by Lemma 2.9. This proves the claim. Then combining (5) and (6) gives

$$\rho_{\text{glob}}(k,n) = \rho_\infty(k,n) \prod_p \rho_p(k,n)$$

as required. □

Corollary 1.3 follows immediately from Theorem 1.1, Theorem 1.2 and the observation in the last proof that the local product is zero for $n \leqslant 2k+1$.

Remark 3.3. We do not know an accurate method for computing the probabilities $\rho_\infty(k,n)$, but we can estimate them using a Monte Carlo simulation. On this basis we record the following numerical values that are likely to be accurate to the number of decimal places recorded.

k	$\prod_p \rho_p(k,2k+2)$	$\rho_\infty(k,2k+2)$	$\rho_{\text{glob}}(k,2k+2)$
1	0.98743625	0.9823	0.9699
2	0.98229463	0.9705	0.9533
3	0.98007620	0.9623	0.9431
4	0.97906880	0.9561	0.9361
5	0.97859528	0.9512	0.9309

Remark 3.4. In [2] (which only treats the case $k=1$) some alternatives to the definition (2) were considered. The global densities so defined may still be computed as a product over all places, and the local contributions at the finite places are the same as before. However the local contributions at infinity can change, and for one natural choice of distribution these were computed exactly. It is possible that something similar could be done for $k>1$, but we did not pursue this.

4 Counting quadratic forms over $\mathbb{F}_p$

In this section we prove some formulae counting quadratic forms over $\mathbb{F}_p$. We consider quadratic forms over $\mathbb{F}_p$ according to their class $[l,m,n]$ as defined in Definition 2.11.

Definition 4.1. Consider a quadratic form

$$Q(x_1,x_2,\dots,x_n) = \sum_{1\leqslant i\leqslant j\leqslant n} a_{ij}x_ix_j$$

over $\mathbb{F}_p$ where the coefficients a_{ij} are chosen independently at random according to counting measure.

Let $\pi_0(l,m,n)$ be the probability that Q belongs to the class $[l,m,n]$.

Let $\pi_1(l,m,n)$ be the probability that Q belongs to the class $[l,m,n]$ given that $a_{11}\neq 0$.

Let $\pi_2(l,m,n)$ be the probability that Q belongs to the class $[l,m,n]$ given that $a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2$ is a regular anisotropic form.

Note that Theorem 2.10(i) implies that $\pi_i(l,m,n)=0$ if $m\geqslant 3$.

The group $\mathrm{GL}_n(\mathbb{F}_p)$ acts on the set of n-dimensional quadratic forms over $\mathbb{F}_p$ by linear substitutions. The class $[l,m,n]$ is the union of either one or two orbits (see below for references), and so its size may be computed as a sum of orbit sizes. To begin with we only consider forms that are regular. In these cases the orbit sizes can be computed using the orbit-stabiliser theorem and the following theorem.

Lemma 4.2. *Let Q_0 be a quadratic form over $\mathbb{F}_p$ belonging to the class $[l,m,n]$. Suppose that Q_0 is regular, equivalently $n = 2l + m$. Then the stabiliser in $\mathrm{GL}_n(\mathbb{F}_p)$ of Q_0 is an orthogonal group of order $S(m,n)$ where*

$$S(0,2k) = 2p^{k(k-1)}(p^k-1)\prod_{i=1}^{k-1}(p^{2i}-1);$$

$$S(1,2k+1) = \begin{cases} 2p^{k^2}\prod_{i=1}^{k}(p^{2i}-1) & \text{if } p \neq 2; \\ p^{k^2}\prod_{i=1}^{k}(p^{2i}-1) & \text{if } p = 2; \end{cases}$$

$$S(2,2k) = 2p^{k(k-1)}(p^k+1)\prod_{i=1}^{k-1}(p^{2i}-1).$$

Proof. See [5, pp. 81–82] for p an odd prime, and [5, pp. 147–150] for the case $p = 2$. □

To find the orbit size when the radical has dimension $r = n - 2l - m$, we multiply the orbit size of the regular part under the action of $\mathrm{GL}_{n-r}(\mathbb{F}_p)$ by the number

$$\binom{n}{r}_p = \prod_{i=0}^{r-1}\frac{p^n - p^i}{p^r - p^i}$$

of r-dimensional subspaces of $\mathbb{F}_p^n$. The orbit size $O(l,m,n)$ of a form in $[l,m,n]$ under the action of $\mathrm{GL}_n(\mathbb{F}_p)$ is therefore given by

$$O(l,m,n) = \binom{n}{n-2l-m}_p \cdot \frac{|\,\mathrm{GL}_{2l+m}(\mathbb{F}_p)|}{S(m,2l+m)}.$$

If $m = 1$ and p is odd, there are two orbits belonging to $[l,m,n]$; other values of m give a unique orbit (see [5, p. 79]). Hence, using that $|\,\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i)$, and dividing by the total number of quadratic forms of dimension n, we obtain the values of $\pi_0(l,m,n)$ recorded in the next lemma. Note that the only form in the class $[0,0,n]$ is the form where all the coefficients are zero.

Lemma 4.3. *For $l + m > 0$ and $n = 2l + m + r$ we have*

$$\pi_0(l,m,n) = \begin{cases} \frac{1}{p^{n(n+1)/2}} \cdot \prod_{i=0}^{r-1}\frac{p^n-p^i}{p^r-p^i} \cdot \frac{\prod_{i=0}^{2l-1}(p^{2l}-p^i)}{2p^{l(l-1)}(p^l-1)\prod_{i=1}^{l-1}(p^{2i}-1)} & \text{if } m = 0; \\ \frac{1}{p^{n(n+1)/2}} \cdot \prod_{i=0}^{r-1}\frac{p^n-p^i}{p^r-p^i} \cdot \frac{\prod_{i=0}^{2l}(p^{2l+1}-p^i)}{p^{l^2}\prod_{i=1}^{l}(p^{2i}-1)} & \text{if } m = 1; \\ \frac{1}{p^{n(n+1)/2}} \cdot \prod_{i=0}^{r-1}\frac{p^n-p^i}{p^r-p^i} \cdot \frac{\prod_{i=0}^{2l+1}(p^{2l+2}-p^i)}{2p^{l(l+1)}(p^{l+1}+1)\prod_{i=1}^{l}(p^{2i}-1)} & \text{if } m = 2. \end{cases}$$

Moreover, $\pi_0(0,0,n) = 1/p^{n(n+1)/2}$.

Next we compute the probabilities $\pi_1(l,m,n)$ in terms of the probabilities $\pi_0(l,m,n)$.

Lemma 4.4. *We have*

$$\pi_1(l,m,n) = \begin{cases} \pi_0(l-1,1,n-1)/2 & \text{if } m = 0 \text{ and } l \geqslant 1; \\ \pi_0(l,0,n-1) + \pi_0(l-1,2,n-1) & \text{if } m = 1 \text{ and } l \geqslant 1; \\ \pi_0(l,1,n-1)/2 & \text{if } m = 2. \end{cases}$$

Moreover, $\pi_1(0,0,n) = 0$ and $\pi_1(0,1,n) = 1/p^{n(n-1)/2}$.

Proof. We first suppose that p is an odd prime. Let Q be a quadratic form in n variables over $\mathbb{F}_p$ with first coefficient $a_{11} \neq 0$. We must compute the probability $\pi_1(l,m,n)$ that Q belongs to the class $[l,m,n]$. By a linear substitution to eliminate the cross-terms containing x_1, we may assume that $Q(x_1,x_2,\ldots,x_n) = a_{11}x_1^2 + F(x_2,x_3,\ldots,x_n)$ for some $F \in \mathbb{F}_p[x_2,\ldots,x_n]$. The class of Q is determined by the class of F and the value of a_{11}. Since the coefficients of F, like those of Q, are randomised according to counting measure (suitably normalised), we can compute $\pi_1(l,m,n)$ in terms of the $\pi_0(l',m',n-1)$ for suitable l' and m'. More precisely, using Lemma 2.6 and Theorem 2.10(i), we note that if F belongs to the class $[l,0,n-1]$ or $[l-1,2,n-1]$ then Q belongs to the class $[l,1,n]$, whereas if F belongs to the class $[l-1,1,n-1]$ then it is equally likely that Q belongs to the class $[l,0,n]$ or $[l-1,2,n]$. The stated formulae follow.

To prove the lemma when $p=2$ we outline an alternative method for computing $\pi_1(l,m,n)$ that gives the answer as a rational function in p. In this alternative method we compute $\pi_1(l,m,n)$ by finding the probability that a form in $[l,m,n]$ satisfies $a_{11} \neq 0$, and then multiply by $\pi_0(l,m,n) \cdot \frac{p}{p-1}$ according to Bayes' formula. The second factor comes from the fact that $a_{11} \neq 0$ with probability $\frac{p-1}{p}$. Since $a_{11} = Q(1,0,\ldots,0)$ and $\mathrm{GL}_n(\mathbb{F}_p)$ acts transitively on $\mathbb{F}_p^n \setminus \{0\}$ it suffices to show that

$$N(Q) = \#\{x \in \mathbb{F}_p^n \mid Q(x) = 0\}$$

is a polynomial in p, where the polynomial depends only on l,m,n. We prove this claim by induction on l, noting that if $Q(x_1,\ldots,x_n) = x_1x_2 + Q'(x_3,\ldots,x_n)$ then $N(Q) = (2p-1)N(Q') + (p-1)(p^{n-2} - N(Q'))$, whereas if $l=0$ then $N(Q) = p^{n-m}$. □

To determine the values of $\pi_2(l,m,n)$, we use a method similar to the one we used for calculating $\pi_1(l,m,n)$ for p an odd prime. However, this proof also includes the case $p=2$.

Lemma 4.5. *We have*

$$\pi_2(l,m,n) = \begin{cases} \pi_0(l-2,2,n-2) & \text{if } m=0 \text{ and } l \geqslant 2; \\ \pi_0(l-1,1,n-2) & \text{if } m=1 \text{ and } l \geqslant 1; \\ \pi_0(l,0,n-2) & \text{if } m=2. \end{cases}$$

Moreover, $\pi_2(0,0,n) = \pi_2(0,1,n) = \pi_2(1,0,n) = 0$.

Proof. It suffices to consider $Q(x_1,x_2,\ldots,x_n) = f(x_1,x_2) + F(x_3,\ldots,x_n)$ for $f \in \mathbb{F}_p[x_1,x_2]$ regular anisotropic and $F \in \mathbb{F}_p[x_3,\ldots,x_n]$. The class of F then determines the class of Q, and again using Lemma 2.6 and Theorem 2.10(i), this gives the formulae as stated. □

5 First method: Reduction modulo p and recursion

In this section we give our first method for computing the probability $\rho_p(k,n)$ that a random p-adic integral quadratic form in n variables is k-isotropic.

Definition 5.1. Let Q be a random p-adic integral quadratic form in n variables.

Let $\delta_0(k;l,m,n)$ be the probability that Q is k-isotropic given that its reduction mod p belongs to the class $[l,m,n]$.

Let $\delta_1(k;l,m,n)$ be the probability that Q is k-isotropic given that its reduction mod p belongs to the class $[l,m,n]$, the coefficients $a_{11},a_{12},\ldots,a_{1n}$ are all divisible by p, but p^2 does not divide a_{11}.

Let $\delta_2(k;l,m,n)$ be the probability that Q is k-isotropic given that its reduction mod p belongs to the class $[l,m,n]$, the coefficients $a_{11},a_{12},\ldots,a_{1n}$ and $a_{22},a_{23},\ldots,a_{2n}$ are all divisible by p, but the reduction of $\frac{1}{p}(a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2)$ mod p is a regular anisotropic form.

By definition $\delta_0(k;0,0,n)$ is the probability of k-isotropy given that Q vanishes mod p. This is the same as $\rho_p(k,n)$. Our next two results establish recursive relations for computing the $\delta_i(k;l,m,n)$.

Lemma 5.2. *For $i \in \{0,1,2\}$ we have*

$$\delta_i(k;l,m,n) = \begin{cases} \delta_i(k-l;0,m,n-2l) & \text{if } k > l; \\ 1 & \text{if } k \leqslant l. \end{cases}$$

Proof. A quadratic form whose reduction modulo p belongs to the class $[l,m,n]$ is equivalent over $\mathbb{Z}_p$ to a form which satisfies

$$Q(x_1,\ldots,x_n) \equiv \sum_{i=1}^{l} x_{r+2i-1}x_{r+2i} + f(x_{r+2l+1},\ldots,x_n) \mod p, \tag{8}$$

for f a regular anisotropic form over $\mathbb{F}_p$ of dimension $m \in \{0,1,2\}$. We claim that Q is equivalent over $\mathbb{Z}_p$ to a form

$$Q'(x_1,\ldots,x_n) = \sum_{i=1}^{l} x_{r+2i-1}x_{r+2i} + Q''(x_1,\ldots,x_r,x_{r+2l+1},\ldots,x_n), \tag{9}$$

where $Q''(x_1,\ldots,x_r,x_{r+2l+1},\ldots,x_n) \equiv f(x_{r+2l+1},\ldots,x_n) \mod p$. If $k \leqslant l$ it follows immediately that Q is k-isotropic. If $k > l$ then by Lemma 2.7, the form Q is k-isotropic if and only if the form Q'' is $(k-l)$-isotropic. So it only remains to prove the claim, and at the same time convince ourselves that, subject to the conditions in Definition 5.1, the coefficients of Q'' are independently distributed according to Haar measure.

For simplicity we consider the case $r = 0$ and $l = 1$. Then the $\mathbb{Z}_p$-equivalence taking (8) to (9) is built out of two sorts of transformations. First we let $\mathrm{GL}_2(\mathbb{Z}_p)$ act on the variables x_1 and x_2 by linear substitution. By the case $k = 1$ of Lemma 2.9, such a transformation exists taking $Q(x_1,x_2,0,\ldots,0)$ to x_1x_2. This shows that Q is $\mathbb{Z}_p$-equivalent to a quadratic form Q_0 satisfying

$$Q_0(x_1,x_2,\ldots,x_n) = x_1x_2 + px_1 \cdot g_1(x_3,\ldots,x_n) + px_2 \cdot g_2(x_3,\ldots,x_n) + Q(0,0,x_3,\ldots,x_n)$$

for some linear forms g_1, g_2 in $\mathbb{Z}_p[x_3,\ldots,x_n]$. Then we make the substitutions $x_1 \leftarrow x_1 - p \cdot g_2(x_3,\ldots,x_n)$ and $x_2 \leftarrow x_2 - p \cdot g_1(x_3,\ldots,x_n)$ to obtain a quadratic form Q' of the shape (9) with $Q''(x_3,\ldots,x_n) \equiv Q(0,0,x_3,\ldots,x_n) \mod p^2$.

For general $r \geqslant 0$ (but still $l = 1$) we follow the same strategy. First we let $\mathrm{GL}_2(\mathbb{Z}_p)$ act on the variables x_{r+1} and x_{r+2}. Then we make substitutions for x_{r+1} and x_{r+2} where we add to each p times a linear combination of the other variables $x_1,\ldots,x_r,x_{r+3},\ldots,x_n$. Again we have

$$Q''(x_1,\ldots,x_r,x_{r+3},\ldots,x_n) \equiv Q(x_1,\ldots,x_r,0,0,x_{r+3},\ldots,x_n) \mod p^2.$$

Since the extra conditions on Q in the definition of the δ_i for $i = 1,2$ are conditions on the coefficients mod p^2, these are not affected by this change. The result for general l follows by induction. □

Lemma 5.3. *For $i,j \in \{0,1,2\}$ and $n \geqslant i+j$ we have*

$$\delta_i(k;0,j,n) = \sum_{l \geqslant 0} \sum_{m=0}^{2} \pi_i(l,m,n-j)\delta_j(k;l,m,n).$$

Moreover, if $n = i+j$ then

$$\delta_i(k;0,j,n) = \begin{cases} 1 & \text{if } k = 0; \\ 0 & \text{if } k \geqslant 1. \end{cases}$$

The condition $n \geqslant i+j$ ensures that $\pi_i(l,m,n-j)$ is defined. It can only be non-zero if $2l+m \leqslant n-j$, in which case $\delta_j(k;l,m,n)$ is defined. In particular the sum over l is finite.

Proof. Let Q be a p-adic integral quadratic form of dimension n whose reduction mod p belongs to the class $[0,j,n]$. By an equivalence over $\mathbb{Z}_p$ we may suppose that the reduction of Q mod p is an anisotropic form in the last $j \in \{0,1,2\}$ variables. We replace $Q(x_1,\ldots,x_n)$ by

$$\frac{1}{p}Q(x_1,\ldots,x_{n-j},px_{n-j+1},\ldots,px_n).$$

This is again a p-adic integral quadratic form, but now the reduction mod p involves only the first $n-j$ variables. If $i=1$ or 2 then the additional conditions in Definition 5.1 give the additional conditions in Definition 4.1. The reduction mod p now has class $[l,m,n]$ with probability $\pi_i(l,m,n-j)$, and in this case the form is k-isotropic with probability $\delta_j(k;l,m,n)$. In checking this last statement, notice that the extra conditions in Definition 5.1 when $j=1$ or 2 are satisfied relative to the last j variables rather than the first j variables. This change clearly does not matter. Summing over all possibilities for l and m gives the result.

For the final part we show that if $n=i+j$ then the forms considered in the definition of $\delta_i(k;0,j,n)$ are anisotropic over $\mathbb{Q}_p$. For example, if $i=j=2$ and $n=4$ then the reduction of $Q(x_1,\ldots,x_4)$ mod p is an anisotropic form in x_3 and x_4, and the reduction of $\frac{1}{p}Q(x_1,x_2,px_3,px_4)$ mod p is an anisotropic form in x_1 and x_2. Supposing that $Q(a_1,\ldots,a_4)=0$ for some $a_1,\ldots,a_4 \in \mathbb{Z}_p$ not all divisible by p these conditions quickly lead to a contradiction. The other cases are similar. □

Proposition 5.4. *The relations in Lemmas 5.2 and 5.3 are sufficient to determine all the $\delta_i(k;l,m,n)$ and to show that they are rational functions in p. The same is therefore true of $\rho_p(k,n)=\delta_0(k;0,0,n)$.*

Proof. Combining the two lemmas shows that

$$\delta_i(k;0,j,n) = \frac{1}{p^{\binom{n+1-i-j}{2}}}\delta_j(k;0,i,n)+\ldots$$

where the terms omitted involve either a smaller value of n or a larger value of $i+j$. Assuming all such previous values have been computed, we can uniquely solve for $\delta_i(k;0,j,n)$ and $\delta_j(k;0,i,n)$ provided that $n>i+j$. It is clear from Definition 5.1 that we must have $n \geqslant i+j$ and the remaining case where $n=i+j$ is covered by the last part of Lemma 5.3. Finally we use Lemma 5.2 to compute the $\delta_i(k;l,m,n)$ with $l>0$.

Since we saw in Section 4 that the $\pi_i(l,m,n)$ are rational functions in p, it follows that the $\delta_i(k;l,m,n)$ are also rational functions in p. □

Proposition 5.4 together with the results of the next section are all we shall need for the proof of Theorem 1.2. It is nonetheless still interesting to find explicit closed formulae for the $\delta_i(k;l,m,n)$. We do this now, leaving some of the details to Appendix A.

Definition 5.5. For $i,j \in \{0,1,2\}$ and $n \geqslant i+j$ we define

$$\phi(i,j,n) = \big((j-1)p^d+(i-1)\big)\cdot\prod_{r=1}^{d}\frac{p^{2r-1}-1}{p^{2r}-1},$$

$$\psi(i,j,n) = \frac{\big((j-1)p^d+(i-1)\big)\big((j-1)p^{d+2}-(i-1)\big)-\delta_{i1}p+\delta_{j1}p^{2d+1}}{(p+1)(p^{2d+1}-1)},$$

where $d=\lfloor\frac{n+1-i-j}{2}\rfloor$ and δ_{ij} is the Kronecker delta.

Proposition 5.6. *Let $i, j \in \{0,1,2\}$ and $n \geqslant i+j$. Then*

$$\phi(i,j,n) = \sum_{l \geqslant 0} \sum_{m=0}^{2} \pi_i(l,m,n-j)\phi(j,m,n-2l),$$

and if n is **even** *then*

$$\psi(i,j,n) = \sum_{l \geqslant 0} \sum_{m=0}^{2} \pi_i(l,m,n-j)\psi(j,m,n-2l).$$

Proof. We prove this in Appendix A by adapting methods of Kovaleva [6]. □

Theorem 1.2 is the special case $i = j = 0$ of the following result.

Theorem 5.7. *For any $i, j \in \{0,1,2\}$ and $n \geqslant i+j$ we have*

$$\delta_i(k;0,j,n) = \begin{cases} 0 & \text{if } n \leqslant 2k-1; \\ \frac{1}{4}\big(-\phi(i,j,n) + \psi(i,j,n)\big) & \text{if } n = 2k; \\ \frac{1}{2}\big(1 - \phi(i,j,n)\big) & \text{if } n = 2k+1; \\ 1 - \frac{1}{4}\big(\phi(i,j,n) + \psi(i,j,n)\big) & \text{if } n = 2k+2; \\ 1 & \text{if } n \geqslant 2k+3. \end{cases}$$

Proof. By Proposition 5.6 these are solutions to the recurrence relations in Proposition 5.4. These particular linear combinations of 1, ϕ and ψ also satisfy the initial conditions, that is, we checked they give the correct answers when $n = i+j$. □

As explained in the introduction, the following corollary is interesting since it generalises a phenomenon studied in [1].

Corollary 5.8. *The probabilities $\delta_i(k;l,j,n)$ and $\delta_j(k;l,i,n)$ are rational functions in p that are exchanged when we replace p by $1/p$. In particular $\rho_p(k,n) = \delta_0(k;0,0,n)$ is unchanged when we replace p by $1/p$.*

Proof. By Lemma 5.2 it suffices to prove the case $l = 0$. The symmetries claimed then follow from Definition 5.5 and Theorem 5.7. □

6 Second method: Using a theorem of Kovaleva

In this section we deduce Theorem 1.2 from a result of Kovaleva [6]. First we recall the classification of quadratic forms over $\mathbb{Q}_p$ up to equivalence.

Definition 6.1. Let a, $b \in \mathbb{Q}_p^*$. The *Norm-Residue symbol*, denoted $\binom{a,b}{p}$ or more simply as (a,b), is set to be 1 when the form $ax^2 + by^2 - z^2$ vanishes for some $x, y, z \in \mathbb{Q}_p$ not all zero, and -1 otherwise.

Definition/Lemma 6.2. Let $Q \in \mathbb{Q}_p[x_1, \ldots, x_n]$ be a quadratic form of rank n which is equivalent to a diagonal form $Q'(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^2$. The *Hasse-Minkowski invariant* of the form Q is defined as $c(Q) = \prod_{i<j}(a_i, a_j)$. This is independent of the choice of diagonal form.

Proof. See [3, pp. 56–58]. □

Theorem 6.3. *A quadratic form $Q \in \mathbb{Q}_p[x_1, \dots, x_n]$ of rank n is uniquely determined up to $\mathbb{Q}_p$-equivalence by its determinant $d(Q) \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ and its Hasse-Minkowski invariant $c(Q) \in \{\pm 1\}$.*

Proof. See [3, p. 61]. □

The next lemma explains why we only need to consider forms of full rank over $\mathbb{Q}_p$.

Lemma 6.4. *A p-adic integral quadratic form, with coefficients chosen independently from $\mathbb{Z}_p$ according to Haar measure, is singular with probability zero.*

Proof. We write the form as $Q(x_1, x_2, \dots, x_n) = a_{11}x_1^2 + x_1 \cdot f(x_2, \dots, x_n) + g(x_2, \dots, x_n)$ for some linear form $f \in \mathbb{Z}_p[x_2, \dots, x_n]$ and quadratic form $g \in \mathbb{Z}_p[x_2, \dots, x_n]$.

If $n = 1$, the form is singular when a_{11} is zero, which happens with probability zero. Inductively, for $n > 1$, we can assume the form g to be non-singular. For each linear form f and non-singular form g, there is only one value of a_{11} that makes Q singular, corresponding to the determinant of the coefficient matrix being zero. This value is attained by a_{11} with probability zero, hence the form is singular with probability zero by induction. □

We now take p an odd prime. The following theorem, due to Kovaleva, gives for each triple (n, d, c) the probability that a random p-adic integral quadratic form Q in n variables has determinant $d(Q) = d$ and Hasse-Minkowski invariant $c(Q) = c$. Since p is an odd prime, the quotient $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ has order 4, with coset representatives $\{1, u, p, up\}$ where u is a quadratic non-residue modulo p.

Theorem 6.5 (Kovaleva)**.** *Let p be an odd prime, and let $Q \in \mathbb{Z}_p[x_1, x_2, \dots, x_n]$ be a random p-adic integral quadratic form in n variables. Let ε and s denote the Legendre symbols $(\frac{-1}{p})$ resp. $(\frac{d}{p})$ and let u be a quadratic non-residue modulo p. Then the probability $\mathbb{P}_n(d(Q) = d, c(Q) = c)$ that Q has determinant $d \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ and Hasse-Minkowski invariant $c \in \{\pm 1\}$ is given by*

$$\mathbb{P}_{2k+1}(d(Q) = d, c(Q) = c) = \begin{cases} \frac{1}{4} \cdot \frac{p}{p+1} + \frac{1}{4} \cdot c \cdot p^{k+1} \cdot \prod_{i=1}^{k+1} \frac{p^{2i-1} - 1}{p^{2i} - 1} & \text{if } d \in \{1, u\}; \\ \frac{1}{4} \cdot \frac{1}{p+1} + \frac{1}{4} \cdot c \cdot \varepsilon^k \cdot \prod_{i=1}^{k+1} \frac{p^{2i-1} - 1}{p^{2i} - 1} & \text{if } d \in \{p, up\}; \end{cases}$$

$$\mathbb{P}_{2k}(d(Q) = d, c(Q) = c) = \begin{cases} \frac{1}{4} \cdot (p^k + s\varepsilon^k) \cdot \left(\frac{(p^{k+2} - s\varepsilon^k)}{(p+1)(p^{2k+1} - 1)} + c \cdot \prod_{i=1}^{k} \frac{p^{2i-1} - 1}{p^{2i} - 1} \right) & \text{if } d \in \{1, u\}; \\ \frac{1}{4} \cdot \frac{p}{p+1} \cdot \frac{p^{2k} - 1}{p^{2k+1} - 1} & \text{if } d \in \{p, up\}. \end{cases}$$

Proof. See [6, Theorem 1.3]. □

We deduce Theorem 1.2 for p odd using the following lemma. Recall that we wrote $\rho_p(k, n)$ for the probability that a random p-adic integral quadratic form in n variables is k-isotropic.

Lemma 6.6. *We have $\rho_p(k,n) = 0$ for $n \leqslant 2k-1$ and $\rho_p(k,n) = 1$ for $n \geqslant 2k+3$. If p is odd then*

$$\rho_p(k, 2k) = \mathbb{P}_{2k}(d(Q) = (-1)^k, c(Q) = 1);$$
$$\rho_p(k, 2k+1) = \sum_{a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2} \mathbb{P}_{2k+1}(d(Q) = (-1)^k a, c(Q) = (-1, a)^k);$$
$$\rho_p(k, 2k+2) = 1 - \mathbb{P}_{2k+2}(d(Q) = (-1)^{k-1}, c(Q) = -1).$$

Proof. We first note that if $n \leqslant 2k-1$ then every k-isotropic form of dimension n is singular, and so $\rho_p(k,n) = 0$ by Lemma 6.4. We now suppose that $n \geqslant 2k$. By Lemma 2.6 every regular quadratic form of dimension n over $\mathbb{Q}_p$ is equivalent to one of the form

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^{l} x_{2i-1}x_{2i} + f(x_{2l+1}, \ldots, x_{2l+m}), \tag{10}$$

where l is the number of hyperbolic planes in the decomposition, $f(x_{2l+1}, \ldots, x_{2l+m})$ is an anisotropic form over $\mathbb{Q}_p$ of rank m, and $n = 2l + m$. By Theorem 2.10(ii) we have $m \leqslant 4$. It follows that if $n \geqslant 2k+3$ then $k \leqslant l$ and so $\rho_p(k,n) = 1$.

We now take p an odd prime. If $n = 2k$ then for the form in (10) to be k-isotropic we need $l = k$ and $m = 0$. There is only one such form up to $\mathbb{Q}_p$-equivalence. It has determinant $d(Q) = (-1)^k$ and Hasse-Minkowski invariant $c(Q) = 1$. This gives the formula for $\rho_p(k, 2k)$ as stated. If $n = 2k+1$ then for k-isotropy we need $l = k$ and $m = 1$. The anisotropic form in (10) is $f(x_n) = ax_n^2$ for some $a \in \{1, u, p, up\}$. This gives four $\mathbb{Q}_p$-equivalence classes of forms, with invariants $d(Q) = (-1)^k a$ and $c(Q) = (-1, a)^k$. Finally we take $n = 2k+2$. For Q *not* to be k-isotropic we need $l = k-1$ and $m = 4$. The rank 4 anisotropic form f has determinant $d(f) = 1$ and Hasse-Minkowski invariant $c(f) = -1$ (see [3, p. 59]). It follows that $d(Q) = (-1)^{k-1}$ and $c(Q) = -1$, giving the result as stated. □

Theorem 1.2 for p odd now follows from Theorem 6.5 and Lemma 6.6. The interesting thing to note is that the Legendre symbols ε and s cancel, giving answers that are rational functions in p. Indeed when $n = 2k$ we have $s\varepsilon^k = 1$. When $n = 2k+1$ the contributions for $a \in \{1, u\}$ have $c = 1$ and the contributions for $a \in \{p, up\}$ have $c = \varepsilon^k$. When $n = 2k+2$ we employ the corresponding formula in Theorem 6.5 with k replaced by $k+1$ and s replaced by ε^{k-1}.

We saw in Proposition 5.4 that $\rho_p(k,n)$ is given by a rational function in p, where the same rational function works for all primes p including the prime $p = 2$. Since we proved Theorem 1.2 in the last paragraph for infinitely many primes (in fact for all odd primes), the theorem is therefore true for all primes.

A Solving the recurrence relations for the first method

In this appendix we prove Proposition 5.6. This is not needed for the proof of our main theorems as stated in the introduction, but is needed to compute all the $\delta_i(k; l, m, n)$ (see Theorem 5.7) and hence to see that they satisfy some interesting symmetries (see Corollary 5.8). The proof is based on that of Theorem 6.5, but we could not see a way to directly cite Kovaleva's work without reworking the details.

The identities we seek to prove are ones between rational functions in p. So it suffices to prove them for any infinite set of primes. There is therefore no loss of generality in assuming (as we now do) that p is odd. This allows us to identify quadratic forms and symmetric matrices in the usual way.

Definition A.1. Let $\lambda(s,n)$ be the probability that a randomly chosen $n \times n$ symmetric matrix over $\mathbb{F}_p$ has rank s. In the notation of Section 4 we have

$$\lambda(s,n) = \begin{cases} \pi_0(l,0,n) + \pi_0(l-1,2,n) & \text{if } s = 2l; \\ \pi_0(l,1,n) & \text{if } s = 2l+1, \end{cases}$$

where the right hand sides are given explicitly in Lemma 4.3. Alternatively, following [6, Section 4.1], we have

$$\lambda(s,n) = p^{-(n-s)(n-s+1)/2} \frac{\pi_n}{\pi_{n-s}\beta_s}, \tag{11}$$

where $\pi_n = \prod_{i=1}^{n}(1-p^{-i})$ and $\beta_s = \prod_{i=1}^{\lfloor s/2 \rfloor}(1-p^{-2i})$.

Lemma A.2. *For any $x \in \mathbb{R}$ we have*

$$\sum_{\substack{s=0 \\ n-s \text{ even}}}^{n} \lambda(s,n)\frac{x-p^s}{p^{n+1}-p^s} + \sum_{\substack{s=0 \\ n-s \text{ odd}}}^{n} \lambda(s,n) = \begin{cases} \dfrac{x-1}{p^{n+1}-1} & \text{if } n \text{ is even;} \\ \dfrac{x}{p^{n+1}} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Since each side is linear in x, it suffices to prove the identity for just two values of x. If $x = p^{n+1}$ then this is just the fact that $\sum_{s=0}^{n} \lambda(s,n) = 1$. If $n = 2k$ and $x = 1$ then the left hand side is

$$\sum_{t=1}^{k} \left(\lambda(2t,n)\frac{1-p^{2t}}{p^{n+1}-p^{2t}} + \lambda(2t-1,n) \right)$$

whereas if $n = 2k+1$ and $x = 0$ then the left hand side is

$$\sum_{t=0}^{k} \left(\lambda(2t,n) - \lambda(2t+1,n)\frac{p^{2t}}{p^{n+1}-p^{2t}} \right).$$

It may be checked using (11) that in each of these last two sums all the summands are zero. $\square$

Lemma A.3. *Let $\pi_n = \prod_{i=1}^{n}(1-p^{-i})$. Then for any $m,n \geqslant 0$ we have*

$$\sum_{s=0}^{\min(m,n)} \frac{\pi_m \pi_n}{p^{(m-s)(n-s)}\pi_s \pi_{m-s}\pi_{n-s}} = 1.$$

Proof. This is [6, Corollary 2.3]. The sth summand is the probability that an $m \times n$ matrix over $\mathbb{F}_p$ has sank s. This may be computed by considering the action of $\mathrm{GL}_m(\mathbb{F}_p) \times \mathrm{GL}_n(\mathbb{F}_p)$ via $(A,B) : X \mapsto AXB^T$ and applying the orbit-stabiliser theorem. $\square$

We define

$$A(l) = \prod_{i=1}^{\lfloor \frac{l+1}{2} \rfloor} \frac{p^{2i}-p}{p^{2i}-1}, \qquad B(l) = \prod_{i=1}^{\lfloor \frac{l+1}{2} \rfloor} \frac{p^{2i-1}-1}{p^{2i}-1}. \tag{12}$$

In Kovaleva's notation, as already used in (11), these may be written

$$A(l) = \frac{\pi_l}{\beta_l \beta_{l+1}}, \qquad B(l) = \frac{\pi_l}{p^{\lfloor \frac{l+1}{2} \rfloor}\beta_l \beta_{l+1}}. \tag{13}$$

Lemma A.4. *For any $x, y, z \in \mathbb{R}$ we have*

$$\sum_{\substack{s=0\\ n-s\ even}}^{n} \lambda(s,n)B(n-s)(x+yp^{n-s}) \ + \sum_{\substack{s=0\\ n-s\ odd}}^{n} \lambda(s,n)B(n-s)(x+zp^{n+1-s})$$
$$= \begin{cases} \left(x+y+\left(1-\dfrac{1}{p^n}\right)z\right)A(n) & \text{if } n \text{ is even;} \\ \left(x+\left(1-\dfrac{1}{p^{n+1}}\right)y+z\right)A(n) & \text{if } n \text{ is odd.} \end{cases}$$

Proof. It suffices to prove this identity for three linearly independent choices of (x, y, z). If $(x, y, z) = (1, -1, 0)$ and n is even or $(x, y, z) = (1, 0, -1)$ and n is odd then by (11) and (13) the terms with $s = 2t$ and $s = 2t + 1$ cancel, giving the result in these cases. The proof is completed by the next lemma which proves the cases $(x, y, z) = (0, 1, 0)$ and $(x, y, z) = (0, 0, 1)$. □

Lemma A.5. *We have*

$$\sum_{\substack{l=0\\ l\ even}}^{n} \lambda(n-l,n)B(l)p^l = \begin{cases} A(n) & \text{if } n \text{ is even;} \\ \left(1-\frac{1}{p^{n+1}}\right)A(n) & \text{if } n \text{ is odd,} \end{cases}$$

and

$$\sum_{\substack{l=0\\ l\ odd}}^{n} \lambda(n-l,n)B(l)p^{l+1} = \begin{cases} \left(1-\frac{1}{p^{n}}\right)A(n) & \text{if } n \text{ is even;} \\ A(n) & \text{if } n \text{ is odd.} \end{cases}$$

Proof. As before we let $\pi_n = \prod_{i=1}^{n}(1-p^{-i})$ and $\beta_{2n} = \prod_{i=1}^{n}(1-p^{-2i})$. If $n = 2k$ or $2k + 1$ then

$$\begin{aligned}\sum_{\substack{l=0\\ l\text{ even}}}^{n} \lambda(n-l,n)B(l)p^l &= \sum_{\substack{l=0\\ l\text{ even}}}^{2k} \frac{\pi_n}{p^{\binom{l+1}{2}}\pi_l\beta_{2k-l}} \cdot \frac{\pi_l}{p^{l/2}\beta_l^2} \cdot p^l \\ &= \frac{\pi_n}{\beta_{2k}^2} \sum_{\substack{l=0\\ l\text{ even}}}^{2k} \frac{\beta_{2k}^2}{p^{l^2/2}\beta_{2k-l}\beta_l^2} \\ &= \frac{\pi_n}{\beta_{2k}^2} \sum_{t=0}^{k} \frac{\beta_{2k}^2}{p^{2(k-t)^2}\beta_{2t}\beta_{2(k-t)}^2}.\end{aligned}$$

The last sum here is 1, as is seen by taking $(m, n) = (k, k)$ in Lemma A.3 and replacing p by p^2. (Since Lemma A.3 is an identity that holds for all primes, and there are infinitely many primes, we may regard it as an identity of rational functions.) This leaves us with π_n/β_{2k}^2 which, upon splitting into the cases n even and n odd, agrees with the answer in the statement of the lemma.

If $n = 2k+1$ or $2k+2$ then

$$\begin{aligned}\sum_{\substack{l=0\\ l \text{ odd}}}^{n} \lambda(n-l,n)B(l)p^{l+1} &= \sum_{\substack{l=1\\ l \text{ odd}}}^{2k+1} \frac{\pi_n}{p^{\binom{l+1}{2}}\pi_l\beta_{2k+1-l}} \cdot \frac{\pi_l}{p^{(l+1)/2}\beta_{l-1}\beta_{l+1}} \cdot p^{l+1} \\ &= \frac{\pi_n}{\beta_{2k}\beta_{2k+2}} \sum_{\substack{l=1\\ l \text{ odd}}}^{2k+1} \frac{\beta_{2k}\beta_{2k+2}}{p^{(l^2-1)/2}\beta_{2k+1-l}\beta_{l-1}\beta_{l+1}} \\ &= \frac{\pi_n}{\beta_{2k}\beta_{2k+2}} \sum_{t=0}^{k} \frac{\beta_{2k}\beta_{2k+2}}{p^{2(k+1-t)(k-t)}\beta_{2t}\beta_{2(k-t)}\beta_{2(k+1-t)}}.\end{aligned}$$

The last sum here is 1, as is seen by taking $(m,n) = (k,k+1)$ in Lemma A.3 and replacing p by p^2. This leaves us with $\pi_n/(\beta_{2k}\beta_{2k+2})$ which, upon splitting into the cases n even and n odd, agrees with the answer in the statement of the lemma. ☐

Lemma A.6. *Let $\pi_i(l,m,n)$ be as defined in Section 4.*

(i). For $i, m \in \{0,1,2\}$ and $n \geqslant i$ we have

$$\pi_i(l,m,n) = \frac{1}{2}\left(1 + \delta_{m1} + \frac{(i-1)(m-1)}{p^{s/2}}\right)\lambda(s, n-i)$$

where $s = 2l + m - i$ and δ_{m1} is the Kronecker delta.

(ii). Suppose that $f(i,j,n) = \sum_{u=0}^{2}(j-1)^u f_u(i, n-i-j)$. Then for $i, j \in \{0,1,2\}$ and $n' = n-i-j \geqslant 0$ we have

$$\begin{aligned}\sum_{l\geqslant 0}\sum_{m=0}^{2} \pi_i(l,m,n-j)f(j,m,n-2l) &= \sum_{s=0}^{n'} \lambda(s,n')f_0(j,n'-s) \\ + (i-1)\sum_{\substack{s=0\\ s \text{ even}}}^{n'} \lambda(s,n')p^{-s/2}f_1(j,n'-s) &+ \sum_{\substack{s=0\\ s+i \text{ even}}}^{n'} \lambda(s,n')f_2(j,n'-s).\end{aligned}$$

Proof. (i) This follows from the formulae for the $\pi_i(l,m,n)$ in Section 4. Notice that the term involving $p^{s/2}$ only contributes when i and m are both even, in which case $s/2$ is an integer.
(ii) Replacing l by $(s+i-m)/2$ and using (i) the left hand side becomes

$$\begin{aligned}&\sum_{\substack{s=0\\ s+i \text{ even}}}^{n'} \left(\frac{1}{2}\left(1 - \frac{i-1}{p^{s/2}}\right)\lambda(s,n')f(j,0,n-i-s)\right. \\ &\qquad \left. + \frac{1}{2}\left(1 + \frac{i-1}{p^{s/2}}\right)\lambda(s,n')f(j,2,n+2-i-s)\right) \\ &\quad + \sum_{\substack{s=0\\ s+i \text{ odd}}}^{n'} \lambda(s,n')f(j,1,n+1-i-s).\end{aligned}$$

Writing f in terms of f_0, f_1, f_2 this becomes

$$\sum_{\substack{s=0\\ s+i \text{ even}}}^{n'} \left(\frac{1}{2}\left(1-\frac{i-1}{p^{s/2}}\right)\lambda(s,n')\big[f_0(j,n'-s)-f_1(j,n'-s)+f_2(j,n'-s)\big] + \frac{1}{2}\left(1+\frac{i-1}{p^{s/2}}\right)\lambda(s,n')\big[f_0(j,n'-s)+f_1(j,n'-s)+f_2(j,n'-s)\big]\right) + \sum_{\substack{s=0\\ s+i \text{ odd}}}^{n'} \lambda(s,n')f_0(j,n'-s).$$

This simplifies to the expression in the statement of the lemma. Notice that the sum involving f_1 only contributes for $i \in \{0,2\}$ and so the condition "$s+i$ even" simplifies to "s even". ☐

The functions $\phi(i,j,n)$ and $\psi(i,j,n)$ were defined in Definition 5.5. The aim of this appendix is to prove Proposition 5.6 which for convenience we now restate.

Proposition A.7. *Let $i,j \in \{0,1,2\}$ and $n \geqslant i+j$. Then*

$$\phi(i,j,n) = \sum_{l\geqslant 0}\sum_{m=0}^{2} \pi_i(l,m,n-j)\phi(j,m,n-2l), \tag{14}$$

and if n is **even** *then*

$$\psi(i,j,n) = \sum_{l\geqslant 0}\sum_{m=0}^{2} \pi_i(l,m,n-j)\psi(j,m,n-2l). \tag{15}$$

The condition $n \geqslant i+j$ ensures that $\pi_i(l,m,n-j)$ is defined. It can only be non-zero if $2l+m \leqslant n-j$, equivalently $n-2l \geqslant j+m$, in which case $\phi(j,m,n-2l)$ and $\psi(j,m,n-2l)$ are defined.

Proof. We have $\phi(i,j,n) = (j-1)A(n-i-j) + (i-1)B(n-i-j)$ where A and B were defined in (12). It follows that $\phi(i,j,n) = \sum_{u=0}^{2}(j-1)^u\phi_u(i,n-i-j)$ where

$$\phi_0(i,n) = (i-1)B(n), \quad \phi_1(i,n) = A(n), \quad \phi_2(i,n) = 0.$$

By Lemma A.6(ii) the right hand side of (14) is

$$(j-1)\sum_{s=0}^{n'}\lambda(s,n')B(n'-s) + (i-1)\sum_{\substack{s=0\\ s \text{ even}}}^{n'}\lambda(s,n')p^{-s/2}A(n'-s)$$

where $n' = n-i-j$. By Lemma A.4 the first sum is $A(n')$ and the second sum is $B(n')$. This gives $(j-1)A(n') + (i-1)B(n') = \phi(i,j,n)$, which is the left hand side of (14) as required.

We have $\psi(i,j,n) = \sum_{u=0}^{2}(j-1)^u\psi_u(i,n-i-j)$ where

$$\psi_0(i,n) = \frac{p^{2d+1}-p^{\delta_{i1}}}{(p+1)(p^{2d+1}-1)}, \quad \psi_1(i,n) = \frac{(i-1)p^d(p^2-1)}{(p+1)(p^{2d+1}-1)}, \quad \psi_2(i,n) = \frac{p^{2d+1}(p-1)}{(p+1)(p^{2d+1}-1)},$$

and $d = \lfloor \frac{n+1}{2} \rfloor$.

Now suppose that n is even. If $j \in \{0,2\}$ then by Lemma A.6(ii) the right hand side of (15) is

$$\frac{1}{p+1}\left(\sum_{\substack{s=0 \\ n'-s \text{ even}}}^{n'} \lambda(s,n') \frac{x-p^s}{p^{n'+1}-p^s} + \sum_{\substack{s=0 \\ n'-s \text{ odd}}}^{n'} \lambda(s,n') \right)$$

where $n' = n-i-j$ and $x = p^{n'+2} + (i-1)(j-1)p^{n'/2}(p^2-1)$. By Lemma A.2 this is equal to $(x-1)/((p+1)(p^{n'+1}-1))$ if $i \in \{0,2\}$ and $p/(p+1)$ if $i = 1$. This is equal to $\psi(i,j,n)$ as required.

If $j = 1$ then by Lemma A.6(ii) the right hand side of (15) is

$$\frac{p}{p+1}\left(\sum_{\substack{s=0 \\ n'-s \text{ even}}}^{n'} \lambda(s,n') \frac{p^{n'}-p^s}{p^{n'+1}-p^s} + \sum_{\substack{s=0 \\ n'-s \text{ odd}}}^{n'} \lambda(s,n') \right).$$

By Lemma A.2 this is equal to $(p^{n'+1}-p)/((p+1)(p^{n'+1}-1))$ if $i = 1$ and $1/(p+1)$ if $i \in \{0,2\}$. This is equal to $\psi(i,j,n)$ as required. □

References

[1] Bhargava, M., Cremona, J. E., Fisher, T. A., and Gajović, S. (2022). *The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$*. Proceedings of the London Mathematical Society, Volume 124, Issue 5, pp. 713–736.

[2] Bhargava, M., Cremona, J. E., Fisher, T. A., Jones, N. G., and Keating, J. P. (2016). *What is the probability that a random integral quadratic form in n variables has an integral zero?*. International Mathematics Research Notices, Issue 12, pp. 3828–3848.

[3] Cassels, J.W.S. (1978). *Rational Quadratic Forms*. Academic Press, London.

[4] Cremona, J. E. and Sadek, M. (2023). *Local and global densities for Weierstrass models of elliptic curves*, Mathematical Research Letters, 30, no. 2, pp. 413–461.

[5] Grove, L. (2002). *Classical Groups and Geometric Algebra*. American Mathematical Society, Providence.

[6] Kovaleva, V. (2023). *On the distribution of equivalence classes of random symmetric p-adic matrices*, Mathematika 69, no. 4, pp. 903–933.

[7] Poonen, B. and Stoll, M. (1999). *The Cassels-Tate pairing on polarized abelian varieties*. Annals of Mathematics (2), Volume 150, Issue 3, pp. 1109–1149.

[8] Serre, J.-P. (1973). *A Course in Arithmetic*. Springer-Verlag, New York.

Lycka Drakengren, Trinity College, Cambridge CB3 9DH, UK
E-mail address: `lyckasbrev@hotmail.com`

Tom Fisher, University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`