Classification of Quadratic Forms

Manuel Araújo

September 14, 2011

Abstract

We present the classification of quadratic forms over the rationals and then describe a partial classification of quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, when $4 \not| m$.

Contents

Introduction

The study of quadratic forms dates back many centuries and is a very important part of Number Theory and Algebra, with applications to other parts of Mathematics, such as Topology.

The theory of quadratic forms is a very vast one and in this article we mention only a very small part of it. In the first section we introduce quadratic forms and their associated bilinear forms and state some general results. The second section is dedicated to the classification of quadratic forms over the rationals (following [1, pp. 19 – 45]) and in the third section we focus on quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, obtaining a classification of suitably regular quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, when $4 \not| m$. Presumably, the full classification is already well understood, but we are not aware of a reference for these results.

We assume some previous knowledge on the part of the reader, the most important being basic linear algebra. We also assume some knowledge of basic abstract algebra, such as the concepts of a ring, a module, and a group and some of their properties, as well as some important facts about finite fields (for finite fields see, for example, [1, p.1–6]). In number theory, we assume knowledge of some important properties of the rings $\mathbb{Z}/m\mathbb{Z}$, quadratic reciprocity and familiarity with the fields $\mathbb{Q}_p$ of p-adic numbers (for quadratic reciprocity and the p-adic fields see, for example, [1, pp.6–18]).

Acknowledgements

This article is based on work developed during the school year of 2010/2011, under the supervision of Professor Gustavo Granja and in the context of the Calouste Gulbenkian Foundation program *Novos Talentos em Matemática.*

I would like to thank the Calouste Gulbenkian Foundation for their support and the organizers of the program for creating this wonderful opportunity to learn about Mathematics and share that knowledge with other students. I would also like to thank Professor Gustavo Granja for all the time he dedicated to helping me with this project.

1 Quadratic Forms

In this section, we introduce *quadratic forms*, as well as some of their general properties.

Definition 1.1. If M is a module over a commutative ring R, then a *quadratic form* on M is a function $q : M \to R$ such that:

1. $q(rm) = r^2 q(m)$, for $r \in R$ and $m \in M$.
2. The function $\beta(x, y) = q(x + y) - q(x) - q(y)$ is bilinear.

The pair (M, q) is called a *quadratic module* and β is called the *associated bilinear form* of q.

We often refer to the module M as a quadratic module, leaving the quadratic form implicit. In the following, we assume that M is a *free* R-module of *finite dimension.* The dimension of M is called the *rank* of the quadratic form.

Definition 1.2. If (M, q) and (M', q') are quadratic modules, then a linear map $f : M \to M'$ is called a *morphism* of quadratic modules (or a *metric morphism*) if $f \circ q = q'$.

We say that the two quadratic modules are *equivalent* (and write $(M, q) \sim (M', q')$) if there is a metric isomorphism (i.e. a bijective metric morphism) $(M, q) \to (M', q')$. If $M = M'$, we abreviate this as $q \sim q'$.

Lemma 1.3. *Let (M, q) be a quadratic module with basis $\{e_1, \cdots, e_n\}$ and let $x \in M$. Writing $x = \sum_i x_i e_i$, we have*

$$q(x) = \sum_{i=1}^{n} \sum_{j>i} x_i x_j \beta(e_i, e_j) + \sum_{i=1}^{n} x_i^2 q(e_i).$$

Therefore $q(x) = x^t Q x$ where Q is a matrix with entries

$$q_{ij} = \begin{cases} \beta(e_i, e_j) & \text{if } i<j \\ q(e_i) & \text{if } i=j \\ 0 & \text{otherwise} \end{cases} .$$

Proof. The proof of the first statement will be done by induction on the number m of nonzero x_i. When $m = 1$, the statement is clearly true. Now

$$q(x_1e_1 + \cdots + x_me_m) =$$

$$x_1^2 q(e_1) + q(x_2e_2 + \cdots + x_me_m) + \beta(x_1e_1, x_2e_2 + \cdots + x_me_m) =$$

$$x_1^2 q(e_1) + q(x_2e_2 + \cdots + x_me_m) + \sum_{j=2}^{m} x_1x_j\beta(e_1, e_j).$$

By the induction hypothesis, we have

$$q(x_2e_2 + \cdots + x_me_m) = \sum_{i=2}^{m}\sum_{j>i} x_ix_j\beta(e_i, e_j) + \sum_{i=2}^{m} x_i^2 q(e_i)$$

and therefore

$$q(x) = \sum_{i=1}^{m}\sum_{j>i} x_ix_j\beta(e_i, e_j) + \sum_{i=1}^{m} x_i^2 q(e_i),$$

as claimed.

The second statement clearly follows from the first.

□

The previous Lemma shows that, given a basis of M, a quadratic form corresponds to a homogeneous polynomial of degree 2 with coefficients in R. For this reason we also say that a quadratic form of rank n is a quadratic form is *n variables.* We often identify a quadratic form with the polynomial to which it corresponds in some basis.

Fixing the module M, an isomorphism of quadratic forms over M is just a linear change of basis of M taking one form to the other, which translates to a linear invertible change of variables in the polynomial.

In the case where 2 is invertible in R, we can define

$$x.y = \frac{1}{2}\beta(x, y).$$

This is a symmetric bilinear form and we have

$$x.x = \frac{1}{2}(q(x + x) - q(x) - q(x)) = q(x).$$

Conversely, given a symmetric bilinear form $(x, y) \mapsto x.y$, we define $q(x) = x.x$ and this is a quadratic form, therefore we see that in this case the study of quadratic forms is essentially the same as the study of symmetric bilinear forms.

Lemma 1.4. *Let (M, q) be a quadratic module over a ring R, with basis $\mathcal{B} = \{e_1, \cdots, e_n\}$ and suppose that 2 is invertible in R. Then, for any $x \in M$, writing $x = \sum_i x_ie_i$, we have*

$$q(x) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_ix_je_i.e_j.$$

Therefore $q(x) = x^tBx$ where B is a matrix with entries $q_{ij} = e_i.e_j$.

Proof. Follows immediately from the previous Lemma. □

Definition 1.5. Let q be a quadratic form on a module M over a ring R and $\mathcal{B}$ a basis of M. If $2 \in R^\times$ then the *matrix representation* of q in the basis $\mathcal{B}$ is the matrix B of Lemma 1.4. When $2 \notin R^\times$, the *matrix representation* of q in the basis $\mathcal{B}$ is the matrix Q of Lemma 1.3.

We often identify a quadratic form with its matrix representation in some basis. Note that if A is the matrix representation of q in the basis $\mathcal{B}$ and X is the column vector whose entries are the coordinates of x in the basis $\mathcal{B}$, then $q(x) = X^tAX$. For simplicity, we write $q(x) = x^tAx$.

Suppose $q \sim p$ are quadratic forms on a module M over R and ϕ is an isomorphism, $q(x) = p(\phi(x))$. Suppose we fix a basis $\mathcal{B}$, let Q and P be the matrix representations of q and p with respect to this basis and let T be the matrix representation of ϕ in this basis. Then

$$x^tQx = (Tx)^tP(Tx) = x^t(T^tPT)x.$$

If $2 \in R^\times$, this implies $Q = T^tPT$ (because Q and T^tPT are symmetric) and thus we have proved the following result:

Proposition 1.6. *Suppose p, q are quadratic forms over a ring R with $2 \in R^\times$ and $p \sim q$. Then, if P, Q are the matrix representations of p, q with respect to a fixed basis, we have $Q = T^tPT$, for some invertible matrix T.*

This does not always hold when $2 \notin R^\times$. For example, the quadratic forms $x^2 + y^2$ and x^2 are equivalent over $\mathbb{F}_2$ (as we will see later on), but there is no invertible matrix T such that

$$T^t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

because the left side is invertible whereas the right side is not.

We have seen that symmetric bilinear forms are closely related to quadratic forms, especially, but not only, in characteristic $\neq 2$. For this reason, we now focus on symmetric bylinear forms, stating some relevant facts whose proof can be found in [2, pp.1–7].

Definition 1.7. Given a symmetric bilinear form $\beta : M \times M \to R$, we call (M, β) a *bilinear form space.*

We say that two bilinear form spaces (M, β) and (M', β') are *isomorphic* if there is a linear bijection $f : M \to M'$ such that $\beta'(f(x), f(y)) = \beta(x, y)$.

Definition 1.8. Picking a basis $(e_i)_i$ of M over R, we define the *matrix representation* B of β in this basis by $b_{ij} = \beta(e_i, e_j)$. If this matrix is invertible, we say that β is *nondegenerate*, and it is not hard to see that this does not depend on the choice of basis.

When β is nondegenerate we say that it is an *inner product* and call (M, β) an *inner product space.*

We now mention the relation between the matrix representation Q of a quadratic form and the matrix representation B of its associated bilinear form

β. When $2 \in R^\times$, we have $Q = \frac{1}{2}B$. When $2 \notin R^\times$, we have $q_{ij} = b_{ij}$ for $i < j$, $q_{ij} = 0$ for $i > j$ and $b_{ii} = 2a_{ii}$, therefore in general we can not find the diagonal of Q just by looking at B.

If β and β' are bilinear forms with matrix representations B and B', respectively, then the bilinear form spaces (M, β) and (M', β') are isomorphic if and only if there is an invertible matrix A such that $B' = ABA^t$. Taking determinants, we get $\det(B') = \det(A)^2 \det(B)$, so we see that the determinant of the matrix associated to a symmetric bilinear form is invariant under isomorphism, up to a product by an element in $(R^\times)^2$. The form is nondegenerate if and only if $\det(B) \in R^\times$.

Definition 1.9. Let β be a nondegenerate symmetric bilinear form. We define its *discriminant* as the element of $R^\times/(R^\times)^2$ determined by the determinant of any associated matrix.

Given a submodule N of M, we define it's orthogonal submodule by

$$N^\perp = \{x \in M : \beta(x, y) = 0, \ \forall\, y \in N\}.$$

Definition 1.10. Given two bilinear form modules (M, α) and (N, β) we define their *orthogonal sum* as the bilinear form module $(M \oplus N, \alpha \oplus \beta)$, where

$$\alpha \oplus \beta(x, y) = \alpha(x) + \beta(y).$$

An *orthogonal basis* of a bilinear form space (M, β) is a basis $(e_i)_i$ of M over R, such that $\beta(e_i, e_j) = \delta_{ij}$.

Theorem 1.11. *([2, p.6, Corollary 3.4])*
If R is a local ring where 2 is a unit and (M, β) is an inner product space over R, then (M, β) has an orthogonal basis.

We say that a bilinear form β is *symplectic* if $\beta(x, x) = 0$ for all $x \in M$. An inner product space (M, β) where β is symplectic is called a *symplectic inner product space.*

Theorem 1.12. *([2, p.7, Corollary 3.5])*
If R is a local ring and (M, β) is a symplectic inner product space over R, then it has a symplectic basis (i.e. a basis such that the matrix associated to β has the form $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$).

Definition 1.13. The *radical* of a quadratic module (V, q) is

$$V^\perp = \{x \in V : \beta(x, y) = 0, \ \forall\, y \in V\},$$

where β is the associated bilinear form.

We say that a quadratic form is *nondegenerate* if its associated symmetric bilinear form is nondegenerate, or equivalently if $V^\perp = 0$.

Definition 1.14. If $2 \in R^\times$ and q is a quadratic form over R, we define its *discriminant* as the discriminant of the symmetric bilinear form $\frac{1}{2}\beta$, where β is the associated symmetric bilinear form. We denote it by $d(q)$ or d.

Specializing to the case where $R = k$ is a field of characteristic $\neq 2$, the previous facts about symmetric bilinear forms tell us that any quadratic form over k can be diagonalized, meaning that there is a basis $(e_i)_i$ of M such that its matrix representation is diagonal. This means that we can always find a change of coordinates such that the polynomial corresponding to the quadratic form becomes $a_1x_1^2 + \cdots + a_nx_n^2$ for some $a_i \in k$. A useful and easily proved fact is that multiplying any of the a_i by a square will produce an equivalent quadratic form.

One important aspect of the theory of quadratic forms is representability:

Definition 1.15. A quadratic form q on a module M over a commutative ring R *represents* an element $r \in R$ if there is an $m \in M \setminus \{0\}$ such that $q(m) = r$.

It is clear that if q represents r, then q represents a^2r for any $a \in R^\times$, because if $q(x) = r$ then $q(ax) = a^2q(x) = a^2r$.

Translating to polynomials, asking whether a quadratic form q over R represents some $r \in R$ is the same as asking if an equation of the form $\sum_{i,j} a_{ij}x_ix_j = r$ with $a_{ij} \in R$ has any solutions $x_i \in R$.

We now state some useful results about quadratic forms over fields of characteristic $\neq 2$.

Definition 1.16. If q and q' are quadratic forms on vector spaces V and V' over the same field k, we denote by $q \oplus q'$ the quadratic form on $V \oplus V'$ defined by $(q \oplus q')(v, v') = q(v) + q'(v')$. Similarly, we denote by $q \ominus q'$ the quadratic form on $V \oplus V'$ defined by $(q \ominus q')(v, v') = q(v) - q'(v')$.

Proposition 1.17. *([1, p.33, Corollary 1])*

Let g be a quadratic form in n variables over a field k of characteristic $\neq 2$ and let $a \in k^\times$. The following are equivalent:

(i) g represents a.

(ii) $g \sim h \oplus aZ^2$, where h is a form in $n-1$ variables.

(iii) $g \ominus aZ^2$ represents 0.

Proposition 1.18. *([1, p.34, Theorem 4])*

Let $f = g \oplus h$ and $f' = g' \oplus h'$ be nondegenerate quadratic forms over the same field k. If $f \sim f'$ and $g \sim g'$, then $h \sim h'$.

2 Quadratic forms over $\mathbb{Q}$

In this section we present the classification of quadratic forms over $\mathbb{Q}$. The proofs of all the results can be read in [1, pp.19–45]. We assume that all quadratic forms are nondegenerate.

As a warm-up, we begin with the classification of quadratic forms over $\mathbb{R}$. As seen in the previous section, any quadratic form over $\mathbb{R}$ can be diagonalized, so we assume we have a quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$, with all the a_i nonzero. It is clear that we can multiply the a_i by nonzero squares without changing the equivalence class of the form and doing so we can turn all the positive a_i into $1's$ and all the negative a_i into $-1's$, because in $\mathbb{R}$ any positive number is a square. This way we see that any form over $\mathbb{R}$ is equivalent to $x_1^2 + \cdots + x_r^2 - y_1^2 - \cdots - y_s^2$

for some $r, s \in \mathbb{N}$ and we call (r, s) the *signature* of the form. It can be seen that the signature is an invariant of the form and therefore we have classifed all quadratic forms over $\mathbb{R}$, the only invariant being the signature.

The case of $\mathbb{Q}$ is much harder, and we can immediately see that the method used for $\mathbb{R}$ fails, because there are many positive rational numbers that are not squares. The fact that it was so easy to do the classification over $\mathbb{R}$, suggests that it might be useful to look at the other completions of $\mathbb{Q}$, namely the p-adic fields $\mathbb{Q}_p$. It turns out that this works, because we can understand the classification of quadratic forms over the p-adic fields and this information is enough to classify the quadratic forms over $\mathbb{Q}$, as will be made precise later.

We now focus on the classification of quadratic forms over the $\mathbb{Q}_p$.

Definition 2.1. Take $a, b \in \mathbb{Q}_v^\times$ and consider the equation $z^2 - ax^2 - by^2 = 0$. We define the *Hilbert symbol* by

$$(a,b)_v = \begin{cases} 1 & \text{if the equation has a nontrivial solution in } \mathbb{Q}_v \\ -1 & \textit{otherwise.} \end{cases}$$

Here v ranges over V, the set of primes together with the symbol ∞, with the convention $\mathbb{Q}_\infty = \mathbb{R}$ and "nontrivial" means $(x, y, z) \neq (0, 0, 0)$.

In view of Proposition 1.17, it is clear that $(a, b)_v = 1$ if and only if the quadratic form $ax^2 + by^2$ represents 1 over $\mathbb{Q}_v$. We see from the definition that $(a, b)_v = (b, a)_v = (a, bc^2)_v$ for any $a, b, c \in \mathbb{Q}_v^\times$.

Definition 2.2. Let $u \in (\mathbb{Z}_2)^\times$. We define

$$\varepsilon(u) = \begin{cases} 0 & \text{if } u \equiv 1 \pmod 4 \\ 1 & \text{if } u \equiv -1 \pmod 4 \end{cases} \qquad \omega(u) = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod 8 \\ 1 & \text{if } u \equiv \pm 5 \pmod 8 \end{cases}.$$

Definition 2.3. We define the *Legendre symbol* by

$$\left(\frac{u}{p}\right) = u^{(p-1)/2} \bmod p = \begin{cases} 1 & \text{if u is a square mod } p \\ -1 & \text{otherwise} \end{cases},$$

where p is an odd prime and $u \in \mathbb{Z}_p^\times$.

The following identities (together with quadratic reciprocity) allow for simple computation of the Hilbert symbol:

Proposition 2.4. *If $a, b \in \mathbb{R}$, we have* $(a,b)_\infty = \begin{cases} 1 & \textit{if } a > 0 \textit{ or } b > 0 \\ -1 & \textit{otherwise} \end{cases}$.

If $a, b \in \mathbb{Q}_p$, we write $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^\times$. Then

i) $(a,b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$, *for* $p \neq 2$.

ii) $(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$.

Setting $k = \mathbb{Q}_v$, the previous identities immediatley imply that

$$(\cdot,\cdot)_v : k^\times/(k^\times)^2 \times k^\times/(k^\times)^2 \to \{\pm 1\}$$

is a symmetric bilinear form on the $\mathbb{F}_2$-vector space $k^\times/(k^\times)^2$. It can also be proved that it is nondegenerate.

Here is another important property of the Hilbert symbol, which is essentially equivalent to quadratic reciprocity:

Theorem 2.5. *If $a, b \in \mathbb{Q}^\times$, we have $(a,b)_v = 1$ for all but finitely many v and*

$$\prod_v (a,b)_v = 1.$$

Definition 2.6. We define the *Hasse-Witt invariant* of a quadratic form $f = a_1x_1^2 + \cdots + a_nx_n^2$ over $\mathbb{Q}_p$ by

$$\epsilon_v(f) = \prod_{i<j}(a_i, a_j).$$

When no confusion should arise, we use ϵ instead of $\epsilon(f)$.

This definition makes sense, because it can be shown that if we pick two different diagonalizations $a_1x_1^2 + \cdots + a_nx_n^2$ and $b_1x_1^2 + \cdots + b_nx_n^2$ of a quadratic form, then $\prod_{i<j}(a_i, a_j) = \prod_{i<j}(b_i, b_j)$. It is also possible to prove that this is in fact an invariant of the quadratic form, meaning that equivalent quadratic forms have the same Hasse-Witt invariant.

We now let $k = \mathbb{Q}_p$ for some prime p. The following results about representability are the key to obtaining the classification of quadratic forms over the $\mathbb{Q}_p$.

Theorem 2.7. *A quadratic form f over k represents 0 if and only if its invariants satisfy one of the following conditions:*

i) $n = 2$ *and* $d = -1$.

ii) $n = 3$ *and* $(-1, -d) = \epsilon$.

iii) $n = 4$ *and* $d \neq 1$.

iv) $n = 4$, $d = 1$ *and* $\epsilon = (-1, -1)$.

v) $n \geq 5$.

(All the identities are in $k^\times/(k^\times)^2$.)

Using this theorem and Proposition 1.17 we obtain the following result:

Corollary 2.8. *Let $a \in k^\times$. A quadratic form f over k represents a if and only if its invariants satisfy one of the following conditions:*

i) $n = 1$ *and* $a = d$.

ii) $n = 2$ *and* $(a, -d)_v = \epsilon$.

iii) $n = 3$ *and* $a \neq -d$.

iv) $n = 3$, $a = -d$ *and* $(-1, -d) = \epsilon$.

v) $n \geq 4$.

(All the identities are in $k^\times/(k^\times)^2$.)

Using the previous results, we can now obtain the classification of quadratic forms over $\mathbb{Q}_p$:

Theorem 2.9. *Two quadratic forms f, g over $k = \mathbb{Q}_p$ are equivalent if and only if they have the same rank, discriminant and Hasse-Witt invariant.*

Proof. We have already mentioned that equivalent forms have the same invariants. For the converse, we use induction on the rank n of f and g. The case $n = 0$ is obvious. For $n \geq 1$, by the previous theorems on representability and the fact that f and g have the same invariants, we know that f and g represent the same elements of k. Therefore, there is some $a \in k^\times$ that is represented by both f and g (because f and g are nondegenerate, hence not identically zero). By Proposition 1.17, we can write

$$f \sim aZ^2 \oplus f' \text{ and } g \sim aZ^2 \oplus g',$$

where f' and g' are forms of rank $n-1$. It is easy to see that f' and g' have the same invariants, therefore, by the induction hypothesis, $f' \sim g'$, hence $f \sim g$.

□

We now go back to the connection between quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$, which is the content of the Hasse-Minkowski Theorem:

Theorem 2.10 (Hasse-Minkowski)**.** *A quadratic form f over $\mathbb{Q}$ represents 0 if and only if f_v represents zero for all v, where f_v is the form over $\mathbb{Q}_v$ obtained from f by looking at its coefficients as elements of $\mathbb{Q}_v$.*

The following is a simple corollary, using Proposition 1.17.

Corollary 2.11. *A quadratic form over $\mathbb{Q}$ represents $a \in \mathbb{Q}^\times$ if and only if f_v represents a for all v.*

Once again, a result about representability is the key to proving a result about equivalence of quadratic forms:

Theorem 2.12. *Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they are equivalent over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p.*

Proof. Equivalence over $\mathbb{Q}$ clearly implies equivalence over the $\mathbb{Q}_v$. For the converse, we use induction on the rank n of f and f'. When $n = 0$, there is nothing to prove. When $n \geq 1$, there exists $a \in \mathbb{Q}^\times$ represented by f and by the previous corollary f' also represents a. By Proposition 1.17, we have

$$f \sim aZ^2 \oplus g \text{ and } f' \sim aZ^2 \oplus g',$$

where g and g' are forms of rank $n-1$. We have $f \sim f'$ over $\mathbb{Q}_v$, for all v, therefore $g \sim g'$ over $\mathbb{Q}_v$ for all v, by Proposition 1.18. By the induction hypothesis, we then have $g \sim g'$ over $\mathbb{Q}$, hence $f \sim f'$ over $\mathbb{Q}$.

□

Using this theorem and the classification of quadratic forms over the $\mathbb{Q}_v$, we obtain a complete set of invariants for quadratic forms over $\mathbb{Q}$:

Theorem 2.13. *Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they have the same rank, discriminant, signature (as forms over $\mathbb{R}$) and Hasse-Witt invariants (over all the $\mathbb{Q}_p$).*

Now the only thing left to complete the classification is to determine whether, given a set of values for the invariants, there is a form whose invariants take those values.

Proposition 2.14. *Let f be a quadratic form over $\mathbb{Q}$ with rank n, discriminant d, signature (r, s) and Hasse-Witt invariants $(\epsilon_v)_{v\in V}$ (where ϵ_v denotes $\epsilon(f_v)$). Then:*

(1) $\epsilon_v = 1$ for all but finitely many v and $\prod_v \epsilon_v = 1$;

(2) If $n = 1$ then $\epsilon_v = 1$;

(3) If $n = 2$ and the image d_v of d in $\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$ is -1 then $\epsilon_v = 1$;

(4) $r, s \geq 0$ and $r + s = n$;

(5) $d_\infty = (-1)^s$;

(6) $\epsilon_\infty = (-1)^{s(s-1)/2}$.

Having identified these relations, we have the following theorem (whose proof depends on Dirichlet's Theorem on primes in arithmetic progression):

Theorem 2.15. *If d, $(\epsilon_v)_{v\in V}$ and (r, s) satisfy the relations of the previous proposition, then there is a quadratic form of rank n over $\mathbb{Q}$ having d, $(\epsilon_v)_v$ and (r, s) for invariants.*

We now present an example of a solution of a representability problem, using the Hasse-Minkowski Theorem and Theorem 2.7.

Lemma 2.16. *If $a, b \in \mathbb{Z}_p^\times$, then $(a, b)_p = 1$ for $p \neq 2$ and $(a, b)_p = (-1)^{\varepsilon(u)\varepsilon(v)}$ for $p = 2$.*

Proof. Clear, from the formulas for the Hilbert Symbol in Proposition 2.4. □

Example 2.17. We claim that the equation $f(x, y, z) = 5x^2 + 7y^2 - 13z^2 = 0$ has a nontrivial rational solution (nontrivial meaning that $(x, y, z) = (0, 0, 0)$). This amounts to saying that the quadratic form f represents 0 over $\mathbb{Q}$. By the Hasse-Minkowski Theorem, we only need to prove that it represents 0 over $\mathbb{R}$ and over the $\mathbb{Q}_p$, for all primes p. It is clear that the equation has a real solution, therefore we concentrate on the p-adic solutions. By Theorem 2.7, we only need to show that, for each p, we have $(-1, -d)_p = \epsilon_p$.

- $p \not| \, 2.5.7.13$

  We have
  $$\epsilon_p = (5, 7)_p(5, -13)_p(7, -13)_p = 1 \times 1 \times 1 = 1$$
  by the previous Lemma, because $5, 7, -13 \in \mathbb{Z}_p^\times$. Similarly,
  $$(-1, -d)_p = (-1, 5 \times 7 \times 13)_p = 1.$$

- $p = 2$

  By the previous Lemma,

  $$(-1,-d)_2 = (-1, 5\times 7\times 13)_2 = (-1)^{\varepsilon(-1)\varepsilon(5\times7\times13)}.$$

  It is easy to check that $\varepsilon(-1) = \varepsilon(5 \times 7 \times 13) = 1$, therefore

  $$(-1,-d)_2 = -1.$$

  Similarly,

  $$(5,7)_2 = (-1)^{\varepsilon(5)\varepsilon(7)} = (-1)^{0\times 1} = 1 = (5,-13)_2$$

  and

  $$(7,-13)_2 = -1,$$

  hence $\epsilon_2 = -1$.

- $p = 5$

  By the formula in Theorem 2.4,

  $$(-1,-d)_5 = (-1, 5{\times}7{\times}13)_5 = (-1)^{0\times1\times\varepsilon(5)}\left(\frac{-1}{5}\right)^1\left(\frac{5\times7\times13}{5}\right)^0 = \left(\frac{-1}{5}\right) = 1.$$

  By the previous Lemma, $(7,-13)_5 = 1$, therefore

  $$\epsilon_5 = (5,-7\times13)_5 = (-1)^{1\times0\times\varepsilon(5)}\left(\frac{1}{5}\right)^0\left(\frac{-7\times13}{5}\right)^1 =$$

  $$\left(\frac{-7}{5}\right)\left(\frac{13}{5}\right) = \left(\frac{-2}{5}\right)\left(\frac{3}{5}\right) = \left(\frac{3}{5}\right)^2 = 1.$$

- $p = 7$

  We have

  $$(-1, 5\times7\times13)_7 = (-1)^{0\times1\times\varepsilon(7)}\left(\frac{-1}{7}\right)^1\left(\frac{-1}{5\times7\times13}\right)^0 = \left(\frac{-1}{7}\right) = -1,$$

  and

  $$\epsilon_7 = (5,7)_7(5,-13)_7(7,-13)_7 = (7,-5{\times}13)_7 = \left(\frac{-5\times13}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{-1}{7}\right) = -1.$$

- $p = 13$

  We have

  $$(-1, 5\times7\times13)_{13} = \left(\frac{-1}{13}\right) = 1$$

  and

  $$\epsilon_{13} = (5,7)_{13}(5,-13)_{13}(7,-13)_{13} = (5\times7,-13)_{13} =$$

$$\left(\frac{5\times 7}{13}\right) = \left(\frac{5}{13}\right)\left(\frac{7}{13}\right) = \left(\frac{13}{5}\right)(-1)^{\varepsilon(5)\varepsilon(13)}\left(\frac{13}{7}\right)(-1)^{\varepsilon(7)\varepsilon(13)} =$$
$$\left(\frac{13}{5}\right)\left(\frac{13}{7}\right) = \left(\frac{3}{5}\right)\left(\frac{-1}{7}\right) = -\left(\frac{3}{5}\right) =$$
$$-\left(\frac{5}{3}\right)(-1)^{\varepsilon(5)\varepsilon(3)} = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

where we have used quadratic reciprocity.

3 Quadratic forms over $\mathbb{Z}/m\mathbb{Z}$

In this section we describe the results obtained regarding the classification of quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, for $m \in \mathbb{N}$. Namely, we present the classification of nondegenerate quadratic forms over $\mathbb{Z}/p^k\mathbb{Z}$ for p an odd prime, and of regular quadratic forms over $\mathbb{Z}/2\mathbb{Z}$. By the Chinese Remainder Theorem, this will give the classification of regular quadratic forms over $\mathbb{Z}/m\mathbb{Z}$ for all $m \in \mathbb{N}$ not divisible by 4.

We begin by stating the classification of nondegenerate quadratic forms over the finite fields $\mathbb{F}_q$ of characteristic $\neq 2$. The proofs of these results can be found in [1, pp. 34, 35].

Theorem 3.1. *There are two equivalence classes of nondegenerate quadratic forms of rank n over $\mathbb{F}_q$:*

i) $x_1^2 + \cdots + x_{n-1}^2 + x_n^2$ *and*

ii) $x_1^2 + \cdots + x_{n-1}^2 + ax_n^2$*, where a is not a square in $\mathbb{F}_q$.*

Theorem 3.2. *A nondegenerate quadratic form over $\mathbb{F}_q$ of rank ≥ 2 (resp. ≥ 3) represents all elements of $\mathbb{F}_q^\times$ (resp. $\mathbb{F}_q$).*

3.1 $\mathbb{Z}/p^k\mathbb{Z}$, $p \neq 2$

Now we present the classification of nondegenerate quadratic forms over $R = \mathbb{Z}/p^k\mathbb{Z}$, with p an odd prime. In this section, "quadratic form" will mean "nondegenerate quadratic form". The ring $R = \mathbb{Z}/p^k\mathbb{Z}$ is a local ring where 2 is a unit, therefore all quadratic forms can be diagonalized, with the elements in the diagonal being units.

We have
$$\frac{(\mathbb{Z}/p^k\mathbb{Z})^\times}{((\mathbb{Z}/p^k\mathbb{Z})^\times)^2} \cong \frac{\mathbb{Z}/\phi(p^k)\mathbb{Z}}{2(\mathbb{Z}/\phi(p^k)\mathbb{Z})} \cong \mathbb{Z}/2\mathbb{Z},$$
where ϕ is the Euler totient function. We can choose 1 as a representative for the squares and denote by a a representative of the non-squares.

Proposition 3.3. *Let f be a quadratic form over R. Then*
$$f \sim x_1^2 + \cdots + x_r^2 + a(y_1^2 + \cdots + y_s^2)$$
for some $r, s \in \mathbb{N}$. Furthermore, if
$$f' = x_1^2 + \cdots + x_{r'}^2 + a(y_1^2 + \cdots + y_{s'}^2),$$
then $f \sim f'$ if and only if $s \equiv s' \pmod 2$ and $r + s = r' + s'$.

Proof. We can write $f \sim a_1x_1^2 + \cdots + a_nx_n^2$ with $a_1, \cdots, a_n \in R^\times$ and then, multiplying the a_i by squares, we get $f \sim x_1^2 + \cdots + x_r^2 + a(y_1^2 + \cdots + y_s^2)$ for some $r, s \in \mathbb{N}$.

If $f \sim f'$, then we have $s \equiv s' \pmod 2$, because the discriminant of a quadratic form is an invariant in $R^\times/(R^\times)^2$ and $d(f) = a^s$, $d(f') = a^{s'}$. It is clear that $n = r + s$ is the rank of f and $n' = r' + s'$ is the rank of f', therefore $r + s = r' + s'$.

Conversely, if $s \equiv s' \bmod 2$ and $r + s = r' + s'$, we will prove that $f \sim f'$, but first we need the following Lemma:

Lemma 3.4. *We have* $x_1^2 + x_2^2 \sim ax_1^2 + ax_2^2$.

Proof. We start by finding

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ and } y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

such that $x^tIy = 0$ and $x^tIx = a$ where I is the 2×2 identity matrix, with the additional constraint that $x_1y_2 - x_2y_1$ must be a unit, to ensure that the matrix

$$A = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

is invertible. If we can do this, we will have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ 0 & y_1^2 + y_2^2 \end{pmatrix} \left(\text{because } A^t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} A = \begin{pmatrix} a & 0 \\ 0 & y_1^2 + y_2^2 \end{pmatrix} \right)$$

and the fact that the discriminant is an invariant forces $y_1^2 + y_2^2$ to be a non-square, so that

$$\begin{pmatrix} a & 0 \\ 0 & y_1^2 + y_2^2 \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

because we can multiply the diagonal coefficients by squares.

To find x and y, we notice that $x_1^2 + x_2^2 \equiv a \pmod p$ has a solution, according to Theorem 3.2, and using Hensel's Lemma we can lift this solution to a solution $\bmod p^k$ (alternatively, one can observe that if the sum of two squares $\bmod p$ was always a square $\bmod p$, than the set of squares would be a nontrivial subgroup of $\mathbb{Z}/p\mathbb{Z}$). We must have $x_1x_2 \not\equiv 0 \bmod p$ because a is a non-square. Now we can solve $x_1y_1 + x_2y_2 \equiv 0 \pmod p$ just by taking $y_1 = x_1^{-1}$ and $y_2 = (-x_2)^{-1}$ and we can lift this to a solution $\bmod p^k$ using Hensel's Lemma. For the invertibility of A, we notice that it suffices to prove the invertibility of A^tA, because $\det(A^tA) = \det(A)^2$. We have

$$A^tA = \begin{pmatrix} a & 0 \\ 0 & y_1^2 + y_2^2 \end{pmatrix},$$

therefore we only need to prove that $y_1^2 + y_2^2$ is invertible $\bmod p$. But

$$y_1^2 + y_2^2 \equiv x_1^{-2} + x_2^{-2} \pmod p$$

and $x_1^{-2} + x_2^{-2} \equiv 0 \pmod p$ is equivalent to $x_1^2 + x_2^2 \equiv 0 \pmod p$ (by clearing denominators, since $x_1x_2 \not\equiv 0 \pmod p$) and we know that $x_1^2 + x_2^2 \not\equiv 0 \pmod p$. □

Now we return to the proof of the Proposition, writing $r' = r + 2m$ and $s' = s - 2m$, for some $m \in \mathbb{Z}$. We can suppose, without loss of generality, that $m \geq 0$ and then we decompose the matrices

$$\begin{pmatrix} I_r & 0 \\ 0 & aI_s \end{pmatrix} \text{ and } \begin{pmatrix} I_{r'} & 0 \\ 0 & aI_{s'} \end{pmatrix}$$

representing f and f', respectively, into three blocks (changing the order of the diagonal elements). The first and second blocks are of the form I_r and $aI_{s'}$, respectively, and are common to both f and f'. The third block is of the form aI_{2m} for f and I_{2m} for f':

$$f \sim \begin{pmatrix} I_r & 0 & 0 \\ 0 & aI_{s'} & 0 \\ 0 & 0 & aI_{2m} \end{pmatrix},$$

$$f' \sim \begin{pmatrix} I_r & 0 & 0 \\ 0 & aI_{s'} & 0 \\ 0 & 0 & I_{2m} \end{pmatrix}.$$

Applying the Lemma, we find that $I_{2m} \sim aI_{2m}$, hence $f \sim f'$.

□

The following Theorem is now clear:

Theorem 3.5. *Let p be an odd prime and $n, k \in \mathbb{N}$. Then there are two equivalence classes of nondegenerate quadratic forms of rank n over $\mathbb{Z}/p^k\mathbb{Z}$:*

i) $x_1^2 + \cdots + x_{n-1}^2 + x_n^2$ and

ii) $x_1^2 + \cdots + x_{n-1}^2 + ax_n^2$, where a is not a square in $\mathbb{Z}/p^k\mathbb{Z}$.

In particular, quadratic forms over $\mathbb{Z}/p^k\mathbb{Z}$ are classified by their discriminant.

3.2 $\mathbb{Z}/2\mathbb{Z}$

Now we explain the classification of quadratic forms over $\mathbb{Z}/2\mathbb{Z}$. Here we have the problem of being in characteristic 2, which implies that we can no longer define the symmetric bilinear form $x.y = \frac{1}{2}(q(x+y) - q(x) - q(y))$. For this reason, we work with the symmetric bilinear form $\beta(x, y) = q(x+y) - q(x) - q(y)$.

Recall that a quadratic form is called *nondegenerate* if the corresponding bilinear form β is nondegenerate and *degenerate* otherwise. Note that, for example, the quadratic form of rank one over $\mathbb{F}_2$ x^2 is degenerate (its associated bilinear form β is such that $\beta(x, y) = 0$ for all x, y) and we don't want to exclude it from our classification. Therefore we need the notion of regularity:

Definition 3.6. A quadratic form q on a vector space V over a field k is called *regular* if there is no nonzero subspace $W \subseteq V^\perp$ such that $q_{|W} = 0$.

It is clear from the definition that a nondegenerate form is always regular, but x^2 is regular and degenerate. However, in the case of fields of characteristic $\neq 2$, regular and nondegenerate forms coincide, because if $x \in V^\perp$, then $q(x) = \frac{1}{2}\beta(x, x) = 0$.

In polynomial terms, a quadratic form is regular if it can not be written using a smaller number of variables. From now on, we assume that all quadratic forms are regular.

Proposition 3.7. *Let q be a quadratic form over $\mathbb{F}_2$. Then*

$$q \sim x_1^2 + \cdots + x_k^2 + (b_1 y_1^2 + y_1 z_1 + d_1 z_1^2) + \cdots + (b_\ell y_\ell^2 + y_\ell z_\ell + d_\ell z_\ell^2),$$

for some $k, \ell \in \mathbb{N}$ and $b_i, d_i \in \mathbb{F}_2$.

Proof. Let $V = \mathbb{F}_2^n$ be the vector space on wich q is defined and β the associated bilinear form. Let $A = V^\perp$ and let B be a subspace of V such that $V = A \oplus B$. We have $A \perp B$, β is zero on A and nondegenerate on B.

We have $\beta(x,x) = q(x+x) - q(x) - q(x) = 0$, therefore β is symplectic, hence the restriction of β to B is a symplectic inner product. By Corollary 1.12, we can choose a basis for B such that the restriction of β to B is represented by the matrix

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

But in characteristic 2 we have $1 = -1$ and by changing the order of the basis vectors, the restriction of β to B becomes

$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{pmatrix}.$$

Then β is of the form

$$\begin{pmatrix} 0_k & & & & & \\ & 0 & 1 & & & \\ & 1 & 0 & & & \\ & & & \ddots & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix},$$

where 0_k is the $k \times k$ zero matrix, $k = \dim(A)$. Recalling the relation between the matrix representations of a quadratic form and of its associated symmetric bilinear form, we conclude that, in this basis, q is associated to the polynomial

$$f = a_1 x_1^2 + \cdots + a_k x_k^2 + (b_1 y_1^2 + y_1 z_1 + d_1 z_1^2) + \cdots + (b_\ell y_\ell^2 + y_\ell z_\ell + d_\ell z_\ell^2).$$

The a_i are all equal to 1, because the form is regular, and this ends the proof. □

Lemma 3.8. *We have $x^2 + y^2 \sim u^2$.*

Proof. Consider the linear change of varibles $u = x + y$ and $v = y$. This change of variables is easily seen to be invertible and furthermore

$$x^2 + y^2 = (u - v)^2 + v^2 = u^2 + v^2 + v^2 = u^2.$$

□

Proposition 3.9. *Let f be a quadratic form of rank n over $\mathbb{F}_2$. Then:*

(i) If n is odd, we have

$$f \sim x^2 + (b_1 y_1^2 + y_1 z_1 + d_1 z_1^2) + \cdots + (b_\ell y_\ell^2 + y_\ell z_\ell + d_\ell z_\ell^2),$$

or in matrix form

$$f \sim \begin{pmatrix} 1 & & & & & \\ & b_1 & 1 & & & \\ & 0 & d_1 & & & \\ & & & \ddots & & \\ & & & & b_\ell & 1 \\ & & & & 0 & d_\ell \end{pmatrix},$$

for some $\ell \in \mathbb{N}$ and $b_i, d_i \in \mathbb{F}_2$.

(ii) If n is even, then

$$f \sim (b_1 y_1^2 + y_1 z_1 + d_1 z_1^2) + \cdots + (b_\ell y_\ell^2 + y_\ell z_\ell + d_\ell z_\ell^2),$$

or in matrix form

$$\begin{pmatrix} b_1 & 1 & & & \\ 0 & d_1 & & & \\ & & \ddots & & \\ & & & b_\ell & 1 \\ & & & 0 & d_\ell \end{pmatrix},$$

for some $\ell \in \mathbb{N}$ and $b_i, d_i \in \mathbb{F}_2$.

Proof. This is immediate from Lemma 3.8, Proposition 3.7 and the regularity of f.

□

Now we focus on forms of even rank. We start by presenting the classification of regular forms of rank 2.

Definition 3.10. The *Arf invariant* of a quadratic form q on a vector space V over $\mathbb{F}_2$ is defined by

$$\#_q = \#\{x \in V : q(x) = 1\}.$$

It is clear that $\#_q$ is in fact an invariant of the quadratic form q, meaning that if $p \sim q$, then $\#_p = \#_q$.

Lemma 3.11. *There are two equivalence classes of regular quadratic forms of rank 2 over $\mathbb{F}_2$: $\{x^2 + y^2 + xy\}$ and $\{xy + y^2, xy + x^2, xy\}$.*

Proof. There are only 5 different homogeneous polynomials of degree 2 in two variables, with coefficients in $\mathbb{F}_2$: x^2+y^2, x^2+y^2+xy, $xy+y^2$, $xy+x^2$ and xy. We have already seen that x^2+y^2 does not correspond to a regular quadratic form. On the other hand it is clear that the remaining quadratic forms are regular, because they are nondegenerate. The change of variables $x = a + b$; $y = b$ provides an equivalence of quadratic forms between xy and $ab + b^2$:

$$xy = (a + b)b = ab + b^2.$$

Moreover, it is clear that $xy + y^2 \sim xy + x^2$, therefore the only thing left to prove is $xy \not\sim x^2 + y^2 + xy$ and this can be seen from the fact that $\#_{xy} = 1$ and $\#_{x^2+y^2+xy} = 3$. □

By the last Lemma, there are only 2 possibilities for each 2×2 block in the matrix representation of Proposition 3.9 for a quadratic form of even rank over $\mathbb{F}_2$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

But not all combinations of these blocks will give different quadratic forms:

Lemma 3.12. *We have*

$$\begin{pmatrix} 1 & 1 & & \\ 0 & 1 & & \\ & & 1 & 1 \\ & & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 0 & 1 \\ & & 0 & 0 \end{pmatrix}.$$

Proof. If we let

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

then we have

$$T^tBT = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

and it is clear that $x^t(T^tBT)x = x^tAx$ for all x, therefore $A \sim B$. This corresponds to the change of variables $x = r+t$; $y = r+s+t$; $z = s+u$; $w = s+t+u$:

$$xy + zw = (r+t)(r+s+t) + (s+u)(s+y+u) = r^2 + rs + s^2 + t^2 + ut + u^2.$$

□

Using this fact, we can transform all 2×2 blocks, except possibly one of them, into

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

therefore the form is always equivalent to

$$\begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 0 & 1 \\ & & & & & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 1 & 1 \\ & & & & & 0 & 1 \end{pmatrix}.$$

These two forms are regular, because they are nondegenerate, and to complete the classification of regular forms of even rank we need to show that they are not equivalent.

Lemma 3.13. *We have*

$$\#_{q\oplus q'} = \#_q(2^k - \#_{q'}) + \#_{q'}(2^\ell - \#_q) = 2^k\#_q + 2^\ell\#_{q'} - 2\#_q\#_{q'},$$

where $k = \dim(V')$ *and* $\ell = \dim(V)$.

Proof. This formula is a direct consequence of the fact that $q(v) + q'(v') = 1$ if and only if exactly one of $q'(v), q'(v')$ is equal to 1. □

Lemma 3.14. *We have*

$$\begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 0 & 1 \\ & & & & & 0 & 0 \end{pmatrix} \not\sim \begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 1 & 1 \\ & & & & & 0 & 1 \end{pmatrix}.$$

Proof. Let B be the form

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

C the form

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and A_k the sum of k copies of B. We want to show that $A_k \oplus B \not\sim A_k \oplus C$ for all $k \in \mathbb{N}$.

Suppose that $A_k \oplus B \sim A_k \oplus C$ for some $k \in \mathbb{N}$ and let a_k, b and c be the Arf invariants of A_k, B and C, respectively. Then we have $\#_{A_k\oplus B} = \#_{A_k\oplus C}$, that is $2^2a_k + 2^{2k}b - 2a_kb = 2^2a_k + 2^{2k}c - 2a_kc$. It is easy to see that $b = 1$ and $c = 3$ and solving the previous equation for a_k, we get $a_k = 2^{2k-1}$.

On the other hand, we have $A_k = A_{k-1} \oplus B$, therefore $a_k = a_{k-1}(2^2 - b) + b(2^{2(k-1)} - a_{k-1})$ which is equivalent to $a_k = 2a_{k-1} + 2^{2(k-1)}$. This recurrence relation allows us to prove, by induction, that $a_k < 2^{2k-1}$ for all $k \in \mathbb{N}$: for $k = 1$, we have $a_1 = 1 < 2$. For $k \geq 2$, we have

$$a_k = 2a_{k-1} + 2^{2(k-1)} < 2 \times 2^{2(k-1)-1} + 2^{2(k-1)} = 2^{2k-1},$$

where we have used the induction hypothesis. This contradicts $a_k = 2^{2k-1}$, thus completing the proof. □

The previous results also imply that all regular forms of odd rank are equivalent to one of the two following forms:

$$\begin{pmatrix} 1 & & & & & & & \\ & 0 & 1 & & & & & \\ & 0 & 0 & & & & & \\ & & & \ddots & & & & \\ & & & & 0 & 1 & & \\ & & & & 0 & 0 & & \\ & & & & & & 0 & 1 \\ & & & & & & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & & & & & & & \\ & 0 & 1 & & & & & \\ & 0 & 0 & & & & & \\ & & & \ddots & & & & \\ & & & & 0 & 1 & & \\ & & & & 0 & 0 & & \\ & & & & & & 1 & 1 \\ & & & & & & 0 & 1 \end{pmatrix}.$$

We start by mentioning that they are regular, because both their radicals have dimension 1 and are generated by an element e with $q(e) = 1$, but we will show that they are actually equivalent. More generally, we have the following Lemma:

Lemma 3.15. *We have*

$$B = \begin{pmatrix} 1 &&&&&&& \\ & 0 & 1 &&&&& \\ & 0 & 0 &&&&& \\ &&& \ddots &&&& \\ &&&& 0 & 1 && \\ &&&& 0 & 0 && \\ &&&&&& 0 & 1 \\ &&&&&& 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 &&&&&&& \\ & b_1 & 1 &&&&& \\ & 0 & d_1 &&&&& \\ &&& \ddots &&&& \\ &&&& b_{\ell-1} & 1 && \\ &&&& 0 & d_{\ell-1} && \\ &&&&&& b_\ell & 1 \\ &&&&&& 0 & d_\ell \end{pmatrix},$$

for any $b_i, d_i \in \mathbb{F}_2$.

Proof. Let $V = (\mathbb{Z}/2\mathbb{Z})^n$, where $n = 2\ell + 1$, and let q be the quadratic form on V represented by the matrix B in the canonical basis $\{e_1, \cdots, e_n\}$. Let $W = \operatorname{span}\{e_2, \cdots, e_n\}$. We have $V^\perp = \operatorname{span}\{e_1\}$ and $V = V^\perp \oplus W$. Let A be the matrix representation of the restriction of q to W in the basis $\mathcal{B} = \{e_2, \cdots, e_n\}$.

Let $\phi : W \to \mathbb{F}_2$ be a linear function and define $W' = \{w + \phi(w)e_1 : w \in W\}$. Now observe that $V^\perp \cap W' = 0$ and $\psi : W \to W'$ given by $\psi(w) = w + \phi(w)e_1$ is an isomorphism of vector spaces. In particular $\dim(W') = \dim(W)$ and therefore $V = V^\perp \oplus W'$, which means that W' is another complement of $V^\perp$ in V. We have

$$q(\psi(w)) = q(w + \phi(w)e_1) = q(w) + \phi(w)^2 q(e_1) + \phi(w)\beta(w, e_1) = q(w) + \phi(w),$$

because $\phi(w)^2 = \phi(w)$, $q(e_1) = 1$ and $\beta(w, e_1) = 0$, therefore $q \circ \psi = q + \phi$.

Now $\mathcal{B}' = \psi(\mathcal{B})$ is a basis of W'. Let A' be the matrix representation of the restriction of q to W' in the basis $\mathcal{B}'$. If $x', y' \in \mathcal{B}'$ then $x' = \psi(x)$ and $y' = \psi(y)$, for some $x, y \in \mathcal{B}$ and we have

$$q(x') = q(\psi(x)) = q(x) + \phi(x),$$

therefore $a'_{ii} = a_{ii} + \phi(e_{i+1})$ for all i (by the definition of matrix representation in section 1, we have $a_{ii} = q(e_{i+1})$ and $a'_{ii} = q(e_{i+1})'$). Moreover

$$\beta(x', y') = q(x' + y') - q(x') - q(y') = q(\psi(x + y)) - q(\psi(x)) - q(\psi(y)) =$$

$$q(x+y) + \phi(x+y) - q(x) - \phi(x) - q(y) - \phi(y) = q(x+y) - q(x) - q(y) = \beta(x, y),$$

therefore $a_{ij} = a'_{ij}$ for $i \neq j$ (by the definition of matrix representation in section 1, we have $a_{ij} = \beta(e_{i+1}, e_{j+1})$ and $a'_{ij} = \beta(e'_{i+1}, e'_{j+1})$, for $i < j$ and $a_{ij} = a'_{ij} = 0$, for $i > j$).

This means that the matrix

$$B' = \begin{pmatrix} 1 & \\ & A' \end{pmatrix}$$

representing q in the basis $\mathcal{B}' \cup \{e_1\}$ is obtained from the matrix

$$B = \begin{pmatrix} 1 & \\ & A \end{pmatrix}$$

representing q in the basis $\{e_1, \cdots, e_n\}$ by adding the value $\phi(e_i)$ to the i^{th} diagonal entry, for all $i \geq 2$. Because ϕ is arbitrary, this ends the proof.

□

The following theorem is now clear:

Theorem 3.16. *(i) If n is even, there are two equivalence classes of regular quadratic forms of rank n over $\mathbb{F}_2$, with representatives*

$$\begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 0 & 1 \\ & & & & & 0 & 0 \end{pmatrix} \textit{ and } \begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 1 & 1 \\ & & & & & 0 & 1 \end{pmatrix}.$$

In particular, regular quadratic forms of even rank over $\mathbb{F}_2$ are classified by their rank and Arf invariant.

(ii) If n is odd, there is only one equivalence class of regular quadratic forms of rank n over $\mathbb{F}_2$, with representative

$$\begin{pmatrix} 1 & & & & & & & \\ & 0 & 1 & & & & & \\ & 0 & 0 & & & & & \\ & & & \ddots & & & & \\ & & & & 0 & 1 & & \\ & & & & 0 & 0 & & \\ & & & & & & 0 & 1 \\ & & & & & & 0 & 0 \end{pmatrix}.$$

In particular, regular quadratic forms of even rank over $\mathbb{F}_2$ are classified by their rank.

3.3 $\mathbb{Z}/m\mathbb{Z}$, with $4 \not| m$

In this section we apply the Chinese Remainder Theorem to obtain the classification of quadratic forms over $\mathbb{Z}/m\mathbb{Z}$ with $4 \not| m$, from the classification of quadratic forms over $\mathbb{Z}/p^k\mathbb{Z}$ for p and odd prime and over $\mathbb{Z}/2\mathbb{Z}$. In this section, the matrix representation of a quadratic form q with respect to a basis $\mathcal{B} = \{e_1, \cdots, e_n\}$ will always mean the matrix Q with entries

$$q_{ij} = \begin{cases} \beta(e_i, e_j) & \text{if i<j} \\ q(e_i) & \text{if i=j} \\ 0 & \text{otherwise} \end{cases} .$$

Definition 3.17. Let q be a quadratic form over $\mathbb{Z}/m\mathbb{Z}$, for some $m, n \in \mathbb{Z}$ and suppose that $c|m$. Let Q be a matrix representation of q. Then the *reduction* of q mod c is the quadratic form q_c over $\mathbb{Z}/c\mathbb{Z}$ represented by the matrix Q_c whose entries are the reduction mod$c$ of the entries of Q.

For this definition to make sense, we need to prove the following Lemma:

Lemma 3.18. *If q, p are forms over $\mathbb{Z}/m\mathbb{Z}$, such that $p \sim q$ and $c|m$, then $p_c \sim q_c$.*

Proof. We can assume that q, p are defined on $(\mathbb{Z}/m\mathbb{Z})^n$ and p_c, q_c are defined on $(\mathbb{Z}/c\mathbb{Z})^n$. Let $\phi : (\mathbb{Z}/m\mathbb{Z})^n \to (\mathbb{Z}/m\mathbb{Z})^n$ be an equivalence of quadratic forms ($q(x) = p(\phi(x))$ for all x) and let P, Q, T be the matrix representations of p, q and ϕ, with respect to the canonical basis. We have $x^tQx = x^t(T^tPT)x$ for all $x \in (\mathbb{Z}/m\mathbb{Z})^n$, therefore, reducing everything $\mod c$, we have $x^tQ_cx = x^t(T_c^tP_cT_c)x$ for all $x \in (\mathbb{Z}/c\mathbb{Z})^n$, where T_c is the reduction $\mod c$ of T. Furthermore, T_c is invertible, because its determinant is the reduction $\mod c$ of $\det(T)$ and $\det(T)$ is invertible in $\mathbb{Z}/m\mathbb{Z}$. We conclude that the function $\phi_c : (\mathbb{Z}/c\mathbb{Z})^n \to (\mathbb{Z}/c\mathbb{Z})^n$ defined by the matrix T_c is an equivalence of quadratic forms between q_c and p_c.

□

Example 3.19. Consider the quadratic form q over $\mathbb{Z}/6\mathbb{Z}$ given in matrix form by

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

or in polynomial form by $f(x, y, z) = xy + 2xz + 4yz$. Its reduction $\mod 2$ is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

or $f_2(x, y, z) = xy$ in polynomial form. Its reduction $\mod 3$ is

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

or $f_2(x, y, z) = xy + 2xz + yz$ in polynomial form.

Definition 3.20. We say that a quadratic form q over $\mathbb{Z}/m\mathbb{Z}$, with $4 \not| m$, is *regular* provided the following conditions are satisfied:

(i) If p is an odd prime such that $p|m$, then q_p is nondegenerate.

(ii) If $2|m$, then q_2 is regular.

Notice that when $m = 2$ this definition coincides with the previous definition of regularity and when m is odd it is equivalent to nondegeneracy. The following result shows that knowing the classification of quadratic forms over $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/p^k\mathbb{Z}$ for odd primes p is enough to classify quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, for $4 \not| m$.

Proposition 3.21. *Suppose f, g are regular quadratic forms over $\mathbb{Z}/m\mathbb{Z}$ ($4 \not| m$) such that:*

(i) If p is an odd prime and $k \geq 1$ is its exponent in the prime factorization of m, then $f_{p^k} \sim g_{p^k}$.

(ii) If $2|m$, then $f_2 \sim g_2$.

Then $f \sim g$.

Proof. Let F, G (resp. F_p, G_p) be the matrix representations of f, g (resp. f_{p^k}, g_{p^k}) and T_p be the matrix representation of an equivalence between f_{p^k} and g_{p^k}, for each prime p dividing m and where k is the exponent of p in the prime factorization of m. Then for each $p|m$, we have $x^t(T_p^t G_p T_p)x = x^t F_p x$, for all x. By the Chinese Remainder Theorem, we can find a unique matrix T whose entries are congruent to those of $T_p \mod p^k$ for each p, k such that $p^k|m$. We then have

$$x^t(T^t G T)x \equiv x^t F x \pmod{p^k}$$

for each p, k such that $p^k|m$ (where we say that $x \equiv y \pmod{k}$ for column vectors x, y when $x_i \equiv y_i \pmod{k}$ for all i). Then, by the CRT, we must have $x^t(T^t G T)x \equiv x^t F x \pmod{m}$. It is also clear that T is invertible, because all the T_p are invertible, therefore $f \sim g$.

□

The following theorem is now clear:

Theorem 3.22. *Let $m = 2^a p_1^{k_1} \cdots p_\ell^{k_\ell}$, where the p_i are odd primes, $a \in \{0, 1\}$, and $k_i \in \mathbb{N}$. Suppose f, g are regular quadratic forms over $\mathbb{Z}/m\mathbb{Z}$, of ranks $n(f)$ and $n(g)$, respectively. Then $f \sim g$ if and only if the following conditions hold:*

(i) $n(f) = n(g)$.

(ii) $d(f_{p_i^{k_i}}) = d(f_{p_i^{k_i}})$ for all i.

(iii) If $n(f)$ is even and $a = 1$, then $\#_{f_2} = \#_{g_2}$.

References

[1] Serre, J. P. (1973). A Course in Arithmetic. Springer-Verlag.

[2] Milnor, J. and Housemoller, D. (1973). Symmetric Bilinear Forms. Springer-Verlag.

[3] Lorenz, F. and Roquette, P. (February 12, 2010). On the Arf invariant in historical perspective. Available online at `http://www.rzuser.uni-heidelberg.de/~ci3/arf.pdf`.