Applications of Number Theory to Ovoids and Translation Planes

U. Dempwolff

A. Guthmann

Abstract: In this paper we show that for each prime $p \geq 7$ there exists a translation plane of order p^2 of Mason-Ostrom type [11]. These planes occur as 6-dimensional ovoids being projections of the 8-dimensional binary ovoids of Conway, Kleidman and Wilson [3]. In order to verify the existence of such projections we prove certain properties of two particular quadratic forms using classical methods form number theory.

Keywords: Translation planes, ovoids, quadratic forms.

Mathematics Subject Classification (1991): Primary 05E25, 51E15, secondary 11H55.

1. Introduction. Mason and Ostrom [10] construct some translation planes of order p^2 admitting $Ex(32) \cdot Sym(5)$ as a group of automorphisms (an extension of an extraspecial group of order 32 by $Sym(5)$). We call such planes of *Mason-Ostrom type*. In [9] Mason constructs translation planes of order 49 admitting $SL(2,9)$ as automorphisms. We call translation planes of order p^2 admitting $SL(2,9)$ of *Mason type*. In [11] Mason and Shult use the Klein correspondence, which relates rank 2 translation planes with 6-dimensional ovoids to produce all planes of Mason-Ostrom type of order p^2, p a prime ≤ 23. Similarly, Biliotti and Korchmaros [1] find all translation planes of Mason type of order p^2, $p \leq 19$. These results give evidence that both types of planes should constitute infinite series of planes, i.e. that for each prime $p \geq 11$ there planes of order p^2 of both types. The aim of this paper is to verify this conjecture. To construct such planes we use projections of the 8-dimensional binary ovoids of Conway, Kleidman and Wilson [3] to 6-dimensional ovoids which transfer by the Klein correspondence to planes of the desired type. The crucial step in the existence proof is the verification that some particular quadratic forms produce certain integers with specific congruence restrictions.

2. Spreads, Ovoids, and Projections. For convenience we repeat some notions and basic facts on spreads and ovoids. Let V be a 4-dimensional space over the finite field $K = GF(q)$. A spread $\mathcal{S}$ on V is a collection of 2-spaces in V such that $V = \cup_{X \in \mathcal{S}} X$, and $X \cap Y = 0$ for $X, Y \in \mathcal{S}$, $X \neq Y$. Let $\mathcal{L}$ be the set of all cosets of the form $v + X$, $v \in V$, $X \in \mathcal{S}$. Then the triple $(V, \mathcal{L}, \in)$ defines an affine plane of order q^2. In fact, this plane is a translation plane, since the maps $x \mapsto x + v$ ($v \in V$ fixed) induce translations.

Let U be an orthogonal space of type $O^+_{2n}(K)$, i.e. a K-space of dimension $2n$ with a symmetric nondegenerate bilinear form $(\cdot, \cdot)$, such that U has Witt index n. An ovoid $\mathcal{O}$

is a set of 1-dimensional isotropic spaces in U such that $|\mathcal{O}| = q^{n-1}+1$ and $(u,u') \neq 0$ for $< u >, < u' > \in \mathcal{O}$, $< u > \neq < u' >$.

Suppose V is a 4-dimensional K-space and $U = \bigwedge^2 V$. Then U has a nondegenerate bilinear symmetric form such that U has type $O_6^+(K)$ and $\{v_1 \wedge v_2 | v_1, v_2 \in V\}$ is the set of isotropic vectors. The Klein correspondence κ maps a 2-space $X =< v_1, v_2 >$ in V on $\kappa(X) =< v_1 \wedge v_2 >$, a 1-space in U. Then [11]:

Proposition 2.1: *κ is a bijection between the set of 2-spaces and V and the set of isotropic 1-spaces in U. It induces a bijection between the set of spreads on V and the set of ovoids on U.*

The natural representation D of $SL(V)$ on V induces on U the representation $\bigwedge^2 D$ and $\bigwedge^2 D\big(SL(V)\big) \simeq \Omega(V)$, i.e. $Ker(\bigwedge^2 D) =< -\mathbf{1} >$. From this we conclude

Proposition 2.2: *a) A spread $\mathcal{S}$ is of Mason-Ostrom type iff $\kappa(\mathcal{O})$ admits the group $E_{16} : Sym(5)$ as automorphisms.*
b) A spread $\mathcal{S}$ is of Mason type iff $\kappa(\mathcal{O})$ admits the group $Alt(6)$.

Proof: If G is a group as in planes of Mason-Ostrom type or Mason type, then $Z(G) =< -\mathbf{1} >$, giving one direction of the assertion. If, however, $\mathcal{O}$ is an ovoid in U which admits $\overline{G} \simeq E_{16} : Sym(5)$ or $Alt(6)$, then the spread $\kappa^{-1}(\mathcal{O})$ does have a group G such that $G < -\mathbf{1} > / < -\mathbf{1} > \simeq \overline{G}$. It is easy to see (but also follows from [12]) that $< -\mathbf{1} > \subseteq G$, proving the other direction.

Assume finally that W is of type $O_8^+(K)$ and $\mathcal{O}$ is an ovoid in W. Let $< u >$ be an isotropic 1-space, $< u > \notin \mathcal{O}$. The bilinear form induces on $U =< u >^\perp / < u >$ again a nondegenerate form such that U is of type $O_6^+(K)$. Moreover if

$$\mathcal{O}_u = \{< \overline{w} > \mid < \overline{w} >= (< w > + < u >)/ < u >, < w > \in \mathcal{O} \cap < u >^\perp\},$$

then $\mathcal{O}_u$ is an ovoid in U (see [3]).

3. E_8 lattice, Binary Ovoids, and the Main Theorem. The set L of all vectors of the form

$$\frac{1}{2}(a_1, \ldots, a_8),\ a_i \in \mathbf{Z},\ a_i \equiv a_j(2),\ 1 \leq i,j \leq 8,\ \sum a_i \equiv 0(4),$$

is the E_8-lattice in $\mathbf{R}^8$. For $x \in L$ the integer $(x,x) = \sum x_i^2$ is divisible by 2. Set $L_n = \{x \in L | (x,x) = 2n\}$. Then $\Delta = L_1$ is the set of 240 root vectors and one has

$$\Delta = \{\pm e_i \pm e_j | 1 \leq i < j \leq 8\} \cup \{\frac{1}{2}\Sigma \varepsilon_i e_i | \varepsilon_i = \pm 1, \Pi \varepsilon_i = 1\}.$$

The Weyl group $W = W(E_8)$ of L is the group $< \sigma_r | r \in \Delta > \subseteq O(\mathbf{R}^8)$, where the reflection σ_r is defined by $\sigma_r(x) = x - (x,r)r$. Let $p \geq 7$ be a prime. Set $V = L/pL$. Then $(\cdot,\cdot)$ induces on the $GF(p)$-space V an orthogonal scalar product such that V is of type $O_8^+\big(GF(p)\big)$. Moreover, W is faithfully represented on V as a subgroup of $O(V)$.

For $x \in L$ set $\mathcal{S}_2(x) = \{v \in L_p | x \equiv v \bmod 2L\}$. In [3] it is shown that for $x \in L_p$ there is $r \in \Delta$ with $\mathcal{S}_2(x) = \mathcal{S}_2(r)$ and that the set $\mathcal{O} = \mathcal{O}_2(x) = \{< \overline{v} > | v \in \mathcal{S}_2(x)\}$ is an ovoid in V (here $\overline{v} = v + pL$). It is shown that the stabilizer of r in W, the group $W_r = Z_2 \oplus W(E_7) \simeq Z_2 \oplus Z_2 \oplus Sp(6,2)$, is the automorphism group of $\mathcal{O}$. In the sequel we choose the fixed root $r = e_1 - e_2$.

Lemma 3.1: *The stabilizer of e_1, e_2, e_3 in W contains a group*

$$W_r \supseteq G_1 \simeq W(D_5) \simeq E_{16} : Sym(5).$$

If $U_1 =< \overline{e_1}, \overline{e_2}, \overline{e_3} > \subseteq V$, then U_1 is nondegenerate with discriminant $\delta(U_1) = 1$.

Proof: The vectors $\{\pm e_i \pm e_j | 4 \leq i < j \leq 8\}$ form a root system of type D_5 and are orthogonal to e_1, e_2, e_3. The assertion about G_1 follows from [2]. The second assertion is obvious.

Lemma 3.2: *The stabilizer of e_1, e_2, $v = e_3 + \ldots + e_8$ in W contains a group $W_r \supseteq G_2 \simeq W(A_5) \simeq Sym(6)$. If $U_2 =< \overline{e}_1, \overline{e}_2, \overline{v} > \subseteq V$, then U_2 is nondegenerate with discriminant $\delta(U_2) = 6$.*

Proof: $\{\pm(e_i - e_j) | 3 \leq i < j \leq 8\}$ is a root system of type A_5. As before all assertions follow.

Lemma 3.3: *Let U be a nondegenerate orthogonal 3-space over $GF(p)$. Then $U =< v_0 > \perp H$, where H is a hyperbolic plane and v_0 is anisotropic. If $u \in U$ is anisotropic then there is an isotropic vector $0 \neq v \in < u >^{\perp}$ iff $(u,u)/(v_0,v_0)$ is a square in $GF(p)$.*

Proof: The first assertion is well known [6]. The second one follows from Witt's theorem.

Lemma 3.4: *Let V, $U = U_1$ or U_2 have the same meaning as in 3.1 and 3.2. For $x \in V$ set $x = x_0 + x^0$ with $x_0 \in U$, $x^0 \in U^{\perp}$. If $< x >, < x' > \in \mathcal{O}$ can be chosen in such a way that (x_0, x_0) is a nontrivial square and (x_0', x_0') a nonsquare in $GF(p)$, then there exists a projection $\mathcal{O}_u$ of $\mathcal{O}$ such that $\kappa^{-1}(\mathcal{O}_u)$ is of Mason-Ostrom type if $U = U_1$ and of Mason type if $U = U_2$.*

Proof: By 3.3 and assumption we can choose $< x > \in \mathcal{O}$ such that x_0 is anisotropic and that there is an isotropic vector $0 \neq u \in < x >^{\perp} \cap U =< x_0 >^{\perp} \cap U$. Moreover, G_i (G_i as in 3.1 or 3.2 for $i = 1, 2$) fixes both $\mathcal{O}$ and u and induces therefore a group of automorphisms on $\mathcal{O}_u$. It is obvious that the representation of G_i on $< u >^{\perp} / < u >$ is faithful. The assertion follows by 2.2.

The elements of $\mathcal{S}_2(r)$ have the form $x = (x_1, \ldots, x_8) \in \mathbf{Z}^8$ such that

$$\sum_{i=1}^{8} x_i \equiv 0(4), \quad x_1 \equiv x_2 \not\equiv x_3 \equiv \ldots \equiv x_8(2) \qquad (*)$$

and

$$F(x) = x_1^2 + \ldots + x_8^2 = 2p.$$

Lemma 3.5: *Suppose the quadratic form F has solutions $x, x' \in \mathbf{Z}^8$ satisfying $(*)$ such that $F_1(x)$ is a square, $F_1(x')$ is a nonsquare in $GF(p)$, where $F_1(x) = x_1^2 + x_2^2 + x_3^2$. Then $\mathcal{O}$ has a projection $\mathcal{O}_u$ such that $\kappa^{-1}(\mathcal{O}_u)$ is of Mason-Ostrom type.*

Proof: Since $x_0 = x_1\overline{e}_1 + x_2\overline{e}_2 + x_3\overline{e}_3$, $x^0 = \sum_{i=4}^{8} x_i\overline{e}_i$, the assertion follows from 3.4 and 3.1.

Choose a new basis of $\mathbf{R}^8$: $u_1 = e_1$, $u_2 = e_2$, $u_3 = v$, $u_4 = e_3 - e_4$, $u_5 = e_5 - e_6$, $u_6 = e_7 - e_8$, $u_7 = e_3 + e_4 - e_5 - e_6$, $u_8 = e_3 + \ldots + e_6 - 2(e_7 + e_8)$. Then $\{u_1, \ldots, u_8\}$ is an orthogonal basis and $U = U_2 =< \overline{u}_1, \overline{u}_2, \overline{u}_3 >$, $U^{\perp} =< \overline{u}_4, \ldots, \overline{u}_8 >$. Express the vector $x = \sum_{i=1}^{8} y_i u_i$ by the basis $\{e_1, \ldots, e_8\}$. We get

$$x = (y_1, y_2, y_3 + y_4 + y_7 + y_8, y_3 - y_4 + y_7 + y_8, y_3 + y_5 - y_7 + y_8,$$
$$y_3 - y_5 - y_7 + y_8, y_3 + y_6 - 2y_8, y_3 - y_6 - 2y_8).$$

We can guarantee that $x \in \mathcal{S}_2(r)$ if $y_1, \ldots, y_8 \in \mathbf{Z}$,

$$y_1, y_2 \text{ odd},\ y_3, \ldots, y_8 \text{ even} \quad \text{or} \quad y_1, y_2, y_4, \ldots, y_8 \text{ even},\ y_3 \text{ odd} \qquad (**)$$

and

$$(x, x) = H(y) = y_1^2 + y_2^2 + 6y_3^2 + 2(y_4^2 + y_5^2 + y_6^2) + 4y_7^2 + 12y_8^2 = 2p.$$

Note that replacing if necessary y_2 by $-y_2$ we ensure $\sum x_i = y_1 + y_2 + 6y_3 \equiv 0(4)$.

Lemma 3.6: *Suppose that the quadratic form H has solutions $y, y' \in \mathbf{Z}^8$ satisfying $(**)$ such that $H_1(y)$ is a square, $H_1(y')$ is a nonsquare in $GF(p)$, where $H_1(y) = y_1^2 + y_2^2 + 6y_3^2$. Then $\mathcal{O}$ has a projection $\mathcal{O}_u$ such that $\kappa^{-1}(\mathcal{O}_u)$ is of Mason type.*

Proof: With the above notation we have

$$x_0 = y_1\overline{u}_1 + y_2\overline{u}_2 + y_3\overline{u}_3, \quad x^0 = \sum_{i=4}^{8} y_i\overline{u}_i$$

and $(x_0, x_0) = y_1^2 + y_2^2 + 6y_3^2$. The assertion follows from 3.4 and 3.2.

Theorem A: *For each prime $p \geq 11$ there are $x, x', y, y' \in \mathbf{Z}^8 \cap \mathcal{S}_2(r)$ such that $F_1(x)$, $H_1(y)$ are squares and $F_1(x')$, $H_1(y')$ are nonsquares in $GF(p)$.*

From Theorem A and 3.5, 3.6 we deduce:

Theorem B: *For each prime $p \geq 11$ there exist translation planes of order p^2 of Mason-Ostrom type and of Mason type.*

Theorem A is proved in the next section by a series of number theoretic results.

4. Tools from Number Theory. This final section is devoted to a proof of the two main theorems stated below which imply the validity of Theorem A from Section 3. We shall

employ a variety of methods from Analytic Number Theory and the theory of quadratic forms. In the sequel we let $(\frac{\cdot}{p})$ denote the Legendre symbol corresponding to the odd prime p.

Let p be a prime and denote by X_p the set of $x = (x_1, \ldots, x_8) \in \mathbf{Z}^8$ such that

$$F(x) = \sum_{i=1}^{8} x_i^2 = 2p, \quad \sum_{i=1}^{8} x_i \equiv 0 \bmod 4, \quad x_1 \equiv x_2 \not\equiv x_3 \equiv \ldots \equiv x_8 \bmod 2.$$

Our first main result is

Theorem 4.1: *Let $p \geq 5$ be prime, $\varepsilon \in \{-1, 1\}$. Then there exists $x \in X_p$ such that*

$$\left(\frac{x_1^2 + x_2^2 + x_3^2}{p}\right) = \varepsilon.$$

To state the second principal theorem we similarly define Y_p as the set of $y = (y_1, \ldots, y_8) \in \mathbf{Z}^8$ satisfying

$$G(y) := y_1^2 + y_2^2 + 6y_3^2 + 2y_4^2 + 2y_5^2 + 2y_6^2 + 4y_7^2 + 12y_8^2 = 2p$$

and either

$$y_1 \equiv y_2 \equiv 1 \bmod 2, \quad y_3 \equiv \ldots \equiv y_8 \equiv 0 \bmod 2,$$

or

$$y_1 \equiv y_2 \equiv 0 \bmod 2, \quad y_3 \equiv 1 \bmod 2, \quad y_4 \equiv \ldots \equiv y_8 \equiv 0 \bmod 2.$$

Our second main result is

Theorem 4.2: *Let $p \geq 11$ be prime, $\varepsilon \in \{-1, 1\}$. Then there exists $y \in Y_p$ such that*

$$\left(\frac{y_1^2 + y_2^2 + 6y_3^2}{p}\right) = \varepsilon.$$

Our results rely on a combination of properties of certain quadratic forms and analytical tools. The latter will be introduced first.

Let k be a positive integer. A *Dirichlet character modulo k* is a map $\chi : \mathbf{Z} \to \mathbf{C}^*$, such that $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in \mathbf{Z}$ and, moreover, $\chi(a) = 0$ if a and k are not coprime. Clearly, any such χ can be viewed as a homomorphism $Z_k^* \to \mathbf{C}^*$ of the group of residues prime to k into the nonzero complex numbers. The set of all Dirichlet characters modulo k is a group isomorphic to Z_k^*. Consequently there are $\varphi(k)$ Dirichlet characters for fixed k. The unit element of the character group is the principal character χ_0 defined by $\chi_0(a) = 1$ whenever $(a, k) = 1$. Let k be a positive integer, $b, r \in \mathbf{Z}$ with $(k, r) = 1$. We make use of the well known orthogonality relation

$$\sum_{\chi \bmod k} \overline{\chi}(r)\chi(b) = \begin{cases} \varphi(k) & \text{if } b \equiv r(k), \\ 0 & \text{if } b \not\equiv r(k). \end{cases} \tag{1}$$

A Dirichlet character χ modulo k obviously is a periodic function on $\mathbf{Z}$ with period k. If k is its least period, we call χ *primitive* and *imprimitive* otherwise. If p denotes an odd prime then the character $\chi(a) = (\frac{a}{p})$ (Legendre symbol) is a primitive character modulo p.

We shall also need the famous *Pólya-Vinogradov inequality* [4] to estimate character sums. Thus let $\chi \neq \chi_0$ be a Dirichlet character modulo k and N, M be integers. Then we have

$$\left| \sum_{a=N+1}^{N+M} \chi(a) \right| \leq C(\chi)\sqrt{k}\log k, \tag{2}$$

where $C(\chi) = 1$ if χ is primitive and $C(\chi) = 2$ otherwise. In this generality the bound is almost sharp.

We shall use inequality (2) as an essential tool in the proof of the next two results.

Proposition 4.3: *Let $p \geq 5$ be prime, $\varepsilon \in \{-1, 1\}$. Then there exists $b \in \mathbf{Z}$ such that*

$$1 \leq b < p, \quad b \equiv 1 \bmod 2, \quad \left(\frac{2b}{p}\right) = \varepsilon.$$

Proof: If $p = 5$ we have $(\frac{2\cdot 1}{5}) = -1$, $(\frac{2\cdot 3}{5}) = 1$, i.e. $b = 1$ or $b = 3$ does the job. Similarly for $p = 7$, since $(\frac{2\cdot 1}{7}) = 1$, $(\frac{2\cdot 3}{7}) = -1$.

Henceforth we assume $p \geq 11$. Let $N(p, \varepsilon)$ denote the number of odd b in the interval $[1, p-2]$ such that $(\frac{2b}{p}) = \varepsilon$. We must show $N(p, \varepsilon) > 0$.

Since

$$1 + \varepsilon\left(\frac{2b}{p}\right) = \begin{cases} 2 & \text{if } (\frac{2b}{p}) = \varepsilon, \\ 0 & \text{if } (\frac{2b}{p}) \neq \varepsilon, \end{cases}$$

we see that

$$N(p,\varepsilon) = \frac{1}{2} \sum_{b=1,\ b \text{ odd}}^{p-2} \left[1 + \varepsilon\left(\frac{2b}{p}\right)\right] = \frac{p-1}{2} + \frac{\varepsilon}{2} \sum_{b=1,\ b\equiv 1(2)}^{p-2} \left(\frac{b}{p}\right). \tag{3}$$

To estimate the last sum note that $\sum_{b=1}^{p-1}(\frac{b}{p}) = 0$. Thus

$$\begin{aligned} \sum_{b=1,\ b\equiv 1(2)}^{p-2} \left(\frac{b}{p}\right) &= \sum_{b=1}^{p-2}\left(\frac{b}{p}\right) - \sum_{b=2, b\equiv 0(2)}^{p-3} \left(\frac{b}{p}\right) \\ &= -\left(\frac{p-1}{p}\right) - \sum_{c=1}^{(p-3)/2} \left(\frac{2c}{p}\right) = -\left(\frac{-1}{p}\right) - \left(\frac{2}{p}\right) \sum_{c=1}^{(p-3)/2} \left(\frac{c}{p}\right). \end{aligned}$$

The Pólya-Vinogradov inequality shows that the last sum is less than $\sqrt{p}\log p$ in absolute value. We therefore get from (3)

$$\begin{aligned} N(p,\varepsilon) &\geq \frac{p-1}{2} - \left| \frac{\varepsilon}{2}\left(\frac{2}{p}\right) \sum_{b=1, b\equiv 1(2)}^{p-2} \left(\frac{b}{p}\right) \right| > \frac{p-1}{2} - \frac{1}{2}(1 + \sqrt{p}\log p) \\ &= \frac{1}{2}(p - 2 - \sqrt{p}\log p) > 0, \end{aligned}$$

since $p \geq 11$. This proves what we want.

Proposition 4.4: *Let $p \geq 137$ be prime, $r \in \mathbf{Z}$, $(r, 24p) = 1$, $\varepsilon \in \{-1, 1\}$. Then there exists $b \in \mathbf{Z}$ such that*

$$1 \leq b < p, \quad b \equiv r \bmod 24, \quad \left(\frac{2b}{p}\right) = \varepsilon.$$

Proof: Denote by $N(p, \varepsilon, r)$ the number of b satisfying the above conditions. We have to show $N(p, \varepsilon, r) > 0$. As in the proof of Proposition 4.3 we have

$$N(p, \varepsilon, r) = \frac{1}{2} \sum_{b=1, b\equiv r(24)}^{p-1} \left[1 + \varepsilon\left(\frac{2b}{p}\right)\right] = \frac{1}{2} \sum_{b=1, b\equiv r(24)}^{p-1} 1 + \frac{1}{2}\varepsilon\left(\frac{2}{p}\right) \sum_{b=1, b\equiv r(24)}^{p-1} \left(\frac{b}{p}\right). \quad (4)$$

Using the orthogonality relation (2) with $k = 24$, $\varphi(k) = 8$, we get

$$\sum_{b=1, b\equiv r(24)}^{p-1} \left(\frac{b}{p}\right) = \frac{1}{8} \sum_{\chi \bmod 24} \overline{\chi}(r) \sum_{b=1}^{p-1} \chi(b)\left(\frac{b}{p}\right). \quad (5)$$

Now observe that $b \mapsto \chi(b)(\frac{b}{p})$ is a Dirichlet ψ character modulo $24p$. Clearly, $\psi \neq \psi_0$ (principal character), but ψ may be imprimitive. In any case, Pólya-Vinogradov yields

$$\left|\sum_{b=1}^{p-1} \chi(b)\left(\frac{b}{p}\right)\right| \leq 2\sqrt{24p}\log(24p).$$

Thus we obtain together with (5)

$$\left|\sum_{b=1, b\equiv r \bmod 24}^{p-1} \left(\frac{b}{p}\right)\right| \leq 4\sqrt{6p}\log(24p).$$

Inserting into (4) gives

$$\left|N(p, \varepsilon, r) - \frac{1}{2} \sum_{b=1, b\equiv r(24)}^{p-1} 1\right| \leq 2\sqrt{6p}\log(24p).$$

Since $\sum_{b=1, b\equiv r(24)}^{p-1} 1 = 1 + \left[\frac{p-r}{24}\right]$ we get

$$\begin{aligned} N(p, \varepsilon, r) &\geq \frac{1}{2} + \frac{1}{2}\left[\frac{p-r}{24}\right] - 2\sqrt{6p}\log(24p) \geq \frac{p-r}{48} - 2\sqrt{6p}\log(24p) \\ &\geq \frac{p-23}{48} - 2\sqrt{6p}\log(24p) > 0, \end{aligned}$$

if p exceeds $4 \cdot 10^5$. Hence our assertion is proved if $p \geq 4 \cdot 10^5$.

It remains to consider the range $137 \leq p < 4 \cdot 10^5$. Here the assertion can be checked numerically as follows. Firstly the prime p and the sign $\varepsilon \in \{-1, 1\}$ are fixed. Then for each integer r such that $1 \leq r \leq 24$ and $(r, 24) = 1$, the integers $b \equiv r(24)$ in the interval $[1, p-1]$ are scanned and tested for $(\frac{2b}{p}) = \varepsilon$. If one b is found, we proceed with the next value of r. Otherwise the assertion would be false for p. These steps are carried out for all p with $137 \leq p < 4 \cdot 10^5$ and for $\varepsilon = -1$ and $\varepsilon = 1$. The entire program takes only a few minutes of CPU time on any common computing device. We thus conclude the proof of Proposition 4.4.

It should be pointed out that Proposition 4.4 is not true for $p = 131$ and hence the bound is sharp. If $p = 131$, $\varepsilon = -1$, $r = 23$, then no b exists satisfying the required conditions.

We now come to some arithmetical results concerning the representation of integers by quadratic forms. Among others we use two classical theorems. The first is due to Lagrange [5, p. 279]: each positive integer can represented as the sum of four squares. We also need Legendre's famous theorem on the representation of integers as the sum of three squares [5, p.261], which is

Proposition L: *Let n be a positive integer. Then the equation $n = x^2 + y^2 + z^2$ is solvable in integers x, y, z if, and only if n is not of the shape $n = 4^a(8b + 7)$ for integers $a, b \geq 0$.*

In addition we need further results of a similar type for special quadratic forms occurring in Section 3. Next we give a result similar to Lagrange's four square theorem.

Proposition 4.5: *The quadratic form $F(x) = x_1^2 + x_2^2 + x_3^2 + 2x_4^2 + 6x_5^2$ represents every positive integer.*

Proof: Let $N \in \mathbf{N}$ be given. If N is not of the form $N = 4^a(8n + 7)$, where $a, n \geq 0$ are integers, then there exist integers x_1, x_2, x_3 such that $N = x_1^2 + x_2^2 + x_3^2 = F(x_1, x_2, x_3, 0, 0)$. This follows from Proposition L.

Thus assume $N = 4^a(8n+7)$ with non negative integers a, n. By Proposition L again, there exist integers x_1, x_2, x_3 such that $8n+5 = x_1^2 + x_2^2 + x_3^2$. If $a = 0$ take $x_4 = 1$, $x_5 = 0$; if $a > 0$ take $x_4 = x_5 = 2^{a-1}$. Then $2x_4^2 + 6x_5^2 = 2 = 2 \cdot 4^a$ for $a = 0$ and, if $a > 0$

$$2x_4^2 + 6x_5^2 = 2(x_4^2 + 3x_5^2) = 2(2^{2a-2} + 3 \cdot 2^{2a-2}) = 2 \cdot 4^a.$$

Therefore in any case $2x_4^2 + 6x_5^2 = 2 \cdot 4^a$. Hence

$$\begin{aligned} N &= N - 2 \cdot 4^a + 2 \cdot 4^a = 4^a(8n + 7) - 2 \cdot 4^a + 2 \cdot 4^a = 4^a(8n + 5) + 2 \cdot 4^a \\ &= 2^{2a}(x_1^2 + x_2^2 + x_3^2) + 2(x_4^2 + 3x_5^2) = F(2^a x_1, 2^a x_2, 2^a x_3, x_4, x_5), \end{aligned}$$

as was to be shown.

The next result is an analogue of Legendre's theorem for the quadratic form $F(x) = x_1^2 + x_2^2 + 6x_3^2$:

Proposition 4.6: *Let N be a positive integer. Then the equation $N = x_1^2 + x_2^2 + 6x_3^2$ is solvable in integers x_1, x_2, x_3 if, and only if N is not of the shape $N = 9^a(9b + 3)$ for integers $a, b \geq 0$.*

Proof: The determinant D of $F(x) = x_1^2 + x_2^2 + 6x_3^2$ is equal to $d = 6$. As is well known [8, Ch. 50], N is represented by a form belonging to the genus of F if $F(x) \equiv N(p^{r+1})$ is solvable for all primes $p|2d$ and $p^r \| N$ $(p > 2)$ or $p^r \| 4N$ $(p = 2)$. If these conditions are not satisfied, then N cannot be represented by any form of the genus of F.

According to Eisenstein [7] there are exactly two reduced forms with $d = 6$, namely F as above and $G(x) = x_1^2 + 2x_2^2 + 3x_3^2$. Since these do not lie in the same genus, we conclude that the class of F coincides with the genus of F.

We now investigate the solvability of the congruences for $p|2d = 12$, i.e. $p \in \{2, 3\}$.

$p = 2$: Let $N = 2^\alpha n$, where n is odd. Then we must show that $F(x) \equiv 2^\alpha n \bmod 2^{\alpha+3}$ is always solvable. If α is even, write $\alpha = 2\beta$. Squares modulo 8 are the residue classes of $0, 1, 4$. From this it follows at once that $x_1^2 + x_2^2 + 6x_3^2 \equiv n(8)$ is solvable for all integers n, and consequently

$$F(2^\beta x_1, 2^\beta x_2, 2^\beta x_3) \equiv 2^\alpha n \bmod 2^{\alpha+3},$$

as desired. If $\alpha = 2\beta + 1$ is odd, we consider the squares modulo 16, i.e. the residue classes of $0, 1, 4, 9$. Again $x_1^2 + x_2^2 + 6x_3^2 \equiv 2n(16)$ can be solved for any integer n, and then

$$F(2^\beta x_1, 2^\beta x_2, 2^\beta x_3) \equiv 2^{2\beta+1} n \equiv 2^\alpha n \bmod 2^{\alpha+3}.$$

$p = 3$: Write $N = 3^\alpha n$, where n is not divisible by 3. We must investigate whether $F(x) \equiv 3^\alpha n \bmod 3^{\alpha+1}$ is solvable. We proceed as before. If α is even consider $F(x) \equiv n(3)$, i.e. $x_1^2 + x_2^2 \equiv n(3)$. Clearly this congruence is solvable for any n. Then $F(3^\beta x_1, 3^\beta x_2, 3^\beta x_3) \equiv 3^\alpha n(3^{\alpha+1})$. If α is odd consider $F(x) \equiv 3n(9)$. Squares modulo 9 are among $Q = \{0, 1, 4, 7\}$, and $6Q = \{0, 6\}$. Thus $Q+Q+6Q = \{0, 1, 2, 4, 5, 6, 7, 8\}$. The congruence is therefore solvable if $3n \not\equiv 3(9)$, i.e. if $n \neq 3b + 1$. Again $F(3^\beta x_1, 3^\beta x_2, 3^\beta x_3) \equiv 3^\alpha n(3^{\alpha+1})$. To complete our argument we show that $F(x) \equiv 3^\alpha n(3^{\alpha+1})$ is not solvable for $n = 3b + 1$. Otherwise, there were integers x_i such that

$$x_1^2 + x_2^2 + 6x_3^2 \equiv 3^\alpha(3b + 1) = 3^{2\beta+2} b + 3^{2\beta+1} \equiv 3^{2\beta+1}(3^{2\beta+2}).$$

In particular, $x_1^2 + x_2^2 + 6x_3^2 \equiv 3(9)$, which is impossible. We have thus shown that $F(x) \equiv 3^\alpha n(3^{\alpha+1})$ is solvable if, and only if $n \neq 3b + 1$. This means that N must not be of the form $3^\alpha(3b + 1)$ with α odd, i.e. $N \neq 9^a(9b + 3)$.

Hence our proof of Proposition 4.6 is complete.

We are now prepared to prove the main theorems of the present section.

Proof of Theorem 4.1: By Proposition 4.3 there exists an odd integer b such that $1 \leq b < p$ and $(\frac{2b}{p}) = \varepsilon$. Since $2b \equiv 2(4)$, Legendre's theorem guarantees the existence of integers x_1, x_2, x_3 with

$$2b = x_1^2 + x_2^2 + x_3^2.$$

Not all of the x_i can be odd, since then $x_1^2 + x_2^2 + x_3^2 \equiv 3(4)$. Thus we may assume x_3 is even. Since then $x_3^2 \equiv 0(4)$, we get $x_1^2 + x_2^2 \equiv 2b \equiv 2(4)$. Hence both x_1 and x_2 are odd. Now choose their signs according to $x_1 \equiv 1(4)$, $x_2 \equiv 3(4)$.

Since b is odd, $\frac{p-b}{2}$ is a positive integer. Write it as a sum of five squares (by Legendre's Theorem it can even be written as a sum of four squares). Hence $\frac{p-b}{2} = \sum_{i=4}^{8} y_i^2$ for suitable y_i. Let $x_i = 2y_i$, $4 \leq i \leq 8$. Then $x = (x_1, \ldots, x_8)$ satisfies

$$x_1 \equiv 1(4),\ x_2 \equiv 3(4),\ x_i \equiv 0(4),\ 3 \leq i \leq 8.$$

Therefore $\sum_{i=1}^{8} x_i \equiv 0(4)$. Moreover,

$$\sum_{i=1}^{8} x_i^2 = x_1^2 + x_2^2 + x_3^2 + \sum_{i=4}^{8} (2y_i)^2 = 2b + 4\frac{p-b}{2} = 2p,$$

which implies $x \in X_p$. Since

$$\left(\frac{x_1^2 + x_2^2 + x_3^2}{p}\right) = \left(\frac{2b}{p}\right) = \varepsilon,$$

we conclude the proof of Theorem 4.1.

Proof of Theorem 4.2: The assertion will first be verified for primes $p \geq 137$, where Proposition 4.4 applies.

We start by considering the case $p \equiv 1(4)$. Take $r = 1$ in Proposition 4.4. Hence there exists $b \in \mathbf{Z}$ with

$$1 \leq b < p, \quad b \equiv 1(24), \quad \left(\frac{2b}{p}\right) = \varepsilon.$$

Since $2b$ is not divisible by 3, Proposition 4.6 tells us that $2b = y_1^2 + y_2^2 + 6y_3^2$ for suitable integers y_i. Since $2b \equiv 2(16)$, we get $y_1^2 + y_2^2 + 6y_3^2 \equiv 2(16)$. If now y_3 were odd, then $y_3^2 \equiv 1(8)$, $6y_3^2 \equiv 6(16)$. But then $2 \equiv 2b \equiv y_1^2 + y_2^2 + 6(16)$ and $y_1^2 + y_2^2 \equiv 12(16)$ which is impossible. Hence we conclude that y_3 is even. We further get $6y_3^2 \equiv 0(8)$ and $2 \equiv 2b \equiv y_1^2 + y_2^2(8)$. Thus y_1, y_2 are both odd.

Now consider the positive integer $\frac{p-b}{4}$. By Proposition 4.5 we can represent it in the form

$$\frac{p-b}{4} = x_4^2 + x_5^2 + x_6^2 + 2x_7^2 + 6x_8^2.$$

Set $y_i = 2x_i$, $4 \leq i \leq 8$. Then $y_1 \equiv y_2 \not\equiv y_3 \equiv \ldots \equiv y_8 \equiv 0(2)$ and

$$\begin{aligned} H(y) &= y_1^2 + y_2^2 + 6y_3^2 + 2y_4^2 + 2y_5^2 + 2y_6^2 + 4y_7^2 + 12y_8^2 \\ &= 2b + 8(x_4^2 + x_5^2 + x_6^2 + 2x_7^2 + 6x_8^2) = 2b + 8\frac{p-b}{4} \\ &= 2p. \end{aligned}$$

Hence $y \in Y_p$. Finally

$$\left(\frac{y_1^2 + y_2^2 + 6y_3^2}{p}\right) = \left(\frac{2b}{p}\right) = \varepsilon,$$

and the theorem follows for $p \equiv 1(4)$.

It remains to treat $p \equiv 3(4)$. This time we take $r = 7$ in Proposition 4.4. Hence we can find $b \in \mathbf{Z}$ with

$$1 \leq b < p, \quad b \equiv 7(24), \quad \left(\frac{2b}{p}\right) = \varepsilon.$$

Again $2b = y_1^2 + y_2^2 + 6y_3^2$ for integers y_i by Proposition 4.6. If y_3 were even, then $6y_3^2 \equiv 0(8)$ and $6 \equiv 2b = y_1^2 + y_2^2 + y_3^2 \equiv y_1^2 + y_2^2(8)$, which is impossible. Therefore y_3 is odd. This leads to $y_3^2 \equiv 1(8)$ and $6y_3^2 \equiv 6(8)$. Hence $6 \equiv 2b \equiv y_1^2 + y_2^2 + 6(8)$, implying $y_1^2 + y_2^2 \equiv 0(8)$. Consequently y_1, y_2 are even.

By Proposition 4.5 we can find integers $x_4, \ldots, x_8$ such that

$$\frac{p-b}{4} = x_4^2 + x_5^2 + x_6^2 + 2x_7^2 + 6x_8^2.$$

If we now define $y_i = 2x_i$ for $4 \leq i \leq 8$, it is easily verified as before that $y \in Y_p$ and

$$\left(\frac{y_1^2 + y_2^2 + 6y_3^2}{p}\right) = \left(\frac{2b}{p}\right) = \varepsilon$$

This finishes the proof for $p \equiv 3(4)$.

We have thus shown that Theorem 4.2 is true for $p \geq 137$. For the primes in the range between 11 and 131 (inclusively) a straightforward computer search shows that for $\varepsilon = \pm 1$ there is always a solution $y \in Y_p$ for the equation in 4.2. Hence the proof is complete.

A final remark. For a given p different solutions of the quadratic form may yield isomorphic or nonisomorphic 6-dimensional ovoids. Similarly our approach may be applied to the ternary ovoids in [3] giving even more projections. However, to decide the isomorphism problem between ovoids would require the concrete structure of the solutions of the quadratic form.

Bibliography

[1] Biliotti, M., Korchmaros, G., Some finite translation planes arising from A_6-invariant ovoids of the Klein quadric, J. Geom. **37**, 23-47 (1990).

[2] Carter, R.W., Simple Groups of Lie Type, New York: Wiley 1972.

[3] Conway, J.H., Kleidman, P.B., Wilson, R.A., New families of ovoids in O_8^+, Geom. Ded. **26**, 157-170 (1988).

[4] Davenport, H., Multiplicative Number Theory, New York: Springer 1980.

[5] Dickson, L.E., History of the Theory of Numbers, Vol. II, New York: Chelsea 1971.

[6] Dieudonné, J., Le géometrie des groupes classiques, Springer 1971.

[7] Eisenstein, G., Tabelle der reduzierten quadratischen Formen, nebst den Resultaten neuer Forschungen über diese Formen, in besonderer Rücksicht auf ihre tabellarische Bestimmung, Crelles J. **41**, 141-190 (1851).

[8] Jones. B.W., The Arithmetic Theory of Quadratic Forms, Carus Mathematical Monographs No. 10, Math. Association of America, 1950.

[9] Mason, G., Some translation planes of order 7^2 which admit $SL(2,9)$, Geom. Ded. **17**, 297-305 (1985).

[10] Mason, G., Ostrom, T.G., Some translation planes of extraspecial type, Geom. Ded. **17**, 307-322 (1985).

[11] Mason, G., Shult, E., The Klein correspondence and the ubiquity of certain translation planes, Geom. Ded. **21**, 29-50 (1986).

[12] Ostrom, T.G., Collineation groups whose order is prime to the characteristic, Math. Z. **156**, 59-71 (1977).

Ulrich Dempwolff
Andreas Guthmann

Fachbereich Mathematik
Universität Kaiserslautern
D-67663 Kaiserslautern