J. Eur. Math. Soc. 10, 173–190 © European Mathematical Society 2008

Koen Thas · Don Zagier

Finite projective planes, Fermat curves, and Gaussian periods

Received October 7, 2006 and in revised form February 20, 2007

Abstract. One of the oldest and most fundamental problems in the theory of finite projective planes is to classify those having a group which acts transitively on the incident point-line pairs (flags). The conjecture is that the only ones are the Desarguesian projective planes (over a finite field). In this paper, we show that non-Desarguesian finite flag-transitive projective planes exist if and only if certain Fermat surfaces have no non-trivial rational points, and formulate several other equivalences involving Fermat curves and Gaussian periods. In particular, we show that a non-Desarguesian flag-transitive projective plane of order n exists if and only if $n > 8$, the number $p = n^2 + n + 1$ is prime, and the square of the absolute value of the Gaussian period $\sum_{a \in \mathcal{D}_n} \zeta^a$ ($\zeta =$ primitive pth root of unity, $\mathcal{D}_n =$ group of nth powers in $\mathbb{F}_p^\times$) belongs to $\mathbb{Z}$. We also formulate a conjectural classification of all pairs (p, n) with p prime and $n \mid p - 1$ having this latter property, and give an application to the construction of symmetric designs with flag-transitive automorphism groups. Numerical computations are described verifying the first conjecture for $p < 4 \times 10^{22}$ and the second for $p < 10^7$.

1. Introduction

A finite *projective plane* Π *of order* n, where $n \in \mathbb{N}$, is a point-line incidence structure satisfying the following conditions:

(i) each point is incident with ("lies on") $n + 1$ lines and each line is incident with ("contains") $n + 1$ points;

(ii) any two distinct lines intersect in exactly one point and any two distinct points lie on exactly one line.

One also traditionally requires that n be ≥ 2 to exclude the uninteresting cases of a single line and a point not on it ($n = -1$), a single line and one point on it ($n = 0$), or the three vertices and three sides of a triangle ($n = 1$). This is equivalent to requiring that Π contains an ordinary quadrangle (four points with no three on a line) as subgeometry.

K. Thas: Department of Pure Mathematics and Computer Algebra, Ghent University, Galglaan 2, B-9000 Ghent, Belgium; e-mail: kthas@cage.UGent.be

D. Zagier: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany, and Collège de France, 3, rue d'Ulm, F-75005 Paris, France; e-mail: zagier@mpim-bonn.mpg.de

Mathematics Subject Classification (2000): 51E15, 05E20, 11L05, 14G05

A *flag* of Π is an incident point-line pair. It is easily seen that a finite projective plane of order n has $n^2 + n + 1$ points, $n^2 + n + 1$ lines, and $(n + 1)(n^2 + n + 1)$ flags.

The obvious examples of finite projective planes are the projective planes $\mathbb{P}^2(\mathbb{F})$ over finite fields $\mathbb{F}$. In this case the order $n = |\mathbb{F}|$ is a prime power, and in fact no examples of finite projective planes of non-prime power order are known, though there are examples of prime power order which are not isomorphic to $\mathbb{P}^2(\mathbb{F})$. A classical theorem of R. Moufang (cf. [9]) states that a finite projective plane is isomorphic to some $\mathbb{P}^2(\mathbb{F})$ if and only if a certain configurational property corresponding to the classical theorem of Desargues is satisfied. Projective planes of this type are therefore often called *Desarguesian*.

We call a projective plane *flag-transitive* if its group of automorphisms acts transitively on the flags. Clearly Desarguesian planes have this property, since the automorphism group of the projective plane $\mathbb{P}^2(\mathbb{F})$ over a finite field $\mathbb{F}$ of characteristic p is the semi-direct product $\mathbf{P\Gamma L}_3(\mathbb{F}) = \mathbf{PGL}_3(\mathbb{F}) \rtimes \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ and already the subgroup $\mathbf{PGL}_3(\mathbb{F})$ acts transitively on the flags. Conversely, it is an old and fundamental conjecture in the theory of projective planes, first mentioned in D. G. Higman and J. E. McLaughlin [8], that every flag-transitive finite projective plane is Desarguesian. The following theorem, which is an amalgam of results from a large number of papers in the literature (see e.g. [6]), strongly limits the possibilities for a counterexample to this conjecture.

Theorem 1.1. *Let Π be a finite flag-transitive projective plane of order n, and suppose that Π is not Desarguesian. Then*

(a) *n is even;*
(b) *the number $p = n^2 + n + 1$ is prime;*
(c) *the automorphism group* $\mathrm{Aut}(\Pi)$ *of* Π *acts regularly (simply transitively) on the flags of* Π.

Note that part (c) implies that $|\mathrm{Aut}(\Pi)| = (n + 1)(n^2 + n + 1)$, the number of flags. This is in stark contrast to the Desarguesian case, where already the subgroup $\mathbf{PGL}_3(\mathbb{F})$ of $\mathrm{Aut}(\Pi)$ has a much larger order. In fact, if Π is Desarguesian of order different from 2 or 8, then it is known [3] that $\mathrm{Aut}(\Pi)$ contains *no* subgroup which acts regularly on the flags of Π.

Remark 1.2. In [4], W. Feit claims that if Π and n are as in Theorem 1.1, then n is not a power of 2, and in a recent paper [12], U. Ott claims that any flag-transitive finite projective plane has prime power order. Together with the above theorem, these two results would imply the non-existence of non-Desarguesian flag-transitive finite projective planes. Unfortunately, both proofs appear to contain mistakes: Feit uses a lemma of B. Gordon, W. H. Mills and L. R. Welch [7] (in the proof of [4, Theorem A]) which is proved only under much more restrictive hypotheses in [7], and there is a mistake in [12] in deriving [12, formula (18)] from [12, formula (17)], as pointed out in [15].

As already mentioned, Theorem 1.1 is a combination of a collection of difficult theorems from a number of different papers, but in fact a large part of it can be deduced in one step from a later theorem of W. M. Kantor, since it is relatively easy to show that any group which acts flag-transitively also acts point-primitively. (This is a corollary of a more general result in [8].) Kantor's result, whose proof invokes the classification of finite simple groups, is as follows.

Theorem 1.3 (W. M. Kantor [10]). *Let Π be a finite projective plane of order n. Suppose that there is a group of automorphisms G which acts primitively on the points of Π and that Π is not Desarguesian. Then n is even, $n^2 + n + 1$ is prime, G is a Frobenius group, and $|G|$ divides $(n + 1)(n^2 + n + 1)$ or $n(n^2 + n + 1)$.*

In the paper of Feit cited above, it is proved that under the assumptions of Theorem 1.1 every divisor d of n must satisfy $d^{n+1} \equiv 1 \pmod{n^2+n+1}$, and also that n must be larger than 14 400 008. An elementary proof of the first assertion is given in a recent paper by the first author [14], which also contains a survey of the most important results on finite flag-transitive projective planes since 1961 and some related problems.

2. Classification of flag-transitive projective planes

A general construction of potential examples of finite projective planes, known in the literature as the method of *difference sets*, is as follows. Suppose we have a finite (not necessarily abelian) group F containing a subset $\mathcal{D}$ for which the map

$$\mathcal{D} \times \mathcal{D} \smallsetminus \{\text{diagonal}\} \to F \smallsetminus \{e\}, \qquad (x, y) \mapsto xy^{-1}, \tag{1}$$

is bijective, so that $|F| = n^2 + n + 1$, where $|\mathcal{D}| = n + 1$. Then we obtain a finite projective plane $\Pi = \Pi(F, \mathcal{D})$ of order n by taking both the set of points and the set of lines of Π to be the elements of F, with the incidence relation that a point x and a line y are incident if and only if yx^{-1} belongs to $\mathcal{D}$. We will be concerned with the special case of this described by the following proposition, which is essentially a restatement of a result of J. Fink [5]. Before stating it, we make two definitions.

We call a prime number or prime power *special* if it has the form $q = n^2 + n + 1$ and every element of the finite field $\mathbb{F}_q$ is a difference of two non-zero nth powers. We call a finite projective plane *flag-regular* if it has a group of automorphisms that acts regularly (simply transitively) on the flags.

Proposition 2.1. *If $q = n^2 + n + 1$ is a special prime or prime power with $n > 1$, then $\Pi(\mathbb{F}_q, (\mathbb{F}_q^\times)^n)$ is a flag-regular finite projective plane. Conversely, if Π is a flag-regular finite projective plane of order n, and if the number $p = n^2 + n + 1$ is prime, then p is special and $\Pi \cong \Pi(\mathbb{F}_p, (\mathbb{F}_p^\times)^n)$.*

Remark 2.2. Note that, since the group law of $\mathbb{F}_q$ is addition, the expression xy^{-1} in the general formula (1) is to be interpreted as $x - y$ when defining $\Pi(\mathbb{F}_q, (\mathbb{F}_q^\times)^n)$.

Remark 2.3. The restriction $n > 1$ in the first part of the proposition is needed only because this is a requirement in the definition of finite projective planes we are using; axioms (i) and (ii) and the flag-regularity hold also for $n = 1$, $p = 3$.

Proof of Proposition 2.1. Let $\mathcal{D}_n = \mathcal{D}_{q,n}$ denote the set of nth powers (or equivalently, of $(n+1)$st roots of unity) in $\mathbb{F}_q^\times$. The fact that every element in $\mathbb{F}_q$ is a difference of two elements of $\mathcal{D}_n$ tells us that the map (1) with $\mathcal{D} = \mathcal{D}_n$ and $F = \mathbb{F}_q$ is surjective, and since the two sides are finite sets of the same cardinality it must be a bijection. Hence $\Pi(\mathbb{F}_q, \mathcal{D}_n)$ is a finite projective plane, and it is also clear that the permutations $x \mapsto ax+b$ $(a \in \mathcal{D}_n,\, b \in \mathbb{F}_q)$ of $\mathbb{F}_q$ give automorphisms of this projective plane and that the group of these automorphisms acts simply transitively on the flags.

Conversely, let Π be a projective plane of order n for which a group of automorphisms G acts regularly on the flags. Let (p_0, L_0) be a fixed flag of Π, so that by assumption every flag can be written as $g(p_0, L_0)$ for a unique $g \in G$. If H and K are the stabilizers of p_0 and L_0 in G, then it follows that $H \cap K = \{e\}$ and that both the map

$$H \times (K \smallsetminus \{e\}) \times H \to G \smallsetminus H \tag{2}$$

given by multiplication and the corresponding map with the roles of H and K interchanged are bijections. (To see the bijectivity of (2), note first that the two sets have the same cardinality, since $(n+1)n(n+1) = (n+1)(n^2+n+1) - (n+1)$, so that it suffices to prove surjectivity. If $g \in G \smallsetminus H$, then the line through p_0 and gp_0 has the form hL_0 for some $h \in H$, so the flag $(h^{-1}gp_0, L_0)$ equals $k(p_0, L_0)$ with $k \in K \smallsetminus \{e\}$, and then $g = hkh'$ with $h' \in H$.) We also mention the converse: if G is any finite group containing subgroups H and K for which both (2) and the analogous map with H and K interchanged are bijections, then we obtain a finite projective plane having G as a group of automorphisms acting regularly on the flags by taking the points and lines to be the left cosets of H and K in G, respectively, and defining "incidence" to mean "non-empty intersection." For instance, two distinct "points" $p_1 = g_1H$ and $p_2 = g_2H$ lie on the unique "line" $L = gK$ given by $g = g_1h_1k = g_2h_2$, where $g_1^{-1}g_2 = h_1kh_2^{-1}$ is the decomposition of $g_1^{-1}g_2 \in G \smallsetminus H$ given by the bijection (2).

If we now further assume that $p = n^2+n+1$ is prime, then the Sylow theorems and the fact that $|G| = p(n+1)$ with $p > n+1$ imply that G has a unique (and hence normal) subgroup F of order p. Since $(|F|, |H|) = 1$ and $|F||H| = |G|$, the map $F \times H \to G$ given by multiplication is a bijection, so G is the semi-direct product $F \rtimes H$. Moreover, the action of H on F by conjugation is faithful, because the uniqueness of the decomposition in (2) shows that there can never be a relation $g = hgh^{-1}$ with $h \in H \smallsetminus \{e\}$ and $g \in G \smallsetminus H$. Identifying F with $\mathbb{F}_p$ and observing that $\mathrm{Aut}(\mathbb{F}_p) = \mathbb{F}_p^\times$ is cyclic and has $\mathcal{D}_n$ as its unique subgroup of order $n+1$, we can make the further identifications $H = \mathcal{D}_n$ and $G = \mathbb{F}_p \rtimes \mathcal{D}_n$ or, in a convenient matrix representation,

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \right\}_{a \in \mathcal{D}_n, b \in \mathbb{F}_p}, \quad F = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}_{b \in \mathbb{F}_p}, \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right\}_{a \in \mathcal{D}_n}.$$

For the same reason the subgroup K of G is also cyclic, generated by some element $\left(\begin{smallmatrix} a_0 & b_0 \\ 0 & 1 \end{smallmatrix}\right)$ with a_0 a generator of $\mathcal{D}_n$ and $b_0 \neq 0$, and conjugating all matrices of G by $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\lambda = (a_0 - 1)/b_0$ we can suppose

$$K = \left\{ \begin{pmatrix} a & a-1 \\ 0 & 1 \end{pmatrix} \right\}_{a \in \mathcal{D}_n}.$$

Now the requirement that the map (2) be an isomorphism says that every matrix $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in \mathcal{D}_n$ and $b \in \mathbb{F}_p^\times$ can be factored uniquely as

$$\begin{pmatrix} a_1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & a_2 - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_3 & 0 \\ 0 & 1 \end{pmatrix},$$

and multiplying this out we find that this is precisely equivalent to the requirement that every element of $\mathbb{F}_p^\times$ is uniquely a difference of two elements of $\mathcal{D}_n$. Hence p is special and $\Pi \cong \Pi(\mathbb{F}_p, \mathcal{D}_n)$. □

In Section 6, we will obtain a generalization of this result (for certain symmetric 2-designs), with an entirely different proof.

The proof of Proposition 2.1 was self-contained. If we combine it with parts (a) and (b) of Theorem 1.1, we obtain the following stronger result:

Theorem 2.4. *Let n be the order of a flag-transitive finite projective plane Π. Then at least one of the following holds:*

(a) *n is a prime power and $\Pi \cong \mathbb{P}^2(\mathbb{F}_n)$;*
(b) *$p = n^2 + n + 1$ is a special prime and $\Pi \cong \Pi(\mathbb{F}_p, (\mathbb{F}_p^\times)^n)$.*

Notice that the two alternatives occurring in the theorem are not necessarily exclusive: it is possible that the number n is both a prime power and is associated to a special prime $p = n^2 + n + 1$, and in this case the projective plane Π of this order, while still unique, has both forms $\mathbb{P}^2(\mathbb{F}_n)$ and $\Pi \cong \Pi(\mathbb{F}_p, (\mathbb{F}_p^\times)^n)$. By the discussion following Theorem 1.1, we know that this can happen for only two values of n, namely $n = 2$ ($p = 7$) and $n = 8$ ($p = 73$). Let us look in detail at these two exceptional cases to see how the isomorphism between the two differently-defined projective plane structures works.

Consider first the case $n = 2$. We define an automorphism A of $\mathbb{P}^2(\mathbb{F}_2)$ of order 7 by

$$A : (x : y : z) \mapsto (y : z : x + y).$$

Then every point of $\mathbb{P}^2(\mathbb{F}_2)$ has the form $p_i = A^i(p_0)$ for a unique $i \in \mathbb{Z}/7\mathbb{Z}$, where p_0 is the point $(1 : 0 : 0)$:

i	0	1	2	3	4	5	6
p_i	$(1:0:0)$	$(0:0:1)$	$(0:1:0)$	$(1:0:1)$	$(0:1:1)$	$(1:1:1)$	$(1:1:0)$

and every line in $\mathbb{P}^2(\mathbb{F}_2)$ has the form $L_j = A^j(L_0)$ for a unique $j \in \mathbb{Z}/7\mathbb{Z}$, where L_0 is the line $\{x = 0\}$:

j	0	1	2	3	4	5	6
L_j	$x = 0$	$x = z$	$x + y + z = 0$	$y = z$	$x = y$	$z = 0$	$y = 0$

Then $L_j = \{p_{j+1}, p_{j+2}, p_{j+4})$ for every j, so the correspondence $(p_i, L_j) \mapsto (i, j)$ defines an isomorphism between the Desarguesian projective plane {points in $\mathbb{P}^2(\mathbb{F}_2)$, lines in $\mathbb{P}^2(\mathbb{F}_2)$, usual incidence} and the special projective plane $\{i \in \mathbb{F}_7, j \in \mathbb{F}_7, i - j \in \mathcal{D}\}$, where $\mathcal{D} = (\mathbb{F}_7^\times)^2 = \langle 2 \rangle = \{1, 2, 4\}$. The automorphism

$$B : (x : y : z) \mapsto (x : y + z : y)$$

of $\mathbb{P}^2(\mathbb{F}_2)$ fixes p_0 and L_0 and sends p_i to p_{2i} and L_j to L_{2j}, and the group of automorphisms generated by A and B, with the relations $A^7 = B^3 = 1$, $BAB^{-1} = A^2$, acts regularly on the flags of $\mathbb{P}^2(\mathbb{F}_2)$.

The case $n = 8$ is similar, but more complicated because now the group of automorphisms of $\mathbb{P}_2(\mathbb{F}_n)$ is not just $\mathbf{PGL}_3(\mathbb{F}_n)$ but the extension of this group by the group $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2)$ of order 3. We represent $\mathbb{F}_8$ as $\mathbb{F}_2[\alpha]$ where $\alpha^3 + \alpha + 1 = 0$. Then $\alpha^7 = 1$ and $\mathbb{F}_8^\times = \{1, \alpha, \ldots, \alpha^6\} = \{1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$. The automorphism

$$A : (x : y : z) \mapsto (\alpha^6 x + \alpha^2 z : \alpha^4 x + \alpha^6 y + \alpha^3 z : \alpha^3 y + z)$$

of $\mathbb{P}^2(\mathbb{F}_8)$ of order 73 acts simply transitively on lines and points, so every point is uniquely representable as $p_i = A^i(p_0)$ and every line uniquely representable as $L_j = A^j(L_0)$, where $p_0 = (1 : 0 : 0)$ as before and L_0 is the line $x + \alpha^5 y + \alpha z = 0$. The points of L_0 are p_i with $i \in \mathcal{D} = (\mathbb{F}_{73}^\times)^8 = \langle 2 \rangle = \{1, 2, 4, 8, 16, 32, 37, 55, 64\}$, so $L_j = \{p_i \mid i - j \in \mathcal{D}\}$ and just as before the correspondence $(p_i, L_j) \mapsto (i, j)$ defines an isomorphism between the Desarguesian projective plane $\mathbb{P}^2(\mathbb{F}_8)$ and the special projective plane $\Pi(\mathbb{F}_{73}, \mathcal{D})$. The only difference is that the group of automorphisms acting transitively on the flags of $\mathbb{P}^2(\mathbb{F}_8)$, generated by A and a second automorphism B of order 9 satisfying $BAB^{-1} = A^2$, can no longer be realized in $\mathbf{PGL}_3(\mathbb{F}_8)$ but only in the full group of automorphisms $\mathbf{P\Gamma L}_3(\mathbb{F}_8)$ of $\mathbb{P}^2(\mathbb{F}_8)$: the automorphism B of $\mathbb{P}^2(\mathbb{F}_8)$ of order 9 fixing p_0 and L_0 and sending p_i and L_j to p_{2i} and L_{2j} for every i and j is given by

$$B : (x : y : z) \mapsto (x' : \alpha^5 x' + y' + \alpha^6 z' : \alpha^6 x' + \alpha y'),$$

where $x \mapsto x'$ denotes the Galois automorphism of order 3 of $\mathbb{F}_8$ that sends α to α^2.

We can summarize the results of this section as follows. Call a finite projective plane *special* if it has the form $\Pi \cong \Pi(\mathbb{F}_p, (\mathbb{F}_p^\times)^n)$ for some special prime $p = n^2 + n + 1$. Then

(i) any flag-transitive finite projective plane is either Desarguesian or special;
(ii) exactly two finite projective planes, of order 2 and 8, are both Desarguesian and special.

Moreover, if there are any special projective planes other than the two in (ii), then they must have order $n > 1.44 \times 10^7$ ($p > 2 \times 10^{14}$) by the result of Feit quoted in the introduction, and from the computations on special primes described later in this paper we can strengthen this to $n > 2 \times 10^{11}$ ($p > 4 \times 10^{22}$). It is thus highly unlikely that any non-Desarguesian flag-transitive finite projective planes exist.

3. Special primes, Fermat surfaces and Gauss periods

We have seen that a non-Desarguesian finite flag-transitive projective plane of order n exists if and only if $p = n^2 + n + 1$ is a special prime, i.e., if and only if p is prime and every element of the finite field $\mathbb{F}_p$ is the difference of two elements of $\mathcal{D} = (\mathbb{F}_p^\times)^n$. In this section we give a number of elementary number-theoretical statements about n and p which are equivalent to this property. These involve the *Fermat surface*

$$\mathfrak{S} \;:\; X_0^n + X_1^n = X_2^n + X_3^n, \tag{3}$$

the *Fermat curves*

$$\mathcal{F}_\eta \;:\; X_0^n - X_1^n = \eta X_2^n \qquad (\eta \in \mathbb{F}_p^\times),$$

and the *Gaussian periods*

$$\omega = \sum_{a\in\mathcal{D}} \zeta^a = \frac{1}{n}\sum_{x\in\mathbb{F}_p^\times} \zeta^{x^n}, \qquad \Omega = \sum_{x\in\mathbb{F}_p} \zeta^{x^n} = 1 + n\omega,$$

where $\zeta = \zeta_p$ denotes a primitive pth root of unity. All of these are classical objects, much studied in number theory. In particular, the Gaussian periods, which are defined for any prime number p and divisor n of $p-1$ (and will be used in this generality in Section 4), generate the unique subfield of degree n of the cyclotomic field $\mathbb{Q}(\zeta)$ and were introduced for essentially this purpose by Gauss.

We will show: the prime $p = n^2 + n + 1$ is special if and only if the Fermat surface $\mathfrak{S}$ has no non-trivial $\mathbb{F}_p$-rational points (by *trivial points* of $\mathfrak{S}$ over $\mathbb{F}_p$ we mean points $(x_0, x_1, x_2, x_3) \in \mathfrak{S}(\mathbb{F}_p)$ with either $x_0x_1x_2x_3 = 0$ or $\{x_0^n, x_1^n\} = \{x_2^n, x_3^n\}$); if and only if the Fermat curves $\mathcal{F}_\eta$ all have the same number of $\mathbb{F}_p$-rational points; and if and only if the absolute value of the Gaussian period ω is the square root of a rational integer.

We denote by $X(\mathbb{F})$ the set of $\mathbb{F}$-rational points of any variety X defined over a finite field $\mathbb{F}$ and by $|X(\mathbb{F})|$ its cardinality.

Theorem 3.1. *Suppose that $p = n^2 + n + 1$ is prime. Then the following are equivalent:*

(a) *p is special;*
(b) *the map $\phi : \mathcal{D} \times \mathcal{D} \smallsetminus \text{(diagonal)} \to \mathbb{F}_p^\times$ sending (x, y) to $x - y$ is bijective;*
(c) *the surface $\mathfrak{S}$ has no non-trivial points over $\mathbb{F}_p$;*
(d) *$|\mathcal{F}_\eta(\mathbb{F}_p)| > 3n$ for every $\eta \in \mathbb{F}_p^\times$;*
(e) *$|\mathcal{F}_\eta(\mathbb{F}_p)| < 2n^2 + n$ for every $\eta \in \mathbb{F}_p^\times$;*
(f) *$|\mathcal{F}_\eta(\mathbb{F}_p)| = n^2 + n$ or $n^2 + 2n$ for every $\eta \in \mathbb{F}_p^\times$;*
(g) *$|\mathfrak{S}(\mathbb{F}_p)| < 2n^4 + 5n^3 + 4n$;*
(h) *$|\mathfrak{S}(\mathbb{F}_p)| = 2n^4 + n^3 + 4n^2 + 4n$;*
(i) *$|\omega|^2 \in \mathbb{Q}$;*
(j) *$|\omega| = \sqrt{n}$;*
(k) $\mathrm{tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(|\Omega|^4) = n^8 + n^7 - 2n^4 - 4n^3 - 5n^2 - 3n.$

Proof. The proofs of the equivalences of (a)–(f) are elementary. By definition, p is special if and only if the map ϕ in (b) is surjective. Since the domain and range of ϕ have the same cardinality, this is equivalent to ϕ being bijective or injective. The injectivity says that the equation $x_1^n - x_2^n = x_3^n - x_0^n$ is possible for $x_i \in \mathbb{F}_p^\times$ only if $x_1^n = x_2^n$ and $x_3^n = x_0^n$ or $x_1^n = x_3^n$ and $x_2^n = x_0^n$, so is equivalent to (c).

For $\eta \in \mathbb{F}_p$, let $t(\eta)$ denote the number of representations of η as the difference of two elements of $\mathcal{D}$. Then $t(0) = n+1$ and $\sum_{\eta\in\mathbb{F}_p} t(\eta) = |\mathcal{D}|^2 = (n+1)^2$, so that the average value of $t(\eta)$ with $\eta \in \mathbb{F}_p^\times$ is 1. This again gives the equivalence of (a)–(c), since (a) says that $t(\eta) \ge 1$ for every $\eta \in \mathbb{F}_p$, (b) that $t(\eta) = 1$ for every $\eta \in \mathbb{F}_p^\times$, and (c) that $t(\eta) \le 1$ for every $\eta \in \mathbb{F}_p^\times$. We now claim that

$$|\mathcal{F}_\eta(\mathbb{F}_p)| = n^2 t(\eta) + \begin{cases} n & \text{if } \eta \in \mathbb{F}_p^\times,\ \pm\eta \notin \mathcal{D}, \\ 2n & \text{if } \pm\eta \in \mathcal{D},\ -1 \notin \mathcal{D}, \\ 3n & \text{if } \eta \in \mathcal{D},\ -1 \in \mathcal{D}. \end{cases} \tag{4}$$

To see this, we observe first that the number of $\mathbb{F}_p$-rational points (x_0, x_1, x_2) on the curve $\mathcal{F}_\eta$ with $x_0x_1x_2 = 0$ equals n, $2n$ or $3n$ in the three cases given, while the number of points with $x_0x_1x_2 \neq 0$ is always divisible by n^2, because the group $(\mu_n^3)/\mu_n$ (where $\mu_n \subset \mathbb{F}_p^\times$ is the subgroup of nth roots of unity and the action is diagonal) acts freely on them. Moreover, the quotient of $\mathcal{F}_\eta(\mathbb{F}_p) \cap (\mathbb{F}_p^\times)^3/\mathbb{F}_p^\times$ by this action is just the set of points $(Y_0 : Y_1 : 1)$ with $Y_0, Y_1 \in \mathcal{D}$ and $Y_1 - Y_0 = \eta$, so its cardinality is $t(\eta)$. This proves (4) and hence the equivalence of (a)–(c) with (d)–(f), since we will see below that n must be odd if p is special, so that the third option in (4) cannot then occur.

To prove the other equivalences, we define a number $\delta(p)$, the *defect* of p, by

$$\delta(p) = \sum_{\eta\in\mathbb{F}_p^\times/\{\pm\mathcal{D}\}} \binom{t(\eta)}{2},$$

where $\pm\mathcal{D} = \mathcal{D} \cup -\mathcal{D} = \mu_{2n+2}$. Using the fact that the average value of $t(\eta)$ with $\eta \in \mathbb{F}_p^\times$ is 1 and that the value of $t(\eta)$ depends only on the class of η in the quotient group $\mathbb{F}_p^\times/(\pm\mathcal{D})$, we obtain the alternative formula

$$\delta(p) = \frac{1}{2}\biggl(\sum_{\eta\in\mathbb{F}_p^\times/\{\pm\mathcal{D}\}} t(\eta)^2 - \frac{n}{2}\biggr).$$

The Cauchy–Schwarz inequality and the fact that the average value of t is 1 then show that the defect is always non-negative and is zero if and only if p is special.

Now observe that $\sum_{\eta\in\mathbb{F}_p} t(\eta)^2$ is the number of 4-tuples (u, v, w, x) in $\mathcal{D}^4$ for which $u+v = w+x$, and by the formula just given this number is equal to $(n+1)(2n+1+4\delta(p))$. Since there are already $(n+1)(2n+1)$ trivial solutions, i.e., solutions with $\{u, v\} = \{w, x\}$, this shows again that p is special if and only if there are no non-trivial solutions, which is just (c), but it also shows that the number of rational points of $\mathfrak{S}$ is given by

$$|\mathfrak{S}| = (2n + 1 + 4\delta(p))n^3 + 4n^2 t(1) + 4n,$$

which equals $(2n+1)n^3 + 4n^2 + 4n$ if p is special (since then $\delta(p) = 0$ and $t(1) = 1$) and is $\geq (2n+5)n^3 + 4n$ if p is not special (since then $\delta(p) \geq 1$ and $t(1) \geq 0$). This proves the equivalence of (g) and (h) with (a).

Finally, the equivalence of (i) and (j) with (a) follows from the observation that $|\omega|^2 = \sum_{\eta\in\mathbb{F}_p} \zeta^{t(\eta)}$, which belongs to $\mathbb{Q}$ if and only if $t(\eta)$ is constant for $\eta \neq 0$ and is equal to n if $t(\eta)$ equals $n+1$ for $\eta = 0$ and 1 otherwise, while the equivalence of (k) with (a) follows from the calculation

$$\begin{aligned} 1 + (p-1)|\mathfrak{S}| &= |\{(x_0, x_1, x_2, x_3) \in \mathbb{F}_p^4 \mid x_0^n + x_1^n = x_2^n + x_3^n\}| \\ &= \frac{1}{p} \sum_{z^p=1} \Big| \sum_{a\in\mathbb{F}_p} z^{a^n} \Big|^4 = p^3 + \frac{1}{p} \operatorname{tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(|\Omega|^4). \end{aligned}$$

This completes the proof of the theorem. □

4. A generalization and a conjecture

The above considerations can be generalized in the following way. Let p be an arbitrary prime number. Then any subgroup of $\mathbb{F}_p^\times$ has the form

$$\mathcal{D}_n = \{x^n \mid x \in \mathbb{F}_p^\times\} = \{x \in \mathbb{F}_p^\times \mid x^k = 1\}$$

for some divisor n of $p-1$ and $k = (p-1)/n$. We define the Gaussian period ω_n as before by

$$\omega_n = \sum_{x\in\mathcal{D}_n} \zeta^x = \frac{1}{n} \sum_{a\in\mathbb{F}_p^\times} \zeta^{a^n} = \operatorname{tr}_{\mathbb{Q}(\zeta)/K_n}(\zeta),$$

where ζ is a primitive pth root of unity and K_n is the unique subfield of $\mathbb{Q}(\zeta)$ of degree n over $\mathbb{Q}$. We further define $t_n(\eta)$ for $\eta \in \mathbb{F}_p$ as the number of representations of η as the difference of two elements of $\mathcal{D}_n$, and call the pair (p, n) *special* if this number is independent of η for $\eta \neq 0$. Since $\sum_{\eta\neq 0} t_n(\eta) = |\mathcal{D}_n|^2 - |\mathcal{D}_n| = k^2 - k$, this common value must then be equal to $(k-1)/n$, which must therefore be an integer. In particular, except in the trivial case when $k = 1$ and $n = p-1$, we always have $k \geq n+1$ and $p \geq n^2 + n + 1$, so that the case of special primes ($k = n+1$, $t_n(\eta) = 1$) is extremal. Using the same arguments as before, we can prove:

Theorem 4.1. *Let $p = nk + 1$ be prime. Then the following are equivalent:*

(a) *the pair (p, n) is special;*
(b) *$t_n(\eta) = (k-1)/n$ for all $\eta \neq 0$;*
(c) *the surface* (3) *in $\mathbb{P}^3$ has precisely $n^3 k + n^2(k-1)^2 + 4nk$ $\mathbb{F}_p$-rational points;*
(d) *$|\omega_n|^2$ is a rational number;*
(e) *$|\omega_n|^2 = k - (k-1)/n$.*

The analogue of the construction given in §2 is now the following. Suppose (p,n) is special, $k=(p-1)/n$. Define a point-line incidence structure Γ as follows: the points of Γ are the elements of $\mathbb{F}_p$; the lines or *blocks* of Γ also consist of the elements of $\mathbb{F}_p$; and a point $\alpha\in\mathbb{F}_p$ is incident with a block $\beta\in\mathbb{F}_p$ if and only if $\alpha-\beta\in\mathcal{D}_n$. Thus there are p points and p blocks, each point is incident with k blocks and each block is incident with k points, any two distinct points are contained in exactly $(k-1)/n$ distinct blocks, and any two distinct blocks intersect in exactly $(k-1)/n$ distinct points. Hence Γ is a 2-$(p,k,(k-1)/n)$ *symmetric block design*. It is clear that for $a\in\mathcal{D}_n$ and $b\in\mathbb{F}_p$ the map $x\mapsto ax+b$ from $\mathbb{F}_p$ to itself defines an automorphism of Γ in a natural way and that the group of these automorphisms acts regularly on the flags (= incident point-block pairs) of Γ. To the knowledge of the authors, the only known examples of such designs other than finite projective spaces (of dimension at least 3) follow from [2, 11, 13]. These constructions are essentially covered by Theorem 4.2 (and Theorem 5.1) below, where among other results the existence results of [2, 11, 13] are re-proved in an alternative fashion.

In view of these observations, and of the known difficulty of producing examples of symmetric designs admitting a flag-regular automorphism group, it is of interest to find examples of special pairs (p,n). These are provided by the following theorem, whose proof will be given together with that of Theorem 5.1 below.

Theorem 4.2. *Let p be a prime and $n\,|\,(p-1)$. Then (p,n) is special in each of the following five cases:*

(a) $n=1$, *p arbitrary,* $|\omega_n|^2=1$,
(b) $n=2$, $p\equiv 3 \pmod 4$, $|\omega_n|^2=(p+1)/4$,
(c) $n=4$, $p=4b^2+1$ *with b odd,* $|\omega_n|^2=(3p+1)/16$,
(d) $n=8$, $p=64b^2+9=8d^2+1$ *with b and d integral,* $|\omega_n|^2=(7p+1)/64$,
(e) $n=p-1$, *p arbitrary,* $|\omega_n|^2=1$,

the corresponding values of ω_n being given by

(a) $\omega_1=-1$,
(b) $\omega_2=\dfrac{-1+i\sqrt{p}}{2}$,
(c) $\omega_4=\dfrac{\sqrt{p}-1}{4}\pm i\sqrt{\dfrac{p+\sqrt{p}}{8}}$,
(d) $\omega_8=\dfrac{\sqrt{p}-1}{8}+\sqrt{\dfrac{p+3\sqrt{p}}{32}}+i\sqrt{\dfrac{\sqrt{p}-1}{16}}\sqrt{\sqrt{p}-\sqrt{\dfrac{p+3\sqrt{p}}{2}}}$,
(e) $\omega_{p-1}=\zeta$.

Cases (a) and (e) of this theorem are trivial and do not lead to interesting designs, but the families (b), (c) and (d) give us three infinite or potentially infinite classes of interesting flag-regular symmetric designs. Note that the family (c) is quite sparse: the only primes up to 40000 belonging to this class are 5, 37, 101, 197, 677, 2917, 4357, 5477, 8101, 8837, 12101, 15877, 16901, 17957, 21317, 22501, and 28901. The family (d), corresponding to the prime solutions of a Pell's equation, is even thinner, though conjecturally still infinite:

the first prime of this form is our old acquaintance $p = 73$, with $b = 1$ and $d = 3$; the next two are 104411704393 ($b = 40391$, $d = 114243$) and 160459573394847767113 ($b = 1583407981$, $d = 4478554083$), with 12 and 21 digits, respectively, and the next four have 103, 119, 425, and 615 decimal digits, respectively.

The conjecture about the non-existence of non-Desarguesian flag-transitive projective planes can now be generalized to the following:

Conjecture 4.3. *The only special pairs are the ones listed in Theorem* 4.2.

We have checked this conjecture by computer for all primes $p < 10\,000\,000$ and all divisors n of $p - 1$. (For the special case when $p = n^2 + n + 1$, as already mentioned, W. Feit's result verifies it for all $p < 2 \times 10^{14}$ and we have extended this to $p < 4 \times 10^{22}$.) These numerical computations are described in an appendix. Apart from this, we have only the partial results and evidence presented in the next section.

5. Special primes, Gauss sums and Jacobi sums

In this section we prove Theorem 4.2 and a partial converse.

Theorem 5.1. *Assume that* $p = kn + 1$ *is prime and that* (p, n) *is special.*

(a) *If* $n > 1$, *then* n *is even and* k *is odd.*
(b) *If* $n < 10$, *then* (p, n) *belongs to one of the families of Theorem* 4.2.

Proof. Let $\zeta = \zeta_p$, K_n and ω_n be defined as at the beginning of the previous section. Then $\omega_n \in K_n$, and it is well known that ω_n generates K_n over $\mathbb{Q}$. If k is even, then -1 belongs to $\mathcal{D}$, so ω_n is a real number. But then $\omega_n^2 = |\omega_n|^2 \in \mathbb{Q}$, so $n = [\mathbb{Q}(\omega_n) : \mathbb{Q}] \leq 2$. Therefore k must be odd if $n > 2$, in which case n is even since $nk = p - 1$ is even, and k is also odd when $n = 2$ since $k \equiv 1 \pmod{n}$ for special (p, n). This proves (a).

To prove (b), we have to look at each value $n \leq 9$ separately. The case $n = 1$ is of course trivial, since $\mathcal{D}_1 = \mathbb{F}_p^\times$, $\omega_1 = -1$, so by virtue of part (a) we need only analyze the cases $n = 2$, 4, 6, and 8. This will at the same time provide the proof of Theorem 4.2, since $n \leq 8$ in all cases of that theorem except for the case $n = p - 1$, which is trivial.

All the proofs will involve Gauss sums, so we begin by recalling the main properties of these. Suppose $p = nk+1$ with n even and k odd (since by part (a) this is the only case that can occur for (p, n) special) and let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character of order n, which we fix by sending some chosen generator of the cyclic group $\mathbb{F}_p^\times$ to a chosen primitive nth root of unity λ_n. To each $r \in \mathbb{Z}/n\mathbb{Z}$ we associate the *Gauss sum*

$$G_r = G(\chi^r) = \sum_{x \in \mathbb{F}_p^\times} \chi(x)^r \zeta^x \qquad (r \in \mathbb{Z}/n\mathbb{Z}).$$

For $r = 0$ this equals -1, but according to Gauss for other values of r we have $|G_r| = \sqrt{p}$ and $G_{-r} = (-1)^r \overline{G_r}$ (the latter because $\chi(-1) = -1$ since k is odd). In particular, $G_{n/2}^2 = (-1)^{n/2} p$ (and in fact $G_{n/2} = +\sqrt{p}$ for $n/2$ even and $G_{n/2} = +i\sqrt{p}$ for $n/2$

odd, as Gauss showed). The key property of the Gauss sums comes from the classical calculation

$$G_r G_s = \sum_{x,y\in\mathbb{F}_p^\times} \chi(x)^r \chi(y)^s \zeta^{x+y} = \sum_{z\in\mathbb{F}_p^\times,\, z\neq -1} \chi(z)^s \sum_{x\in\mathbb{F}_p^\times} \chi(x)^{r+s} \zeta^{x(z+1)}$$

if r, s and $r+s$ are $\not\equiv 0 \pmod{n}$ (set $y = zx$ and observe that the sum of the terms with $z = -1$ vanishes); now substituting $x = x'(z+1)^{-1}$ we find that $G_r G_s = G_{r+s} J_{r,s}$ where the *Jacobi sum* $J_{r,s} = \sum_{z\in\mathbb{F}_p^\times\smallsetminus\{-1\}} \chi(z)^s \bar{\chi}(z)^{r+s}$ is an element of the ring $\mathbb{Z}[\lambda_n]$ of absolute value $\sqrt{p}$. On the other hand, the Gaussian period and Gauss sums are related by

$$\omega_n = \frac{1}{n} \sum_{r \pmod{n}} G_r,$$

because $\sum_{r \pmod{n}} \chi(x)^r$ equals 0 if $x \notin \mathcal{D}_n$ and n if $x \in \mathcal{D}_n$. These two facts together combine to give sufficiently strong information about ω_n to contradict the hypothesis $|\omega_n|^2 \in \mathbb{Q}$ in many cases. We now look at each case separately.

- $n = 2$. Here $G_1 = i\sqrt{p}$, so $\omega_2 = \frac{1}{2}(-1 + i\sqrt{p})$ and $|\omega_2|^2 = (p+1)/4 \in \mathbb{Z}$ for any $p \equiv 3 \pmod{4}$, proving part (b) of the theorem (as well as part (b) of Theorem 4.2) in this case, since we already know that $(p, 2)$ can only be special for k odd. We could also use Gauss sums to show this latter fact without using part (a), since if $p \equiv 1 \pmod{4}$ we have $\omega_2 = \frac{1}{2}(-1 + \sqrt{p})$ and hence $|\omega_2|^2 = \frac{1}{4}(p + 1 - 2\sqrt{p}) \notin \mathbb{Z}$.

- $n = 4$. Here $G_0 = -1$, $G_2 = \sqrt{p}$, $G_3 = -\overline{G}_1$ and $G_1^2/G_2 = J_{1,1} \in \mathbb{Z}[i]$, where $J_{1,1} = A + Bi$ with $A^2 + B^2 = p$ and $A \equiv 3 \pmod{4}$ and B even. Hence

$$\omega_4 = \frac{-1 + G_1 + G_2 + G_3}{4} = \frac{\sqrt{p} - 1}{4} \pm i\sqrt{\frac{p - A\sqrt{p}}{8}},$$

so $16|\omega_4|^2 = 3p + 1 - 2(A+1)\sqrt{p}$. Clearly this is a rational number if and only if $A = -1$, i.e., if and only if $p = B^2 + 1$, corresponding to case (c) of Theorem 4.2.

- $n = 6$. This time the relationship with the Jacobi sums gives

$$G_1 = ip^{1/6}\alpha^2, \quad G_2 = p^{1/3}\alpha\bar{\rho}, \quad G_3 = ip^{1/2}, \quad G_4 = p^{1/3}\bar{\alpha}\rho, \quad G_5 = ip^{1/6}\bar{\alpha}^2,$$

where $\alpha^3 = \frac{1}{2}(M + N\sqrt{-3})$ is an element of $\mathbb{Z}[\lambda_3]$ of norm p and ρ is a cube root of unity. (In fact one has $M \equiv 1 \pmod{3}$ and $N \equiv 0 \pmod{3}$, and z is equal to 1 if $M \equiv N \equiv 0 \pmod{2}$ and to $(-1 \mp i\sqrt{3})/2$ if $MN \equiv \pm 1 \pmod{4}$, with the former case occurring if and only if 2 is congruent to a cube modulo p, but we do not need to know any of this.) Hence

$$6\Re(\omega_6) = -1 + 2p^{1/3}\Re(\alpha\bar{\rho}), \qquad 6\Im(\omega_6) = \sqrt{p} + 2p^{1/6}\Re(\alpha^2).$$

Write $2p^{1/3}\alpha\bar{\rho} = \gamma + i\delta$ with γ and δ real. Then γ is one of the three roots (all of which are real) of the cubic equation $\gamma^3 - 3p\gamma - pM = 0$, and $\delta = \sqrt{4p - \gamma^2}$. Hence

$$6\Re(\omega_6) = \gamma - 1, \qquad 6\Im(\omega_6) = \frac{\gamma^2 - p}{\sqrt{p}} \quad \text{or} \quad \frac{4p - \gamma^2 \pm \gamma\sqrt{12p - 3\gamma^2}}{2\sqrt{p}},$$

depending on whether ρ equals 1 or not. Using the equation $\gamma^3 - 3p\gamma - pM = 0$, we find

$$36|\omega_6|^2 = 2\gamma^2 + (M-2)\gamma + p + 1 \quad \text{or} \quad \frac{\gamma^2 - (M+4)\gamma + 8p + 2 \pm (\gamma - M)\sqrt{12p - 3\gamma^2}}{2}.$$

The first of these two expressions cannot be rational since then γ would satisfy a quadratic as well as a cubic equation and hence would belong to $\mathbb{Q}$, contradicting the fact that ω_6 has degree 6 over $\mathbb{Q}$. Hence the second equation must hold if $(p, 6)$ is special, and since we know from Theorem 4.1(e) that $36|\omega_6|^2 = 5p + 1$ in this case, we find

$$\begin{aligned}(p, 6) \text{ is special } &\Rightarrow \ (\gamma^2 - (M+4)\gamma - 2p)^2 = (\gamma - M)^2(12p - 3\gamma^2)\\ &\Rightarrow \ (M^2 + 2M + 4 - p)\gamma^2 + 2p(M-1)\gamma + p(p - 5M^2 - 2M) = 0,\end{aligned}$$

where in the last line we have again used the equation of γ. Since γ has degree 3 over $\mathbb{Q}$, this can only happen if $M = 1$ and $p = M^2 + 2M + 4 = 5M^2 + 2M = 7$.

• $n = 8$. The analysis in this case is more complicated and we will be even sketchier than before. As in the case $n = 4$ we find $G_4 = \sqrt{p}$, $G_6 = \overline{G}_2$ and $G_2^2/G_4 = A + Bi$ with $A^2 + B^2 = p$, now with $A \equiv 3 \pmod 8$ and $B \equiv 0 \pmod 4$, so

$$\Re(\omega_8) = \frac{\sqrt{p} - 1 + 2\gamma}{8}, \qquad \gamma := \Re(G_2) = \pm\sqrt{\frac{p + A\sqrt{p}}{2}}.$$

The odd-index Gauss sums are given by $G_1 = \sigma\tau$, $G_3 = -\varepsilon\overline{\sigma}\tau$, $G_5 = \varepsilon\sigma\overline{\tau}$ and $G_7 = -\overline{\sigma\tau}$, where $\varepsilon = (-1)^{B/4}$, $\sigma^2 = G_2$, and $\tau^2 = C + D\sqrt{-2}$ with $D \equiv C - 5 \equiv \varepsilon + 1 \pmod 8$, so

$$2\Im(\omega_8) = \frac{(\sigma - \varepsilon\overline{\sigma})(\tau + \varepsilon\overline{\tau})}{4i} = \Im(\sigma)\Re(\tau) \quad \text{or} \quad \Re(\sigma)\Im(\tau),$$

depending on whether $\varepsilon = 1$ or -1. This gives

$$16\Im(\omega_8)^2 = (\sqrt{p} - \varepsilon\gamma)(\sqrt{p} + \varepsilon C),$$

and combining this with the formula just given for $\Re(\omega_8)$ we obtain

$$64|\omega_8|^2 = 7p + 1 + 2(A - 1 + 2\varepsilon C)\sqrt{p} - 4(C+1)\gamma + 4(1-\varepsilon)\gamma\sqrt{p}.$$

This is rational if and only if the coefficients of $\sqrt{p}$, γ and $\gamma\sqrt{p}$ all vanish, i.e., if $\varepsilon = 1$, $C = -1$ and $A = 1 - 2\varepsilon C = 3$, and this corresponds (with $B = 8b$, $D = 2d$) exactly to the conditions $p = 64b^2 + 9$ and $p = 8d^2 + 1$ given in part (d) of Theorem 4.2. □

As the proof makes clear, the analysis of the Gaussian periods becomes more and more difficult as n increases, and we cannot hope to progress much further by these methods (though a few more cases might still be tractable). On the other hand, the proof also makes it clear that the conditions on the Gauss sums and Jacobi sums imposed by the assumption that $|\omega_n|^2$ is rational become more and more restrictive as n increases, with the condition in the case $n = 8$ already strong enough to lead to a doubly exponentially thin set of solutions, so that the conjecture that there are no other solutions than the ones we have already found is at least quite plausible.

6. Flag-regular symmetric designs with k dividing $v - 1$

In the examples of flag-regular symmetric 2-designs that we constructed via special pairs, the parameter k divided the number of points minus one. The following theorem describes how, conversely, this (rather strong) algebraic assumption affects the design.

Theorem 6.1. *Let Γ be a symmetric 2-(v, k, λ) design admitting a flag-regular automorphism group G. Suppose that k divides $v - 1$. Then*

(a) *$v = p^h$ for some prime p and natural number h, and we can identify the point set P of Γ with the points of the h-dimensional vector space $\mathbb{F}_p^h$ over $\mathbb{F}_p$;*

(b) *$G \cong \mathbb{F}_p^h \rtimes H$ where H is a subgroup of $\mathbf{GL}_h(\mathbb{F}_p)$ that is isomorphic to G_x for any point x of Γ.*

Proof. Since Γ is a symmetric design, we have (see e.g. [1])

$$\lambda(v - 1) = k(k - 1).$$

Together with the assumption that k divides $v - 1$, this implies that λ divides $k - 1$, so that $(\lambda, k) = 1$. But the number of blocks of Γ incident with a point equals k. By 8(b) of [3, p. 80], it follows that G acts as a Frobenius group on the points (and blocks) of Γ. So the Frobenius kernel F acts regularly on the points. Also, by 7(a) of [3, p. 79], G acts primitively on the points of Γ. As the Frobenius kernel F is nilpotent, it is the direct product of its Sylow subgroups, say

$$F = S_{p_1} \times \cdots \times S_{p_j},$$

where $\{p_1, \ldots, p_j\}$ is the set of distinct primes dividing F. Let Z be the center of F (which is non-trivial). As $F \trianglelefteq G$, G acts on the Z-orbits of points, contradicting the point-primitivity of G unless $Z = F$. Since each S_{p_i} is a characteristic subgroup of F, in the same way we find that $j = 1$. So F is an abelian p-group ($p = p_1$). Now let A be the unique maximal elementary abelian p-subgroup of F. Then A is a characteristic subgroup of F, so if $A \neq F$ the A-orbits of points of Γ are non-trivial blocks of imprimitivity, again a contradiction. Hence F is elementary abelian. Put $|F| = p^h$. As F acts regularly on the points of Γ, we can identify both F and the point set of Γ with the additive group $\mathbb{F}_p^h$, acting on itself by translation. This proves part (a). Since $F \trianglelefteq G$, we also see that for any point x of Γ, G_x acts as an automorphism group on F by conjugation. As F acts regularly on the points of Γ, G_x acts faithfully on F, so is isomorphic to a subgroup of $\mathbf{GL}_h(\mathbb{F}_p)$. Part (b) follows. □

Remark 6.2. Note that for symmetric designs, points and blocks play interchangeable roles, so we could equally well formulate Theorem 6.1 with points replaced by blocks.

In the case when v is prime the analysis is easier and leads to the same conclusion as in the special case $\lambda = 1$, namely, that the only flag-regular 2-designs with $k \mid (v - 1)$ are the ones constructed in Section 4. In fact, we need only the assumption $k < v$.

Theorem 6.3. *Let Γ be a symmetric 2-(p, k, λ) design admitting a flag-regular automorphism group G, with p prime and $k < p$. Then $k = (p-1)/n$, $\lambda = (k-1)/n$ where (p, n) is a special pair and Γ is isomorphic to the design constructed in Section* 4.

Proof. The argument is essentially the same as in the proof of Proposition 2.1. If H and K are the stabilizers of p_0 and L_0 for some flag (p_0, L_0) of Γ, then it follows just as before that $H \cap K = \{e\}$ and that both the map (2) and the corresponding map with H and K interchanged are exactly $\lambda : 1$, i.e., every element $g \in G \setminus H$ has precisely λ representations as hkh' with $h, h' \in H$ and $e \neq k \in K$ (and similarly with H and K interchanged). Since $|G| = kp$ and $k < p$, the Sylow theorems again imply that the p-Sylow subgroup F of G has order p and is normal, so that we can again identify G/H and G/K with $F \cong \mathbb{F}_p$, and H and K with the unique subgroup of $\mathbb{F}_p^\times$ of order k, which is then $\mathcal{D}_n = (\mathbb{F}_p^\times)^n$ with $n = (p-1)/k$. Everything else goes through exactly as before: we again have compatible isomorphisms $G \cong \left(\begin{smallmatrix} \mathcal{D}_n & \mathbb{F}_p \\ 0 & 1 \end{smallmatrix}\right)$, $F \cong \left(\begin{smallmatrix} 1 & \mathbb{F}_p \\ 0 & 1 \end{smallmatrix}\right)$, $H \cong \left(\begin{smallmatrix} \mathcal{D}_n & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $K = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) H \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and the fact that the map (2) is $\lambda : 1$ translates directly into the property that every element of $\mathbb{F}_p^\times$ can be written in exactly λ ways as a difference of two elements of $\mathcal{D}_n$, i.e., (p, n) is a special pair. □

Appendix. Numerical computations

In the text we mentioned several numerical results, specifically, that there are no special primes less than 2×10^{22} and no special pairs (p, n) with $p < 10^7$. We indicate briefly how these calculations were carried out.

We start with the discussion of special pairs. If (p, n) is special, then p has the form $tn^2 + n + 1$ for some $t \geq 1$. By Dirichlet's theorem the number of primes $p < X$ satisfying $p \equiv n + 1 \pmod{n^2}$ with n fixed is asymptotically $\varphi(n^2)^{-1} X/\log X$ for X large, so the total number of pairs (p, n) with $p < X$ of the form $tn^2 + n + 1$ is roughly $CX/\log X$ with $C = \sum_{n=1}^{\infty} \varphi(n^2)^{-1} = 2.203856596437859\ldots$. If we use the results of Section 5, then we can assume that n is even and larger than 8, which reduces the number of pairs to be tested to $C' X/\log X$ with

$$C' = \sum_{2|n,\, n>8} \frac{1}{\varphi(n^2)} = \frac{2C}{5} - \frac{1}{2} - \frac{1}{8} - \frac{1}{12} - \frac{1}{32} = 0.14195282662358\ldots,$$

a saving of a factor of about 16. We initially tested all pairs with $p < 10^5$, finding only solutions with $n = 2, 4, 6$ or 8. This led to the statements of Theorems 4.2 and 5.1. Once they were proved, the tests in larger ranges were carried out only for even $n \geq 10$.

Two methods were used to test whether a given pair (p, n), where $p = tn^2 + n + 1$ is prime, is special. The first uses part (e) of Theorem 4.1, i.e., the equality $|\omega_n|^2 = k - t$, where $k = (p-1)/n = tn + 1$ as usual. To compute ω_n, we choose a primitive root g modulo p and set $G = g^n$. Then G generates the group $\mathcal{D}_n$ and $\omega_n = \sum_{j \pmod{k}} \zeta^{G^j}$, where $\zeta = e^{2\pi i/p}$. The corresponding program in GP/PARI is very short:

```
{try(p,n)=z=exp(2*Pi*I/p); G=znprimroot(p)^n;
om=sum(j=1,p\n,z^lift(G^j)); kk=norml2(om);
if(abs(n*kk-p+p\n)<.1,print(p," ",n," ",kk))}
```

and is quite efficient for small p (for instance, the time to check the 5101 pairs (p, n) with $p < 10^5$ and $n > 3$ on a SUN Sparc workstation was 34 minutes, and under 4 minutes if one considered only the 1352 pairs with n even and > 8), but grows quadratically with the size of the bound X.

The second method, which is somewhat faster, is based on part (b) of Theorem 4.1, i.e., on checking that the number $t_n(\eta)$ of representations of $\eta \in \mathbb{F}_p^\times$ as a difference of two elements of $\mathcal{D}_n$ is always equal to t. We can compute $t_n(\eta)$ as the number of $j \pmod{k}$ for which $(G^j + \eta)^k$ equals 1 (mod p), where $G = g^n$ as before. This is done in PARI-GP by the program

```
t(p,n,eta) = k=p\n; G=znprimroot(p)^n;
sum(j=1,k,(g^j+r)^k==1)
```

(A slightly different approach, of comparable speed for a single value of η but more efficient if one is going to compute $t_n(\eta)$ for several η's for the same n and p, is to precompute the subset $\mathcal{D}_n \subset \mathbb{Z}/p\mathbb{Z}$ by sorting the set $\{G^j\}_{j \,(\mathrm{mod}\, k)}$ and then to count the number of $m \in \mathcal{D}_n$ with $m + \eta \in \mathcal{D}_n$. The sorting algorithm is included in PARI and similar languages.) Checking the equality $t_n(\eta) = t$ for all $\eta \in \mathbb{F}_p^\times$ would be very time-consuming, but we can of course abort the test as soon as it has failed for a single value of η, and this leads to a considerable speeding-up. For instance, the prime $p = 1021$ has the form $tn^2 + n + 1$ for $n = 3, t = 113$ and for $n = 12, t = 7$, and since $t_3(1) = 111$ and $t_{12}(1) = 6$ both pairs can immediately be eliminated. Of the 6702 pairs (p, n) of the form $p = tn^2 + n + 1$ with $p < 10^5$ and $2 < n < p - 1$, only 147 pass the first test $t_n(1) = t$ and only 27 satisfy $t_n(\eta) = t$ for $1 \le \eta \le 6$, and all but three of these are in fact special pairs, the exceptions being $(p, n, t) = (601, 24, 1)$, $(6079, 3, 675)$ and $(54679, 3, 6075)$. It is interesting to note that in each of these three cases, the non-zero values of $t_n(\eta) - t$ (for all η in the first two cases and for at least the first few thousand η in the third) are all the same up to sign, assuming only the values ±1, ±15 and ±45, respectively. Moreover, the set of η's for which $t_n(\eta) \ne t$ also seems not to be random (e.g., in the three cases mentioned one has $t_n(\eta) = t$ not only for $\eta \le 6$, but for all $\eta \le 20$ except 7, 11, 13, 14, 17 and 19). These observations suggest that the distribution of the cardinalities of the Fermat curves $\mathcal{F}_\eta$ may have some possibly interesting additional structure.

The total computational time with the second method for $p < 10^5$ was about 16 minutes if we looked at all pairs with $2 < n < p - 1$, and about 1 minute if we restricted to even $n > 8$, as opposed to 34 minutes and 4 minutes with the first method.

A further speeding up is obtained by noting that the number $t = (p - n - 1)/n^2$ must have a specific parity in order for the pair (p, n) to be special. Indeed, the number $t_n(1)$ is the cardinality of the set of $x \in \mathcal{D}_n$ for which $x + 1$ also belongs to $\mathcal{D}_n$, and this set has an involution $x \mapsto x^{-1}$ which is fixed-point free if $2 \notin \mathcal{D}_n$ and has exactly one fixed point if $2 \in \mathcal{D}_n$. Hence, unless 2 belongs to $\mathcal{D}_n$ (which happens only rarely, with frequency $1/n$), the number $t_n(1)$ is even and hence t must also be even if (p, n) is special, and similarly t must be odd in the remaining cases when $2 \in \mathcal{D}_n$. This eliminates about half of the possible pairs (p, n) right away and hence speeds up the calculations roughly by a factor of 2.

In the range $10^5 < p < 10^7$ we used only the second method and considered only pairs with even $n \geq 10$ that passed the parity test. The running times were 20 minutes up to 10^6 and 25 hours up to 10^7. Of the 92782 pairs (p, n) with $10^5 < p < 10^7$, $8 < n < p-1$ and n even, only 913 passed the first test $t_n(1) = t$ and only two satisfied $t_n(\eta) = t$ for $1 \leq \eta \leq 6$, namely $(226129, 336)$ and (3041407,18), with $t = 2$ and $t = 9387$, respectively, and in both cases the test failed for $\eta = 7$, so that these pairs are also not special. (The above-noted constancy of $t_n(\eta) - t$ did not occur here.) This verifies Conjecture 4.3 for all (p, n) with $p < 10^7$.

We now turn to special primes. Here we could of course use the same methods, with $t = 1$, but now there is a much faster way. By the parity observation above, a prime $p = n^2 + n + 1$ can only be special if $2 \in \mathcal{D}_n$, i.e., if $2^{n+1} \equiv 1 \pmod{p}$. (This is a special case of the fact mentioned in Section 1 that $d \in \mathcal{D}_n$ for every divisor d of n.) This can be tested extremely rapidly—so rapidly, indeed, that it is not even worth testing first whether p is prime, since this actually takes longer. (Even the weaker pseudoprimality tests for a large number p involve calculating a^{p-1} or $a^{(p-1)/2}$ for several values of a, and here we need only a single such calculation and with a smaller exponent.) We can speed up the search even more by restricting n to certain congruence classes, as indicated below, but since it is so rapid to search for solutions of $2^{n+1} \equiv 1 \pmod{n^2 + n + 1}$ we first did this for all (even) n up to 5×10^9 (this took about four hours), finding only the following seven solutions in this range:

n	2	8	24	90	512	134217728	297474474
p	7	73	601	8191	262657	18014398643699713	88491062979051151

The third, fourth and fifth of these can be checked directly not to be special. The sixth can be eliminated because p is not prime (it factors as $2593 \times 71119 \times 97685839$) and the seventh because it fails to satisfy the congruence $n \equiv 8 \pmod{24}$, which is a necessary condition for (n, p) to be special. (The divisibility of n by 8 was proved by Feit in the previously cited paper [4], and we must have $n \equiv 2 \pmod{3}$ because both n^3 and n^{n+1} are congruent to 1 modulo p.) Hence in this range only the values $n = 2$ and $n = 8$ give special primes. Continuing the search up to 2×10^{11}, now with n restricted to the congruence class 8 (mod 24), led to no further solutions (computation time roughly 3 days), verifying the non-existence of non-Desarguesian flag-transitive projective planes for $n < 2 \times 10^{11}$, or $p < 4 \times 10^{22}$.

Acknowledgments. The first author is a Postdoctoral Fellow of the Fund for Scientific Research — Flanders (Belgium).

References

[1] Beth, T., Jungnickel, D., Lenz, H.: Design Theory, Vol. I. 2nd ed., Encyclopedia Math. Appl. 69, Cambridge Univ. Press, Cambridge (1999) Zbl 0945.05004 MR 1729456

[2] Chowla, S. A.: A property of biquadratic residues. Proc. Nat. Acad. Sci. India Sect. A **14**, 45–46 (1944) Zbl 0063.00871 MR 0014119

[3] Dembowski, P.: Finite Geometries. Ergeb. Math. Grenzgeb. 44, Springer, New York (1968) Zbl 0159.50001 MR 0233275

[4] Feit, W.: Finite projective planes and a question about primes. Proc. Amer. Math. Soc. **108**, 561–564 (1990) Zbl 0737.05022 MR 1002157

[5] Fink, J. B.: A note on sharply flag-transitive projective planes. In: N. L. Johnson, M. J. Kallaher and C. T. Long (eds.), Finite Geometries, in honor of T. G. Ostrom (Pullman, WA, 1981), Lecture Notes in Pure Appl. Math. 82, Dekker, New York, 161–164 (1983) Zbl 0532.51011 MR 0690803

[6] Fink, J. B.: Flag-transitive projective planes. Geom. Dedicata **17**, 219–226 (1985) Zbl 0569.51006 MR 0779176

[7] Gordon, B., Mills, W. H., Welch, L. R.: Some new difference sets. Canad. J. Math. **14**, 614–625 (1962) Zbl 0111.24201 MR 0146135

[8] Higman, D. G., McLaughlin, J. E.: Geometric ABA-groups. Illinois J. Math. **5**, 382–397 (1961) Zbl 0104.14702 MR 0131216

[9] Hughes, D. R., Piper, F. C.: Projective Planes. Springer, New York (1973) Zbl 0267.50018 MR 0333959

[10] Kantor, W. M.: Primitive groups of odd degree and an application to finite projective planes. J. Algebra **106**, 15–45 (1987) Zbl 0606.20003 MR 0878466

[11] Lehmer, E.: On residue difference sets. Canad. J. Math. **5**, 425–432 (1953) Zbl 0052.03904 MR 0056007

[12] Ott, U.: Flag-transitive projective planes and power residue difference sets. J. Algebra **276**, 663–673 (2004) Zbl 1049.05013 MR 2058461

[13] Paley, R. E. A. C.: On orthogonal matrices. J. Math. Phys. **12**, 311–320 (1933) Zbl 0007.10004

[14] Thas, K.: Finite flag-transitive projective planes: a survey and some remarks. Discrete Math. **266**, 417–429 (2003) Zbl 1026.51005 MR 1991732

[15] Yuan, P., Yahui, H.: A note on power residue difference sets. J. Algebra **291**, 269–273 (2005) Zbl 1074.05019 MR 2158523