PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 2, February 1990

FINITE PROJECTIVE PLANES AND A QUESTION ABOUT PRIMES

WALTER FEIT

(Communicated by Andrew Odlyzko)

ABSTRACT. Let n be an even integer not divisible by 3. Suppose that $p = n^2+n+1$ is a prime and $2^{n+1} \equiv 1 \pmod{p}$. The question is asked whether this can only occur if n is a power of 2. It is noted that an affirmative answer to this question implies that a finite projective plane with a flag transitive collineation group is Desarguesian.

1. INTRODUCTION

Let n be an even natural number such that $p = n^2 + n + 1$ is a prime. The following additional hypotheses about n will be considered.

H1. $d^{n+1} \equiv 1 \pmod{p}$ *for every divisor* d *of* n.

H2. $n + 1 \equiv 0 \pmod{3}$ *and* $2^{n+1} \equiv 1 \pmod{p}$.

H3. $n \equiv 0 \pmod{8}$ *and* (H2) *is satisfied.*

If (H1) is satisfied then $n^{n+1} \equiv 1 \pmod{p}$. Thus $3 \mid (n + 1)$ since n has order 3 modulo p and so (H2) is satisfied.

If k is a natural number not divisible by 3 then a primitive cube root of unity is a root of $x^{2k} + x^k + 1$, thus $(x^2 + x + 1) \mid (x^{2k} + x^k + 1)$. Hence if $q = m^{2k} + m^k + 1$ is a prime for some integer $m > 1$ then k is a power of 3. In particular, if $m \neq 3$ is a prime then $m^{3k} \equiv 1 \pmod{q}$ and the order of m modulo q is a power of 3 and so is relatively prime to m. Hence $m^{m^k+1} \equiv 1 \pmod{q}$. Thus if $m = 2$ and $n = m^k$ then (H1) is satisfied. It is not known whether there are infinitely many primes of this form. Section 3 contains some numerical results in this connection. The following questions for $I = 1, 2, 3$ are related to the converse of this statement.

Question I. *If* (HI) *is satisfied is* n *necessarily a power of* 2?

If Question 2 has an affirmative answer then so do Questions 1 and 3. If Question 2 or 3 is to have an affirmative answer then the condition $n + 1 \equiv 0 \pmod{3}$ (which is equivalent to the condition $n \not\equiv 0 \pmod{3}$) is essential.

Received by the editors June 28, 1988, and, in revised form, February 17, 1989.
1980 *Mathematics Subject Classification.* (1985 Revision) Primary 05B10,11A41,51E15.
Key words and phrases. Finite projective plane, flag transitive, prime.
The work on this paper was partially supported by NSF grant DMS-8512904.

Otherwise for instance $n = 24$ provides a counter example. Here $p = 601$ and $2^{25} \equiv 1 \pmod{p}$.

I have verified that Questions 2 and 3 have an affirmative answer for $n \leq 14,400,008$ (and $p \leq 207,360,244,800,073$). This was done on a PC so that it should not be difficult to check the results for much larger values of n.

These questions may be of independent interest. In fact one could consider analogues of Question 1 without assuming that n is even. However in the form above they arise naturally in the study of finite projective planes.

A finite projective plane is said to be flag transitive if its collineation group is transitive on the set of flags (incident point-line pairs). It has been conjectured that a finite flag transitive projective plane is necessarily Desarguesian. The following result is relevant to this conjecture.

Theorem A. *Let π be a finite flag transitive projective plane of order n which is not Desarguesian. Then $p = n^2 + n + 1$ is a prime, $n \equiv 0 \pmod{8}$, n is not a power of 2 and* (H1) *is satisfied.*

Corollary. *If Question 3 has an affirmative answer then every finite flag transitive projective plane is Desarguesian.*

In view of the remarks above, Theorem A implies that a finite non-Desarguesian flag transitive projective plane has order $n > 14,400,008$.

The proof of Theorem A is quite short. However it is, amongst other things, based on a result of W. Kantor [4] which depends not only on the classification of the finite simple groups, but also on a detailed knowledge of all their maximal subgroups of odd index.

2. The proof of Theorem A

Throughout this section π is a finite flag transitive non-Desarguesian projective plane, G is the collineation group of π. Thus there are $n + 1$ points on each line and $n^2 + n + 1$ points in π. By [4], Theorem A, n is even, $p = n^2 + n + 1$ is a prime and G is a Frobenius group of order $p(n + 1)$.

In particular, π is a cyclic plane. Thus if D is the subgroup of $\mathbf{F}_p^\times$ of order $n+1$ then D is a difference set modulo p. Furthermore, π and D determine each other up to isomorphism. See e.g. [3], Chapter 11.

Lemma 2.1. (H1) *and* (H2) *are satisfied.*

Proof. This follows from the multiplier theorem of M. Hall [3], Theorem 11.4.1. □

Lemma 2.2. *If $n > 2$ then* (H3) *is satisfied.*

Proof. As (H2) is satisfied, 2 has odd order and so is a quadratic residue modulo p. Thus $p \equiv \pm 1 \pmod{8}$ and so $n \equiv 0$ or $2 \pmod{8}$. Hence it suffices to show that $n \not\equiv 2 \pmod{8}$. This result is known [5], [6], but we include a short proof here.

Let ζ be a primitive p^{th} root of unity and let $\alpha = \sum_{d \in D} \zeta^d$. Then $\alpha\bar{\alpha} = n$ as D is a difference set with $|D| = n+1$. Let $K = \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\zeta)$. Then $[K : \mathbf{Q}] = n$ and α is the trace of ζ from $\mathbf{Q}(\zeta)$ to K. As $K \subseteq \mathbf{Q}(\zeta)$, 2 is not ramified in K. As $2^{n+1} \equiv 1 \pmod{p}$, 2 has residue class degree 1 in K. Therefore $(2) = \prod_1^n \mathfrak{p}_i$, where $\{\mathfrak{p}_i\}$ is a set of n distinct prime ideals of K. As $\alpha\bar{\alpha} = n = 2n_0$ with n_0 odd, it follows that exactly one of each pair $\mathfrak{p}_i, \bar{\mathfrak{p}}_i$ divides (α). Therefore $\alpha + \bar{\alpha} \not\equiv 0 \pmod{\mathfrak{p}_i}$ for each i. As 2 has residue class degree 1, this implies that $\alpha + \bar{\alpha} + 1 \equiv 0 \pmod{\mathfrak{p}_i}$ for each i and so $\alpha + \bar{\alpha} + 1 \equiv 0 \pmod{2}$. The coefficient of 1 in $\alpha + \bar{\alpha} + 1$ is odd and $\alpha + \bar{\alpha} + 1$ is the sum of $2(n+1)+1$ p^{th} roots of unity. Any set of $p-1$ p^{th} roots of unity forms an integral basis in $\mathbf{Q}(\zeta)$. Therefore $2(n+1)+1 > p-1 = n(n+1)$. Hence $n \leq 2$ contrary to assumption. □

Proof of Theorem A. In view of Lemmas 2.1 and 2.2 it suffices to show that n is not a power of 2. Suppose on the contrary that $n = 2^k$.

A result of Gordon, Mills and Welch, see [2] or [1], p. 89, implies that D consists of all the powers of 2 modulo p. Thus 2 has order $n+1$ modulo p. Since $2^{3k} \equiv n^3 \equiv 1 \pmod{p}$ this yields that $2^k + 1 = n + 1 \leq 3k$. Hence $k \leq 3$ and so $k = 1$ or 3. Thus $n = 2$ or 8. In these cases let D_0 be a difference set corresponding to the Desarguesian plane of order n. By the multiplier theorem D_0 can be chosen to consist of all the powers of 2 modulo p. Hence $D = D_0$ and so π is Desarguesian contrary to assumption. □

3. Some numerical results

For an integer $f \geq 0$ let $v(f) = n^2 + n + 1$, where $n = 2^k$ with $k = 3^f$. It is not known whether there are infinitely many values of f for which $v(f)$ is a prime.

Table 1

f	d(f)
3	2593
4	487
5	80191
6	39367
7	209953
8	141560137
9	472393
11	88219207
12	4361981634559
14	258280327
16	3357644239
17	12040253957143
19	662489036191
21	251048476873
23	35586121596607

If $0 \leq f \leq 2$ then $v(f)$ is a prime: $v(0) = 7, v(1) = 73$ and $v(2) = 262,657$. If $3 \leq f \leq 23$ then $v(f)$ is composite except possibly for $f = 10, 13, 15, 18, 20$ or 22. Table I contains the smallest prime divisor $d(f)$ of $v(f)$ in the remaining cases. It may not be easy to check whether $v(f)$ is a prime for some of the values of f listed above since $v(13)$ is already larger than the largest known prime.

References

1. L.D. Baumert, *Cyclic difference sets*, Lecture Notes in Math. **182** Springer, New York, 1971.
2. B. Gordon, W.H. Mills and L.R. Welch, *Some new difference sets*, Canad. J. Math **14** (1962), 614-625.
3. M. Hall, Jr., *Combinatorial theory*, Blaisdell, Waltham, Massachusetts (1967).
4. W.M. Kantor, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. of Algebra **106** (1987), 15-45.
5. D. Jungnickel and K. Vedder, *On the geometry of planar difference sets*, European J. Combin. **5** (1984), 143–148.
6. H.A. Wilbrink, *A note on planar difference sets*, J. of Combin. Theory **38** (1985), 94–95.

Department of Mathematics, Yale University, New Haven, Connecticut 06520