PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 4, December 1993

ON A COMBINATORIAL PROBLEM ASSOCIATED WITH THE ODD ORDER THEOREM

GEORGE GLAUBERMAN AND SIMON P. NORTON

(Communicated by Ronald M. Solomon)

ABSTRACT. We prove a conjecture about finite fields that arose in Péterfalvi's study of the Feit-Thompson Theorem.

1. INTRODUCTION

Let p and q be primes, and set

$$F_p = \mathrm{GF}(p), \quad F = \mathrm{GF}(p^q), \quad F^* = F - \{0\}, \quad U = \{b^{p-1} | b \in F^*\},$$
$$E = \{b \in U | 2 - b \in U\}, \quad \text{and} \quad E^{-1} = \{b^{-1} | b \in E\}. \tag{1}$$

Let N be the norm function from F into F_p. Since F^* is a cyclic group under multiplication, it is easy to see that U is a subgroup of F^* and consists of all $b \in F$ for which

$$1 = b^{(p^q-1)/(p-1)} = bb^p b^{p^2} \cdots b^{p^{q-1}} = N(b).$$

In a simplification [3] of the last chapter of the proof of the Feit-Thompson odd order theorem [1], Péterfalvi proves the following results (their statements have been generalized somewhat, since no change in the proofs is required):

Lemma 1. *Suppose* $E = E^{-1}$ *and* $|E| \geq 2$. *Then*

(a) *for each* $b \in E$ *and* $k \in \mathrm{GF}(p)$, $1 + k(1 - b) \in U$, *and*

(b) $p \leq q$.

Lemma 2. *If* p *and* q *are odd, then* $|E| \geq 2$.

(Note that $|E| \geq 1$ because $1 \in E$.)

Lemma 3. *Given the existence of a group satisfying certain restrictions* (*i.e., the hypothesis of Proposition* 9), $E = E^{-1}$.

The proofs of Lemmas 1 and 2 are fairly short and based on Lemmas 38.9–38.11 of [1]; the bulk of [3] is occupied with the proof of Lemma 3. In the chapters of [1] preceding the last chapter, the authors prove that for any minimal simple group G of odd order, there are distinct odd primes p and q such that, for both (p, q) and (q, p), the restrictions in Lemma 3 are satisfied by some

Received by the editors April 13, 1992.
1991 *Mathematics Subject Classification.* Primary 11T06; Secondary 20D05.

subgroup of G. Therefore, these lemmas yield a contradiction, which completes the proof of the solubility of any finite group of odd order.

It is easy to show (Lemma 5) that Lemma 2 remains valid if $p = 2$. In private communication, Péterfalvi conjectured that if $E = E^{-1}$ then $p \leq 3$. The main result of this paper is to prove this conjecture (Proposition 7). Although this does not appear to simplify further the proof of [1], it may be of some interest. We also discuss a related open question in §3.

Lemma 4. (a) *If* $p = 2$, *then* $U = E = E^{-1}$.

(b) *If* $p = 3$, *then* $E = E^{-1}$.

Proof. Since (a) is trivial, we prove (b). Assume $p = 3$ and $c \in E$. Writing N for the norm function from F into F_p (as before), we have

$$N(c) = N(2 - c) = 1.$$

Therefore, $N(c^{-1}) = 1$. Since $2 - c^{-1} = c^{-1}(2c - 1) = c^{-1}(2 - c)$ (because $p = 3$),

$$N(2 - c^{-1}) = N(c^{-1})N(2 - c) = 1.$$

Thus, $c^{-1} \in E$, as desired.

Lemma 5. *For any primes* p *and* q,

(a) $E = \{1\}$ *if* p *is odd and* $q = 2$, *and*

(b) $|E| \geq 2$ *otherwise.*

Proof. If $p = 2$, then $|E| = |U| \geq 2$ by Lemma 4. If p and q are odd, then $|E| \geq 2$ by Lemma 2.

Now we may assume that P is odd and $q = 2$. Let N be the norm function from F into F_p, and take any $b \in E$. Let $c = b + b^p$, and let $f(x)$ be the polynomial $(x - b)(x - b^p)$. Then

$$1 = N(b) = bb^p, \qquad f(x) = x^2 - (b + b^p)x + bb^p = x^2 - cx + 1,$$

and

$$1 = N(2 - b) = (2 - b)(2 - b^p) = f(2) = 4 - 2c + 1.$$

Therefore,

$$c = 2, \quad f(x) = x^2 - 2x + 1 = (x - 1)^2, \quad \text{and} \quad b = 1,$$

as claimed.

2. Main results

Here, we continue using the notation in (1) but also regard F as an affine space over F_p.

Proposition 6. *Let* A *be an affine space of finite dimension* r *over a field* F_p *of prime order* p. *Let* V *be a vector space over* F_p *associated with* A. *Suppose a subset* S *of* A *satisfies the condition*:

(C) *Whenever* $b \in A$, $x \in V$, *and* $b - x, b, b + x \in S$, *then* $b + kx \in S$ *for all* $k \in F_p$.

Assume $p \geq 5$ *and* $|S| \geq \frac{1}{2}|A|$. *Then* $S = A$.

Remark. Condition (C) asserts that any affine line intersecting S in at least three points, one midway between two others, lies in S. It is trivially true if p is 2 or 3, which makes it easy to construct counterexamples to the proposition in these cases (e.g., with $|A| = 2^2$ or 3).

Proof. We divide the proof into two cases.

Case 1. $r = 1$. Here, we may assume that $A = F_p$. Let $m = \frac{1}{2}(p-1)$. Then $|S| > \frac{1}{2}p$. So

$$|S| \geq \tfrac{1}{2}(p+1) = m + 1 \geq 3.$$

Take distinct elements $b, c \in S$, and let

$$S' = \{(b-c)^{-1}(x-c) | x \in S\}.$$

It is easy to see that all translations and nonzero scalar multiplications preserve condition (C). Hence, S' satisfies (C). Replacing S by S', we may assume that $0, 1 \in S$.

Now suppose that S is a proper subset of A. We will obtain a contradiction. Let us identify the elements of A with the integers $-m$, $-(m-1), \ldots, -1, 0, 1, \ldots, m$ in the obvious manner. For each integer k such that $1 \leq k \leq m$, the set S cannot contain the sequence $-k, 0, k$, because S satisfies (C) and does not contain the line A. Hence, for each k, S contains at most one of the elements $k, -k$. Since there are m pairs $k, -k$, and since $|S - \{0\}| = |S| - 1 \geq (m+1) - 1 = m$,

(2) S must contain precisely one element from each pair $k, -k$.

Now $0, 1 \in S$. To avoid the sequence $0, 1, 2$, we must have $-2 \in S$. Thus,

(3) $$0, 1, -2 \in S.$$

If $p = 5$, then $1 + 2 = -2$ and $(-2) + 2 = 0$, so that the sequence $b - x, b, b + x$ lies in S for $b = -2$ and $x = 2$, a contradiction. Thus, $p \geq 7$.

If $p \geq 11$, then, by (2) and (3), S contains one of the sequences $0, -2, -4$ or $-2, 1, 4$, a contradiction. But then $p = 7$, and similarly S contains one of the sequences $0, -2, 3$ or $-2, 1, -3$, again a contradiction.

Case 2. *General case.* Again we assume $S \neq A$ and work by contradiction. Take $\lambda \in A \backslash S$, and let $\mathscr{L}$ be the set of all lines of A that contain λ. Let

$$A' = A - \{\lambda\} \quad \text{and} \quad L' = L - \{\lambda\} \text{ for each } L \in \mathscr{L}.$$

Then A' is the disjoint union of the sets L'.

For each $L \in \mathscr{L}$, Case 1 yields that $|L \cap S| \leq \frac{1}{2}|L| = \frac{p}{2}$, and hence

$$|L' \cap S| = |L \cap S| \leq \tfrac{1}{2}(p-1) = \tfrac{1}{2}|L'|.$$

Therefore,

$$|S| = |A' \cap S| = \sum_{L \in \mathscr{L}} |L' \cap S| \leq \frac{1}{2} \sum_{L \in \mathscr{L}} |L'| = \frac{1}{2}|A'| < \frac{1}{2}|A|, \tag{4}$$

contrary to hypothesis. This completes the proof of Case 2 and of Proposition 6.

Remark. We thank Curtis Bennett for a suggestion which shortened part of the proof above.

Proposition 7. *Let p and q be primes, and assume the notation of* (1). *Then $E = E^{-1}$ if and only if $p \leq 3$.*

Proof. If $p \leq 3$, then $E = E^{-1}$ by Lemma 4.

Assume $p \geq 5$ and $E = E^{-1}$. We shall obtain a contradiction. By Lemma 5, we have

$$E = E^{-1} \quad \text{and} \quad |E| \geq 2. \tag{5}$$

We regard F as an affine space over F_p.

Step 1. For every affine subspace A of F over F_p, condition (C) of Proposition 6 is satisfied for $S = A \cap U$.

Proof. Recall that, for each A and each $b \in A$, $A = b + V$ for some vector subspace V of F over F_p.

Suppose $b \in A$, $x \in V$, and $b - x, b, b + x \in A \cap U$. Let $d = b^{-1}x$ and $c = 1 - d$. Since U is a group under multiplication, U contains $b^{-1}(b - x)$ and $b^{-1}(b + x)$; that is,

$$c = 1 - d = b^{-1}(b - x) \in U \quad \text{and} \quad 2 - c = 1 + d = b^{-1}(b + x) \in U.$$

So $c \in E$. By (5) and Lemma 1,

$$1 + kd = 1 + k(1 - c) \in U \quad \text{for every } k \in F_p.$$

Hence

$$b + kx = b(1 + kd) \in U \quad \text{for every } k \in F_p.$$

This verifies condition (C) for $S = A \cap U$ and completes the proof of Step 1.

By (5), E contains some element $c \neq 1$. Let $b = 1 - c$. Then $b \neq 0$. For each positive integer $r = 1, 2, \ldots, q$, let

$$A_r = \{1 + k_1 b + k_2 b^2 + \cdots + k_r b^r | k_1, \ldots, k_r \in F_p\}.$$

Then each A_r is an affine subspace of F over F_p.

Step 2. We have

$$A_1 \subseteq U \quad \text{and} \quad |A_r| = p^r \text{ for } r = 1, 2, \ldots, q.$$

Proof. By Lemma 1, $A_1 \subseteq U$. Since $b \neq 0$ and $0 \notin U$, this shows that $b \notin F_p$. Since q is a prime and $b \in F = \mathrm{GF}(p^q)$,

$$b \text{ has degree } q \text{ over } F_p.$$

Now, for each $r = 1, \ldots, q$, the affine space A_r consists of all elements of the form

$$1 + bf(b) \quad \text{for } f \text{ the zero polynomial or a polynomial over } F_p \text{ of degree at most } q - 1.$$

We claim that distinct polynomials give distinct elements. To see this, assume that $1 + bf_1(b) = 1 + bf_2(b)$. Since $b \neq 0$, $f_1(b) = f_2(b)$ and $(f_1 - f_2)(b) = 0$. Since b has degree q and $f_1 - f_2$ has degree at most $q - 1$, it follows that $f_1 = f_2$, as claimed. This shows that $|A_r| = p^r$ for $r = 1, 2, \ldots, q$, as desired, and completes the proof of Step 2.

Step 3. For $r = 1, 2, \ldots, q$, $A_r \subseteq U$.

Proof. By Step 2, $A_1 \subseteq U$. Suppose $2 \leq r \leq q$ and $A_{r-1} \subseteq U$. A typical element c of A_r has the form $c = 1 + bf(b)$ for some polynomial

$$f(X) = k_1 + k_2X + \cdots + k_rX^{r-1}$$

over F_p. If $1 + Xf(x)$ has degree less than r, or is a reducible polynomial, then induction yields that $c \in U$ (since U is closed under multiplication and any factors of $1 + Xf(X)$ may be assumed to have constant term equal to 1). Otherwise, $1 + Xf(X)$ is irreducible of degree r; that is,

$$X^r + k_r^{-1}(k_{r-1}X^{r-1} + \cdots + k_1X + 1)$$

is irreducible. Each such polynomial corresponds to a set of r distinct roots of the form $\lambda, \lambda^p, \ldots, \lambda^{p^{r-1}}$ in the field $\mathrm{GF}(p^r)$. Now, each such root generates $\mathrm{GF}(p^r)$ over F_p and thus lies in $\mathrm{GF}(p^r)\backslash F_p$. Hence, there are at most $(p^r-p)/r$ distinct such polynomials. Consequently,

$$\begin{aligned} |A_r \cap U| &\geq |A_r| - r^{-1}(p^r - p) \geq p^r - \tfrac{1}{2}(p^r - p) \\ &= \tfrac{1}{2}p^r + \tfrac{1}{2}p > \tfrac{1}{2}p^r = \tfrac{1}{2}|A_r|. \end{aligned}$$

Since $p \geq 5$, Step 1 and Proposition 6 yield that $A_r \subseteq U$. This completes the proof of Step 3.

Step 4. Contradiction.

Proof. By Steps 2 and 3,

$$|F| = p^q = |A_q| \leq |U| = (p^q - 1)/(p - 1) < |F|.$$

This shows Step 4 and completes the proof of Proposition 7.

3. Further questions

As in the previous sections we use the notation of (1) for arbitrary primes p, q. Proposition 7 asserts that $E = E^{-1}$ if and only if $p \leq 3$. Lemma 3 asserts that the existence of a group satisfying certain restrictions yields that $E = E^{-1}$ and hence, by Proposition 7, that $p \leq 3$. In this section, we will specify the restrictions and investigate whether such a group can actually occur.

Lemma 8. *For any primes p and q, $(p^q - 1)/(p - 1)$ is relatively prime to $p - 1$ if and only if q does not divide $p - 1$.*

Proof. Let $r = p - 1$. Then, modulo r,

$$(p^q - 1)/(p - 1) \equiv p^{q-1} + p^{q-2} + \cdots + 1 \equiv q,$$

which yields the result.

Lemma 8 allows us to restate the main result of [3] slightly differently:

Proposition 9 [3, Lemma 3]. *Let p and q be arbitrary primes, and assume the notation of* (1). *Let P be the additive group of F, and let U act on P by multiplication. Identify P and U with their images in the semidirect product $H = PU$. Let P_0 be the image of the additive group of F_p. Assume that:*

(A) *q does not divide $p - 1$; and*

(B) *there exist a monomorphism* σ *of* H *into a group* G, *a finite abelian* p'*-subgroup* Q *of* G, *and an element* $y \in Q$ *such that* $\sigma(P_0)$ *normalizes* Q *and* $\sigma(P_0)^y$ *normalizes* U. *Then* $E = E^{-1}$.

As mentioned above, we must have $p \leq 3$ in the situation of Proposition 9. In a personal communication, Péterfalvi gave the following examples and problem.

Example 10 (for Proposition 9). Let $p = 2$ and let q be any prime. Take

$$G = \mathrm{SL}(2, 2^q), \quad \sigma(P) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in F \right\},$$

$$\sigma(U) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| \, a \in F \backslash \{0\} \right\},$$

$$\sigma(P_0) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \quad y = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad Q = \langle y \rangle.$$

Example 11 (for Proposition 9). Let $p = 2$ and let q be any odd prime. Take $G = Sz(2^q)$, and choose σ so that $\sigma(P) = \Omega_1(S)$ for some Sylow 2-subgroup S of G and $\sigma(U)$ is a (cyclic) subgroup of order $2^q - 1$ in $N_G(S)$. Let P_1 be any subgroup of order 2 in $N_G(U)$. Then

$$\sigma(P_0) = \langle x_0 \rangle \quad \text{and} \quad P_1 = \langle x_1 \rangle$$

for some elements x_0, x_1 of order 2. Let $Q = \langle x_0 x_1 \rangle$.

Suppose Q has even order. Then it contains a unique element x_2 of order 2. Since x_0 and x_1 invert Q, they centralize x_2. From the structure of $Sz(2^q)$ [2, §§XI.1, XI.3], $\Omega_1(S)$ is abelian and $S = C_G(x)$ for each $x \in \Omega_1(S)^\sharp$. Hence

$$x_2 \in C_G(x_0) = S, \quad x_1 \in C_G(x_2) = S, \quad [x_1, U] \subseteq [S, U] \cap U \subseteq S \cap U = 1.$$

But then $U \subseteq C_G(x_1) = S$, which is absurd. Thus, Q has odd order.

Now, $\sigma(P_0)$ and P_1 are Sylow 2-subgroups of $\langle x_0, Q \rangle$, and $\sigma(P_0)^y = P_1$ for some $y \in Q$.

Problem (Péterfalvi). Can the hypothesis of Proposition 9 be satisfied for $p = 3$?

Note that condition (A) forces q to be odd and $\sigma(P_0)^y$ must centralize $\sigma(U)$ if $|\mathrm{Aut}\, U|$ is not divisible by 3 (e.g., if $q = 5$ and $|U| = (3^5 - 1)/(3 - 1) = 11^2$).

References

1. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.
2. B. Huppert and N. Blackburn, *Finite groups*. III, Springer-Verlag, Berlin, 1982.
3. T. Peterfalvi, *Simplification du chapitre* VI *de l'article de Feit et Thompson sur les groupes d'ordre impair*, C. R. Acad. Sci. Paris Sér. I Math. **229** (1984), 531–534.

Department of Mathematics, University of Chicago, 5734 S. University Avenue, Chicago, Illinois 60637

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge CB 2 1SB, England

E-mail address: spn1@phx.cam.ac.uk