QUADRATIC RESIDUES AND DIFFERENCE SETS

VSEVOLOD F. LEV AND JACK SONN

Abstract. It has been conjectured by Sárközy that with finitely many exceptions, the set of quadratic residues modulo a prime p cannot be represented as a sumset $\{a+b\colon a\in A, b\in B\}$ with non-singleton $A,B\subseteq \mathbb{F}_p$. The case $A=B$ of this conjecture has been recently established by Shkredov. The analogous problem for differences remains open: is it true that for all sufficiently large primes p, the set of quadratic residues modulo p is not of the form $\{a'-a''\colon a',a''\in A,\ a'\ne a''\}$ with $A\subseteq\mathbb{F}_p$?

We attack here a presumably more tractable variant of this problem, which is to show that there is no $A\subseteq\mathbb{F}_p$ such that every quadratic residue has a *unique* representation as $a'-a''$ with $a',a''\in A$, and no non-residue is represented in this form. We give a number of necessary conditions for the existence of such A, involving for the most part the behavior of primes dividing $p-1$. These conditions enable us to rule out all primes p in the range $13<p<10^{20}$ (the primes $p=5$ and $p=13$ being conjecturally the only exceptions).

1. Background and Motivation

Sárközy [Sa12] conjectured that the set $\mathcal{R}_p$ of all quadratic residues modulo a prime p is not representable as a sumset $\{a+b\colon a\in A,\ b\in B\}$, whenever $A,B\subseteq\mathbb{F}_p$ satisfy $\min\{|A|,|B|\}>1$. Shkredov [Sh14] has recently established the particular case $B=A$ of this conjecture, showing that $\{a'+a''\colon a',a''\in A\}\ne\mathcal{R}_p$, except if $p=3$ and $A=\{2\}$. He has also proved that $\mathcal{R}_p$ cannot be represented as a *restricted sumset*: $\{a'+a''\colon a',a''\in A,\ a'\ne a''\}\ne\mathcal{R}_p$ for $A\subseteq\mathbb{F}_p$, with several exceptions for $p\le 13$.

The argument of [Sh14] does not seem to extend to handle differences (instead of sums) and to show that

$$\{a'-a''\colon a',a''\in A,\ a'\ne a''\}\ne\mathcal{R}_p,\quad A\subseteq\mathbb{F}_p. \tag{1}$$

We notice that for equality to hold in (1), one needs to have $2\binom{|A|}{2}\ge|\mathcal{R}_p|$, which readily yields

$$|A|>\sqrt{p/2}. \tag{2}$$

2010 *Mathematics Subject Classification.* Primary: 11B13; Secondary: 11A15, 11B34, 11P70, 11T21, 05B10.

Key words and phrases. Sumsets; Difference sets; Quadratic Residues.

At the same time, there is a famous, long-standing conjecture saying that for every $\varepsilon > 0$, if $A \subseteq \mathbb{F}_p$ has the property that $a' - a'' \in \mathcal{R}_p$ for all $a', a'' \in A$ with $a' \neq a''$, then

$$|A| < p^{\varepsilon} \tag{3}$$

provided that p is sufficiently large. (We refer the reader to [Sh14] for several more related conjectures and discussion.) Combining (2) and (3), one immediately derives that (1) is true for all but finitely many primes p.

Unfortunately, the conjecture just mentioned is presently out of reach, and neither could we prove (1). As a step in this direction, we investigate the following, presumably easier, problem:

> *Does there exist a subset $A \subseteq \mathbb{F}_p$ such that the differences $a' - a''$, with $a', a'' \in A$, $a' \neq a''$, list all quadratic residues modulo p, and every quadratic residue is listed exactly once?*

Even this question does not eventually receive a complete answer. However, we were able to establish a number of necessary conditions, and use them to show that in the range $13 < p < 10^{20}$, there are no "exceptional primes". This makes it extremely plausible to conjecture that no such primes exist at all, with just two exceptions $p = 5$ and $p = 13$ addressed below.

2. Summary of Results

In this section we introduce basic notation and present our results. Most of the proofs are postponed to subsequent sections; see the "proof locator" at the very end of the section.

Recall, that for a prime p we denote by $\mathbb{F}_p$ the finite field of order p, and by $\mathcal{R}_p$ the set of all quadratic residues modulo p. We also denote by $\mathcal{N}_p$ the set of all quadratic non-residues modulo p, to have the decomposition $\mathbb{F}_p = \mathcal{R}_p \cup \mathcal{N}_p \cup \{0\}$.

For subsets A and S of an additively written abelian group, the notation $A - A \overset{!}{=} S$ will indicate that every element of S has a unique representation as a difference of two elements of A and, moreover, every such non-zero difference belongs to S. (In our context, the underlying group is always the additive group of the field $\mathbb{F}_p$, and S is one of the sets $\mathcal{R}_p$ and $\mathcal{N}_p$.) Our goal is thus to show that, with few exceptions,

$$A - A \overset{!}{=} \mathcal{R}_p \tag{4}$$

does not hold.

One immediate observation is that for (4) to hold, letting $n := |A|$, one needs to have $n(n-1) = \frac{p-1}{2}$; that is, $p = 2n(n-1) + 1$. As a result, $p \equiv 1 \pmod 4$ — a conclusion which also follows by observing that the set of all differences $a' - a''$ is symmetric, whence $\mathcal{R}_p$ must be symmetric too.

Experimenting with small values of p, one finds two remarkable counterexamples to (4): namely, the sets $A_5 := \{2,3\} \subseteq \mathbb{F}_5$ and $A_{13} := \{2,5,6\} \subseteq \mathbb{F}_{13}$. Clearly, all affinely equivalent sets of the form $\{\mu a + c \colon a \in A_p\}$, where $\mu \in \mathcal{R}_p$ and $c \in \mathbb{F}_p$ are fixed parameters (and $p \in \{5, 13\}$) work too, and it is not difficult to see that no other sets A satisfying (4) exist for $p \le 13$; indeed, we believe that there are no more such sets at all.

What makes the two sets A_5 and A_{13} special? An interesting feature they have in common is that both of them are cosets of a subgroup of the multiplicative group of the corresponding field; indeed, A_{13} is a coset of the subgroup $\{1,3,9\} < \mathbb{F}_{13}^\times$, while A_5 is a coset of the subgroup $\{1,4\} < \mathbb{F}_5^\times$. In addition, A_5 is affinely equivalent to the set $\{0,1\}$, which is a union of 0 and a subgroup of $\mathbb{F}_5^\times$. Our first two theorems show that constructions of this sort do not work for $p > 13$.

Theorem 1. *For a prime $p > 13$, there is no coset $A = gH$, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that $A - A \overset{!}{=} \mathcal{R}_p$.*

Theorem 2. *For a prime $p > 5$, there is no coset gH, with $H < \mathbb{F}_p^\times$ and $g \in \mathbb{F}_p^\times$, such that, letting $A := gH \cup \{0\}$, we have $A - A \overset{!}{=} \mathcal{R}_p$.*

For integer μ and a subset A of an additively written abelian group, by μA we denote the dilate of A by the factor of μ:

$$\mu A := \{\mu a \colon a \in A\}.$$

Extending slightly one of the central notions of the theory of difference sets, we say that μ is a *multiplier* of A if μ is co-prime with the exponent of the group, say e, and there exists a group element g such that $\mu A = A + g$. Clearly, in this case every integer from the residue class of μ modulo e is also a multiplier of A. This shows that the multipliers of a given set A can be considered as elements of the group of units $(\mathbb{Z}/e\mathbb{Z})^\times$, and it is immediately seen that they actually form a subgroup; we denote this subgroup by M_A, and call it the *multiplier subgroup* of A.

It is readily seen that all translates of a subset A of an abelian group have the same multiplier subgroup. If, furthermore, $|A|$ is co-prime with the exponent e of the group, then there is a translate of A whose elements add up to 0. Denoting this translate by A_0 and observing that $\mu A_0 = A_0 + g$ implies $g = 0$ (as follows by comparing the sums of elements of each side), we conclude that if $\gcd(|A|, e) = 1$, then A has a translate which is fixed by every multiplier $\mu \in M_A$.

Here we are interested in the situation where the underlying group has prime order. In this case, every subset A has a translate fixed by its multiplier subgroup M_A. This translate is then a union of several cosets of M_A and, possibly, the zero element of the group. Consequently, using multipliers, Theorems 1 and 2 can be restated as follows: if $p > 13$ and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$, then choosing $g \in \mathbb{F}_p$ so that the elements of the translate $A - g$ add up to 0, the set $(A - g) \setminus \{0\}$ is a union of at least two cosets of M_A.

Our next result shows, albeit in a rather indirect way, that "normally", a set $A \subseteq \mathbb{F}_p$ satisfying $A - A \overset{!}{=} \mathcal{R}_p$ must have a large multiplier subgroup.

For a prime $p \equiv 1 \pmod 4$, let G_p denote the greatest common divisor of the orders modulo p of all primes dividing $\frac{p-1}{4}$:

$$G_p := \gcd \left\{ \mathrm{ord}_p(q) \colon q \mid \tfrac{p-1}{4},\ q \text{ is prime} \right\}.$$

Theorem 3. *If p is a prime and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$, then the multiplier subgroup M_A lies above the order-G_p subgroup of $\mathbb{F}_p^\times$; equivalently, $|M_A|$ is divisible by G_p.*

The quantity G_p is difficult to study analytically, but one can expect that it is usually quite large: for, if $r^v \mid p-1$ with r prime and $v > 0$ integer, then in order for r^v not to divide G_p, there must be a prime $q \mid \frac{p-1}{4}$ which is a degree-r residue modulo p, the "probability" of which for every specific q is $1/r$. Computations show that, for instance, among all primes $p \le 10^{12}$ of the form $p = 2n(n-1)+1$, there are less than 1.4% satisfying $G_p < \sqrt{p}$.

Recalling that $A - A \overset{!}{=} \mathcal{R}_p$ implies $p = 2n(n-1)+1$ with $n = |A|$, from Theorem 3 and in view of Theorems 1 and 2 we get

Corollary 1. *Suppose that p is a prime. If there exists a subset $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$ then, writing $p = 2n(n-1)+1$, either G_p is a proper divisor of n, or G_p is a proper divisor of $n-1$.*

To give an impression of how strong Corollary 1 is, we remark that it sieves out over 99.7% of all primes $p = 2n(n-1)+1$ with $p < 10^{12}$.

For integer $k \ge 1$, let Φ_k denote the kth cyclotomic polynomial. Yet another useful consequence of Theorem 3 is

Corollary 2. *Let p be a prime, and suppose that there exists a subset $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$. If an element $z \in \mathbb{F}_p^\times$ and an integer $k \ge 2$ satisfy $\mathrm{ord}_p(z) \nmid k$ and $\mathrm{ord}_p(z) \mid G_p$, then $\Phi_k(z) \in \mathcal{R}_p$.*

The practical implication of Corollary 2 is that if we can find a residue $z \in \mathbb{F}_p^\times$ of degree $\frac{p-1}{G_p}$ and an integer $k \geq 2$ such that $z^k \neq 1$ and $\Phi_k(z) \in \mathcal{N}_p$, then there is no set $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$.

To prove Corollary 2, denote by H the order-G_p subgroup of $\mathbb{F}_p^\times$, and consider the differences $h' - h''$ with $h', h'' \in H$, $h' \neq h''$. By Theorem 3, either all these differences are quadratic residues, or they all are quadratic non-residues. If $\mathrm{ord}_p(z) \mid G_p$ and $\mathrm{ord}_p(z) \nmid k$, then both z and z^k are non-unit elements of H, and consequently either both $z-1$ and $z^k - 1$ are quadratic residues, or they both are quadratic non-residues. In either case,

$$\prod_{\substack{d \mid k \\ d>1}} \Phi_d(z) = \frac{z^k - 1}{z - 1} \in \mathcal{R}_p,$$

and the claim follows by induction on k.

It is somewhat surprising that if a set $A \subseteq \mathbb{F}_p$ with $A - A \stackrel{!}{=} \mathcal{R}_p$ exists, then all orders $\mathrm{ord}_p(q)$ appearing in the definition of the quantity G_p are odd.

Theorem 4. *Let p be a prime. If there exists a subset $A \subseteq \mathbb{F}_p$ satisfying $A - A \stackrel{!}{=} \mathcal{R}_p$, then for every prime $q \mid \frac{p-1}{4}$, the order $\mathrm{ord}_p(q)$ is odd.*

Corollary 3. *Let p be a prime. If there exists a subset $A \subseteq \mathbb{F}_p$ satisfying $A - A \stackrel{!}{=} \mathcal{R}_p$, then writing $p = 2n(n-1) + 1$ we have $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$; hence, $p \equiv 5 \pmod 8$.*

To derive Corollary 3 from Theorem 4, observe that if we had $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$, then $\frac{p-1}{4}$ were even and, consequently, $\frac{p-1}{4}$ and $p-1$ would have same prime divisors. As a result, all prime divisors of $p-1$ would be of odd order modulo p, which is impossible as $p-1$ itself has even order.

Using a biquadratic reciprocity law due to Lemmermeyer [Le00], from Theorem 4 we will derive

Theorem 5. *Let p be a prime. If there exists a subset $A \subseteq \mathbb{F}_p$ satisfying $A - A \stackrel{!}{=} \mathcal{R}_p$ then, writing $p = 2n(n-1) + 1$, neither n nor $n-1$ have prime divisors congruent to 7 modulo 8. Moreover, of the two numbers n and $n-1$, the odd one has no prime divisors congruent to 5 modulo 8, and the even one has no prime divisors congruent to 3 modulo 8.*

Computations show that there are very few primes passing both the test of Corollary 1 and that of Theorem 5. In the range $13 < p < 10^{20}$, there are only five such primes, corresponding to the values of n listed in the following table:

n	δ	$(n-\delta)/G_p$	$n-1,\ n$
51	1	2	$2\cdot 5^2,\ 3\cdot 17$
650	0	2	$11\cdot 59,\ 2\cdot 5^2\cdot 13$
32283	1	2	$2\cdot 16141,\ 3^2\cdot 17\cdot 211$
57303490	1	3	$3\cdot 1579\cdot 12097,\ 2\cdot 5\cdot 5730349$
377687811	0	3	$2\cdot 5\cdot 17\cdot 113\cdot 19661,\ 3\cdot 1787\cdot 70451$

FIG. 1. The second column gives the value of $\delta\in\{0,1\}$ such that $G_p \mid n-\delta$, the last column contains the prime decompositions of $n-1$ and n.

Every individual value of n in the table is easy to rule out using Corollary 2. For instance, the first exceptional value $n=51$ corresponds to the prime $p=5101$; since $(5101-1)/G_{5101}=204$, applying Corollary 2 with $k=2$ we conclude that if $A\subseteq\mathbb{F}_{5101}$ satisfying $A-A\overset{!}{=}\mathcal{R}_{5101}$ existed, then every degree-204 residue $z\in\mathbb{F}_p$ with $z^2\neq 1$ would satisfy $z+1\in\mathcal{R}_{5101}$; this conclusion, however, is violated for $z=2^{204}$.

The remaining four exceptional cases can be dealt with in an analogous way; say, one can take $z=2^{(p-1)/G_p}$ for $n=650$ and $n=377687811$, and $z=3^{(p-1)/G_p}$ for $n=32283$ and $n=57303490$ (with $k=2$ in each case). We thus conclude that there are no primes $13<p<10^{20}$ for which $A\subseteq\mathbb{F}_p$ with $A-A\overset{!}{=}\mathcal{R}_p$ exists.

Theorem 4 will be derived as a straightforward corollary of the Semi-primitivity Theorem from the theory of difference sets. Recall, that for positive integer v, k, and λ, a (v,k,λ)-*difference set* is a k-element subset of a v-element group such that (assuming additive notation) every non-zero group element has exactly λ representations as a difference of two elements of the set. The following somewhat unexpected claim shows how difference sets come into the play, and allows us to apply the well-established machinery of difference sets in our problem.

Claim 1. *Suppose that p is a prime and $A\subseteq\mathbb{F}_p$ satisfies $A-A\overset{!}{=}\mathcal{R}_p$. Write $n:=|A|$ and fix arbitrarily a quadratic non-residue $\nu\in\mathcal{N}_p$. Then the n^2 sums $a'+\nu a''$ with $a',a''\in A$ are pairwise distinct, and the set D of all these sums is a $(p,n^2,n(n+1)/2)$-difference set in $\mathbb{F}_p$.*

We remark that the Multiplier Conjecture [La83, Conjecture 6.7] along with Claim 1 lead to a conclusion much stronger than Corollary 1: namely, if there is a subset $A\subseteq\mathbb{F}_p$ with $A-A\overset{!}{=}\mathcal{R}_p$, then, writing $p=2n(n-1)+1$, the *least common multiple* $\operatorname{lcm}\left\{\operatorname{ord}_p(q)\colon q\mid \frac{p-1}{4}\right\}$ is a divisor of either n or $n-1$.

On a historical note, it was Broughton [B95] who first used biquadratic reciprocity to study $(2n(n-1)+1,n^2,n(n+1)/2)$-difference sets.

Our last result is a lemma which is used in the proof of Theorems 1 and 2, and which we believe is also of independent interest.

Lemma 1. *If $p > 5$ is a prime and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$, then $|M_A|$ is odd; that is, $-1 \notin M_A$.*

The rest of the paper is devoted to the proofs of the above-discussed results. We prove Lemma 1 in the next section, and Theorems 1 and 2 in Section 4. In Section 5 we prove Claim 1, present the Semi-primitivity Theorem, and derive Theorem 4. In Section 6 we state Lemmermeyer's biquadratic reciprocity law and prove Theorem 5. Theorem 3 is proved in Section 7; the proof uses some basic algebraic number theory. Finally, in the Appendix we give an equivalent restatement of the problem studied in this paper in terms of algebraic number theory.

3. $|M_A|$ is Odd: the Proof of Lemma 1

Suppose that p is a prime and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$; we want to show that the multiplier subgroup $M_A < \mathbb{F}_p^\times$ has odd order.

For a subset $S \subseteq \mathbb{F}_p$ and integer $j \geq 0$, let

$$\sigma_j(S) = \sum_{s \in S} s^j,$$

subject to the agreement that if $0 \in S$ and $j = 0$, then the corresponding summand is equal to 1 (so that $\sigma_0(S) = |S|$). For every $1 \leq k < (p-1)/2$ we have

$$\sum_{a',a'' \in A} (a' - a'')^k = \sum_{x \in \mathcal{R}_p} x^k = 0;$$

expanding the binomial and changing the order of summation, we get

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} \sigma_j(A) \sigma_{k-j}(A) = 0. \tag{5}$$

Write $m := |M_A|$. Having A suitably translated, we can assume that $A \setminus \{0\}$ is a union of cosets of M_A, and let then C be the set of arbitrarily chosen representatives of these cosets. We distinguish two cases.

Suppose first that $0 \notin A$. In this case $\sigma_j(A) = \sigma_j(C)\sigma_j(M_A)$ and

$$\sigma_j(M_A) = \begin{cases} m & \text{if } m \mid j, \\ 0 & \text{otherwise,} \end{cases}$$

whence (5) is non-trivial only if $m \mid k$, and in this case (with a minor change of notation) it can be re-written as

$$\sum_{j=0}^{k} (-1)^{jm} \binom{km}{jm} \sigma_{jm}(C) \sigma_{(k-j)m}(C) = 0, \quad 0 < k < \frac{p-1}{2m}. \tag{6}$$

Taking $k=1$ gives $(1+(-1)^m)\sigma_0(C)\sigma_m(C)=0$, and if m were even (contrary to the assertion of the lemma) then, in view of $\sigma_0(C)=|C|\ne 0$, we would have $\sigma_m(C)=0$. Furthermore, we could then re-write (6) as

$$2|C|\sigma_{km}(C)=-\sum_{j=1}^{k-1}\binom{km}{jm}\sigma_{jm}(C)\sigma_{(k-j)m}(C),$$

and substituting subsequently $k=2,3,\dots$ we conclude that $\sigma_{km}(C)=0$ whenever $0<k<(p-1)/(2m)$. Equivalently, the $|C|$ elements c^m ($c\in C$) have the property that the sum of their kth powers vanish for all $0<k<(p-1)/(2m)$; hence for all $0<k\le |C|$ in view of

$$|C|=\frac{|A|}{|M_A|}=\frac{n}{m}<\frac{n(n-1)}{m}=\frac{p-1}{2m}.$$

(we use here our standard notation: $n=|A|$ and $p=2n(n-1)+1$. Notice that this estimate assumes $p>5$.) As a result, all these elements, and therefore also all elements of C, are equal to 0, a contradiction establishing the assertion in the case $0\notin A$.

Turning to the situation where $0\in A$, we write $A_0:=A\setminus\{0\}$ and notice that in this case $\sigma_0(A)=|A|=m|C|+1$ and $\sigma_j(A)=\sigma_j(A_0)=\sigma_j(C)\sigma_j(M_A)$ for every $j>0$; as a result,

$$\sigma_j(A)=\begin{cases} m|C|+1 & \text{if } j=0,\\ m\sigma_j(C) & \text{if } m\mid j \text{ and } j>0,\\ 0 & \text{if } m\nmid j.\end{cases}$$

Hence, assuming that m is even, from (5) we get

$$2(m|C|+1)\cdot m\sigma_{km}(C)=-m^2\sum_{j=1}^{k-1}\binom{km}{jm}\sigma_{jm}(C)\sigma_{(k-j)m}(C),\quad 0<k<\frac{p-1}{2m}.$$

Now taking $k=1$ yields $\sigma_m(C)=0$, and then subsequently $\sigma_{km}(C)=0$ for each $0<k<(p-1)/(2m)$, leading to a contradiction exactly as above.

This completes the proof of Lemma 1.

4. Proofs of Theorems 1 and 2: One Coset is Not Enough

For a prime p, let χ_p denote the quadratic character modulo p extended onto the whole field $\mathbb{F}_p$ by $\chi_p(0)=0$. We need the following well-known identity (which is equivalent, for instance, to [IR90, Chapter 5, Exercise 8]):

$$\sum_{x\in\mathbb{F}_p}\chi_p((x+a)(x+b))=\begin{cases} p-1 & \text{if } a=b,\\ -1 & \text{if } a\ne b,\end{cases}\qquad a,b\in\mathbb{F}_p. \tag{7}$$

Recall, that we are interested in the situation where $p \equiv 1 \pmod 4$, in which case $\chi_p(-1) = 1$; equivalently, $\chi_p(-x) = \chi_p(x)$ for all $x \in \mathbb{F}_p$.

Proof of Theorem 1. Clearly, it suffices to show that for $p > 13$ prime and $H < \mathbb{F}_p^\times$, one cannot have $H - H \stackrel{!}{=} \mathcal{R}_p$ or $H - H \stackrel{!}{=} \mathcal{N}_p$. For a contradiction, suppose that one of these relations holds true. Write $n := |H|$, so that $p = 2n(n-1)+1$. From Lemma 1 (as applied to a suitable coset of H in the case $H - H \stackrel{!}{=} \mathcal{N}_p$), we know that n is odd, implying $-1 \notin H$; hence, H is disjoint with $-H := \{-h \colon h \in H\}$.

For any $h_1, h_2 \in H$ with $h_1 \neq h_2$, either both $h_1^2 - h_2^2$ and $h_1 - h_2$ are quadratic residues, or they both are quadratic non-residues. In either case, their quotient h_1+h_2 is a quadratic residue; that is,

$$\chi_p(h_1+h_2) = 1, \quad h_1, h_2 \in H,\ h_1 \neq h_2. \tag{8}$$

We distinguish two cases, according to whether $H - H \stackrel{!}{=} \mathcal{R}_p$ or $H - H \stackrel{!}{=} \mathcal{N}_p$.

Suppose first that $H - H \stackrel{!}{=} \mathcal{R}_p$, and let in this case

$$\sigma(x) := \sum_{h \in H} \big(\chi_p(x+h) + \chi_p(x-h)\big), \quad x \in \mathbb{F}_p.$$

In view of (8) and our present assumption $H - H \stackrel{!}{=} \mathcal{R}_p$, for each $x \in H$ we have

$$\sigma(x) \geq (n-2) + (n-1) = 2n-3.$$

Along with $\sigma(-x) = \sigma(x)$ (following from $p \equiv 1 \pmod 4$ and $\chi_p(-1) = 1$ resulting from it), this yields

$$\sum_{x \in H \cup (-H)} \sigma^2(x) \geq 2n(2n-3)^2. \tag{9}$$

On the other hand, the sum extended over *all* $x \in \mathbb{F}_p$ can be computed explicitly:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_p} \sigma^2(x) &= \sum_{x \in \mathbb{F}_p} \sum_{h_1, h_2 \in H} \big(\chi_p(x+h_1) + \chi_p(x-h_1)\big)\big(\chi_p(x+h_2) + \chi_p(x-h_2)\big) \\
&= \sum_{h_1, h_2 \in H} \sum_{x \in \mathbb{F}_p} \big(\chi_p((x+h_1)(x+h_2)) + \chi_p((x-h_1)(x-h_2)) \\
&\qquad\qquad + \chi_p((x+h_1)(x-h_2)) + \chi_p((x-h_1)(x+h_2))\big) \\
&= 2pn - 4n^2 \\
&= 2n(2n^2 - 4n + 1),
\end{aligned} \tag{10}$$

as it follows from (7) and since $h_1 \neq -h_2$ whenever $h_1, h_2 \in H$ in view of $-1 \notin H$. Comparing (9) and (10) we conclude that $2n(2n-3)^2 \leq 2n(2n^2-4n+1)$, which simplifies to $(n-2)^2 \leq 0$ and thus yields $n = 2$, contrary to the assumption $p > 13$.

Addressing now the case where $H-H \overset{!}{=} \mathcal{N}_p$, we re-define the sum $\sigma(x)$ letting this time

$$\sigma(x) := \sum_{h\in H} \big(\chi_p(x+h) - \chi_p(x-h)\big), \quad x \in \mathbb{F}_p.$$

In view of (8) and the assumption $H-H \overset{!}{=} \mathcal{N}_p$, we have again

$$\sigma(x) \geq (n-2) + (n-1) = 2n-3, \quad x \in H.$$

Since $\sigma(-x) = -\sigma(x)$, we derive that

$$\sum_{x\in H\cup(-H)} \sigma^2(x) \geq 2n(2n-3)^2.$$

On the other hand, a computation similar to (10) gives

$$\sum_{x\in\mathbb{F}_p} \sigma^2(x) = 2pn = 2n(2n^2-2n+1).$$

As a result, $2n(2n-3)^2 \leq 2n(2n^2-2n+1)$, leading to $n \leq 4$. To complete the proof we notice that $n \leq 3$ correspond to $p \leq 13$, while $n=4$ yields $p=25$, which is composite. □

Proof of Theorem 2. The proof is a variation of that of Theorem 1.

Aiming at a contradiction, suppose that $p > 5$ is prime, $H < \mathbb{F}_p^\times$, $g \in \mathbb{F}_p^\times$, and $A := gH \cup \{0\}$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$. Since g is representable as a difference of two elements of A, we have $g \in \mathcal{R}_p$, and dilating A by the factor g^{-1} we can assume that, indeed, $g = 1$; that is, $A = H \cup \{0\}$.

Write $n := |A|$, so that $p = 2n(n-1)+1$ and $|H| = n-1$. From Lemma 1, we know that $|H|$ is odd, whence $-1 \notin H$ and therefore H is disjoint with $-H$.

For any $h \in H$ and $a_1, a_2 \in A$ with $a_1 \neq a_2$, both $a_1h - a_2h$ and $a_1 - a_2$ are quadratic residues, and so must be their quotient h; thus,

$$\chi_p(h) = 1, \quad h \in H. \tag{11}$$

Similarly,

$$\chi_p(h_1+h_2) = 1, \quad h_1, h_2 \in H,\ h_1 \neq h_2 \tag{12}$$

in view of $h_1 + h_2 = (h_1^2 - h_2^2)/(h_1 - h_2)$.

Let

$$\sigma(x) := \sum_{a\in A} \big(\chi_p(x+a) + \chi_p(x-a)\big), \quad x \in \mathbb{F}_p.$$

From (11) and (12), and since $A - A \overset{!}{=} \mathcal{R}_p$, we have

$$\sigma(x) \geq (n-2) + (n-1) = 2n-3, \quad x \in H$$

and

$$\sigma(0) = 2(n-1).$$

Observing that $\sigma(-x) = \sigma(x)$ we derive that

$$\sum_{x \in H \cup (-H) \cup \{0\}} \sigma^2(x) \ge 2(n-1)(2n-3)^2 + 4(n-1)^2 = 2(n-1)(4n^2 - 10n + 7).$$

On the other hand, a computation similar to (10) gives

$$\sum_{x \in \mathbb{F}_p} \sigma^2(x) = 2(n+1)p - 4n^2 = 2(n-1)(2n^2-1).$$

As a result, $4n^2 - 10n + 7 \le 2n^2 - 1$, implying $n \le 4$. The assumption $p > 5$ now gives $n = 3$; consequently, $p = 13$ and $|H| = 2$, whence $H = \{1, -1\}$. However, the set $A = \{0, 1, -1\} \subseteq \mathbb{F}_{13}$ does not have the property $A - A \overset{!}{=} \mathcal{R}_{13}$. □

5. Proofs of Claim 1 and Theorem 4

Proof of Claim 1. To see that the sums $a' + \nu a''$ are pairwise distinct, we notice that $a_1' + \nu a_1'' = a_2' + \nu a_2''$ with $(a_1', a_1'') \ne (a_2', a_2'')$ would result in $\nu = (a_1' - a_2')/(a_2'' - a_1'')$, while for $a_1', a_1'', a_2', a_2'' \in A$, both the numerator and the denominator are quadratic residues in view of $A - A \overset{!}{=} \mathcal{R}_p$.

It remains to show that every non-zero element of $\mathbb{F}_p$ has exactly $n(n+1)/2$ representations as a difference of two elements of the set $D := \{a' + \nu a'' \colon a', a'' \in A\}$.

Let ζ be a fixed primitive root of unity of degree p, and denote by $\mathbb{K}$ the pth cyclotomic field; that is, $\zeta \ne \zeta^p = 1$ and $\mathbb{K} = \mathbb{Q}[\zeta]$. Write $\alpha := \sum_{a \in A} \zeta^a$, so that $A - A \overset{!}{=} \mathcal{R}_p$ yields

$$|\alpha|^2 = n + \rho, \tag{13}$$

where

$$\rho := \sum_{x \in \mathcal{R}_p} \zeta^x = \frac{\sqrt{p} - 1}{2} \tag{14}$$

is a quadratic Gaussian period (see, for instance, [D82, Chapter 3,]).

Set $\delta := \sum_{d \in D} \zeta^d$; thus,

$$\delta = \sum_{a' \in A} \zeta^{a'} \cdot \sum_{a'' \in A} \zeta^{\nu a''} = \alpha \varphi(\alpha), \tag{15}$$

with $\varphi \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ defined by $\varphi(\zeta) = \zeta^\nu$. Let $\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ denote the complex conjugation automorphism. Since $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is abelian ([IR90, Chapter 13, §2, Corollary 2] or [M77, Page 18, Corollary 2]), we have

$$\varphi(|\alpha|^2) = \varphi(\alpha\tau(\alpha)) = \varphi(\alpha)\tau(\varphi(\alpha)) = |\varphi(\alpha)|^2. \tag{16}$$

From (13)–(16) and

$$\varphi(\rho) = \sum_{x\in\mathcal{R}_p} \zeta^{\nu x} = \sum_{x\in\mathcal{N}_p} \zeta^x = -1 - \sum_{x\in\mathcal{R}_p} \zeta^x = -1-\rho,$$

we obtain

$$\begin{aligned}|\delta|^2 &= |\alpha|^2|\varphi(\alpha)|^2 = |\alpha|^2\varphi(|\alpha|^2)\\ &= (n+\rho)(n-1-\rho) = \frac{n(n-1)}{2} = |D| + \frac{n(n+1)}{2}\sum_{x\in\mathbb{F}_p^\times}\zeta^x.\end{aligned}$$

Comparing this equality with

$$|\delta|^2 = |D| + \sum_{x\in\mathbb{F}_p^\times} r(x)\zeta^x,$$

where $r(x)$ is the number of representations of x as a difference of two elements of D, we conclude that $r(x) = n(n+1)/2$ for every $x \in \mathbb{F}_p^\times$. $\square$

We remark that the second assertion of Claim 1 can also be proved using the group ring approach. Namely, identifying subsets $A, D, \mathcal{R}_p, \mathcal{N}_p, \mathbb{F}_p^\times \subseteq \mathbb{F}_p$ with the corresponding elements of the group ring $\mathbb{Z}\mathbb{F}_p$, we have

$$D = AA^{(\nu)},\ AA^{(-1)} = n + \mathcal{R}_p,\ \mathcal{R}_p^{(\nu)} = \mathcal{N}_p,\ \text{and } \mathcal{R}_p\mathcal{N}_p = \frac{n(n-1)}{2}\,\mathbb{F}_p,$$

the last equality reflecting the well-known fact that for $p \equiv 1 \pmod 4$, every element of $\mathbb{F}_p^\times$ has exactly $\frac{p-1}{4}$ representations as a sum of quadratic residue and a quadratic non-residue. Hence, we have the chain of group ring equalities

$$\begin{aligned}DD^{(-1)} &= AA^{(\nu)}A^{(-1)}A^{(-\nu)} = (n+\mathcal{R}_p)(n+\mathcal{R}_p)^{(\nu)}\\ &= (n+\mathcal{R}_p)(n+\mathcal{N}_p) = n^2 + n\mathbb{F}_p^\times + \frac{n(n-1)}{2}\,\mathbb{F}_p^\times = n^2 + \frac{n(n+1)}{2}\,\mathbb{F}_p^\times,\end{aligned}$$

proving the assertion.

We now state the part of the Semi-primitivity Theorem that is relevant for our purposes. For co-prime integer $q, e \ge 1$, by $\langle q\rangle_e$ we denote the subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$, multiplicatively generated by q.

Theorem 6 ([La83, Theorem 4.5])**.** *Suppose that G is a finite abelian group of exponent e. If G possesses a (v,k,λ)-difference set, then for any prime q with $q \mid k-\lambda$ and $q \nmid e$, we have $-1 \notin \langle q\rangle_e$.*

To deduce Theorem 4 from Theorem 6, we apply the latter to the set D of Claim 1. Since

$$n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2} = \frac{p-1}{4},$$

we conclude that if $q \mid \frac{p-1}{4}$ is prime, then $\langle q\rangle_p$ is an odd-order subgroup of $\mathbb{F}_p^\times$; that is, $\mathrm{ord}_p(q)$ is odd. This proves Theorem 4.

6. Bi-quadratic Reciprocity and the Proof of Theorem 5

The proof of Theorem 5 relies on Lemmermeyer's biquadratic reciprocity law. To state it, we recall that the *rational biquadratic residue symbol* is defined for prime $p \equiv 1 \pmod 4$ and quadratic residue $b \in \mathcal{R}_p$ by

$$\left(\frac{b}{p}\right)_4 = \begin{cases} 1 & \text{if } b \text{ is a biquadratic residue modulo } p, \\ -1 & \text{if } b \text{ is not a biquadratic residue modulo } p. \end{cases}$$

Notice, that $(b/p)_4 \equiv b^{\frac{p-1}{4}} \pmod p$ implies multiplicativity of the rational biquadratic residue symbol.

For consistency, in this section we use the Legendre symbol $(\cdot/p)$ for the quadratic character modulo p (which was denoted $\chi_p(\cdot)$ in Section 4, mostly for typographical reasons).

Theorem 7 ([Le00, Proposition 5.5])**.** *Suppose that $p \equiv 1 \pmod 4$ is prime, and write $p = u^2 + v^2$ with u odd and v even. Suppose also that $q > 2$ is a prime with $(p/q) = 1$, and let c be an integer such that $c^2 \equiv p \pmod q$. Finally, let $q^* := (-1)^{(q-1)/2} q$, so that $(q^*/p) = 1$ by multiplicativity of the Legendre symbol and the quadratic reciprocity law. Then*

$$\left(\frac{q^*}{p}\right)_4 = \begin{cases} \left(\frac{c(v+c)}{q}\right) & \text{if } q \nmid v + c, \\ \left(\frac{2}{q}\right) & \text{if } q \mid v + c. \end{cases}$$

We remark that, strictly speaking, the case where $q \mid v + c$ is not addressed in [Le00], but it is easy to deduce from the case where $q \nmid v + c$. For, if $q \mid v + c$, then $q \nmid v - c$ in view of $q \nmid c$, and applying then the original Lemmermeyer's theorem with c replaced by $-c$, we get

$$\left(\frac{q^*}{p}\right)_4 = \left(\frac{-c(v-c)}{q}\right) = \left(\frac{-c(-2c)}{q}\right) = \left(\frac{2}{q}\right).$$

Proof of Theorem 5. Suppose that p is a prime and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$; thus, $p = 2n(n-1) + 1$ where $n := |A|$. From Corollary 3, we have $p \equiv 5 \pmod 8$, whence

$$\left(\frac{-1}{p}\right)_4 = (-1)^{\frac{p-1}{4}} = -1. \tag{17}$$

Let u and v denote the odd and the even of the two numbers $n-1$ and n, respectively; notice that this is consistent with the notation of Theorem 7 as $p =$

$(n-1)^2+n^2=u^2+v^2$. Since $p\equiv 5 \pmod 8$, a prime q divides $\frac{p-1}{4}=\frac12 uv$ if and only if it is odd and divides either u, or v. In this case $p\equiv 1 \pmod q$, and we apply Theorem 7 with $c=1$ to obtain

$$\left(\frac{q^*}{p}\right)_4=\begin{cases}\left(\frac{v+1}{q}\right) & \text{if } q\nmid v+1,\\ \left(\frac{2}{q}\right) & \text{if } q\mid v+1,\end{cases} \tag{18}$$

where $q^*:=(-1)^{(q-1)/2}q$. On the other hand, Theorem 4 shows that q is a biquadratic residue modulo p, and therefore using (17) we get

$$\left(\frac{q^*}{p}\right)_4=\left(\frac{(-1)^{(q-1)/2}}{p}\right)_4\left(\frac{q}{p}\right)_4=\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right)_4=\left(\frac{-1}{q}\right). \tag{19}$$

From(18) and (19),

$$\left(\frac{v+1}{q}\right)=\left(\frac{-1}{q}\right) \quad \text{if } q\nmid v+1, \tag{20}$$

and

$$\left(\frac{2}{q}\right)=\left(\frac{-1}{q}\right) \quad \text{if } q\mid v+1. \tag{21}$$

If $q\mid v$, then the former of these equalities immediately gives $q\in\{1,5\} \pmod 8$. If $q\mid u$, we distinguish two further sub-cases: $q\mid v+1$ and $q\nmid v+1$. If $q\mid v+1$, then (21) gives $q\in\{1,3\} \pmod 8$. If $q\nmid v+1$, then $u\in\{v-1,v+1\}$ along with our present assumption $q\mid u$ show that $u=v-1$; thus, $q\mid v-1$, and (20) leads to the same conclusion $q\in\{1,3\} \pmod 8$ as above.

We have shown that for a prime $q>2$, if q divides the even of the two numbers $n-1$ and n, then $q\equiv 1 \pmod 8$ or $q\equiv 5 \pmod 8$, and if q divides the odd of these two numbers, then $q\equiv 1 \pmod 8$ or $q\equiv 3 \pmod 8$. This is equivalent to the assertion of Theorem 5. □

7. Proof of Theorem 3: M_A Lies Above the Order-G_p Subgroup of $\mathbb{F}_p^\times$

In this section and the Appendix we use several basic algebraic number theory facts, such as for instance:

i) the Galois group of the mth cyclotomic field is isomorphic to the group of units $(\mathbb{Z}/m\mathbb{Z})^\times$; hence, it is abelian;
ii) if p and q are distinct odd primes, then, letting $f:=\operatorname{ord}_p(q)$, the principal ideal (q) in the pth cyclotomic field splits into a product of $(p-1)/f$ pairwise distinct prime ideals, all of which are fixed by the order-f subgroup of the corresponding Galois group;

iii) Kronecker's theorem: an algebraic integer all of whose algebraic conjugates lie on the unit circle is a root of unity; consequently, any cyclotomic integer of modulus 1 is a root of unity;

iv) if m is odd, then the only roots of unity of the mth cyclotomic field are the roots of degree $2m$.

The proofs can be found in any standard algebraic number theory textbook, as [IR90] or [M77].

Proof of Theorem 3. Suppose that p is a prime and $A \subseteq \mathbb{F}_p$ satisfies $A - A \overset{!}{=} \mathcal{R}_p$. Write $n := |A|$, so that $p = 2n(n-1)+1$. Let ζ be a primitive root of unity of degree p, and denote by $\mathbb{K}$ the pth cyclotomic field (thus, $\mathbb{K} = \mathbb{Q}[\zeta]$), and by $\mathcal{O}$ the ring of integers of $\mathbb{K}$. As in the proof of Claim 1, write $\alpha := \sum_{a\in A} \zeta^a$, so that $\alpha \in \mathcal{O}$ and

$$|\alpha|^2 = n + \rho \tag{22}$$

with

$$\rho := \sum_{x\in\mathcal{R}_p} \zeta^x = \frac{\sqrt{p}-1}{2}. \tag{23}$$

It is well known that every rational prime $q \neq p$ splits in $\mathcal{O}$ into a product of $(p-1)/\operatorname{ord}_p(q)$ pairwise distinct prime ideals, all of which are fixed by the subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ of order $\operatorname{ord}_p(q)$. The intersection of these subgroups over all primes $q \mid \frac{p-1}{4}$ is the subgroup $H \le \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ of order $|H| = G_p$, and since, by (22), α is a divisor of $n+\rho$, which in turn is a divisor of $\frac{p-1}{4} = (n+\rho)(n-1-\rho)$, we conclude that the ideal generated by α is fixed by H. Hence, for every automorphism $\varphi \in H$ there exists a unit $u \in \mathcal{O}$ (depending on φ) such that

$$\varphi(\alpha) = u\alpha. \tag{24}$$

Since p is a quadratic residue modulo every odd prime q dividing $p-1$, by quadratic reciprocity, q is a quadratic residue modulo p; that is, $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. This shows that $\operatorname{ord}_p(q)$ is a divisor of $(p-1)/2$. As a result, G_p divides $(p-1)/2$; that is, H is contained in the subgroup of order $(p-1)/2$, which is easily seen to have $\mathbb{Q}[\sqrt{p}]$ as its fixed field. Therefore, re-using equality (16) from the proof of Claim 1 and in view of (22), for every automorphism $\varphi \in H$ we have

$$|\varphi(\alpha)|^2 = \varphi(|\alpha|^2) = n + \rho = |\alpha|^2.$$

Comparing this with (24), we conclude that $|u| = 1$. From the fact that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is abelian it follows then that all algebraic conjugates of u have modulus 1, and by Kronecker's theorem u is a root of unity; thus, either $u = \zeta^v$, or $u = -\zeta^v$ with some $v \in \mathbb{F}_p$ depending on φ. The latter option is ruled out by considering traces from $\mathbb{K}$ to

$\mathbb{Q}$: we have $\operatorname{tr}(\varphi(\alpha)) = \operatorname{tr}(\alpha)$ and $\operatorname{tr}(-\zeta^v\alpha) \equiv -\operatorname{tr}(\alpha) \pmod p$, while $\operatorname{tr}(\alpha) \equiv -n \not\equiv 0 \pmod p$. Therefore,

$$\varphi(\alpha) = \zeta^v\alpha; \quad \varphi \in H,\ v = v(\varphi) \in \mathbb{F}_p. \tag{25}$$

Recalling the definition of α and identifying $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ with $\mathbb{F}_p^\times$, we can interpret (25) as saying that for every $\varphi \in H < \mathbb{F}_p^\times$, there exists $v = v(\varphi) \in \mathbb{F}_p$ such that the dilate $\varphi A = \{\varphi a\colon a \in A\}$ satisfies $\varphi A = A + v$; that is, φ is a multiplier of A. □

Appendix: An Algebraic Number Theory Restatement

We aim here to pursue a little further the algebraic approach that was employed in the proofs of Claim 1 and Theorem 3, in the hope that it can ultimately give more insights into the problem. We keep using the notation introduced in these proofs: namely, given a prime p, we denote by ζ a fixed primitive root of unity of degree p, by $\mathbb{K}$ the pth cyclotomic field, by $\mathcal{O}$ the ring of integers of $\mathbb{K}$, and we let $\rho := (\sqrt{p}-1)/2$. By tr we denote the trace function from $\mathbb{K}$ to $\mathbb{Q}$. Our goal is to prove the two following results.

Proposition 1. *Let p be a prime number. For a subset $A \subseteq \mathbb{F}_p$ with $A - A \overset{!}{=} \mathcal{R}_p$ to exist, it is necessary and sufficient that $p = 2n(n-1)+1$ with an integer n, and that there is an algebraic integer $\alpha \in \mathcal{O}$ such that $|\alpha|^2 = n+\rho$ and $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$ for every integer k.*

Proposition 2. *Let p be a prime of the form $p = 2n(n-1)+1$ with n an integer. For an algebraic integer $\alpha \in \mathcal{O}$ with $|\alpha|^2 = n+\rho$ to exist, it is necessary and sufficient that for every prime q dividing $p-1$ to an odd power, the order $\operatorname{ord}_p(q)$ is odd.*

To prove Proposition 1, we need

Lemma 2. *Let p be a prime and $n \in [1, p-1]$ an integer. In order for $\alpha \in \mathcal{O}$ to satisfy $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$ for every integer k, it is necessary and sufficient that $\alpha = \sum_{a\in A}\zeta^a$, where A is an n-element subset of $\mathbb{F}_p$.*

Proof. It is readily seen that the condition is sufficient: if $\alpha = \sum_{a\in A}\zeta^a$ with $A \subseteq \mathbb{F}_p$ and $|A| = n$, then

$$\operatorname{tr}(\alpha\zeta^{-k}) = \begin{cases} -n & \text{if } k \notin A, \\ p-n & \text{if } k \in A. \end{cases}$$

To prove necessity, write $\alpha = \sum_{x\in\mathbb{F}_p} a_x\zeta^x$ with integer coefficients a_x. For every $k \in \mathbb{Z}$ we have then

$$\operatorname{tr}(\alpha\zeta^{-k}) = pa_k - \sum_{x\in\mathbb{F}_p} a_x$$

(where k in the right-hand side is identified with its canonical image in $\mathbb{F}_p$), and the assumption $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$ implies that the coefficients a_x attain at most two distinct integer values. Since adding simultaneously the same integer to all a_x does not affect the value of the sum $\sum_{x\in\mathbb{F}_p} a_x\zeta^x$, we can assume without loss of generality that actually at most one value assumed by a_x is distinct from 0; hence, writing $A := \{x \in \mathbb{F}_p \colon a_x \neq 0\}$, there is an integer c such that

$$\alpha = c \sum_{a\in A} \zeta^a. \tag{26}$$

In fact, the subset $A \subseteq \mathbb{F}_p$ is proper and non-empty and $c \neq 0$, as otherwise we would have $\alpha = 0$ which is inconsistent with $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$. Consequently, (26) implies that $\operatorname{tr}(\alpha\zeta^{-k})$ assumes exactly two distinct values, both divisible by c. Observing, on the other hand, that $\gcd(-n, p-n) = \gcd(n, p) = 1$, we conclude that $c \in \{-1, 1\}$. Replacing now A with its complement in $\mathbb{F}_p$, if necessary, we can assume that, indeed, $c = 1$ holds. Thus, $\alpha = \sum_{a\in A} \zeta^a$, and it remains to notice that this yields $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-|A|, p-|A|\}$, whence $|A| = n$. □

Proof of Proposition 1. We know from Lemma 2 (see also the proofs of Claim 1 and Theorem 3) that if $A - A \stackrel{!}{=} \mathcal{R}_p$ for a subset $A \subseteq \mathbb{F}_p$ then, writing $n := |A|$ and $\alpha := \sum_{a\in A} \zeta^a$, we have $p = 2n(n-1)+1$, $|\alpha|^2 = n + \rho$, and $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$ for every integer k.

Conversely, suppose that $p = 2n(n-1)+1$ and that for some $\alpha \in \mathcal{O}$ we have $|\alpha|^2 = n + \rho$ and $\operatorname{tr}(\alpha\zeta^{-k}) \in \{-n, p-n\}$ for every integer k. By Lemma 2, there is an n-element subset $A \subseteq \mathbb{F}_p$ such that $\alpha = \sum_{a\in A} \zeta^a$. Hence,

$$\sum_{x\in\mathcal{R}_p} \zeta^x = \rho = |\alpha|^2 - n = \sum_{\substack{a',a''\in A\\ a'\neq a''}} \zeta^{a'-a''},$$

implying $A - A \stackrel{!}{=} \mathcal{R}_p$. □

Proof of Proposition 2. Consider a prime divisor q of $p-1$ and denote by v the power to which q divides $(p-1)/4$; thus, v is either equal, or smaller by 2 than the power to which q divides $p-1$. Since $p \equiv 1 \pmod q$ and, consequently, p is a square mod q, if q is odd, then it splits into two ideal primes in $\mathbb{Q}(\sqrt{p})$. This conclusion stays true also if $q = 2$ and $v > 0$: for, in this case $p \equiv 1 \pmod 8$ (see, for instance, [IR90, Propositions 13.1.3 and 13.1.4] or [M77, Chapter 3, Theorem 25]). Now the decomposition

$$\frac{p-1}{4} = (n+\rho)(n-1-\rho)$$

and the fact that $n+\rho$ and $n-1-\rho$ are co-prime elements of $\mathbb{Q}(\sqrt{p})$ show that the v th power of one of the two ideal primes into which q splits divides $n+\rho$, while the v th power of another one divides $n-1-\rho$. Denote by $\mathfrak{q}$ the prime whose v th power divides $n+\rho$; we thus have $(n+\rho)=\mathfrak{q}^v\mathfrak{I}$, where $\mathfrak{I}<\mathcal{O}$ is an ideal co-prime with q.

Write $f:=\mathrm{ord}_p(q)$, so that q splits into $(p-1)/f$ pairwise distinct ideal primes in $\mathcal{O}$ and, accordingly, $\mathfrak{q}$ splits into $k:=(p-1)/(2f)$ pairwise distinct ideal primes: $\mathfrak{q}=\mathfrak{q}_1\dots\mathfrak{q}_k$, where each $\mathfrak{q}_i$ is stable under the subgroup $H<\mathrm{Gal}(\mathbb{Q}/\mathbb{K})$ of order f. Assuming $|\alpha|^2=n+\rho$ and observing that $|\alpha|^2=\alpha\tau(\alpha)$, where τ is the complex conjugation automorphism of $\mathbb{K}$, we thus have

$$(\alpha)\tau((\alpha))=\mathfrak{q}_1^v\dots\mathfrak{q}_k^v\,\mathfrak{I}. \tag{27}$$

Suppose now that f is even, so that $\tau\in H$ and, consequently, $\tau(\mathfrak{q}_i)=\mathfrak{q}_i$ for each $i\in[1,k]$. Comparing this with (27) we conclude that the factor $\mathfrak{q}_i^v$ in its right-hand side must split evenly between the two factors (α) and $\tau((\alpha))$; therefore, v must be even. This proves necessity.

To prove sufficiency we invoke the Hasse norm theorem [J73, Theorem V.4.5] which says that if K is a cyclic extension of a number field L, then an element of L is the norm (from K to L) of an element of K if and only if it is a norm locally everywhere. The reader will see that, in fact, the theorem also gives necessity; however, we prefer to keep the simple "elementary" argument presented above.

Specified to our situation, Hasse's theorem gives the following. Let $\mathbb{K}^+$ be the real subfield of $\mathbb{K}$. For a prime ideal $\mathfrak{p}\subset\mathbb{K}^+$, denote by $\mathbb{K}^+_{\mathfrak{p}}$ the completion of $\mathbb{K}^+$ at $\mathfrak{p}$, and by $\mathbb{K}_{\mathfrak{p}}$ the corresponding completion of $\mathbb{K}$; thus, $\mathbb{K}_{\mathfrak{p}}=\mathbb{K}\mathbb{K}^+_{\mathfrak{p}}$. Then, according to the Hasse theorem, $n+\rho$ is a norm from $\mathbb{K}$ to $\mathbb{K}^+$ if and only if it is a norm from $\mathbb{K}_{\mathfrak{p}}$ to $\mathbb{K}^+_{\mathfrak{p}}$ for every prime $\mathfrak{p}$ of $\mathbb{K}^+$, including the infinite primes.

Accordingly, let $\mathfrak{p}\subset\mathbb{K}^+$ be a prime. We first show that $n+\rho$ is always a norm from $\mathbb{K}_{\mathfrak{p}}$ to $\mathbb{K}^+_{\mathfrak{p}}$ whenever $\mathfrak{p}\nmid\frac{p-1}{4}$. For notational convenience, we write below $\mathbb{K}^{\surd}:=\mathbb{Q}(\sqrt{p})$.

If $\mathfrak{p}$ is an infinite prime, then it is a real prime and $\mathbb{K}^+_{\mathfrak{p}}$ is the field $\mathbb{R}$ of real numbers, as $\mathbb{K}^+$ is totally real. Furthermore, every real square, hence every positive real number, and in particular $n+\rho$, is a norm from the quadratic extension $\mathbb{K}_{\mathfrak{p}}=\mathbb{C}$.

If $\mathfrak{p}$ is a finite prime dividing p, then it is unique with this property, and p is totally and tamely ramified in $\mathbb{K}$. Thus the extension $\mathbb{K}_{\mathfrak{p}}/\mathbb{K}^+_{\mathfrak{p}}$ is a tamely ramified quadratic extension. Since $n+\rho$ is not divisible by $\mathfrak{p}$, it is a unit in $\mathbb{K}^+_{\mathfrak{p}}$, so by [Se79, Chapter V, §3, Proposition 5] it is a norm from $\mathbb{K}_{\mathfrak{p}}$ if and only if it is a square modulo $\mathfrak{p}$. As the residue field of $\mathbb{K}_{\mathfrak{p}}$ modulo $\mathfrak{p}$ is $\mathbb{F}_p$, this is equivalent to $n+\rho$ being a square modulo the uniformizer $\sqrt{p}$ of $\mathbb{K}^{\surd}\mathbb{Q}_p$, where $\mathbb{Q}_p$ is the field of p-adic rationals, i.e. the completion of $\mathbb{Q}$ at p. Now $n+\rho\equiv n-\frac12 \pmod{\sqrt{p}}$, with the congruence in (a localization of) the ring of integers of $\mathbb{K}^{\surd}$. At the same time, $p=2n(n-1)+1$ implies $n-\frac12\equiv n^2$

(mod p). It follows that $n - \frac{1}{2} \equiv n^2 \pmod{\sqrt{p}}$, hence $n + \rho \equiv n^2 \pmod{\sqrt{p}}$, and so $n + \rho \equiv n^2 \pmod{\mathfrak{p}}$.

Finally, if $\mathfrak{p}$ is a finite prime not dividing p (and also not dividing $\frac{p-1}{4}$), then the extension $\mathbb{K}_\mathfrak{p}/\mathbb{K}^+_\mathfrak{p}$ is unramified, in which case every unit of $\mathbb{K}^+_\mathfrak{p}$ is a norm from $\mathbb{K}_\mathfrak{p}$ [Se79, Chapter V, §2, Corollary to Proposition 3]. But $n+\rho$ is a unit of $\mathbb{K}^+_\mathfrak{p}$, as follows from the observation that $N_{\mathbb{K}^\checkmark/\mathbb{Q}}(n+\rho) = \frac{p-1}{4}$ is not divisible by $\mathfrak{p}$.

We have thus shown that $n + \rho$ is always a norm from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$ whenever $\mathfrak{p} \nmid \frac{p-1}{4}$, and it remains to determine when $n + \rho$ is a norm for the primes $\mathfrak{p} \mid \frac{p-1}{4}$. Fix such a prime $\mathfrak{p} \subseteq \mathbb{K}^+$, and let $\mathfrak{q}$ be the prime in $\mathbb{K}^\checkmark$ lying below $\mathfrak{p}$, and q be the rational prime lying below $\mathfrak{p}$ and $\mathfrak{q}$. Also, let $\mathfrak{q}'$ be the conjugate of $\mathfrak{q}$ over $\mathbb{Q}$; since q splits into two primes in $\mathbb{K}^\checkmark$ (see the very beginning of the proof for the explanation), we have the prime factorization $q\mathcal{O}_{\mathbb{K}^\checkmark} = \mathfrak{q}\mathfrak{q}'$.

Let $v_\mathfrak{p}, v_\mathfrak{q}, v_{\mathfrak{q}'}$, and v_q be the valuations on $\mathbb{K}^+, \mathbb{K}^\checkmark, \mathbb{K}^\checkmark$, and $\mathbb{Q}$, corresponding to $\mathfrak{p}, \mathfrak{q}, \mathfrak{q}'$, and q, respectively. Since q is unramified in $\mathbb{K}$ (the only ramified prime in $\mathbb{K}$ is p), we may assume that all these valuations are normalized; that is, their value groups are $\mathbb{Z}$.

Trivially, $n + \rho$ is a norm from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$ if $\mathbb{K}_\mathfrak{p} = \mathbb{K}^+_\mathfrak{p}$. This happens if and only if $\mathfrak{p}$ splits completely in $\mathbb{K}$; that is, if and only if the complex conjugation automorphism τ does not lie in the decomposition group of a prime $\mathfrak{P} \subset \mathbb{K}$ lying above $\mathfrak{p}$. Since the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic, τ is its unique involution. Hence for $\mathbb{K}_\mathfrak{p} = \mathbb{K}^+_\mathfrak{p}$ to hold it is necessary and sufficient that the decomposition group of $\mathfrak{P}$ has odd order; equivalently, the inertia degree of q in $\mathbb{K}/\mathbb{Q}$ is odd; that is, the order $\mathrm{ord}_p(q)$ is odd. Thus, if $\mathrm{ord}_p(q)$ is odd, then $n + \rho$ is a norm from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$.

To complete the proof, we show that for $\mathrm{ord}_p(q)$ even, $n + \rho$ is a norm from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$ if and only if $v_q(\frac{p-1}{4})$ is also even. So assume now that $\mathrm{ord}_p(q)$ is even. Since $\mathbb{K}_\mathfrak{p}/\mathbb{K}^+_\mathfrak{p}$ is an unramified quadratic extension, by [Se79, Chapter V, §2, Corollary to Proposition 3], the group of norms from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$ inside $(\mathbb{K}^+_\mathfrak{p})^\times$ is $\langle \pi_\mathfrak{p}^2 \rangle \times U_{\mathbb{K}^+_\mathfrak{p}}$, where $\pi_\mathfrak{p}$ is a uniformizer of $\mathbb{K}^+_\mathfrak{p}$ (i.e. $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$) and $U_{\mathbb{K}^+_\mathfrak{p}}$ is the unit group of $\mathbb{K}^+_\mathfrak{p}$. Thus, $n + \rho$ is a norm from $\mathbb{K}_\mathfrak{p}$ to $\mathbb{K}^+_\mathfrak{p}$ if and only if $v_\mathfrak{p}(n + \rho)$ is even. Let $\rho' := \frac{-\sqrt{p}-1}{2}$ be the conjugate of ρ over $\mathbb{Q}$. Observe that

$$0 = v_q(2n-1) = v_\mathfrak{q}(2n-1) = v_\mathfrak{q}(n+\rho+n+\rho') \geq \min\{v_\mathfrak{q}(n+\rho), v_\mathfrak{q}(n+\rho')\}$$

implies

$$\min\{v_\mathfrak{q}(n+\rho), v_\mathfrak{q}(n+\rho')\} = 0, \tag{28}$$

and also that

$$v_q(\tfrac{p-1}{4}) = v_\mathfrak{q}(\tfrac{p-1}{4}) = v_\mathfrak{q}((n+\rho)(n+\rho')) = v_\mathfrak{q}(n+\rho) + v_\mathfrak{q}(n+\rho'). \tag{29}$$

If $v_q(\frac{p-1}{4})$ is odd, then either $v_{\mathfrak{q}}(n+\rho)$ is odd, or $v_{\mathfrak{q}}(n+\rho') = v_{\mathfrak{q}'}(n+\rho)$ is odd; hence, either $n+\rho$ is not a norm from $\mathbb{K}_{\mathfrak{p}}$ to $\mathbb{K}^+_{\mathfrak{p}}$, or it is not a norm from $\mathbb{K}_{\mathfrak{p}'}$ to $\mathbb{K}^+_{\mathfrak{p}'}$ for some prime $\mathfrak{p}'$ of $\mathbb{K}^+$ lying above $\mathfrak{q}'$. It follows that if $v_q(\frac{p-1}{4})$ is odd, then $n+\rho$ is not a norm from $\mathbb{K}$ to $\mathbb{K}^+$. On the other hand, if $v_q(\frac{p-1}{4})$ is even, then by (28) and (29), $v_{\mathfrak{q}}(n+\rho)$ is also even and, similarly, $v_{\mathfrak{q}'}(n+\rho) = v_{\mathfrak{q}}(n+\rho')$ is even. Therefore if $v_q(\frac{p-1}{4})$ is even, then $n+\rho$ is a norm from $\mathbb{K}_{\mathfrak{p}}$ to $\mathbb{K}^+_{\mathfrak{p}}$ for all $\mathfrak{p}$ lying above q.

This completes the proof. $\square$

References

[B95] W.J. Broughton, *Symmetric Designs, Difference Sets, and Autocorrelations of Finite Binary Sequences*, Ph.D. Thesis, California Institute of Technology, Pasadena, CA (1995).

[D82] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics, Vol. 74, Springer (1982).

[IR90] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (Second edition)*, Graduate Texts in Mathematics, 84. Springer-Verlag, New York (1990).

[J73] G. Janusz, *Algebraic Number Fields*, Academic Press (1973).

[La83] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Series **74**, Cambridge University Press (1983).

[Le00] F. Lemmermeyer, *Reciprocity Laws: from Euler to Eisenstein*, Berlin: Springer (2000).

[M77] D. Marcus, *Number Fields*, Springer-Verlag, New York – Heidelberg (1977).

[Sa12] A. Sárközy, On additive decompositions of the set of quadratic residues modulo p, *Acta Arith.* **155** (2012), 41–51.

[Se79] J.-P. Serre, *Local Fields*, New York: Springer 1979

[Sh14] Shkredov, I.D., Sumsets in quadratic residues, *Acta Arith.* **164** (3) (2014), 221–243.

Department of Mathematics, The university of Haifa at Oranim, Tivon 36006, Israel

E-mail address: seva@math.haifa.ac.il

Department of Mathematics, Technion – Israel Institute of Technology, Haifa 32000, Israel

E-mail address: sonn@math.technion.ac.il