Math. J. Okayama Univ. 39 (1989), 1–8

SETS WHICH CONTAIN A QUADRATIC RESIDUE MODULO p FOR ALMOST ALL p

MICHAEL A. FILASETA and DAVID R. RICHMAN

1. Introduction. M. Hall, Jr. showed ([2, p. 759] and [3, Th. 3, p. 57]) that if an integer is a quadratic residue modulo p for all but finitely many primes p, then it is a square. Define the density of a set P of primes to be the limit, as x tends to infinity, of (the number of primes $\leq x$ in P)/(the number of primes $\leq x$), provided the limit exists. If the density of the set of primes with a given property is 1, then we say that the given property holds for almost all primes. One can establish easily from the result of M. Hall, Jr. (together with the law of quadratic reciprocity and the Prime Number Theorem for primes in arithmetic progressions [4, p.404]) that if an integer is a quadratic residue modulo p for almost all primes p, then it is a square. Furthermore, if u and v are integers such that, for almost all primes p, either u or v is a quadratic residue modulo p, then either u or v is a square. This latter fact was proved by Funakura and Morimoto [1, p.138], and was used to establish a Hasse principle for 2×2 matrices. This paper describes generalizations of these results ; in particular the following theorem is established.

Theorem 1. *Let S denote a finite set of non-zero integers. The following conditions are equivalent.*

(i) *For almost all primes p, the set S contains a quadratic residue modulo p.*

(ii) *There is an odd-sized subset T of S such that the product of the elements of T is a square.*

(iii) *For every prime p not dividing the product of the elements of S, S contains a quadratic residue modulo p.*

Later, in Theorem 2, we will describe necessary and sufficient conditions for a finite set S of integers to have the following property : for every map $f: S \to \{-1, 1\}$, there is a prime $p = p(f)$ such that $f(x) = (x/p)$ for every x in S. Theorem 3 and its Corollaries will describe conditions which guarantee that an infinite set of integers contains a quadratic residue modulo p or a quadratic non-residue modulo p for almost all primes p. Finally, Theorem 4 will show that Theorems 1 and 2 do not hold for infinite sets of integers.

2. Proofs of Theorem 1 and Related Results. Let (x/p) denote the Jacobi symbol. Let M denote the set of completely multiplicative functions from the non-zero integers to $\{-1,1\}$. We now describe three different proofs of Theorem 1, all of which use the following Lemma.

Lemma. *Let S denote a finite set of non-zero integers and let $f \in M$; then there is an odd prime p such that $f(x) = (x/p)$ for every x in S.*

Proof. Let s denote the product of the elements of S. For every odd prime factor q of s, let $r(q)$ denote an integer such that $(r(q)/q) = f(q)$. If $f(2) = -1$, define $r(2) = f(-1)+4$; otherwise, define $r(2) = f(-1)$. Let p denote a prime such that $p \equiv f(-1)\, r(q) \pmod q$ for every odd prime factor q of s and $p \equiv r(2) \pmod 8$. Observe that p is odd and $(2/p) = f(2)$.

Let q denote an odd prime factor of s. If $q \equiv 1 \pmod 4$ or $f(-1) = 1$, then q or p is congruent to $1 \pmod 4$ and, by the law of quadratic reciprocity,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{f(-1)\, r(q)}{q}\right) = \left(\frac{r(q)}{q}\right) = f(q).$$

If $q \equiv -1 \pmod 4$ and $f(-1) = -1$, then $p \equiv q \equiv -1 \pmod 4$ and

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{-r(q)}{q}\right) = \left(\frac{r(q)}{q}\right) = f(q).$$

Thus, $(w/p) = f(w)$ for every prime factor w of s. Note also that $(-1/p) = f(-1)$. Therefore, $(x/p) = f(x)$ for every x in S.

First Proof of Theorem 1. Let s denote the product of the elements of S and let p and p' denote primes. The law of quadratic reciprocity implies that if $p \equiv p' \pmod{4s}$, then $(x/p) = (x/p')$ for every x in S. This observation and the Prime Number Theorem for primes in arithmetic progressions [4, p.404] imply that

(1) there is a prime p such that $(x/p) = -1$ for every x in S

$\Leftrightarrow$ the density (which necessarily exists) of the set of primes p that satisfy $(x/p) = -1$ for every x in S is greater than or equal to $1/\phi(4s)$.

It is easy to see that (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) in Theorem 1. Suppose now that statement (ii) does not hold. It will be shown, by induction on the size of S, that there is a map $g \in M$ such that $g(x) = -1$ for every x in S.

If $S = \{x\}$, then x is not a square because statement (ii) does not hold.

Therefore, there is a map $g \in M$ such that $g(x) = -1$. Suppose now that S has more than one element and let $y \in S$. The induction hypothesis implies that there is a map $g_y \in M$ such that $g_y(x) = -1$ for every x in $S-\{y\}$. If $g_y(y) = -1$ for some y in S, then $g_y(x) = -1$ for every x in S. If $g_y(y) = 1$ for every y in S and the size of S is even, then define g to be the product of the maps g_y, as y ranges over the elements of S. Observe that in this case $g(x) = -1$ for every x in S. Suppose finally that $g_y(y) = 1$ for every y in S and the size of S is odd. The number s, i.e., the product of the elements of S, is not a square because statement (ii) does not hold. Therefore, there is a map h in M such that $h(s) = -1$. Let $T = h^{-1}(\{-1\}) \cap S$ and observe that the size of T is odd. Let $g = h \prod_{t \in T} g_t$ and observe that $g(x) = -1$ for every x in S. Thus, in all cases there is a map g in M such that $g(x) = -1$ for every x in S. Therefore, the Lemma and statement (1) imply that statement (i) of the theorem does not hold.

Second Proof of Theorem 1. Since (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) in Theorem 1, it suffices to show that (i) $\Rightarrow$ (ii). Let F_2 denote the field of size two and let h denote the isomorphism from the multiplicative group $\{-1, 1\}$ to the additive group of F_2. Let $x_1, x_2, \cdots, x_n$ be a listing of the elements of S and, for every map g in M, define

$$r(g) = (h(g(x_1)), h(g(x_2)), \cdots, h(g(x_n))) \in (F_2)^n.$$

Let $R = \{r(g) : g \in M\}$ and note that $r(fg) = r(f) + r(g)$ for all $f, g \in M$. Therefore, R is a vector subspace of $(F_2)^n$.

If $V \subset (F_2)^n$, let $V^{\perp}$ denote the set of vectors w in $(F_2)^n$ such that $vw^T = 0$ for every v in V. For every subset T of S, define $v(T) = (b_1, b_2, \cdots, b_n)$, where $b_i = 1$ if x_i lies in T and $b_i = 0$ otherwise. Observe that

(2) the product of the elements of T is a square
$\Leftrightarrow \sum_{x \in T} h(g(x)) = 0$ for every g in M
$\Leftrightarrow v(T) \in R^{\perp}$.

Therefore,

(3) statement (ii) of the theorem does not hold
$\Leftrightarrow$for every odd-sized subset T of S, $v(T)$ does not lie in $R^{\perp}$
$\Leftrightarrow R^{\perp} \subseteq \{(1, 1, \cdots, 1)\}^{\perp}$
$\Leftrightarrow R^{\perp\perp} \supseteq \{(1, 1, \cdots, 1)\}^{\perp\perp}$
$\Leftrightarrow R$ contains $(1, 1, \cdots, 1)$ (because $R^{\perp\perp} = R$)
$\Leftrightarrow$there is an element g in M such that $g(x) = -1$ for every x in S
$\Leftrightarrow$statement (i) of the theorem does not hold (by the Lemma and (1)).

Third Proof of Theorem 1. As in the first proof of the theorem, it suffices to establish the following claim :

Claim. If statement (ii) of the theorem does not hold, then there is a map g in M such that $g(x) = -1$ for every x in S.

Let q denote a prime which does not divide the product of the elements of S and define $S^* = \{x : x \in S \text{ and } x > 0\} \cup \{q|x| : x \in S \text{ and } x < 0\}$. Note that it suffices to establish the claim for S^* ; therefore, we assume for the rest of the proof that every element of S is positive.

Let s denote the product of the elements of S and suppose that statement (ii) of the theorem does not hold. The claim will be established by induction on s. The induction hypothesis allows us to reduce to the case that every element of S is square-free ; assume that we are in this case. For every prime factor p of s, define $S_p = \{x \in S : p \nmid x\} \cup \{x/p : x \in S \text{ and } p|x\}$.

Case 1. There is a prime p dividing s such that, for every odd-sized subset T of S_p, the product of the elements of T is not a square.

The induction hypothesis implies that there is a map h in M such that $h(x) = -1$ for every x in S_p. Let g denote an element of M such that $g(x) = h(x)$ for every x in S_p and $g(p) = 1$. Observe that $g(x) = -1$ for every x in S, so g has the desired properties.

Case 2. For every prime factor p of s, p lies in S.

Let g denote an element of M such that $g(p) = -1$ for every prime factor p of s. Since statement (ii) of the theorem does not hold and every element of S is square-free, every element of S is a product of an odd number of primes. Therefore, $g(x) = -1$ for every x in S.

Case 3. There is a prime p dividing s and an odd-sized subset T^* of S_p such that p does not lie in S and the product of the elements of T^* is a square.

Let $T_1 = \{px : x \in T^* - S\}$ and $T = T_1 \cup (T^* \cap S)$. Note that $T \subset S$ (because $T^* \subset S_p$) and the size of T is odd (because the size of T equals the size of T^*). Therefore, since condition (ii) of Theorem 1 does not hold, the product of the elements of T is not a square. Note also that the product of the elements of T equals $p^{|T_1|}$ (the product of the elements of T^*), which equals $p^{|T_1|}m^2$ for some integer m. Therefore $|T_1|$ must be odd and the product of the elements of T is of the form $p^{2e+1}m^2$ for some integers e and m. Let t denote an element of T which is a multiple of p and let S' denote the set which is obtained from S by replacing t with p. Note that $t > p$ since t is a multiple of p and p does not lie in S. Suppose at first that there is an odd-sized subset T' of S' such that the product of the elements of T' is a square. Note that T' is not a subset of S (because condition (ii) of Theorem 1 does not hold), so $p \in T'$. Therefore the product of the elements of $T'-\{p\}$ equals (the product of the elements of T')$/p$, which is a number of the form k^2/p for some integer k. This observation and the fact that the product of the elements of T is of the form $p^{2e+1}m^2$ imply that the product of the elements of $((T'-\{p\}) \cup T)-((T'-\{p\}) \cap T)$ is a square. Note also that $((T'-\{p\}) \cup T)-((T'-\{p\}) \cap T)$ is an odd-sized subset of S (because the size of $T'-\{p\}$ is even and the size of T is odd). This contradicts the assumption that statement (ii) of the theorem does not hold. Therefore, for every odd-sized subset T' of S', the product of the elements of T' is not a square. The induction hypothesis implies that there is a map g in M such that $g(x) = -1$ for every x in S'. Let w denote the product of the elements of T, and observe that, since $T-\{t\} \subset S'$, $g(w/t) = (-1)^{|T-\{t\}|} = 1$. Since $g(w/t) = 1$ and the product of the elements of T is of the form $p^{2e+1}m^2$, $g(t) = g(w) = g(p)$. Recall that $p \in S'$, so $g(p) = -1$. Hence, $g(t) = -1$, so $g(x) = -1$ for every x in S.

Thus, the claim holds in all cases.

Theorem 2. *Let S denote a finite set of non-zero integers. The following statements are equivalent.*

(i) *For every map $f : S \rightarrow \{-1, 1\}$, there is an odd prime $p = p(f)$ such that $(x/p) = f(x)$ for every x in S.*

(ii) *For every map $f : S \rightarrow \{-1, 1\}$, the density of the set of primes p satisfying $(x/p) = f(x)$ for every x in S is $2^{-|S|}$.*

(iii) *For every non-empty subset T of S, the product of the elements of T is not a square.*

Proof. It is easy to see that (ii) $\Rightarrow$ (i) $\Rightarrow$ (iii). Suppose that statement (iii) holds and define R as in the second proof of Theorem 1. Statement (iii) implies that $R^{\perp} = \{0\}$. Since $R^{\perp} = \{0\}$ and R is a vector space over F_2, $R = (F_2)^n$. This observation and the Lemma imply statement (i).

Let s denote the product of the elements of S. If v and v' are odd positive integers such that $v \equiv v' \pmod{4s}$, then $(x/v) = (x/v')$ for every x in S. Let t denote an integer which is relatively prime to $4s$. Define V_t to be the set of congruence classes $v \pmod{4s}$ such that, when v' lies in the congruence class v, $(x/v') = (x/t)$ for every x in S. Multiplication by t induces a bijection from V_1 to V_t, so the size of V_1 equals the size of V_t.

This observation and the Prime Number Theorem for primes in arithmetic progressions imply that (i) $\Rightarrow$ (ii).

One can also prove that (iii) $\Rightarrow$ (i) in Theorem 2 by induction on the size of S, as in the first proof of Theorem 1, or by induction on the product of the elements of S, as in the third proof of Theorem 1.

Note that if S is a set of primes, then condition (iii) of Theorem 2 is satisfied.

Theorem 3. *Let S denote a set of non-zero integers and let f denote a map from S to $\{-1, 1\}$. Assume that there is an infinite subset U of S such that the product of two distinct elements of U is never a square ; then for almost all primes p, there is an element $x = x(p)$ in S such that $(x/p) = f(x)$.*

Proof. The assumption about S implies that, for every positive integer n, there is a subset S_n of S such that $|S_n| = n$ and the product of the elements in any non-empty subset of S_n is not a square. Theorem 2 implies that the density of the set of primes p satisfying $(x/p) = -f(x)$ for every x in S_n is 2^{-n}. Therefore, the set of primes p which satisfy $(x/p) = f(x)$ for some x in S_n has density $1-2^{-n}$. The theorem follows immediately from this by letting $n \to \infty$.

Corollary 1. *The following conditions are equivalent.*

(i) *For almost all primes p, S contains a quadratic non-residue modulo p.*

(ii) *There is an infinite subset U of S such that the product of two distinct elements of U is never a square.*

Proof. Theorem 3, with $f(x) = -1$ for all x, implies that (ii) $\Rightarrow$ (i). Suppose now that condition (ii) does not hold. Let S' denote a maximal subset of S such that the product of two distinct elements of S' is never a square, and let s' denote the product of the elements of S'. If p is a prime which is congruent to 1 (mod $4s'$), then every element of S is either a quadratic residue modulo p or divisible by p. Therefore, condition (i) does not hold.

Corollary 2. *The following conditions are equivalent.*

(i) *For almost all primes p, S contains a number $x = x(p)$ such that $(x/p) = 1$.*

(ii) *Either there is an odd-sized subset T of S such that the product of* *the elements of T is a square, or there is an infinite subset U of S such that the product of two distinct elements in U is never a square.*

This Corollary follows from Theorems 1 and 3 ; we omit the details of the proof.

The next theorem demonstrates that the implication (iii) ⇨ (i) in Theorem 2 strongly requires the hypothesis that S is finite.

Theorem 4. *Let $e_1, e_2, \cdots$ denote an infinite sequence of elements of $\{-1, 1\}$. There is an infinite set $S = \{s_1 < s_2 < \cdots\}$ of positive integers such that*

(i) *for every odd prime p, there are only finitely many elements s_i in S such that (s_i/p) equals 0 or e_i, and*

(ii) *for every non-empty finite subset T of S, the product of the elements of T is not a square.*

Proof. Let w_n denote the product of the first n odd primes. Let r_n denote an integer such that $(r_n/p) = -e_n$ for all primes p dividing w_n. Note that r_n is relatively prime to w_n ; therefore, for each n there are infinitely many primes which are congruent to $r_n \pmod{w_n}$. Let $s_1, s_2, \cdots$ denote primes such that $s_n \equiv r_n \pmod{w_n}$ for all n and $s_1 < s_2 < \cdots$. If p denotes the k-th odd prime, then p divides w_n for all $n \geq k$; hence, $(s_n/p) = (r_n/p) = -e_n$ for all $n \geq k$. Therefore, there are less than k subscripts i for which $(s_i/p) = 0$ or e_i. This finishes the proof.

Note that in the case that $e_i = -1$ for every i, the set S of Theorem 4 contains a quadratic residue modulo p for every odd prime p, but it does not satisfy condition (ii) of Theorem 1. Thus Theorem 1 does not hold for infinite sets S ; Corollary 2 of Theorem 3 also implies that Theorem 1 does not hold for infinite sets.

Acknowledgements. We are grateful to Professor John Brillhart for bringing our attention to reference [2].

REFERENCES

[1] T. FUNAKURA and N. MORIMOTO : Some arithmetical properties on 2×2 integral matrices, Math. J. Okayama Univ. 27 (1985), 135–146.

[2] M. HALL, Jr. : Quadratic residues in factorization, Bull. Amer. Math. Soc. 39 (1933), 758–763.

[3] K. IRELAND and M. ROSEN : A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1982.

[4] H. N. SHAPIRO : Introduction to the Theory of Numbers, Wiley, New York, 1983.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SOUTH CAROLINA 29208, U.S.A.

(*Received August 6, 1987*)