Journal of Number Theory 133 (2013) 2398–2430

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Quadratic residues and non-residues in arithmetic progression

Steve Wright

Department of Mathematics and Statistics, Oakland University, Rochester, MI 48309, United States

ARTICLE INFO

Article history:
Received 9 January 2013
Accepted 11 January 2013
Available online 20 March 2013
Communicated by David Goss

MSC:
primary 11D09
secondary 11M99, 11L40

Keywords:
Quadratic residue
Quadratic non-residue
Arithmetic progression
Asymptotic approximation
Weil sum

ABSTRACT

Let $\mathcal{S}$ be an infinite set of nonempty, finite subsets of the positive integers. If p is an odd prime, let $c(p)$ denote the cardinality of the set $\{S \in \mathcal{S}\colon\ S \subseteq \{1, \dots, p-1\}$ and S is a set of quadratic residues (respectively, non-residues) of $p\}$. When $\mathcal{S}$ is constructed in various ways from the set of all arithmetic progressions of positive integers, we determine the sharp asymptotic behavior of $c(p)$ as $p \to +\infty$. Generalizations and variations of this are also established, and some problems connected with these results that are worthy of further study are discussed.

1. Introduction

If p is an odd prime, an integer z is said to be a *quadratic residue* (respectively, *quadratic non-residue*) of p if the equation $x^2 \equiv z \bmod p$ has (respectively, does not have) a solution x in integers. It is a theorem going all the way back to Euler that exactly half of the integers from 1 through $p-1$ are quadratic residues of p, and it is a fascinating problem to investigate the various ways in which these residues are distributed among $1, 2, \dots, p-1$. In this paper, our particular interest lies in studying the problem of the distribution of residues and non-residues among the arithmetic progressions which can occur in the set $\{1, 2, \dots, p-1\}$.

We begin with a litany of notation and terminology that will be used systematically throughout the rest of this paper. If $m \leqslant n$ are integers, then $[m, n]$ will denote the set of all integers that are at least m and no greater than n, listed in increasing order, and $[m, +\infty)$ will denote the set of

E-mail address: wright@oakland.edu.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.01.004

all integers that exceed $m-1$, also listed in increasing order. For any odd prime p, we let $R(p)$ (respectively, $NR(p)$) denote the set of all quadratic residues (respectively, non-residues) of p in the interval $[1, p-1]$. If $\{a(p)\}$ and $\{b(p)\}$ are sequences of real numbers defined for all primes p in an infinite set S, then we will say that $a(p)$ is (sharply) *asymptotic to* $b(p)$ *as* $p \to +\infty$ *inside* S, denoted as $a(p) \sim b(p)$, if

$$\lim_{\substack{p\to+\infty \\ p\in S}} \frac{a(p)}{b(p)} = 1,$$

and if $S = [1, +\infty)$, we simply delete the phrase "inside S". If x is a real number, $[x]$ will denote the greatest integer that does not exceed x. Finally, if A is a set then $|A|$ will denote the cardinality of A, 2^A will denote the set of all subsets of A, $\mathcal{E}(A)$ will denote the set of all nonempty finite subsets of A of even cardinality, and $\emptyset$ will denote the empty set. We also note once and for all that p will always denote a generic odd prime.

Our work here, in both spirit and method, has its origins in some classical results of H. Davenport. In the papers [5–7], Davenport considers the problem of estimating the number $R_s(p)$ (respectively, $N_s(p)$) of sets of s consecutive quadratic residues (respectively, non-residues) of an odd prime p that occur inside $[1, p-1]$. The expected number is about $2^{-s}p$, and in [7, Corollary of Theorem 5], Davenport showed that as $p \to +\infty$, both $R_s(p)$ and $N_s(p)$ are asymptotic to $2^{-s}p$. His method of proof is based on the following clever idea. If $\mathbb{Z}_p$ is the field of p elements, then the Legendre symbol of p defines a real (primitive) multiplicative character $\chi_p : \mathbb{Z}_p \to [-1, 1]$ on $\mathbb{Z}_p$. If $\varepsilon \in \{-1, 1\}$, form the sum

$$2^{-s}\sum_{x=1}^{p-s}\prod_{i=0}^{s-1}\bigl(1+\varepsilon\chi_p(x+i)\bigr) \tag{1.1}$$

and note that the value of this sum is $R_s(p)$ (respectively, $N_s(p)$) when $\varepsilon = 1$ (respectively, $\varepsilon = -1$). Davenport rewrote this sum as

$$2^{-s}(p-s) + 2^{-s}\sum_{\emptyset\neq T\subseteq[0,s-1]}\varepsilon^{|T|}\left(\sum_{x=1}^{p-s}\chi_p\left(\prod_{i\in T}(x+i)\right)\right) \tag{1.2}$$

and then used the theory of Hasse L-functions to prove that there exist positive absolute constants $\sigma < 1$ and C such that for all p sufficiently large,

$$\left|\sum_{x=1}^{p-s}\chi_p\left(\prod_{i\in T}(x+i)\right)\right| \leqslant Csp^{\sigma}. \tag{1.3}$$

When this estimate is applied in (1.2), it follows immediately that $R_s(p)$ and $N_s(p)$ are asymptotic to $2^{-s}p$, with an asymptotic error which does not exceed Csp^{σ}, for all p sufficiently large. In 1945, A. Weil's landmark work on arithmetic algebraic geometry [16] appeared, one consequence of which is that the estimate (1.3) holds with $C = 2$ and $\sigma = 1/2$, which produces an essentially optimal estimate for the asymptotic error. More generally, if χ_p is replaced in the sum in (1.3) by an arbitrary non-principal multiplicative character χ on a finite field F, Weil's work implies that the resulting sum also satisfies this improved estimate. Consequently, if f is a polynomial over F, then sums of the form

$$\sum_{x\in F}\chi\bigl(f(x)\bigr)$$