1. Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **22 (1976)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **09.08.2024**

CLASSICAL THEOREMS ON QUADRATIC RESIDUES

by Bruce C. BERNDT

1. INTRODUCTION

In 1839, Dirichlet [23] proved that if p is a prime with $p \equiv 3 \pmod 4$, then

$$\sum_{0<n<p/2} \left(\frac{n}{p}\right) > 0\,, \tag{1.1}$$

where $\left(\frac{n}{p}\right)$ denotes the Legendre symbol. In other words, the number of quadratic residues in the interval $(0, p/2)$ always exceeds the number of quadratic non-residues in that interval. Dirichlet's deduction of (1.1) was an immediate consequence of one of his class number formulas for binary quadratic forms. All known proofs of (1.1) are nonelementary in that they use infinite series. Many authors have expressed the desire for a truely elementary proof of (1.1). In fact, Landau [43, p. 129] remarks "Aber noch kein Mensch hat diese wahre Tatsache mit elementaren Mitteln beweisen können." Although we give some new proofs of (1.1) here, unfortunately, none can be considered elementary.

Another result with its origins in a class number formula of Dirichlet is the following. If p is a prime with $p \equiv 1 \pmod 4$, then

$$\sum_{0<n<p/4} \left(\frac{n}{p}\right) > 0\,. \tag{1.2}$$

Thus, the number of quadratic residues in the interval $(0, p/4)$ always exceeds the number of quadratic non-residues there. As with (1.1), an elementary proof of (1.2) does not exist. Furthermore, (1.2) does not appear to be as widely known as (1.1). All published proofs of (1.2) follow from class number formulas. We give here some proofs of (1.2) that do not involve class number considerations, although, admittedly, the use of L-functions gives an undeniable link with class numbers.

The main purpose of this study is to make a systematically thorough attempt to discover which sums of the Legendre symbol, or more generally, sums of real primitive characters, are always positive (or negative). In other words, on which intervals for which classes of primes are results like (1.1) and (1.2) possible ? The quadratic excess on (a, b) is defined to be $\sum_{a<n<b} \left(\frac{n}{p}\right)$ Thus, for example, if $p > 3$ is prime, we show that the quadratic excess on $(0, p/3)$ is always positive. If $p \equiv 11, 19 \pmod{40}$, then the quadratic excess on $(0, p/10)$ is positive. If $p \equiv 5 \pmod{24}$, then the quadratic excess on $(3p/8, 5p/12)$ is negative. We establish many results of this type. Many of our results are not new and can be found scattered throughout the literature since 1839. In particular, Lerch [44], Holden [36-39], and Karpinski [42] have established many of the results proved here. However, a goodly number of our findings appear to be new. Moreover, our results are most often proven with greater generality than elsewhere in the literature.

Many intervals are found for which the quadratic excess is zero. Such results, however, can invariably be proved by purely elementary techniques. Many examples of this sort of result may be found in a paper by Chowla and the author [8] and, even moreso, in the work of Johnson and Mitchell [41]. A related question is examined in a paper of Wolke [61].

Let $h(d)$ denote the class number of the quadratic field of discriminant d over the rational numbers. For $d < 0$, we obtain many congruences for class numbers as easy corollaries of our efforts to find positive character sums. Again, many of these results are scattered throughout the literature, but many do not appear to have been previously noticed. As an example of the type of result obtained, we state a lemma of Stark [59] which was important in his proof that there are exactly 9 imaginary quadratic fields of class number 1. If p is a prime with $p \equiv 19 \pmod{24}$, then $h(-12p) \equiv 4 \pmod{8}$. As other examples, we mention that if $p \equiv 7 \pmod{20}$, then $h(-5p) \equiv 2h(-p) \pmod{8}$; if $p \equiv 7 \pmod{24}$, then $h(-24p) \equiv 4 \pmod{8}$; and if $p \equiv 17 \pmod{48}$, then $h(-24p) - 2h(-8p) + 2h(-3p) \equiv 0 \pmod{16}$.

Our work involving congruences for class numbers overlaps considerably with that of Pizer [53]. However, the techniques are entirely dissimilar. Pizer uses the theory of type numbers of Eichler orders [52], while we use the theory of Dirichlet L-functions. Pizer [53] proves congruences for class numbers with discriminants containing three or fewer primes. We concentrate primarily on discriminants with just one odd prime or small multiples of one odd prime. It should be mentioned, however, that our methods are applicable to imaginary quadratic fields with discriminants containing any number of distinct odd prime factors. Perhaps Hurwitz [40] was the first to prove congruences for class numbers with discriminants involving two distinct prime factors. Brown [11], [12], [14] and Hasse [34], [35] have achieved several results for two distinct prime factors. For congruences relating class numbers for imaginary quadratic fields with discriminants containing three distinct prime factors, see,in particular, papers of Pumplün [55], Brown [11], and Brown and Parry [15]. Finally, the divisibility by a power of 2 of class numbers for imaginary quadratic fields with discriminants containing an arbitrary number of distinct odd primes has been studied by Plancherel [54], Rédei [56], and Rédei and Reichardt [58]. A related paper is [1].

An elementary argument [60] shows that (1.1) is equivalent to another theorem of Dirichlet [23]. Let p be a prime with $p \equiv 3 \pmod 4$. Let r denote an arbitrary quadratic residue and n an arbitrary quadratic non-residue modulo p in the interval $(0, p)$. Then

$$\sum_{0<n<p} n - \sum_{0<r<p} r > 0 . \tag{1.3}$$

In other words, the sum of the non-residues in $(0, p)$ always outweighs the sum of the residues in the same interval. In the penultimate section of this paper, many other results of this type are established. Most of these theorems appear to be new.

In the last section of the paper, we state several open problems and conjectures on positive sums of the Legendre symbol and on class numbers.

The organization for the paper is now briefly described. We shall, in turn, examine various intervals for which positivity results can be obtained. Our techniques are generally applicable to arbitrary primitive characters. Thus, for each class of intervals we first give theorems for arbitrary primitive characters that express character sums over these intervals in terms of L-functions. Next, we determine for real primitive characters when the character sum is always positive, negative, or zero. Thirdly, we translate our representations of real primitive character sums into statements involving class numbers. Fourthly, we deduce congruences for class numbers.

Our techniques can be classified into four main types. In section 3, we use the partial fraction decomposition of the cotangent function to effect a very simple proof of Dirichlet's theorem in the form (1.3). Our second technique uses contour integration and also appears to be completely new. The third technique uses Fourier series and is an extension of the method used, for example, by Dirichlet [24], Chowla [18], and Moser [47] to prove (1.1). The fourth method is similar to the third and uses character analogues of the Poisson summation formula which have been established in various versions by Berger [5], Lerch [44], Mordell [46], Guinand [30], the author [6], and Schoenfeld and the author [9]. The application of the character Poisson formula to problems of this type appears to be new. However, Yamamoto [62] has recently used essentially the same technique to derive some of the results of this paper. The method is also briefly described by the author in [7].

In most cases, we have chosen a direct, analytic method of proof, whereas a possibly less direct but more elementary argument *with* the use of Dirichlet's main theorems is possible. In fact, throughout the literature, the latter attack is generally the tact that is chosen. In particular, see the aforementioned papers of Holden and Karpinski and a paper of Rėdei [57].

The author is very grateful to his colleague Samuel Wagstaff, Jr. who computed lengthy tables of sums of the Legendre symbol. These computations were immensely helpful to the author in formulating conjectures and testing conjectures. The author is also very grateful to Duncan Buell for extensive calculations in connection with some inequalities for class numbers conjectured by the author. (See section 14.)

2. Notation and preliminary results

Throughout the sequel, χ shall denote a non-principal, primitive character of modulus k. To indicate the dependence upon the modulus k, we shall often write χ_k for χ. Always, p denotes an odd prime. If $p_1, ..., p_r$ denote distinct odd primes, let

$$d = \pm 2^{\alpha} \prod_{i=1}^{r} (-1)^{(p_i-1)/2} p_i .$$

Here, $r \geqq 0$ and $\alpha = 0, 2$ or 3; if $\alpha = 0$, then $r > 0$ and the plus sign must be taken, if $\alpha = 2$, the minus sign must be taken, and if $\alpha = 3$, either sign may be taken. If n is a positive integer, let $\left(\frac{d}{n}\right)$ denote the Kronecker symbol. Every real primitive character is of the form $\left(\frac{d}{n}\right)$, and the modulus of each such character is $|d|$ [20, p. 42]. Furthermore, $\left(\frac{d}{n}\right)$ is even or odd according to whether $d > 0$ or $d < 0$, respectively.