Fermat Quotients and the Ankeny–Artin–Chowla Conjecture

Nic Fellini and M. Ram Murty

Abstract In this article, we present streamlined proofs of results of Ankeny, Artin, and Chowla concerning the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ for primes $p \equiv 1 \pmod 4$ while providing a generalization of their conjecture. Using our generalization, we relate Fermat quotients of quadratic non-residues (mod p) to sums of harmonic numbers.

Keywords Fermat quotients · Ankeny-Artin-Chowla conjecture · Class numbers · p-adic logarithm

1.1 Introduction

In 1951, Ankeny et al. [1] derived four congruence relations for the class number of real quadratic fields $\mathbb{Q}(\sqrt{p})$ with p a prime. It seems that a similar independent investigation was undertaken several years earlier by Kiselev [2]. In a later paper, [3], they published proofs of only three relations and perhaps inadvertently omitted the proof of the fourth relation. This gap was filled in by Carlitz [4] who gave a proof but again omitted to write out several key steps of the proof. The missing steps involve the use of the p-adic logarithm, a profound idea introduced in [3] and developed later by Iwasawa [5]. Looking back at the paper of Ankeny, Artin and Chowla, one cannot fail to see the birth of two fundamental concepts of number theory: one is the p-adic logarithm and the other is the use of the group ring to study cyclotomic fields, both of which had a transformative influence in the number theory of the twentieth century.

Research partially supported by an NSERC Discovery grant.

N. Fellini · M. Ram Murty (✉)
Queen's University, Kingston, Canada
e-mail: murty@queensu.ca

N. Fellini
e-mail: n.fellini@queensu.ca

K. Chakraborty et al. (eds.), *Class Groups of Number Fields and Related Topics*, Springer Proceedings in Mathematics & Statistics 470,
https://doi.org/10.1007/978-981-97-6911-7_1

In this paper, we will amplify this idea by giving simplified proofs of the results in [1, 3]. At the same time, we extend these results and investigate a conjecture of Ankeny, Artin, and Chowla explained in the next section.

1.2 An Extension of the Ankeny-Artin-Chowla Congruence

Let p be a prime $\equiv 1 \pmod 4$. The fundamental unit of $\mathbb{Q}(\sqrt{p})$ can be written as

$$\varepsilon = \frac{t + u\sqrt{p}}{2} \tag{1.1}$$

for positive integers t and u. Ankeny et al. [1] stated the result

$$\frac{2hu}{t} \equiv \frac{A + B}{p} \pmod p \tag{1.2}$$

where h is the class number of $\mathbb{Q}(\sqrt{p})$, A is the product of the quadratic residues (mod p) lying in $[1, p]$ and B is the product of the quadratic non-residues (mod p) lying in $[1, p]$. This was one of the four results stated in [1] and three of these four results were proved in [3]. Carlitz [4] noted this gap and provided a proof but was vague in several key steps. The essential ingredient of the p-adic logarithm needed to derive (1.2) is not clearly enunciated in [4] or [3]. We will fill this gap in our discussion below. We will also use this occasion to give streamlined proofs of the results in [1, 3].

In their paper, Ankeny, Artin and Chowla conjecture that for primes $p \equiv 1 \pmod 4$, we always have $p \nmid u$. They verified their conjecture when $p \equiv 5 \pmod 8$ and $p < 2000$. Van der Poorten, te Riele and Williams [6, 7] verified the conjecture for all primes $p < 2 \cdot 10^{11}$. The interest in this conjecture lies in the following observation. In 1960, Ankeny and Chowla [8] proved that $h < p$. For any given prime p, the quantities A, B and ε are easily computed (using the continued fraction of $\sqrt{p}$ in the case of ε) and so, (1.2) provides a congruence for $h \pmod p$. But since $h < p$, the reduced residue gives the exact value of h **provided** u **is not divisible by** p.

We briefly address remarks made by Ankeny and Chowla [8] regarding $h < p$. In their paper, they wrote that this estimate is not well-known and cite a comment of Carlitz [4] to this effect. They then give a proof of the stronger estimate $h = O(\sqrt{p})$. In a postscript to their paper, they provide another proof of the weaker estimate $h = O(p^{1/2+\varepsilon})$ due to Mordell which uses the theory of reduced binary quadratic forms. The proof given in [8] employs Dirichlet's class number formula though the authors never say so. In fact, the formula on top of page 146 is pulled out of the "hat of Dirichlet."

It is relatively painless to give a proof that $h = O(\sqrt{p})$ using Dirichlet's formula in the form

$$\frac{2h\log\varepsilon}{\sqrt{|d_K|}} = \sum_{n=1}^{\infty}\frac{\chi(n)}{n}, \tag{1.3}$$

where $\chi(n) = (d_K/n)$ is the Kronecker symbol, d_K is the discriminant of $K = \mathbb{Q}(\sqrt{p})$. From (1.1), we see that $\varepsilon \gg \sqrt{p}$ so that the left hand side of (1.3) is

$$\gg \frac{h\log p}{\sqrt{p}}.$$

On the other hand, the right hand side of (1.3) can be re-written (by partial summation) as

$$\sum_{n=1}^{p-1}\frac{\chi(n)}{n} + \int_{p}^{\infty}\frac{S(x)}{x^2}dx,$$

where $S(x) = \sum_{n<x}\chi(n)$. As $S(x) = O(p)$, we see that the right hand side of (1.3) is bounded by $O(\log p)$ and the claim is now immediate. We remark that an identical proof shows that the class number $h(D)$ of $\mathbb{Q}(\sqrt{D})$ with D a fundamental discriminant is also $O(\sqrt{|D|})$. We will use this fact in a later section.

A natural question that arises is what result emerges in (1.2) if we replace A and B by complete sets $\{a_s\}_{s=1}^{(p-1)/2}$, $\{b_s\}_{s=1}^{(p-1)/2}$ of quadratic residues and non-residues (respectively) but not lying necessarily in $[1, p]$. We will assume that the a_s, b_s are all positive. This question is easily answered as follows.

Writing

$$a_s = \langle a_s\rangle + p\left[\frac{a_s}{p}\right]$$
$$b_s = \langle b_s\rangle + p\left[\frac{b_s}{p}\right]$$

where $\langle x\rangle$ denotes the reduced residue of $x \pmod p$. Then,

$$A = \prod_{s=1}^{(p-1)/2}\left(a_s - p\left[\frac{a_s}{p}\right]\right)$$
$$B = \prod_{s=1}^{(p-1)/2}\left(b_s - p\left[\frac{b_s}{p}\right]\right).$$

We easily see that

$$A \equiv A^* - pA^*\sum_{s=1}^{(p-1)/2}\left[\frac{a_s}{p}\right]\frac{1}{a_s} \pmod{p^2}$$

$$B \equiv B^* - pB^* \sum_{s=1}^{(p-1)/2} \left[\frac{b_s}{p}\right] \frac{1}{b_s} \pmod{p^2}$$

where

$$A^* = \prod_{s=1}^{(p-1)/2} a_s \quad \text{and} \quad B^* = \prod_{s=1}^{(p-1)/2} b_s.$$

Thus,

$$A + B \equiv A^* + B^* - p\left(A^* \sum_{s=1}^{(p-1)/2} \left[\frac{a_s}{p}\right] \frac{1}{a_s} + B^* \sum_{s=1}^{(p-1)/2} \left[\frac{b_s}{p}\right] \frac{1}{b_s}\right) \pmod{p^2}.$$

Therefore,

$$\frac{A+B}{p} \equiv \frac{A^*+B^*}{p} - \left(A^* \sum_{s=1}^{(p-1)/2} \left[\frac{a_s}{p}\right] \frac{1}{a_s} + B^* \sum_{s=1}^{(p-1)/2} \left[\frac{b_s}{p}\right] \frac{1}{b_s}\right) \pmod{p}.$$

This leads to the following variant of (1.2).

Theorem 1 *Let $p \equiv 1 \pmod 4$ be a prime and $\{a_s\}$, $\{b_s\}$ be positive numbers representing a complete set of quadratic residues and non-residues* (mod p) *respectively. Let A^* and B^* be the product of the a_s and b_s respectively. If $\varepsilon = \frac{1}{2}(t + u\sqrt{p})$ is the fundamental unit of $\mathbb{Q}(\sqrt{p})$, then*

$$\frac{A^*+B^*}{p} \equiv \frac{2hu}{t} + \left(A^* \sum_{s=1}^{(p-1)/2} \left[\frac{a_s}{p}\right] \frac{1}{a_s} + B^* \sum_{s=1}^{(p-1)/2} \left[\frac{b_s}{p}\right] \frac{1}{b_s}\right) \pmod{p}.$$

Remark If $1 \le a_s, b_s \le p$, then the two sums in the congruence above vanish identically and we retrieve the Ankeny, Artin, and Chowla congruence (1.2).

1.3 Relation to Fermat Quotients and Harmonic Numbers

Let R be a complete set of quadratic residues (mod p) all lying in $[1, p-1]$ and N a complete set of quadratic non-residues (mod p) all lying in $[1, p-1]$. Then $A^* = A$ and $A \equiv -1 \pmod p$. Moreover, $B^* = B$ and $B \equiv 1 \pmod p$. Now we fix a quadratic non-residue $m \pmod p$ and define the two sequences

$$b_r = mr \ \ (r \in R) \quad \text{and} \quad a_n = mn \ \ (n \in N).$$

In this set-up, Theorem 1 reads as

$$\frac{A+B^*}{p} \equiv \frac{2hu}{t} + B^* \sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p}$$

and

$$\frac{A^*+B}{p} \equiv \frac{2hu}{t} + A^* \sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p}$$

respectively. Observing that $B^* = m^{(p-1)/2}A$ and $A^* = m^{(p-1)/2}B$ respectively, and that $m^{(p-1)/2} \equiv -1 \pmod{p}$, we deduce

$$A\left(\frac{m^{\frac{p-1}{2}}+1}{p}\right) \equiv \frac{2hu}{t} - A \sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p} \tag{1.4}$$

$$B\left(\frac{m^{\frac{p-1}{2}}+1}{p}\right) \equiv \frac{2hu}{t} - B \sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p} \tag{1.5}$$

This then leads to a refinement of [1].

Theorem 2 *Suppose p is a prime $\equiv 1 \pmod 4$ and let R a complete set of quadratic residues lying in $[1, p-1]$, N a complete set of quadratic non-residues lying in $[1, p-1]$,*

$$\varepsilon = \frac{t+u\sqrt{p}}{2}$$

be the fundamental unit of $\mathbb{Q}(\sqrt{p})$, and h the class number of $\mathbb{Q}(\sqrt{p})$. Then for any quadratic non-residue $m \pmod p$,

$$\frac{m^{p-1}-1}{p} \equiv \frac{4hu}{t} + 2\sum_{r\in R} \left[\frac{mr}{p}\right] \frac{1}{mr} \pmod{p} \tag{1.6}$$

$$\frac{m^{p-1}-1}{p} \equiv -\frac{4hu}{t} + 2\sum_{n\in N} \left[\frac{mn}{p}\right] \frac{1}{mn} \pmod{p} \tag{1.7}$$

Proof By the above discussion, the theorem follows at once by noting that $A \equiv -1 \pmod{p}$ and $B \equiv 1 \pmod{p}$ and by multiplying equations (1.4) and (1.5) by $m^{(p-1)/2} - 1 \equiv -2 \pmod{p}$. □

Definition For p a prime number, the base a Fermat quotient is the integer defined as

$$F(a) = \frac{a^{p-1}-1}{p}.$$

Adding the two congruences in Theorem 2 we deduce.

Corollary 3 *Suppose $p \equiv 1 \pmod 4$ and m is a quadratic non-residue $\pmod p$. Then,*

$$mF(m) \equiv 2\sum_{k=1}^{p-1}\left[\frac{mk}{p}\right]\frac{1}{k}$$

where $F(m)$ is the Fermat quotient.

Remark We observe that this congruence relation for the Fermat quotient is unconditional of the Ankeny-Artin-Chowla conjecture. If $p \mid u$, then the terms involving the class number in Theorem 2 vanish. If $p \nmid u$, these same two terms cancel when added.

Definition The k-th harmonic number H_k is defined as

$$H_k = \sum_{j=1}^{k}\frac{1}{j}$$

where we understand that $H_0 = 0$.

Lemma 4 *For any odd prime p, $H_{p-1} \equiv 0 \pmod{p}$.*

Proof This is a simple matter of pairing up additive inverses. As k runs through $\{1, \ldots, \frac{p-1}{2}\}$, $p-k$ will run through $\{p-1, \ldots, \frac{p+1}{2}\}$. Hence,

$$H_{p-1} = \sum_{k=1}^{p-1}\frac{1}{k} \equiv \sum_{k=1}^{\frac{p-1}{2}}\left(\frac{1}{k}+\frac{1}{p-k}\right) \equiv \sum_{k=1}^{\frac{p-1}{2}}\left(\frac{1}{k}-\frac{1}{k}\right) \equiv 0 \pmod{p}\,. \qquad \square$$

An immediate corollary of Lemma 4 is the following:

Corollary 5 *Suppose p is prime and $a < b$ are positive integers such that $a + b = p - 1$, then*

$$H_a \equiv H_b \pmod{p}\,.$$

Proof By Lemma 4, we have

$$0 \equiv H_{p-1} \equiv \sum_{j=1}^{a}\frac{1}{j} + \sum_{j=a+1}^{p-1}\frac{1}{j} \pmod{p}\,.$$

By assumption, $a + 1 = p - b$ and hence

$$H_a \equiv -\sum_{j=p-b}^{p-1}\frac{1}{j} \pmod{p}\,.$$

Making the change of variables, $j \to p - j$ we have,

$$H_a \equiv \sum_{j=1}^{b}\frac{1}{j} \equiv H_b \pmod{p}\,. \qquad \square$$

Setting $x_k = H_{k-1}$, Corollary 3 reads as

$$mF(m) \equiv \sum_{k=1}^{p-1} \left[\frac{mk}{p}\right] (x_{k+1} - x_k) \pmod{p}.$$

Using summation by parts this becomes

$$mF(m) \equiv x_p \left[\frac{m(p-1)}{p}\right] - \sum_{k=2}^{p-1} x_k \left(\left[\frac{mk}{p}\right] - \left[\frac{m(k-1)}{p}\right]\right) \pmod{p}.$$

The first term on the right hand side vanishes by Lemma 4. Now in the summand, we simplify the difference of the floor functions using the following lemma:

Lemma 6 *Suppose p is prime and that M is any positive coset representative of a positive reduced residue $m \pmod{p}$. Then,*

$$\left[\frac{Mk}{p}\right] - \left[\frac{M(k-1)}{p}\right] = \left[\frac{M}{p}\right] + \left[\frac{mk}{p}\right] - \left[\frac{m(k-1)}{p}\right]$$

for all $1 \le k \le p-1$. In particular, if $M = m$ then

$$\left[\frac{mk}{p}\right] - \left[\frac{m(k-1)}{p}\right] = \begin{cases} 1 & \text{if } k = \left[\frac{p\ell}{m}\right] + 1 \text{ for some } \ell \in [0, m-1] \\ 0 & \text{otherwise.} \end{cases}$$

Proof Write $M = m + p\left[\frac{M}{p}\right]$. Then,

$$\left[\frac{Mk}{p}\right] - \left[\frac{M(k-1)}{p}\right] = \left[\frac{mk}{p} + k\left[\frac{M}{p}\right]\right] - \left[\frac{m(k-1)}{p} + (k-1)\left[\frac{M}{p}\right]\right].$$

As $[x+n] = [x] + n$ for any positive integer n, we deduce the first part of the statement.

For the second statement, we note that $\left[\frac{mk}{p}\right] - \left[\frac{m(k-1)}{p}\right] \ne 0$ if and only if there exists some positive integer $\ell \le m-1$ such that

$$\frac{m(k-1)}{p} < \ell \le \frac{mk}{p}.$$

Rearranging this inequality, we have that

$$k - 1 < \frac{p\ell}{m} \le k$$

and hence $k - 1 = \left[\frac{p\ell}{m}\right]$. For these values of k, we seek to simplify:

$$\left[\frac{m}{p}\left(\left[\frac{p\ell}{m}\right]+1\right)\right]-\left[\frac{m}{p}\left[\frac{p\ell}{m}\right]\right].$$

Writing $p\ell = \theta + m\left[\frac{p\ell}{m}\right]$ for $0 < \theta < m$ we deduce that

$$\frac{m}{p}\left[\frac{p\ell}{m}\right] = \ell - \frac{\theta}{p}.$$

Using this relation we have:

$$\left[\frac{m}{p}\left(\left[\frac{p\ell}{m}\right]+1\right)\right]-\left[\frac{m}{p}\left[\frac{p\ell}{m}\right]\right]=\left[\ell-\frac{\theta}{p}+\frac{m}{p}\right]-\left[\ell-\frac{\theta}{p}\right]=\left[\frac{m-\theta}{p}\right]-\left[-\frac{\theta}{p}\right]$$

Since $0 < \theta < m$, the first floor function on the right is zero as $0 < m - \theta < p$. The second term is -1 as $-1 < -\theta/p < 0$. The result then follows. □

Lemma 7 *Fix p and some $q < p$. Then for all $1 \le k \le q-1$ we have*

$$\left[\frac{pk}{q}\right]+\left[\frac{p(q-k)}{q}\right]=p-1.$$

Proof Suppose $\left[\frac{pk}{q}\right] = \ell$. Then we have that

$$\left[\frac{p(q-k)}{q}\right]=p+\left[\frac{-pk}{q}\right]$$

and since $\left[\frac{pk}{q}\right] = \ell$ we deduce that $\left[\frac{-pk}{q}\right] = -\ell - 1$. Hence,

$$\left[\frac{pk}{q}\right]+\left[\frac{p(q-k)}{q}\right]=\ell+(p-\ell-1)=p-1.$$ □

Therefore, by Lemma 6, and partial summation we deduce:

Theorem 8 *If $p \equiv 1 \pmod 4$ is a prime and M is any positive coset representative of a quadratic non-residue $m \pmod p$, then*

$$-MF(M) \equiv \left[\frac{M}{p}\right]+\sum_{j=1}^{m-1} H_{\left[\frac{pj}{m}\right]}.$$

Remark One can shorten the sum on the right in Theorem 8 by applying Corollary 5 and Lemma 7. The length of the resulting sum depends only on the parity of m.

Remark Note that if $p \equiv 5 \pmod 8$, so that 2 is a quadratic non-residue, Theorem 8 yields

$$-2F(2) \equiv H_{\left[\frac{p}{2}\right]} \pmod{p}$$

as the sum contains only a single term. Moreover, as p is odd, $\left[\frac{p}{2}\right] = \frac{p-1}{2}$. In effect, we recover Eisenstein's congruence

$$-2F(2) \equiv H_{\frac{p-1}{2}} \pmod{p}$$

for all primes $p \equiv 5 \pmod 8$ [9]. In fact, we get a slight generalization of this result. Suppose $1 < m < p$ is an odd quadratic non-residue with $p \equiv 1 \pmod m$. From the previous remark, Theorem 8, and the fact that $\left[\frac{pj}{m}\right] = \frac{(p-1)j}{m}$, we deduce that

$$-mF(m) \equiv 2 \sum_{j=1}^{(m-1)/2} H_{\left(\frac{p-1}{m}\right)j} \pmod{p}.$$

Remark The Fermat quotient $F(a) = \frac{a^{p-1}-1}{p}$ satisfies the "logarithmic" functional equation

$$F(ab) = F(a) + F(b) \pmod{p}$$

for a and b coprime to p. Indeed, $a^{p-1} = 1 + pF(a)$ so that

$$1 + pF(ab) = (ab)^{p-1} = a^{p-1}b^{p-1} = (1 + pF(a))(1 + pF(b)) \equiv 1 + p(F(a) + F(b)) \left(\mathrm{mod}\ p^2\right)$$

from which the desired additive congruence is immediate. It is important to note that the Fermat quotient is a function from $(\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z}$.

Theorem 9 *Suppose $p \equiv 1 \pmod 4$ is prime. Then the Fermat quotient of any quadratic residue $\pmod p$ can be written as some linear combination of Fermat quotients of quadratic non-residues $\pmod p$. Precisely, if r is a quadratic residue $\pmod p$ such that $r \equiv \overline{a}\overline{b} \left(\mathrm{mod}\ p^2\right)$ for quadratic non-residues $\overline{a}, \overline{b} \left(\mathrm{mod}\ p^2\right)$ such that $\overline{a} \equiv a \pmod p$ and $\overline{b} \equiv b \pmod p$ then,*

$$-rF(r) \equiv \overline{b}\left[\frac{\overline{a}}{p}\right] + \overline{a}\left[\frac{\overline{b}}{p}\right] + \overline{b}\sum_{j=1}^{a-1} H_{\left[\frac{pj}{a}\right]} + \overline{a}\sum_{k=1}^{b-1} H_{\left[\frac{pk}{b}\right]} \pmod{p}.$$

Proof This follows from Theorem 8 and the logarithmic property of the Fermat quotients □

1.4 A Generalized Ankeny-Artin-Chowla Conjecture

In a recent paper [10], Yang and Fu formulated a generalization of the Ankeny-Artin-Chowla conjecture as follows. Let D be a positive integer which is not a perfect square. Consider the set of all solutions of the Brahmagupta-Pell equation

$$u^2 - Dv^2 = 1,$$

with u, v natural numbers. Let (u_1, v_1) be the least positive integer solution in this set and denote by $h(4D)$ the class number of primitive binary quadratic forms of discriminant $4D$. For D odd, they conjecture that

$$v_1 h(4D) \not\equiv 0 \pmod{D}.$$

We will refer to this as the generalized Ankeny-Artin-Chowla conjecture (GAAC). Assuming this conjecture, Fu and Yang show that the equation

$$x^y + y^x = z^2, \quad \min(x, y) > 1, \quad (x, y) = 1, \quad 2 \nmid xy, \quad x, y, z \in \mathbb{N}$$

has no solution. However, it appears that their conjecture has been made prematurely. Indeed, in [11, 12] independently have found a a list of six positive squarefree $D < 10^8$ such that $v_1 \equiv 0 \pmod{D}$. Of the six counterexamples only $D = 3 \cdot 69997$ and $D = 41 \cdot 79 \cdot 541$ are odd and congruent to 3 (mod 4). These two values of D represent counterexamples to GACC.

We will use an elementary sieve argument and basic algebraic number theory to show that GAAC is true for infinitely many discriminants D. We begin with a very simple set-theoretic sieve inequality:

Lemma 10 (The simple sieve) *Let S be a finite non-empty set and I a finite indexing set. For each $i \in I$, we assign a set $A_i \subset S$. If $J \subseteq I$, then*

$$\left| S \setminus \bigcup_{i \in I} A_i \right| \geq \left| S \setminus \bigcup_{j \in J} A_j \right| - \sum_{i \in I \setminus J} |A_i|.$$

An application of the simple sieve plus an elementary counting argument yields:

Lemma 11 *The number of $n \in \mathbb{N}$ less than x such that $n^2 - 1$ is square free is*

$$|\{n \leq x : n^2 - 1 \text{ is square free}\}| = Ax + O\left(\frac{x}{\log\log x}\right)$$

where

$$A = \prod_{p \leq \log\log x} \left(1 - \frac{2}{p^2}\right).$$

Proof Let x be sufficiently large. For each prime $p \leq x$ we define:

$$A_p = \{n \leq x : p^2 \mid (n^2 - 1)\}.$$

Then our goal is to estimate

$$\left|\{n \leq x\} \setminus \bigcup_{p \leq x} A_p\right|.$$

A straightforward application of the simple sieve gives the lower bound

$$\left|\{n \leq x\} \setminus \bigcup_{p \leq x} A_p\right| \geq \left|\{n \leq x\} \setminus \bigcup_{p \leq z} A_p\right| - \sum_{z \leq p \leq x} |A_p|.$$

where z is some parameter we will choose later.

We make the observation that if $n \in A_p$, then $p^2 \mid (n^2 - 1)$ and in particular, p^2 can only divide one of $n - 1$ or $n + 1$. Therefore, A_p will be the number of $n \leq x$ that reduce to $1 \pmod{p^2}$ or $-1 \pmod{p^2}$. From this we deduce that

$$|A_p| = \frac{2x}{p^2} + O(1).$$

Hence,

$$\sum_{z \leq p \leq x} |A_p| = 2x \sum_{z \leq p \leq x} \frac{1}{p^2} + O(\pi(x)).$$

By the integral test, we see that the sum is bounded above by $1/z$ and therefore we can bound the sum as

$$\sum_{z \leq p \leq x} |A_p| \ll \frac{x}{z} + O(\pi(x)).$$

Let $P_z = \prod_{p \leq z} p$. Then we have that

$$|\{n \leq x : n \notin A_p \text{ for any} p \leq z\}| = \sum_{n \leq x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d).$$

Switching the order of summation we have

$$\sum_{n \leq x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d) = \sum_{d \mid P_z} \mu(d) \sum_{\substack{n \leq x \\ n^2 \equiv 1 (d^2)}} 1.$$

The inner sum is $\frac{x 2^{\omega(d)}}{d^2} + O(2^{\omega(d)})$. Putting this into the above equality we have that

$$\sum_{n \leq x} \sum_{\substack{d^2 \mid (n^2-1) \\ d \mid P_z}} \mu(d) = x \sum_{d \mid P_z} \frac{\mu(d) 2^{\omega(d)}}{d^2} + O\left(\sum_{d \mid P_z} 2^{\omega(d)}\right).$$

Noting that $\mu(a)2^{\omega(a)}a^{-2}$ and $2^{\omega(a)}$ are multiplicative functions, we can write the two sums as products over all the primes less than z, i.e.,

$$\sum_{n\leq x}\sum_{\substack{d^2|(n^2-1)\\ d|P_z}}\mu(d) = x\prod_{p\leq z}\left(1-\frac{2}{p^2}\right)+O\left(\prod_{p\leq z}(1+2)\right).$$

The first product converges to a non-zero constant and the product in the error term can be estimated as $3^{\pi(z)}$. In all, we deduce that

$$|\{n\leq x : n^2-1 \text{ is square free}\}| = Ax + O\left(3^{\pi(z)}\right)+O\left(\frac{x}{z}+\pi(x)\right)$$

for some absolute non-zero constant A. Choosing $z=\log\log x$, we can bound the first big-O term by $O((\log x)^B)$ for some absolute constant B and the second term by $O(\frac{x}{\log\log x})$. In all,

$$|\{n\leq x : n^2-1 \text{ is square free}\}| = Ax + O\left(\frac{x}{\log\log x}\right) \qquad \square$$

For a more detailed analysis of squarefree values of quadratic functions $f(n)=n^2+c$, we refer the reader to section two of [13].

Theorem 12 *If $D=n^2-1$ is squarefree, then $\varepsilon = n+\sqrt{n^2-1}$ is the fundamental unit of $\mathbb{Q}(\sqrt{D})$. For such D, GAAC is true for D sufficiently large.*

Proof The fact that ε is the fundamental unit of $\mathbb{Q}(\sqrt{D})$ is an exercise in [14] (see Exercise 8.3.1 on page 115). In the notation of conjecture GAAC, we have $v_1=1$. As remarked earlier, $h(D)=O(\sqrt{|D|})$ and the assertion is now evident by Lemma 11. $\square$

1.5 The p-Adic Logarithm

One can define the p-adic logarithm using the power series

$$-\log(1-x)=\sum_{n=1}^{\infty}\frac{x^n}{n}.$$

Let $v_p(n)$ be the largest power of p dividing n. We denote by $|\cdot|_p$ the standard p-adic metric on $\mathbb{Q}$. Thus if $x=a/b$, $a,b\in\mathbb{Z}$, $\gcd(a,b)=1$ and $b\neq 0$, then

$$|x|_p = p^{v_p(b)-v_p(a)}.$$

Since for a given prime p, $v_p(n) \leq \left[\log n / \log p\right]$, we see that if $|x|_p = \lambda < 1$ then

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

converges p-adically because

$$\left|\frac{x^n}{n}\right|_p \leq \lambda^n p^{v_p(n)} \to 0$$

as $n \to \infty$.

As usual, we denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Given $\mathbb{Q}_p$, we take its algebraic closure $\overline{\mathbb{Q}_p}$, we then complete it to obtain the p-adic analogue of the complex numbers denoted by $\mathbb{C}_p$. This field is algebraically closed (see for example, Proposition 5.2 of [5]).

The p-adic logarithm defined above for $|x|_p < 1$ can now be extended to all of $\mathbb{C}_p^{\times}$ such that

$$\log xy = \log x + \log y$$

and $\log p = 0$. To avoid confusion with the usual logarithm, we denote the p-adic logarithm as $\log_p$.

To say that $|x|_p < 1$ is equivalent to saying $v_p(x) > 0$. If $v_p(x) \geq 1/(p-1)$, then in the series

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n},$$

we see that

$$v_p\left(\frac{x^{rp^v}}{p^v}\right) \geq \frac{rp^v - v(p-1)}{p-1} = \frac{r((p-1)+1)^v - v(p-1)}{p-1} \geq \frac{r\binom{v}{2}(p-1)^2}{p-1} \geq 1$$

if $v \geq 2$, $r \geq 1$ or if $v = 1$, $r \geq 2$ or if $v = 0$ and $r \geq p-1$. Thus, we have

$$\left|\log(1-x) - \sum_{j=1}^{p} \frac{x^j}{j}\right|_p < \frac{1}{p}.$$

In other words,

$$\log(1-x) = -\sum_{j=1}^{p} \frac{x^j}{j} \pmod{p}.$$

A simple extension of Wilson's theorem shows that for $1 \leq j \leq p-1$,

$$\frac{1}{p}\binom{p}{j} \equiv \frac{(-1)^{j-1}}{j} \pmod{p}.$$

Therefore,

$$\begin{aligned}\log(1-x) &\equiv \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(-1)^j x^j + \frac{1}{p}(-1)^p x^p \pmod{p} \\ &\equiv \frac{1}{p}\left((1-x)^p - 1\right) \pmod{p}.\end{aligned}$$

This proves:

Theorem 13 (Ankeny et al. 1952) *If* $v_p(x-1) \geq 1/(p-1)$, *then*

$$\log_p(x) \equiv \frac{x^p - 1}{p} \pmod{p}.$$

We can relate this to Fermat quotients

$$F(a) = \frac{a^{p-1} - 1}{p}$$

for $(a, p) = 1$ as follows. Writing $a^{p-1} = 1 + pF(a)$, we have

$$\log_p(a) = \frac{1}{p-1}\log_p a^{p-1} = \frac{1}{p-1}\log_p(1 + pF(a)).$$

On the other hand, we have the p-adic series

$$\frac{1}{p-1} = -1 - p - p^2 - \cdots$$

and

$$-\log_p(1+x) = -x + \frac{x^2}{2} - \cdots$$

so that

$$\begin{aligned}\log_p(a) &= (-1 - p - p^2 - \cdots)\left(pF(a) - \frac{p^2 F(a)^2}{2} + \cdots\right) \\ &\equiv -pF(a) \left(\text{mod } p^2\right).\end{aligned}$$

Thus, we have:

Theorem 14 *If* $(a, p) = 1$, *then*

$$F(a) \equiv -\frac{\log_p(a)}{p} \pmod{p}.$$

In particular, if we have sets of integers $\{a_s\}_{s=1}^{(p-1)/2}$ *and* $\{b_s\}_{s=1}^{(p-1)/2}$ *such that*

$$\prod_{s=1}^{(p-1)/2} a_s = -1 + p\Omega$$

and

$$\prod_{s=1}^{(p-1)/2} b_s = 1 + p\Omega^*,$$

then taking p-adic logarithms, we derive formula (3.2 ff) of [4]:

$$\Omega \equiv \sum_{s=1}^{(p-1)/2} F(a_s) \pmod{p}$$
$$\Omega^* \equiv \sum_{s=1}^{(p-1)/2} F(b_s) \pmod{p}$$

Remark It is this crucial discussion regarding the p-adic logarithm that is missing in [4].

1.6 The Group Ring, Gauss Sums, and Congruences

Another important idea of [3] is the use of the group ring attached to a Galois group Γ and how it operates on the field elements. More precisely, let $K/\mathbb{Q}$ be a finite Galois extension with Galois group Γ. The group ring $\mathbb{Q}[\Gamma]$ consists of elements

$$\sum_{g\in\Gamma} a_g g, \quad a_g \in \mathbb{Q}$$

and we define multiplication via

$$\left(\sum_{g\in\Gamma} a_g g\right)\left(\sum_{h\in\Gamma} b_h h\right) = \sum_{z\in\Gamma}\left(\sum_{gh=z} a_g b_h\right) z.$$

If Γ is abelian, then $\mathbb{Q}[\Gamma]$ is also abelian.

One can extend the action of Γ on the field elements K to the action of $\mathbb{Q}[\Gamma]$ in the obvious way: for $\alpha \in K$,

$$\left(\sum_{g\in\Gamma} a_g g\right)(\alpha) := \sum_{g\in\Gamma} a_g g(\alpha).$$

In the case of the cyclotomic field $\mathbb{Q}(\zeta_m)$ where ζ_m denotes a primitive m-th root of unity, the Galois group Γ, of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is $\Gamma \cong (\mathbb{Z}/m\mathbb{Z})^\times$, where the automorphism σ_a corresponding to the coprime residue class $a \pmod m$ is given via

$$\sigma_a(\zeta_m) = \zeta_m^a.$$

If $m = p$ is prime, we let $\zeta = \zeta_p$ and following [3], we denote by

$$G = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sigma_j$$

the element in the group ring $\mathbb{Q}[(\mathbb{Z}/p\mathbb{Z})^\times]$. Here $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. This element can be viewed as a "Gauss sum". Precisely we have:

Lemma 15 *Let $p \equiv 1 \pmod 4$ be a prime. Suppose ζ is a primitive p-th root of unity. Then for any $1 \le a \le p-1$,*

$$G(\zeta^a) \equiv \sqrt{p}\left(\frac{a}{p}\right)$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Proof By definition we have

$$G(\zeta^a) = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj}.$$

Making the change of variables, $k = aj$ we have

$$G(\zeta^a) = \sum_{k=1}^{p-1} \left(\frac{a^{-1}k}{p}\right) \zeta^k.$$

By multiplicativity of the Legendre symbol and $(a/p) = (a^{-1}/p)$ we have

$$G(\zeta^a) = \left(\frac{a^{-1}}{p}\right) \tau$$

where

$$\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

By Corollary 4.6 of [5], τ evaluates to

$$\tau = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$

The result follows. □

Given an element $\alpha \in K$ and $\beta = \sum_{g\in\Gamma} a_g g \in \mathbb{Q}[\Gamma]$, we will use the notation

$$\alpha^\beta := \prod_{g\in\Gamma} g(\alpha)^{a_g}.$$

We remark that given $x \in \mathbb{Q}$,

$$x^G = 1$$

as the character sum vanishes, and x is fixed by every group element.

The Dirichlet class number formula can then be written using the group ring formalism as follows. If $p \equiv 1 \pmod 4$, ε is the fundamental unit of $\mathbb{Q}(\sqrt{p})$ and h is the class number, then we have the familiar formula

$$2h \log \varepsilon = -\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \log(1 - \zeta^j). \tag{1.8}$$

Here, we have crucially used that $p \equiv 1 \pmod 4$ to evaluate the Gauss sum that appears in deriving (1.8). Exponentiating the expression in (1.8), we have that

$$\varepsilon^{2h} = (1 - \zeta)^{-G},$$

using our group ring formalism. As noted above, $x^G = 1$ for any $x \in \mathbb{Q}$, so

$$\varepsilon^{2h} = (1 - \zeta)^{-G} = (\zeta - 1)^{-G}.$$

If n is a quadratic non-residue (mod p), we make a change of variables in the sum defining G by sending $j \mapsto nj$. Under this change of variables, we have

$$G = \sum_{j=1}^{p-1} \left(\frac{nj}{p}\right) \sigma_{nj} = -\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sigma_{nj}.$$

Hence,

$$(1 - \zeta)^{-G} = (1 - \zeta^n)^G$$

from which it follows that

$$\varepsilon^{2h} = (\zeta^n - 1)^G.$$

Combining the two formulas for ε^{2h} gives

$$\varepsilon^{4h} = \left(\frac{\zeta^n - 1}{\zeta - 1}\right)^G = \left(\frac{\zeta^n - 1}{n(\zeta - 1)}\right)^G \tag{1.9}$$

since $n^G = 1$.

We then have the following lemma,

Lemma 16 *Let ζ be a primitive p-th root of unity for p a rational prime. For a quadratic non-residue* (mod p)*, set*

$$\alpha_j = \frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}.$$

Then $v_p(\alpha_j - 1) \geq 1/(p-1)$.

Proof Writing $\omega = \zeta^j$, we have that

$$\alpha_j = \frac{1 - \omega^n}{n(1-\omega)} = \frac{1}{n}\sum_{k=0}^{n-1} \omega^k.$$

Since $\zeta \equiv 1 \pmod{1-\zeta}$, we deduce that $\omega^k \equiv 1 \pmod{1-\zeta}$ for all $1 \leq k \leq n-1$. Hence, $\alpha_j \equiv 1 \pmod{1-\zeta}$. Therefore, $(1-\zeta)^{p-1}$ divides $(\alpha_j - 1)^{p-1}$. We have that $(p) = (1-\zeta)^{p-1}$. Hence,

$$(\alpha_j - 1)^{p-1} \equiv 0 \pmod{p}.$$

In particular, as $v_p(x)$ is multiplicative we have that

$$(p-1)v_p(\alpha_j - 1) \geq 1.$$

From which the desired conclusion follows. □

Observing that

$$\left(\frac{\zeta^n - 1}{n(\zeta - 1)}\right)^G = \prod_{j=1}^{p-1}\left(\frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}\right)^{\left(\frac{j}{p}\right)}$$

and applying the p-adic logarithm to both sides of (1.9), we have that

$$4h \log_p \varepsilon \equiv \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\log_p\left(\frac{\zeta^{nj} - 1}{n(\zeta^j - 1)}\right) \pmod{p}.$$

By Theorem 13 and Lemma 16 we deduce the congruence

$$4h\log_p \varepsilon \equiv \frac{1}{p}\sum_{j=1}^{p}\left(\frac{j}{p}\right)\left(\left(\frac{\zeta^{nj}-1}{n(\zeta^j-1)}\right)^p - 1\right) \equiv \frac{1}{n^p}G\left(\frac{\left(\frac{\zeta^n-1}{\zeta-1}\right)^p - n}{p}\right) \pmod p\,.$$

This is equivalent to

$$4h\log_p(\varepsilon) \equiv \frac{1}{n}G(f(\zeta)) \pmod p \tag{1.10}$$

where

$$f(x) = \frac{1}{p}\left\{\left(\frac{x^n-1}{x-1}\right)^p - \left(\frac{x^{np}-1}{x^p-1}\right)\right\}.$$

Noting that we can factor the two rational functions in the definition of $f(x)$, we deduce that $f(x)$ is a polynomial in x:

$$f(x) = \frac{1}{p}\left(\left(\sum_{k=0}^{n-1}x^k\right)^p - \sum_{j=0}^{n-1}x^{kp}\right). \tag{1.11}$$

Moreover, as $\zeta^p = 1$, we see that the second sum in (1.11) equals n when evaluated at ζ. Therefore, $f(\zeta) = \frac{1}{p}\left(\left(\frac{\zeta^n-1}{\zeta-1}\right)^p - n\right)$. Following [3] we wish to simplify $f(x) \pmod p$. In particular:

Lemma 17 *For $f(x)$ as defined above,*

$$f(x) \equiv -\sum_{k=1}^{p-1}\sum_{j=0}^{\infty}\frac{1}{k}x^{nk+pj} + \sum_{k=1}^{p-1}\sum_{j=0}^{n-1}\frac{j+1}{k}x^{k+pj} \pmod p$$

where the first sum is over $nk + pj < pn$.

Proof We write $f(x)$ as

$$f(x) = \frac{(x^n-1)^p(x^p-1) - (x^{pn}-1)(x-1)^p}{p}\cdot\frac{1}{(x-1)^p(x^p-1)}.$$

Noting that $\frac{1}{p}\binom{p}{k} \equiv \frac{(-1)^{k-1}}{k} \pmod p$ for $1 \le k \le p-1$ we have

$$\frac{(x-1)^p}{p} \equiv \frac{x^p-1}{p} - \sum_{k=1}^{p-1}\frac{x^{p-k}}{k} \pmod p\,.$$

Writing $\ell = p-k$, the above expansion $f(x)$ can be written as

$$f(x) \equiv \sum_{\ell=1}^{p-1} \frac{x^{n\ell}}{\ell(x^p-1)} - \sum_{\ell=1}^{p-1} \frac{x^\ell}{\ell} \cdot \frac{x^{pn}-1}{(x^p-1)^2} \pmod{p}.$$

Writing

$$\frac{1}{1-x^p} = \sum_{j=0}^{\infty} x^{pj} \quad \text{and} \quad \frac{1}{(1-x^p)^2} = \sum_{j=0}^{\infty} (j+1)x^{pj},$$

$$f(x) \equiv -\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{x^{n\ell+pj}}{\ell} + \sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{j+1}{\ell} x^{pj+\ell} - \sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{j+1}{\ell} x^{pj+pn+\ell} \pmod{p}.$$

Changing the index of summation in the last sum above from $j \mapsto j-n$ we have

$$f(x) \equiv -\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{x^{n\ell+pj}}{\ell} + \sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{j+1}{\ell} x^{pj+\ell} - \sum_{\ell=1}^{p-1}\sum_{j=n}^{\infty} \frac{j+1}{\ell} x^{pj+\ell} + \sum_{\ell=1}^{p-1}\sum_{j=n}^{\infty} \frac{n}{\ell} x^{pj+\ell} \pmod{p}.$$

The two middle sums cancel to give a finite sum. Next, we observe that the exponent in the last sum is over numbers greater than pn and coprime to p. As such, we can write the exponent $u = nv + pj$ for some $v \in \{1, \ldots, p-1\}$. As such,

$$u = nv + pj > pn \Rightarrow pj > n(p-v) > 0.$$

Hence, the exponent u appears in the first sum as well. Making a change of variables in the first sum of $\ell \mapsto n\ell$ we see that the term corresponding to the exponent u in the first sum has coefficient $-n/u$. Therefore, the last sum entirely vanishes. In effect,

$$f(x) \equiv -\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{1}{\ell} x^{n\ell+pj} + \sum_{\ell=1}^{p-1}\sum_{j=0}^{n-1} \frac{j+1}{\ell} x^{pj+\ell} \pmod{p}$$

where the first sum is over all $n\ell + pj < pn$. □

Finally, we require one more computational tool.

Lemma 18 *Suppose* $p \equiv 1 \pmod 4$. *Then*

$$S = \sum_{k=1}^{p-1} \frac{1}{k} \left(\frac{k}{p}\right) \equiv 0 \pmod{p}.$$

Proof We observe that

$$S \equiv \sum_{k=1}^{p-1} \frac{1}{p-k}\left(\frac{p-k}{p}\right) \equiv -\sum_{k=1}^{p-1} \frac{1}{k}\left(\frac{-k}{p}\right) \pmod{p}.$$

Since $p \equiv 1 \pmod 4$, $(-1/p) = 1$. Adding the two representations of S, we deduce that

$$2S \equiv 0 \pmod{p}.$$

Hence, $S \equiv 0 \pmod{p}$. □

Theorem 19 *(*Ankeny et al. 1952*) Suppose $p \equiv 1 \pmod 4$. Let h denote the class number of $\mathbb{Q}(\sqrt{p})$ and $\varepsilon = (t + u\sqrt{p})/2$ be the fundamental unit. Then*

$$4h\frac{u}{t} \equiv -\frac{1}{n}\sum_{k=1}^{p-1} \frac{1}{k}\left[\frac{nk}{p}\right]\left(\frac{k}{p}\right) \pmod{p}$$

for any quadratic non-residue $n \pmod p$.

Proof Suppose ζ is a primitive p-th root of unity. Then by Lemma 17,

$$f(\zeta) = -\sum_{\ell=1}^{p-1}\sum_{j=0}^{\infty} \frac{1}{\ell}\zeta^{n\ell} + \sum_{\ell=1}^{p-1}\sum_{j=0}^{n-1} \frac{1}{\ell}(j+1)\zeta^{\ell} \pmod{p}$$

where the first sum is over all $n\ell + pj < pn$. In particular, there are $1 + [n\ell/p]$ such j in the first sum. Changing the index of summation in the first sum from $\ell \mapsto p - \ell$ we have

$$f(\zeta) \equiv \sum_{\ell=1}^{p-1} \frac{1 + \left[\frac{n\ell}{p}\right]}{\ell}\zeta^{-n\ell} + \frac{n(n+1)}{2}\sum_{\ell=1}^{p-1} \frac{1}{\ell}\zeta^{\ell} \pmod{p}.$$

Then applying the element G as defined in (1.10) and using linearity of G, we have

$$G(f(\zeta)) \equiv \sum_{\ell=1}^{p-1} \frac{1 + \left[\frac{n\ell}{p}\right]}{\ell}G(\zeta^{-n\ell}) + \frac{n(n+1)}{2}\sum_{\ell=1}^{p-1} \frac{1}{\ell}G(\zeta^{\ell}) \pmod{p}.$$

By Lemma 15, this reduces to

$$G(f(\zeta)) \equiv \sqrt{p}\sum_{\ell=1}^{p-1}\left(\frac{-n\ell}{p}\right)\frac{1 + \left[\frac{n\ell}{p}\right]}{\ell} + \frac{n(n+1)}{2}\sqrt{p}\sum_{\ell=1}^{p-1} \frac{1}{\ell}\left(\frac{\ell}{p}\right) \pmod{p}.$$

Expanding the first sum out, applying Lemma 18, and noting that $-n$ is a quadratic non-residue $\pmod p$, we deduce that

$$G(f(\zeta)) \equiv -\sqrt{p} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \left[\frac{n\ell}{p} \right] \left(\frac{\ell}{p} \right) \pmod{p}.$$

Therefore,

$$4h \log_p(\varepsilon) \equiv -\frac{\sqrt{p}}{n} \sum_{\ell=1}^{p-1} \frac{1}{\ell} \left[\frac{n\ell}{p} \right] \left(\frac{\ell}{p} \right) \pmod{p}.$$

Noting that

$$\log_p(\varepsilon) \equiv \frac{u\sqrt{p}}{t} \pmod{p},$$

we conclude the result. □

1.7 Concluding Remarks

We have presented a self-contained treatment of some of the results in [3, 4]. We generalized the AAC conjecture in Theorem 1 and thus, related the AAC conjecture to a congruence of Fermat quotients. This generalization allowed us to obtain a generalization of a result of Eisenstein relating Fermat quotients to sums of harmonic numbers.

The function field analogue of the Ankeny-Artin-Chowla conjecture has been studied by Yu and Yu [12]. The case $p \equiv 3 \pmod 4$ has been studied by Mordell [15, 16] and he made a similar conjecture. In all cases, we have an interesting connection to Bernoulli numbers. In particular, if there are infinitely many regular primes (that is, primes p that do not divide the class number of the p-th cyclotomic field), then the Ankeny-Artin-Chowla and the Mordell conjectures are true for those primes p. It is unknown at present whether there are infinitely many regular primes though the conjecture is that there is a positive density of such primes. A relevant survey article by Slavutskii [17] is worth a careful study.

Acknowledgements We thank the referee for helpful comments.

References

1. Ankeny, N.C., Artin, E., Chowla, S.: The class-number of real quadratic fields. Proc. Natl. Acad. Sci. **37**(8), 524–525 (1951)
2. Kiselev, A.A.: An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers. Doklady Akad. Nauk SSSR (N.S.) **61**, 777–779 (1948)
3. Ankeny, N.C., Artin, E., Chowla, S.: The class-number of real quadratic number field. Ann. Math. **56**(3), 479–493 (1952)

4. Carlitz, L.: Note on the class number of real quadratic fields. Proc. Am. Math. Soc. **4**(4), 535–537 (1953)
5. Washington, L.: Introduction to cyclotomic fields. In: Graduate Texts in Mathematics, vol. 83. Springer, New York (1982)
6. van der Poorten, A.J., te Riele, H.J.J., Williams, H.C.: Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000. Math. Comput. **70**(235), 1311–1328 (2001)
7. Van Der Poorten, A.J., te Riele, H.J.J., Williams, H.C.: Corrigenda and addition to: "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000" [Math. Comput. **70**(235), 1311–1328 (2001); MR1709160 (2001j:11125)]. Math. Comput. **72**(241), 521–523 (2003)
8. Ankeny, N.C., Chowla, S.: A note on the class number of real quadratic fields. Acta Arith **6**, 145–147 (1960)
9. Eisenstein, F.: Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen ahhängen und durch gewisse lineare Funktional-Gleichungen definirt werden. Berichte Königl. Preuß. Akad **15**, 36–42 (1850)
10. Yang, H., Fu, R.: The exponential diophantine equation $x^y + y^x = z^2$ via a generalization of the Ankeny-Artin-Chowla conjecture. Int. J. Number Theory **14**(5), 1223–1228 (2018)
11. Stephens, A.J., Williams, H.C.: Some computational results on a problem concerning powerful numbers. Math. Comput. **50**(182), 619–632 (1988)
12. Yu, J., Yu, J.-K.: A note on a geometric analogue of Ankeny-Artin-Chowla's conjecture. Contemp. Math. **210**, 101–105 (1998)
13. Ram Murty, M.: Exponents of Class Groups of Quadratic Fields. Mehta Research Institute of Mathematics and Mathematical Physics, Allahabad, India (1999)
14. Ram Murty, M., Esmonde, J.: Problems in Algebraic Number Theory, Volume 190 of Graduate Texts in Mathematics, 2nd edn. Springer, New York (2005)
15. Mordell, L.J.: On a pellian equation conjecture. Acta Arith. **6**, 137–144 (1960)
16. Mordell, L.J.: On a Pellian equation conjecture. II. J. Lond. Math. Soc. **36**, 282–288 (1961)
17. Slavutskii, ISh.: Real quadratic fields and the Ankeny-Artin-Chowla conjecture. J. Math. Sci. **122**(6), 3673–3678 (2004)