TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 11, Pages 4445–4467
S 0002-9947(99)02325-9
Article electronically published on June 10, 1999

CLASS NUMBERS OF CYCLOTOMIC FUNCTION FIELDS

LI GUO AND LINGHSUEH SHU

ABSTRACT. Let q be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. For each polynomial $Q(T)$ in $\mathbb{F}_q[T]$, one could use the Carlitz module to construct an abelian extension of $\mathbb{F}_q(T)$, called a Carlitz cyclotomic extension. Carlitz cyclotomic extensions play a fundamental role in the study of abelian extensions of $\mathbb{F}_q(T)$, similar to the role played by cyclotomic number fields for abelian extensions of $\mathbb{Q}$. We are interested in the tower of Carlitz cyclotomic extensions corresponding to the powers of a fixed irreducible polynomial in $\mathbb{F}_q[T]$. Two types of properties are obtained for the l-parts of the class numbers of the fields in this tower, for a fixed prime number l. One gives congruence relations between the l-parts of these class numbers. The other gives lower bound for the l-parts of these class numbers.

Systematic study of cyclotomic field extensions of rational numbers started in the nineteenth century with Kummer and was essential in his work on Fermat's Last Theorem. Towers of cyclotomic number fields were first investigated by Iwasawa in the mid 1950's. One major application of his theory is to determine the growth of the p-divisibility of the class numbers for the fields in the tower [Iw].

The study of the cyclotomic theory of function fields started with Carlitz [Ca] in 1930. Let p be a prime and let q be a power of p. Carlitz regarded the rational function field $\mathbf{k} = \mathbb{F}_q(T)$ and the associated polynomial ring $\mathbf{A} = \mathbb{F}_q[T]$ as analogs of the rational number field $\mathbb{Q}$ and its ring of integers $\mathbb{Z}$. He constructed an $\mathbf{A}$-module, later called the "Carlitz module" , out of the completion of the algebraic closure of $\mathbb{F}_q((T))$, an analog of the field of complex numbers. For each polynomial P in $\mathbf{A}$, one could use the Carlitz module to construct a field extension $\mathbf{k}(P)$ of $\mathbf{k}$. The extensions obtained this way are called cyclotomic extensions and are essential in the study of all abelian extensions of $\mathbf{k}$. Fix an irreducible polynomial P in $\mathbf{A}$, and let n run through the set of positive integers. The cyclotomic extensions of $\mathbf{k}$ associated to P^n via the Carlitz module form a tower of extensions:

$$n\mathbf{k} \subset \mathbf{k}(P) \subset \mathbf{k}(P^2) \subset \cdots \subset \mathbf{k}(P^n) \subset \cdots .$$

It would be interesting to study the growth of the p-divisibility of the the class numbers for these fields along this tower, as Iwasawa did for cyclotomic extensions of a number field. This is the problem we would like to investigate in this paper.

As in the case of a cyclotomic number field, one can decompose the class number $h(\mathbf{k}(P^n))$ of $\mathbf{k}(P^n)$ into two integer factors $h^+(\mathbf{k}(P^n))$ and $h^-(\mathbf{k}(P^n))$, called the real part and the relative part of the class number. Let p be the unique prime

Received by the editors May 15, 1997.
1991 *Mathematics Subject Classification.* Primary 11R29, 11R58; Secondary 11R23.
Key words and phrases. Function fields, class numbers.
The authors were supported in part by NSF Grants #DMS-9301098 and #DMS-9525833.

©1999 American Mathematical Society

dividing q, the number of elements in the base field of $\mathbf{k}$. The main results of this paper are:

1. If the degree of the polynomial $P(T)$ is one, then both the relative part and real part of the class number $h(\mathbf{k}(P^n))$ are congruent to one modulo p (Theorem 2.3 and Theorem 2.4).
2. Let l be a prime number and assume $l \nmid \deg P$ if $l = p$. Then the l-part of the class number $h(\mathbf{k}(P^n))$ is congruent to the l-part of $h(\mathbf{k}(P))$ modulo p (Theorem 2.9).
3. Let l be a prime factor of $q-1$ and let a_0 be the exact exponent of l dividing $q-1$. The exponent of l dividing the relative part of the class number $h^-(\mathbf{k}(P^n))$ is at least $a_0(q^{(n-1)\deg P} - 1)$ (Theorem 3.1).
4. The exponent of p dividing the relative/real part of the class number $h^{\mp}(\mathbf{k}(P^n))$ is at least $\dfrac{a^{\mp}}{p-1}\dfrac{q^{(n-1)\deg P}-1}{n}$, where $a^{\mp}$ is a non-negative integer depending only on $\mathbf{k}(P)$. In most cases, $a^{\mp} = 0$ if and only if $p \nmid h^{\mp}(\mathbf{k}(P))$. In particular, this is so when $\deg P = 1$ (Theorem 3.4).

It is interesting to compare the last result with its known analog for number fields. Let $K_n = \mathbb{Q}(\zeta_{p^n})$, $\zeta_{p^n} = e^{2\pi i/p^n}$. Iwasawa [Iw2] proved that the power of p dividing the relative class number of K_n has exponent $\lambda n + \mu p^n + \nu$ for some integers λ, μ, ν and for all sufficiently large n. Later it was proved by Ferrero and Washington [F-W] that the invariant μ is zero. Thus the exponent of p dividing the relative class number of K_n grows linearly as n grows. The last result listed above shows that the exponent of p dividing the relative class number of $\mathbf{k}(P^n)$ grows at least exponentially as n grows if a^- is not zero. There are examples where a^- is not zero (see the remark following Theorem 3.4 for more detail). This phenomenon might be related to the fact that the extension we have here is much larger than a $\mathbb{Z}_p$-extension as in number field case.

Lower and upper bounds for the class numbers of the function fields were studied earlier by Gold-Kisilevski [G-K] and by Thakur [Th] using the genus formula. We study lower bounds for the individual primes dividing the class numbers. Thus the formulas here provide information for the prime factorization of the class numbers. In particular, this approach gives a lower bound for the exponent of p, the characteristic of the field, dividing the class number in analogy to Iwasawa's formula for number fields, as we have mentioned above. More comments and examples can be found in section 4.

The layout of this article is as follows. In section one, we give notations for cyclotomic extensions of rational function fields and earlier results needed in this paper. In section two, the real part and relative part of the class numbers are studied by using formulas recalled in section one. A Gauss sum-like formula is proved which enables us to obtain the first main result listed above. The second main result can then be proved by studying the characters of the Galois group and by using class field theory. In section three we focus on deducing lower bounds for the l-part and p-part of $h^-(\mathrm{k}(P^n))$, where l is a prime factor of $q-1$. Several variations of the lower bound are provided. In the last section, some numerical data is collected for small values of p and n, using the PARI library and Mathematica.

1. Notations and background

Let p be a prime number. Let q be a power of p and let $\mathbf{k} = \mathbb{F}_q(T)$ be the rational function field with base field $\mathbb{F}_q$, the finite field with q elements. Let $\mathbf{A} = \mathbb{F}_q[T]$ be the corresponding polynomial ring. Let Q be a polynomial in $\mathbf{A}$, and Ω be the completion of the algebraic closure of $\mathbb{F}_q((T))$. The Carlitz module associates each polynomial $Q \in \mathbf{A}$ to an additive endomorphism of Ω, denoted by $C(Q)$. More precisely, the map $C(Q)$ is given by an $\mathbb{F}_q$-linear polynomial with coefficients in $\mathbf{A}$. The cyclotomic extension of $\mathbf{k}$ associated to Q, denoted by $\mathbf{k}(Q)$, is then defined to be the field extension of $\mathbf{k}$ obtained by adjoining roots of $C(Q)$. The extension $\mathbf{k}(Q)$ of $\mathbf{k}$ is abelian and the Galois group of the extension is isomorphic to the multiplicative group $(\mathbf{A}/(Q))^\times$. Hayes showed [Ha] that there is a subfield $\mathbf{k}(Q)^+$ of $\mathbf{k}(Q)$, called the maximal real subfield, such that the infinite prime $(1/T)$ of $\mathbf{k}$ splits completely in $\mathbf{k}(Q)^+$. Further, the Galois group of $\mathbf{k}(Q)$ over $\mathbf{k}(Q)^+$ is isomorphic to $\mathbb{F}_q^\times$, similar to what happens in the cyclotomic number field extensions. One then follows the number field case to decompose the class number $h = h(\mathbf{k}(Q))$ of $\mathbf{k}(Q)$ into two integer factors, namely the real part $h^+ = h^+(\mathbf{k}(Q))$, which is the class number of the maximal real subfield $\mathbf{k}(Q)^+$, and the relative part $h^- = h^-(\mathbf{k}(Q))$, which is the quotient of the class number of $\mathbf{k}(Q)$ over the real part.

Let G be the Galois group $\mathrm{Gal}(\mathbf{k}(Q)/\mathbf{k})$. It is isomorphic to $(\mathbf{A}/(Q))^\times$. Let N be the set of coset representatives of $(\mathbf{A}/(Q))^\times$ that consists of all polynomials relatively prime to Q with degree less than the degree of Q. We can then identify the group G with the set N in which the subgroup $\mathrm{Gal}(\mathbf{k}(Q)/\mathbf{k}(Q)^+)$ is identified with the set of constant polynomials $a \in \mathbb{F}_q^\times$. We use M to denote the set of all monic polynomials in N, i.e., polynomials in $\mathbf{A}$ which are relatively prime to $Q(T)$, have degrees less than $\deg Q$ and have leading coefficients equal to 1. In this way, characters on G can be regarded as characters on the polynomials in $(\mathbb{F}_q[T]/(P^n))^\times$. A character χ is called real if the restriction of χ to $\mathbb{F}_q^\times$ is trivial, and is called non-real otherwise.

We now recall two earlier results about the real class number h^+ and relative class number h^- of $\mathbf{k}(Q)$ which are fundamental to our work in this paper. These results express the class numbers in terms of the values of characters on the set M of monic polynomials in $(\mathbf{A}/(Q))^\times$ that we have just described. The formula for h^+ was obtained by Galovich and Rosen [G-R] in 1981. They gave a class number formula for the special value of the L-function $L(t, \chi)$ at $t = 1$ with χ real. They then proved a formula for h^+ by combining this with the known result that

$$h^+ = \prod_{\chi \neq \mathrm{id}} L(1, \chi),$$

where the product runs through all non-trivial real characters. Let

$$r = \mid (\mathbf{A}/(Q))^\times \mid /(q-1) - 1,$$

their formula is

(1.1)

$$h^+(\mathbf{k}(Q)) = (q-1)^{-r} \prod_{\chi \text{ real},\ \chi \neq \mathrm{id}} \left(\sum_{a \in M} \chi(a) \left((\deg Q - 1 - \deg a)(q-1) - 1 \right) \right).$$

The following formula can then be deduced easily from the fact that $\sum_{a\in M}\chi(a)=0$ for each non-trivial real character χ:

$$h^+(\mathbf{k}(Q)) = \prod_{\chi \text{ real},\ \chi\neq \mathrm{id}} \left(\sum_{a\in M}(\deg Q - 1 - \deg a)\chi(a)\right) \tag{1.2}$$

$$= \prod_{\chi \text{ real},\ \chi\neq \mathrm{id}} \left(-\sum_{a\in M}\deg(a)\chi(a)\right). \tag{1.3}$$

A formula for h^- in the case of cyclotomic number fields was proved by Iwasawa [Iw] in 1960. Applying his idea to function fields, a formula for $L(1,\chi)$ when χ is non-real was obtained in [Sh]:

$$L(1,\chi) = \sum_{a \text{ monic}}\left(\frac{q-2}{q-1}\chi(a)\right) + \sum_{a \text{ non-monic}}\left(\frac{-1}{q-1}\chi(a)\right)$$

where a runs through all polynomials in N, i.e., the polynomials relatively prime to Q of degree less than $\deg Q$. (The formula in [Sh] was proved for much more general function fields than $\mathbb{F}_q(T)$.) Since $\sum_{a\in N}\chi(a)=0$, we have

$$L(1,\chi) = \sum_{a\in M}\chi(a). \tag{1.4}$$

Applying this equation to the known formula $h^-(\mathbf{k}(Q)) = \prod_{\chi \text{non-real}} L(1,\chi)$, it is proved that

$$h^-(\mathbf{k}(Q)) = \prod_{\chi \text{ non-real}}\left(\sum_{a\in M}\chi(a)\right). \tag{1.5}$$

These formulas make it possible to compute (in theory) h^+ and h^- for any given Q. In the last section of this paper, some values of class numbers are computed by using computer programs based on these formulas.

In all the above formulas, the characters are considered as primitive characters. However, when Q is a prime power P^n, which is the case we study in this paper, one could regard the characters as non-primitive ones also. Thus in this paper, we will feel free to use the characters in both senses.

Let P be an irreducible polynomial and let $Q=P^n$. Then for the Galois group $G_n = \mathrm{Gal}(\mathbf{k}(P^n)/\mathbf{k})$, we have the canonical isomorphism $G_n \cong G_n' \times G_n''$, where $G_n' \cong (\mathbb{F}_q[T]/(P(T)))^\times$ consists of the polynomials of degree less than $n\deg P$ whose orders modulo P^n are prime to p, and G_n'' is the finite p-group consisting of polynomials of degree less than $n\deg P$ which are invertible modulo P^n and are congruent to 1 modulo P. G_n'' can be further decomposed into a product of cyclic p-groups $G_n^{(1)},\cdots,G_n^{(m)}$. We will arrange the groups such that $G^{(i)}$ is of order $p^{g(i)}$ with $g(1)\geq\cdots\geq g(m)$.

2. Congruences of class numbers

Let $P(T)\in\mathbf{A}$ be an irreducible polynomial. Recall that we have identified $G_n = \mathrm{Gal}(\mathbf{k}(P^n)/\mathbf{k}) \cong (\mathbf{A}/(P^n))^\times$ with the set N_n of coset representatives of $(\mathbf{A}/(P^n))^\times$ consisting of all polynomials relatively prime to $P(T)$ with degree less than the degree of $P(T)^n$. Under this identification, we write M_n for the set of

monic polynomials in $(\mathbf{A}/P^n)^\times$. Use h_n, h_n^+, and h_n^- to denote the class numbers $h(\mathbf{k}(P^n))$, $h^+(\mathbf{k}(P^n))$, and $h^-(\mathbf{k}(P^n))$, respectively. We first give a direct consequence of formulas (1.2) and (1.5).

Theorem 2.1. *Let $Q = P^n$.*

(1) *If $\deg P = 1$ and $n = 1$, then the corresponding relative class number h_n^- is equal to one.*
(2) *If $\deg P = 1$ and $n = 1$ or 2, then the class number h_n^+ is equal to one.*

Proof. (1) If $\deg P = 1$, then the only monic polynomial with degree less than $\deg P$ is the identity polynomial. Then (1) follows from Equation (1.5).

(2) When $n = 1$, then one has $G_n \cong (\mathbf{A}/(P))^\times \cong \mathbb{F}_q^\times$. Also, there is a unique real character, i.e., the trivial character. So the product in equation (1.2) is over an empty index set; hence $h_n^+ = 1$. When $n = 2$, and $\deg P = 1$, equation (1.2) gives

$$nh_n^+ = \prod_{\chi \neq \mathrm{id}} \left(\sum_{a \in M_n} (2 - 1 - \deg a)\chi(a) \right).$$

Further, $\sum_{a \in M_n}(1 - \deg a)\chi(a) = 1$, since if $\deg a = 1$, then $1 - \deg a = 0$, and if $\deg a = 0$, then $a = 1$. □

We now study congruence properties of the L-values and class numbers.

Let χ be a character of G_n. Then χ decomposes into a product of χ' on G_n' and χ'' on G_n'' according to the decomposition $G_n \cong G_n' \times G_n''$. Thus if the character χ is non-real, then χ' is non-trivial. To compute $L(1, \chi)$ we use formula (1.4)

$$L(1, \chi) = \sum_{a \in M_n} \chi(a).$$

Here we regard χ as a character of $(\mathbb{F}_q[T]/(P^n))^\times$ and a is chosen with $\deg a < n \deg P$. First we need to get more information about the monic polynomials in M_n.

For any $x \in G_n$, write $x = x' + Px''$ with $\deg x' < \deg P$ and $x'' \in \mathbf{A}$. For $b \in G_n'$ and $c \in G_n''$, write $b = b' + Pb''$ and $c = 1 + Pc''$ as above and define $b * c = b' + Pc''$. The following properties of the operation $*$ are essential to the rest of this section.

Lemma 2.2. 1. *The projection of $b * c$ onto G_n' is b.*
2. *Let M_n'' be the subset of M_n consisting of all monic polynomials with degree greater than or equal to $\deg P$. Let $\mathcal{J}_n$ be the set of non-identity monic polynomials in G_n''. Then M_n'' is the disjoint union of $G_n' * c$ as c runs through $\mathcal{J}_n$.*

Proof. Let $f_n : G_n = (\mathbf{A}/(P^n))^\times \to (\mathbf{A}/(P))^\times$ be the modulo P map. More precisely, for $a \in G_n$, write $a = a' + Pa''$ with $\deg a' < \deg P$ and $a'' \in \mathbf{A}$; then the modulo P map is given by $a \mapsto a'$. This map is surjective and induces an isomorphism from G_n' onto $(\mathbf{A}/(P))^\times$ since they have the same cardinality. If we use $b(a')$ to denote the element of G_n' congruent to a' modulo P, then the projection of $a \in G_n$ onto G_n' is $b(a')$. Thus the decomposition of a in $G_n \cong G_n' \times G_n''$ is given by $a \mapsto (b(a'), b(a')^{-1}a)$ where $b(a')^{-1}$ is the inverse of $b(a')$ in $(\mathbf{A}/(P^n))^\times$. Now (1) is clear since b and $b * c$ are the same modulo P.

For $a \in M_n''$ with $a = a' + Pa''$ as above, write $b = b(a')$ for the element of G_n' congruent to a' modulo P and write $c = 1 + Pa''$. Then $a = b * c$. This expresses

M_n'' as the union $\bigcup G_n' * c$ where c runs through $\mathcal{J}_n$. From the definition, it is clear that $b_1 * c \neq b_2 * c$ if $b_1' \neq b_2'$. Thus the union is disjoint and (2) is proved. □

Theorem 2.3. *Let χ be a non-real character. Let K_χ be the extension of $\mathbb{Q}$ formed by adjoining all values of χ. Let $\wp$ be any prime ideal of K_χ over p.*

(1) *$L(1,\chi)$ is congruent to $\sum_{a\in M_n, \deg a<\deg P} \chi(a)$ modulo $\wp$.*
(2) *p divides the relative class number h_n^- of $\mathbf{k}(P^n)$ if and only if p divides the relative class number h_1^- of $\mathbf{k}(P)$.*
(3) *If $\deg P = 1$, then $L(1,\chi)$ is congruent to 1 modulo $\wp$.*
(4) *If $\deg P = 1$, then h_n^- is congruent to 1 modulo p. In particular, p does not divide h_n^-.*

Proof. (1) By Lemma 2.2,

$$\begin{aligned}\sum_{a\in M''} \chi(a) &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'} \chi(b*c)\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'} \chi'(b)\chi''(b^{-1}(b*c))\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'} \chi'(b)(\chi''(b^{-1}(b*c))-1)\right)\end{aligned}$$

since $\sum_{b\in G_n'} \chi'(b) = 0$. By definition, $\chi(a) \in K_\chi$. Let $\wp$ be a prime ideal of K_χ over p. Since G'' is a p-group, $\chi''(b^{-1}(b*c))$ is a p-power root of unity and $(\chi''(b^{-1}(b*c))-1)$ is divisibly by $\wp$. Thus $\wp$ divides $(\sum_{a\in M''}\chi(a))$. Therefore,

$$\begin{aligned}L(1,\chi) &= \sum_{a\in M_n} \chi(a)\\ &= \sum_{a\in M_n,\ \deg a<\deg P} \chi(a) + \sum_{a\in M_n''} \chi(a)\\ &\equiv \sum_{a\in M_n,\ \deg a<\deg P} \chi(a) \pmod{\wp}.\end{aligned}$$

This proves (1).

(2) From formula (1.5), p divides h_n^- if and only if $\wp$ divides $L(1,\chi)$ for some non-real character χ on $\mathrm{Gal}(\mathbf{k}(P^n)/\mathbf{k})$. By (1), this is equivalent to $\wp$ dividing $\sum_{a\in M_n,\deg a<\deg P} \chi(a)$. Let χ' be the restriction of χ to G_n'. From the equation

$$\chi(a) = \chi'(a)\chi''(a) = \chi'(a)(\chi''(a)-1) - \chi'(a)$$

and the fact that $\wp$ divides $\chi''(a)-1$, we see that $\wp$ dividing $\sum_{a\in M_n,\deg a<\deg P} \chi(a)$ is equivalent to $\wp$ dividing $\sum_{a\in M_n,\deg a<\deg P} \chi'(a)$. However χ' is a character on $\mathrm{Gal}(\mathbf{k}(P)/\mathbf{k})$. So by (1) again, the last statement is equivalent to $\wp$ dividing $L(1,\chi')$, which is equivalent to p dividing h_1^-, the relative class number of $\mathbf{k}(P)$.

When $\deg P = 1$, the only monic polynomial of M_n of degree less than $\deg P$ is 1. Thus $L(1,\chi) \equiv 1 \pmod{\wp}$. This is (3). Since $h^- = \prod_{\chi \text{ non}-\text{real}} L(1,\chi) \equiv 1 \pmod{\wp}$ and h^- is an integer, (4) follows. □

For the real part of the class number, we have

Theorem 2.4. *Let χ be a non-trivial real character of G_n. Let χ' be the restriction of χ to G'_n. Let $\wp$ be any prime ideal of K_χ over p.*

(1) *If χ' is non-trivial, then $\sum_{a \in M_n} \deg(a)\chi(a)$ is congruent modulo $\wp$ to $\sum_{a \in M_n, \deg a < \deg P} \deg(a)\chi(a)$. If χ' is trivial, then $\sum_{a \in M_n} \deg(a)\chi(a)$ is congruent modulo $\wp$ to $-\deg P$.*

(2) *If $p \nmid \deg P$, then p divides the real class number h_n^+ of $\mathbf{k}(P^n)$ if and only if p divides the real class number h_1^+ of $\mathbf{k}(P)$. If $p \mid \deg P$, then p divides h_n^+ for any $n > 1$.*

(3) *If $\deg P = 1$, then $\sum_{a \in M_n} \deg(a)\chi(a)$ is congruent to -1 modulo $\wp$.*

(4) *If $\deg P = 1$, then h_n^+ is congruent to 1 modulo p. In particular, p does not divide h_n^+.*

Remark 2.5. In part 2 of the theorem, when $p \mid \deg P$ and $n = 1$, it is possible that $p \mid h_1^+$ for some P, while $p \nmid h_1^+$ for some other P. See section 4 for examples.

Remark 2.6. Parts 3 and 4 of Theorem 2.3 and Theorem 2.4 are no longer true if the degree of P is greater then one. See Section 4 for examples.

Proof. The proof is similar to the case for relative class numbers. Let M''_n be the set of monic polynomials with degree less than or equal to $\deg P$. As in the proof of Theorem 2.3, applying Lemma 2.2 and using the fact that $\chi''(a) - 1$ is congruent to zero modulo $\wp$, we have

$$\begin{aligned}
\sum_{a \in M''_n} \deg(a)\chi(a) &= \sum_{c \in \mathcal{J}_n} \sum_{b \in G'_n} \deg(b*c)\chi(b*c) \\
&= \sum_{c \in \mathcal{J}_n} \sum_{b \in G'_n} \deg(c)\chi'(b)\chi''(b^{-1}(b*c)) \\
&= \sum_{c \in \mathcal{J}_n} \deg(c) \sum_{b \in G'_n} \chi'(b)\chi''(b^{-1}(b*c)) \\
&\equiv \sum_{c \in \mathcal{J}_n} \deg(c) \sum_{b \in G'_n} \chi'(b) \bmod \wp.
\end{aligned}$$

If χ' is non-trivial, then $\sum_{b \in G'_n} \chi'(b)$ is zero. Thus

$$\sum_{a \in M_n} \deg(a)\chi(a) \equiv \sum_{a \in M_n, \deg(a) < \deg(P)} \deg(a)\chi(a) \bmod \wp.$$

Now assume that χ' is trivial. Since χ is non-trivial, we necessarily have $n > 1$. Since $\deg(\alpha c) = \deg c$ for $\alpha \in \mathbb{F}_q^\times$, from the above equations we get

$$\sum_{a \in M''_n} \deg(a)\chi(a) \equiv (q^{\deg P} - 1) \sum_{c \in \mathcal{J}_n} \deg(c) \equiv \frac{q^{\deg P} - 1}{q - 1} \sum_{c \in G''_n - \{1\}} \deg(c) \bmod \wp.$$

So we only need to compute $\sum_{a\in G_n''-\{1\}}\deg(a)$. The polynomial $a\in G_n''$ can be uniquely expressed as $a=bP+1,\ b\neq 0,\ 0\le\deg(b)<(n-1)\deg P$. Then

$$\begin{aligned}
\sum_{a\in G_n''-\{1\}}\deg(a) &= \sum_{b\neq 0,\ 0\le\deg b<(n-1)\deg P}(\deg P+\deg(b))\\
&= (p^{(n-1)\deg P}-1)\deg P+\sum_{k=0}^{(n-1)\deg P-1}k\#\{b|\deg(b)=k\}\\
&= (p^{(n-1)\deg P}-1)\deg P+\sum_{k=1}^{(n-1)\deg P-1}k[(q^{k+1}-1)-(q^k-1)]\\
&= (p^{(n-1)\deg P}-1)\deg P+[(n-1)\deg P-1]q^{(n-1)\deg P}-\sum_{i=1}^{(n-1)\deg P-1}q^i\\
&= (p^{(n-1)\deg P}-1)\deg P+[(n-1)\deg P-1]q^{(n-1)\deg P}+1-\frac{1-q^{(n-1)\deg P}}{1-q}\\
&\equiv -\deg P \bmod \wp.
\end{aligned}$$

Therefore,

$$\sum_{a\in M_n''}\deg(a)\chi(a)\equiv\frac{q^{\deg P}-1}{q-1}(-\deg P)\equiv-\deg P \bmod \wp.$$

On the other hand,

$$\sum_{a\neq 0,\ \deg(a)<\deg P}\deg(a)=\sum_{k=0}^{\deg P-1}k(q^{k+1}-q^k)\equiv 0 \bmod \wp.$$

Hence $\sum_{a\in M_n,\ \deg(a)<\deg P}\deg(a)\equiv 0 \bmod \wp$. Therefore, when χ' is trivial,

$$\sum_{a\in M_n}\deg(a)\chi(a)\equiv-\deg P \bmod \wp.$$

This finishes the proof of (1).

To prove (2), note that when $p\nmid\deg P$

$$\begin{aligned}
p\mid h_n^+ &\iff \wp\mid\sum_{a\in M_n}\deg(a)\chi(a),\ \text{for some } \chi \text{ with } \chi' \text{ non-trivial}\\
&\iff \wp\mid\sum_{a\in M,\ \deg(a)<\deg P}\deg(a)\chi(a),\ \text{for some } \chi \text{ with } \chi' \text{ non-trivial}\\
&\iff \wp\mid\sum_{a\in M_n,\ \deg(a)<\deg P}\deg(a)\chi'(a),\ \text{for some non-trivial } \chi'\\
&\iff p\mid h_1^+
\end{aligned}$$

When $p\mid\deg P$, (2) clearly follows from (1).

When $\deg P=1$, χ real means that χ' is trivial. When $n=1$, (3) is proved in Theorem 2.1.(2). When $n>1$, (1) shows that $\sum_{a\in M}\deg(a)\chi(a)\equiv-1 \bmod \wp$. This proves (3). Part (4) follows from (3) and equation (1.2). □

Now we consider the special case that $\deg P = 1$ and $n = 2$. Then the Galois group $\mathrm{Gal}(\mathbf{k}(P^2)/\mathbf{k})$ is isomorphic to $(\mathbb{F}_q[T]/(T^2))^\times$ and we have an isomorphism

$$(\mathbb{F}_q[T]/(T^2))^\times \cong \mathbb{F}_q^\times \times \{f(T) \pmod{T^2} \mid f(0) = 1\}$$

and an isomorphism $\{f(T) \pmod{T^2} \mid f(0) = 1\} \cong \mathbb{F}_q$ is given by $f(T) = 1+\alpha T \mapsto \alpha,\ \alpha \in \mathbb{F}_q$. Thus the decomposition of χ on $G_n \cong G_n' \times G_n''$ into $\chi'\chi''$ is, in fact, a decomposition into a multiplicative character χ' on $\mathbb{F}_q^\times$ and an additive character χ'' on $\mathbb{F}_q$. Moreover, for $a = c+T = c(1+c^{-1}T)$, we have $\chi(a) = \chi'(c)\chi''(1+c^{-1}T)$, which is $\chi'(c)\chi''(c^{-1})$ regarded as characters on $\mathbb{F}_q$ and $\mathbb{F}_q^\times$. This shows that the sum $\sum_{a\in M,\ a\neq 1}\ \chi(a)$ is actually a Gauss sum $\sum_{c\in\mathbb{F}_q^\times} \overline{\chi'(c)}\chi''(c)$. Consequently,

$$nL(1,\chi) = \sum_{a\in M} \chi(a) = 1 + \sum_{c\in\mathbb{F}_q^\times} \overline{\chi'(c)}\chi''(c).$$

As $\mid \sum_{c\in\mathbb{F}_q^\times} \overline{\chi'(c)}\chi''(c) \mid = \sqrt{q}$, the absolute value $\mid L(1,\chi) \mid$ is asymptotically given by $\sqrt{q}$ for q large. Since $h^- = \prod_{\chi\ \mathrm{non-real}} L(1,\chi)$ and there are $q(q-2)$ non-real characters, we obtain the following theorem.

Theorem 2.7. *Let $h^-(q)$ be the relative class number of $\mathbf{k}(P^2)$, where $\mathbf{k} = \mathbb{F}_q(T)$ and P is a polynomial of degree one. Then for q large, $h^-(q)$ is asymptotic to $q^{q(q-2)/2}$.*

Recall from Theorem 2.1 that $h^+ = 1$ for $\mathbf{k}(P^2)$. Thus we get

Corollary 2.1. *Let P be a polynomial in of degree one. The class number of $\mathbf{k}(P^2)$ is asymptotic to $q^{q(q-2)/2}$ for q large.*

We next study the l-part of the class number h_n for each prime integer l by using equations (1.2) and (1.5). We first give a lemma on the characters of $G = G_n = \mathrm{Gal}(\mathbf{k}(P^n)/\mathbf{k}) \cong (\mathbb{F}_q[T]/(P^n))^\times$. For such a character χ, let K_χ be the field extension of $\mathbb{Q}$ obtained by adjoining the values of χ.

Lemma 2.8. *Let χ be a character on G_n.*

(1) *The element $L(1,\chi)$ is contained in K_χ for all χ.*
(2) *If $\chi \neq \mathrm{id}$ is trivial when restricted to G'', then*

$$\sum_{a\in M_n} \chi(a) = \sum_{a\in M_n, \deg(a)<\deg P} \chi(a)$$

and

$$\sum_{a\in M_n} \deg(a)\chi(a) = \sum_{a\in M_n, \deg(a)<\deg P} \deg(a)\chi(a).$$

(3) *If χ is non-real and is trivial when restricted to G_n'', and if $\deg P = 1$, then $L(1,\chi) = 1$.*

Proof. The first statement follows from formulas (1.2) and (1.5) in section 1. Next assume that χ is a non-trivial character but is trivial on G_n''. Then χ'' is trivial and

χ' must be non-trivial. Thus, as in the proof of Theorem 2.3, we have

$$\begin{aligned}\sum_{a\in M_n''}\chi(a) &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\chi(b*c)\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\chi'(b)\chi''(b^{-1}(b*c))\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\chi'(b)\right)=0.\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{a\in M_n}\chi(a) &= \sum_{a\in M_n,\ \deg a<\deg P}\chi(a)+\sum_{a\in M_n''}\chi(a)\\ &= \sum_{a\in M_n,\ \deg a<\deg P}\chi(a).\end{aligned}$$

Moreover, since $\deg(b*c)=\deg(c)$ from the definition of $b*c$,

$$\begin{aligned}\sum_{a\in M_n''}\deg(a)\chi(a) &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\deg(b*c)\chi(b*c)\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\deg(b*c)\chi'(b)\chi''(b^{-1}(b*c))\right)\\ &= \sum_{c\in\mathcal{J}_n}\left(\sum_{b\in G_n'}\deg(c)\chi(b)\right)\\ &= \sum_{c\in\mathcal{J}_n}\deg(c)\left(\sum_{b\in G_n'}\chi(b)\right)=0.\end{aligned}$$

Therefore,

$$\begin{aligned}&\sum_{a\in M_n}\deg(a)\chi(a)\\ =&\sum_{a\in M_n,\ \deg a<\deg P}\deg(a)\chi(a)+\sum_{a\in M_n''}\deg(a)\chi(a)\\ =&\sum_{a\in M_n,\ \deg a<\deg P}\deg(a)\chi(a).\end{aligned}$$

This proves the second part.

(3) follows from (2) since $L(1,\chi)=\sum_{a\in M_n}\chi(a)$ and the only monic polynomial with degree less than $\deg P=1$ is 1. □

Theorem 2.9. *Let l be any prime number.*

(1) *The l-part of h_n^- is congruent to the l-part of h_1^- modulo p. Assuming $l\nmid\deg P$ when $l=p$, the l-part of h_n^+ is congruent to the l-part of h_1^+ modulo p.*

(2) *Assuming* $p \nmid \deg P$ *when* $l = p$, *the* l*-part of* h_n *is congruent to the* l*-part of* h_1 *modulo* p.
(3) *When* $\deg P = 1$, *the* l*-part of* $h_n^{\mp}$ *is congruent to* 1 *modulo* p.

Proof. (1) We start with h_n^-. By Theorem 2.3.(2), the p-part of h_n^- is congruent to the p-part of h_1^- modulo p. So we can assume that the prime l is different from p. Let χ be any non-real character. By Lemma 2.8, the norm $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$ is a rational integer. We decompose χ into $\chi'\chi''$ according to the decomposition $G_n \cong G_n' \times G_n''$.

Claim 1. For any non-real character χ that is non-trivial on G_n'', and for any prime number l not equal to p, the exact power of l dividing $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$ is congruent to 1 modulo p.

Proof of Claim 1. We fix such a character χ. Let l be a prime number different from p. Note that

$$N_{\mathbb{Q}}^{K_\chi} L(1,\chi) = N_{\mathbb{Q}}^{K_{\chi''}} (N_{K_{\chi''}}^{K_\chi} L(1,\chi)).$$

Write the principle ideal of $K_{\chi''}$ generated by $N_{K_{\chi''}}^{K_\chi} L(1,\chi)$ as

$$(N_{K_{\chi''}}^{K_\chi} L(1,\chi)) = (\prod_i \mathcal{L}_i)\mathcal{B}$$

with $\mathcal{L}_i \mid l$ and $(\mathcal{B}, l) = 1$. Then the prime power of l dividing $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$ is a positive generator of $N_{\mathbb{Q}}^{K_{\chi''}}(\prod_i \mathcal{L}_i)$. Let p^c be the order of χ''. By definition, $K_{\chi''}$ is the ray class field of p^c. Since $(\prod_i \mathcal{L}_i)$ is relatively prime to p, it follows from class field theory that $N_{\mathbb{Q}}^{K_{\chi''}}(\prod_i \mathcal{L}_i)$ has a positive generator that is congruent to one modulo p^c. Thus the prime power of l dividing $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$ is congruent to one modulo p^c. Since χ'' is non-trivial, the number c is positive, so the prime power of l dividing $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$ is congruent to one modulo p. This proves the claim. □

We next use the Galois action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the characters of G_n to divide the set of non-real characters into conjugacy classes. Note that taking conjugates preserves the properties that a character is non-real and that a character is trivial on G_n''. Let Σ_n be a set of representatives of distinct conjugacy classes of non-trivial characters. Further, let Σ_n' be the subset of Σ_n consisting of the characters trivial on G_n''. Let Σ_n'' be the subset of Σ_n consisting of the non-real characters. For a fixed $\chi \in \Sigma_n$, let C_χ be the conjugacy class of χ. From formula (1.5) we have $\prod_{\psi \in C_\chi} L(1,\psi) = N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$. Thus

$$h_n^- = \prod_{\chi \text{ non real}} L(1,\chi) = \prod_{\chi \in \Sigma_n''} \prod_{\psi \in C_\chi} L(1,\psi) = \prod_{\chi \in \Sigma_n''} N_{\mathbb{Q}}^{K_\chi} L(1,\chi).$$

By Claim 1, the p-part of h_n^- is congruent to the p-part of $\prod_{\chi \in \Sigma_n'' \cap \Sigma_n'} \prod_{\psi \in C_\chi} L(1,\psi)$ modulo p.

For a character $\chi \in \Sigma_n'$ and $\psi \in C_\chi$, ψ is trivial on G_n''. So by Lemma 2.8.2, we have $L(1,\psi) = \sum_{a \in M_n,\ \deg a < \deg P} \psi(a)$. Consider the modulo P map

$$f_n : G_n \cong (\mathbf{A}/(P^n))^\times \to G_1 \cong (\mathbf{A}/(P))^\times.$$

The kernel is G_n''. The map induces an isomorphism from the group of characters of G_n which are trivial on G_n'' to the group of characters of G_1. It also induces a one-to-one correspondence between the set $\{a_n \in M_n,\ \deg a_n < \deg P\}$ and the

set M_1. Here and in the rest of the proof, we use M_n to denote the set of monic polynomials from $G_n \cong (\mathbf{A}/(P^n))^\times$, use a_n to denote an element in M_n, and use ψ_n or χ_n to denote a character on G_n.

Claim 2. Let ψ_n be a character of G_n that is trivial on G_n'', and let ψ_1 be the corresponding character on G_1. Then

$$\sum_{a_n \in M_n,\ \deg a_n < \deg P} \psi_n(a_n) = \sum_{a_1 \in M_1} \psi_1(a_1)$$

and

$$\sum_{a_n \in M_n,\ \deg a_n < \deg P} \deg(a_n)\psi_n(a_n) = \sum_{a_1 \in M_1} \deg(a_1)\psi_1(a_1).$$

Proof. This is clear since $\psi_n = \psi_1 \circ f_n$ and, for $a_n \in M_n$ such that $\deg a_n < \deg P$ and $f_n(a_n) = a_1 \in M_1$, we have $\psi_n(a_n) = \psi_1 \circ f_n(a_n) = \psi_1(a_1)$ and $\deg(a_n) = \deg(f_n(a_n))$. □

Now, putting everything together, we have

$$\begin{aligned}
&l\text{-part of } h_n^- \\
&= \quad l\text{-part of } \prod_{\psi_n \text{ non-real}} L(1,\psi_n) \\
&= \quad l\text{-part of } \prod_{\chi_n \in \Sigma_n''} \left(\prod_{\psi_n \in C_{\chi_n}} L(1,\psi_n) \right) \\
&\equiv \quad l\text{-part of } \prod_{\chi_n \in \Sigma_n'' \cap \Sigma_n'} \left(\prod_{\psi_n \in C_{\chi_n}} L(1,\psi_n) \right) \pmod{p} \quad \text{(Claim 1)} \\
&= \quad l\text{-part of } \prod_{\psi_n \text{ non-real},\ \psi_{n|G_n''} = \mathrm{id}} \left(\sum_{a_n \in M_n,\ \deg a_n < \deg P} \psi_n(a_n) \right) \quad \text{(Lemma 2.8)} \\
&= \quad l\text{-part of } \prod_{\psi_1 \text{ non-real}} \left(\sum_{a_1 \in M_1} \psi_1(a_1) \right) \quad \text{(Claim 2)} \\
&= \quad l\text{-part of } \prod_{\psi_1 \text{ non-real}} L(1,\psi_1) \pmod{p} \quad \text{(Formula (1.5))} \\
&= \quad l\text{-part of } h_1^-.
\end{aligned}$$

This proves the statement for h_n^-.

The proof for the congruence of h_n^+ is similar. The congruence for the p-part follows from Theorem 2.4.(2). Now consider a prime $l \neq p$. Let χ_n be a non-trivial real character of G_n. So χ_n is trivial on the subgroup $\mathbb{F}_q^\times$ of $(\mathbf{A}/(P^n))^\times$. Since any polynomial can be uniquely written as the product of an element in $\mathbb{F}_q^\times$ and a monic polynomial, we see that $(\mathbf{A}/(P^n))^\times$ is the disjoint union of $\mathbb{F}_q^\times a_n$ as a_n runs through M_n. Thus we have

$$n \sum_{a_n \in M_n} \chi_n(a_n) = (1/(q-1)) \sum_{x_n \in (\mathbf{A}/(P^n))^\times} \chi_n(x_n) = 0$$

since χ_n is non-trivial. Therefore formula (1.2)

$$h_n^+ = \prod_{\chi_n \text{ real},\ \chi_n \neq \mathrm{id}} \left(\sum_{a_n \in M_n} (\deg P^n - 1 - \deg a_n)\chi_n(a_n) \right)$$

can be further simplified to

$$h_n^+ = \prod_{\chi_n \text{ real},\ \chi_n \neq \mathrm{id}} \left(- \sum_{a_n \in M_n} \deg(a_n)\chi_n(a_n) \right).$$

The same argument used to prove Claim 1 can also be used to prove

Claim 3. For any character χ_n of G_n that is non-trivial on G_n'', and for any prime number l not equal to p, the exact power of l dividing

$$N_{\mathbb{Q}}^{K_{\chi_n}} \left(\sum_{a_n \in M_n} \deg(a_n)\chi_n(a_n) \right)$$

is congruent to 1 modulo p.

Let Σ_n and Σ_n' be as defined earlier in the proof. Let Σ_n^r be the subset of Σ_n consisting of the non-trivial real characters of G_n. We have

$$\begin{aligned}
&l\text{-part of } h_n^+ \\
&= l\text{-part of } \prod_{\psi_n \text{ real},\ \psi_n \neq \mathrm{id}} \left(- \sum_{a_n \in M_n} \deg(a_n)\psi_n(a_n) \right) \quad \text{(Formula (1.2))} \\
&= l\text{-part of } \prod_{\chi_n \in \Sigma_n^r} \left(\prod_{\psi_n \in C_{\chi_n}} \left(- \sum_{a_n \in M_n} \deg(a_n)\psi_n(a_n) \right) \right) \\
&\equiv l\text{-part of } \prod_{\chi_n \in \Sigma_n^r \cap \Sigma_n'} \left(\prod_{\psi_n \in C_{\chi_n}} \left(- \sum_{a_n \in M_n} \deg(a_n)\psi_n(a_n) \right) \right) \pmod{p} \\
&\qquad \text{(Claim 3)} \\
&= l\text{-part of } \prod_{\psi_n \text{ real},\ \psi_n \neq \mathrm{id},\ \psi_{n|G_n''} = \mathrm{id}} \left(- \sum_{a_n \in M_n} \deg(a_n)\psi_n(a_n) \right) \\
&= l\text{-part of } \prod_{\psi_n \text{ real},\ \psi_n \neq \mathrm{id},\ \psi_{n|G_n''} = \mathrm{id}} \left(- \sum_{a_n \in M_n,\ \deg a_n < \deg P} \deg(a_n)\psi_n(a_n) \right) \\
&\qquad \text{(Lemma 2.8)} \\
&= l\text{-part of } \prod_{\psi_1 \text{ real},\ \psi_1 \neq \mathrm{id}} \left(- \sum_{a_1 \in M_1} \deg(a_1)\psi_1(a_1) \right) \quad \text{(Claim 2)} \\
&= l\text{-part of } h_1^+ \quad \text{(Formula (1.2))}.
\end{aligned}$$

This proves the statement for h_n^+.

Part 2 of the theorem clearly follows from part 1. Finally, when $\deg P = 1$, Theorem 2.3 and Theorem 2.4 show that $h_n^{\mp}$ is relatively prime to p. So we only need to consider primes $l \neq p$. Then (3) follows from (1) and Theorem 2.1. □

3. Asymptotic formulas

The purpose of this section is to get some asymptotic formulas for lower bounds of the power of a fixed prime l dividing the class number of $\mathbf{k}(P^n)$ as n goes to infinity. The prime p and some other primes are considered.

We first consider the case where l is different from p. Recall that we have the decomposition of $G_n = (\mathbb{F}_q[T]/(P(T))^n)^\times$ into $G'_n \times G''_n \cong G'_n \times \prod_{i=1}^m G_n^{(i)}$ with $G'_n \cong (\mathbb{F}_q[T]/(P(T)))^\times$ of order $q^{\deg P} - 1$ and $G_n^{(i)}$ cyclic of order $p^{g_n^{(i)}}$ such that $g_n^{(1)} \geq g_n^{(2)} \geq \cdots \geq g_n^{(m)}$.

Theorem 3.1. *Let h_n^- be the relative class number of $\mathbf{k}(P^n)$. Let l be a prime factor of $q-1$, and let a_0 be the highest power of l dividing $q-1$. A lower bound for the l-part of h_n^- is given by $a_0(q^{(n-1)\deg P} - 1)$.*

In order to prove this theorem, we start with a lemma on the set M_n of monic polynomials in the multiplicative group $(\mathbf{A}/(P^n))^\times = (\mathbb{F}_q[T]/(P(T))^n)^\times$. Recall that this is the set of monic polynomials with degree less than $n \deg P$ that are relatively prime to P. The quotient map from $(\mathbf{A}/(P^n))^\times$ to $(\mathbf{A}/(P))^\times$ gives an isomorphism of G'_n onto $(\mathbf{A}/(P))^\times$. Let $\mathcal{H}_n$ be the set of polynomials of G'_n whose coefficients modulo P have leading coefficient one. Recall that G''_n is the set of polynomials modulo $P(T)^n$ which are congruent to 1 modulo $P(T)$. For any $h \in \mathcal{H}_n$ and $g \in G''_n$, define $h \star g$ to be the unique monic polynomial associated to the polynomial product $hg \pmod{P^n}$, i.e., the monic polynomial obtained by dividing $hg \pmod{P^n}$ by its leading coefficient.

Warning. Do not confuse the operation $\star$ and the next lemma with the operation $*$ and Lemma 2.2 in Section 2.

Lemma 3.2. (1) *The projection of $h \star g$ onto G''_n is g.*
(2) *M_n is the disjoint union of the sets $h \star G''_n$ for $h \in \mathcal{H}_n$.*

Proof. (1). Since $h \star g$ and hg differ by a factor from $\mathbb{F}_q^\times \subseteq G'_n$, $h \star g$ has the same projection onto G''_n as hg. Since the projection of h onto G''_n is one, the projection of $h \star g$ onto G''_n is the same as the projection of g, which is g itself by definition.

To prove (2), we first prove that the union $\bigcup_{h \in \mathcal{H}_n} h \star G''_n$ is disjoint. If $h_1 \star g_1 = h_2 \star g_2$ for $h_1, h_2 \in \mathcal{H}_n,\ g_1, g_2 \in G''_n$, then $c_1^{-1}(h_1 g_1) = c_2^{-1}(h_2 g_2)$ where c_1 (resp. c_2) is the leading coefficient of $h_1 g_1$ (resp. $h_2 g_2$). Writing $g_i = Q_i P + 1,\ i = 1, 2$, then $h_1 \star g_1 = h_2 \star g_2$ means $c_1^{-1} h_1 Q_1 P + c_1^{-1} h_1 = c_2^{-1} h_2 Q_2 P + c_2^{-1} h_2$. Taking the two sides modulo P, we get $c_1^{-1} h_1 = c_2^{-1} h_2$ modulo P. By the definition of $\mathcal{H}_n$, $c_1 = c_2$. Thus $h_1 = h_2$ modulo P. As h_1 and h_2 are in G'_n, and the reduction modulo P gives an isomorphism between G'_n and $(A/(P))^\times$, we have $h_1 = h_2$. Multiplying two sides of the equation $h_1 Q_1 P + h_1 = h_2 Q_2 P + h_2$ by the inverse of $h_1 = h_2$ modulo $P(T)^n$, we get $Q_1 P + 1 = Q_2 P + 1$. That is $g_1 = g_2$.

There are $q^{\deg P} - 1$ polynomials in $(A/(P))^\times$ and $(q^{\deg P} - 1)/(q-1)$ of them are monic. This is also the cardinality of $\mathcal{H}_n$ because of the 1-1 correspondence provided by the quotient map modulo P. Therefore the cardinality of $\bigcup_{h \in \mathcal{H}_n} h \star G''_n$ is

$$|\mathcal{H}_n|\ |G''_n| = (\frac{q^{\deg P} - 1}{q-1})(q^{(n-1)\deg P}) = \frac{q^{n \deg P} - q^{(n-1)\deg P}}{q-1}.$$

On the other hand, there are $q^{n\deg P}-q^{(n-1)\deg P}$ polynomials in G_n. After we divide them by their leading coefficients, we get $(q^{n\deg P}-q^{(n-1)\deg P})/(q-1)$ monic polynomials. Therefore $M_n=\bigcup_{h\in\mathcal{H}_n} h\star G_n''$. □

Proof of the theorem. Fix a j with $1\le j\le a_0$, where l^{a_0} is the highest power of l dividing $q-1$. The characters on the group G_n' with order l^j form a conjugacy class under the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Similarly, the Galois action on the set of characters of G_n gives a partition of G_n into conjugacy classes. Let C_χ be the conjugacy class of χ and let Σ_n be a set of representatives of distinct conjugacy classes. Let $\widehat{G_n}$ be the group of characters on G_n. Then $\widehat{G_n}$ is the disjoint union of C_χ, for $\chi\in\Sigma_n$. Moreover, let K_χ be the field extension of $\mathbb{Q}$ formed by adjoining the values of χ. Then $\prod_{\psi\in C_\chi}\psi=N_{\mathbb{Q}}^{K_\chi}\chi$. Therefore,

$$nh_n^-=\prod_{\psi\in\widehat{G_n},\ \psi_1\neq\mathrm{id}} L(1,\psi)=\prod_{\chi\in\Sigma_n,\ \chi'\neq\mathrm{id}}\ \prod_{\psi\in C_\chi} L(1,\psi).$$

Let χ be a character on the group $G_n\cong G_n'\times G_n''$ of order l^jp^i, for $1\le j\le a_0$ and $i\ge 1$. Then $K_\chi=\mathbb{Q}(\mu_{l^jp^i})$, the extension of $\mathbb{Q}$ from adjoining l^jp^i-th roots of unity. By Lemma 3.2,

$$\begin{aligned}\sum_{a\in M_n}\chi(a) &= \sum_{h\in\mathcal{H}_n}\sum_{g\in G_n''}\chi(h\star g)\\ &= \sum_{h\in\mathcal{H}_n}\sum_{g\in G_n''}\chi'((h\star g)g^{-1})\chi''(g)\\ &= \sum_{h\in\mathcal{H}_n}\sum_{g\in G_n''}(\chi'((h\star g)g^{-1})-1)\chi''(g),\end{aligned}$$

since $\sum_{g\in G_n''}\chi''(g)=0$. Let $\mathcal{L}_1$ be the unique prime of $K_{\chi'}$ dividing l. Then the ideal of $K_{\chi'}$ generated by $\chi'((h\star g)g^{-1})-1$ is a power of $\mathcal{L}_1$ for each term in above sum. Thus the ideal of K_χ generated by $(\chi'((h\star g)g^{-1})-1)\chi''(g)$ is divisible by any prime ideal of K_χ over $\mathcal{L}_1$. If $\mathcal{L}$ is such a prime ideal, then $\mathcal{L}$ divides each term of the above sum and hence divides $L(1,\chi)=\sum_{a\in M_n}\chi(a)$. Thus there is a prime ideal $\mathcal{L}_2$ of $K_{\chi''}$ over l dividing $N_{K_{\chi''}}^{K_\chi}(\mathcal{L})$. Therefore, the integral ideal $N_{\mathbb{Q}}^{K_{\chi''}}(\mathcal{L}_2)$ of $\mathbb{Z}$ divides the integral ideal $N_{\mathbb{Q}}^{K_\chi}(\mathcal{L})=N_{\mathbb{Q}}^{K_{\chi''}}N_{K_{\chi''}}^{K_\chi}(\mathcal{L})$. However, $N_{\mathbb{Q}}^{K_{\chi''}}(\mathcal{L}_2)$ is a power of the ideal (l) of $\mathbb{Z}$. Since $l\neq p$, by class field theory, $N_{\mathbb{Q}}^{K_{\chi''}}(\mathcal{L}_2)$ has a positive generator which is congruent to 1 modulo p^i. Let a_i be the order of l modulo p^i; then $l^{a_i}\mid N_{\mathbb{Q}}^{K_\chi}(\mathcal{L})$. By class field theory, there are precisely $(p^i-p^{i-1})/a_i$ primes $\mathcal{L}$ of K_χ dividing $\mathcal{L}_1$. Thus the power of l dividing $\prod_{\mathcal{L}|\mathcal{L}_1}N_{\mathbb{Q}}^{K_\chi}(\mathcal{L})$ has exponent greater than or equal to p^i-p^{i-1}. Since $\prod_{\mathcal{L}|\mathcal{L}_1}N_{\mathbb{Q}}^{K_\chi}(\mathcal{L})=N_{\mathbb{Q}}^{K_\chi}(\prod_{\mathcal{L}|\mathcal{L}_1}\mathcal{L})$ and $N_{\mathbb{Q}}^{K_\chi}(\prod_{\mathcal{L}|\mathcal{L}_1}\mathcal{L})$ divides $N_{\mathbb{Q}}^{K_\chi}(L(1,\chi))$, the power of l dividing $N_{\mathbb{Q}}^{K_\chi}(L(1,\chi))$ has exponent greater than or equal to p^i-p^{i-1}. Then the relation $L(1,\chi)=\sum_{a\in M_n}\chi(a)$ shows that $l^{p^i-p^{i-1}}$ divides $\prod_{\psi\in C_\chi}L(1,\psi)$.

Let b_i be the number of elements of G_n'' of order p^i. Then the number of elements of G_n of order l^jp^i is b_i for each j with $1\le j\le a_0$. By the isomorphism $G_n\cong\widehat{G_n}$, b_i is also the number of characters of G_n with order l^jp^i. Thus the number of conjugacy classes in Σ_n of characters of G_n whose orders are l^jp^i for some $1\le i\le a_0$

is $a_0 b_i/(p^i - p^{i-1})$, since there are $p^i - p^{i-1}$ characters in each conjugacy class. This shows that the power of l dividing $h_n^- = \prod_{\chi\in\Sigma_n,\chi\neq \mathrm{id}} \prod_{\psi\in C_\chi} L(1,\psi)$ is at least

$$\sum_{i=1}^{g_n^{(1)}} (p^i - p^{i-1}) \frac{a_0 b_i}{p^i - p^{i-1}} = a_0 \sum_{i=1}^{g_n^{(1)}} b_i = a_0(|G_n''| - 1) = a_0(q^{(n-1)\deg P} - 1).$$

This proves the theorem. □

Theorem 3.1 applies in particular to the Fermat primes.

Corollary 3.1. *Let $q = p$ be a prime of the form $2^c + 1$. Let $P(T)$ be a polynomial of degree 1. The exponent of 2 dividing the relative class number h_n^- of $\mathbf{k}(P^n)$ is at least $c(p^{(n-1)} - 1)$.* □

We next consider the power of p dividing h_n^- and h_n^+. For a character χ of $G_n \cong G_n' \times G_n''$, let $\chi'\chi''$ be the decomposition of χ. Let Σ_n' be the set of conjugacy classes of characters on G_n'. For $\{\chi'\} \in \Sigma_n'$, the order of χ' is prime to p. Let $d_{\chi'}$ be the order of p modulo the order of the character χ'. When χ' is the trivial character, we take $d_{\chi'}$ to be one. Define

$$a^- = a^-(p) = \sum_{\{\chi'\}\in\Sigma_n',\ \chi' \text{ non-real},\ p|N_{\mathbb{Q}}^{K_{\chi'}} L(1,\chi')} d_{\chi'}.$$

$$a^+ = a^+(p) = \sum_{\{\chi'\}\in\Sigma_n',\ \chi' \text{ real},\ p|N_{\mathbb{Q}}^{K_{\chi'}} \sum_{a\in M_n} \deg(a)\chi'(a)} d_{\chi'}.$$

Note that a^- and a^+ are independent of n since G_n' are isomorphic for all n and thus Σ_n' is the same for all n. If the index set of any of the sums is empty, then define the sum to be zero. Also define e_n to be the number of conjugacy classes of non-trivial characters on G_n''.

Theorem 3.3. 1. *The exponent of p dividing $h_n^\mp = h^\mp(\mathbf{k}(P^n))$ is at least $a^\mp e_n$.*
2. *If p divides $h_n^\mp$, then p^{e_n} divides $h_n^\mp$.*
3. *p^{e_n} divides h_n^- if and only if p divides h_1^-.*
4. *p^{e_n} divides h_n^+ for $n > 1$ if and only if p divides $\deg P$ or h_1^+.*

Proof. For part 1, we first prove the bound for h_n^-. Let χ be a non-real character on the group $G_n \cong G_n' \times G_n''$ of order cp^i, with $p \nmid c$. Suppose p divides $N_{\mathbb{Q}}^{K_\chi} L(1,\chi)$. Then $L(1,\chi)$ is divisible by a prime ideals $\wp$ of K_χ over p. Therefore $N_{\chi'}^{\chi} L(1,\chi)$ is divisible by a prime $\wp'$ of K_χ' over p. Thus $N_{\mathbb{Q}}^{\chi} L(1,\chi)$ is divisible by $N_{\mathbb{Q}}^{\chi'} \wp'$. Since the order of χ' is relative prime to p, class field theory shows that $N_{\mathbb{Q}}^{\chi'} \wp'$ is a power of p that is congruent to 1 modulo c. Since $d_{\chi'}$ is the order of p modulo d, we see that $p^{d_{\chi'}}$ divides $N_{\mathbb{Q}}^{\chi'} \wp'$, and hence divides $N_{\mathbb{Q}}^{\chi} L(1,\chi)$. Since $L(1,\chi) = \sum_{a\in M_n} \chi(a)$, we have $N_{\mathbb{Q}}^{\chi} L(1,\chi) = \prod_{\psi\in\{\chi\}} L(1,\chi)$. Therefore, the exponent of p dividing $\prod_{\psi\in\{\chi\}} L(1,\psi)$ is at least $d_{\chi'}$.

Now let ϕ be a character of G_n such that $\phi' = \chi'$. By assumption, $\wp$ divides $L(1,\chi) = \sum_{a\in M_n} \chi(a)$, and by Theorem 2.3.(1), $\wp$ divides $\sum_{a\in M_n,\ \deg a < \deg P} \chi(a)$. Since

$$n \sum_{a\in M_n,\ \deg a<\deg P} \chi(a) = \sum_{a\in M_n,\ \deg a<\deg P} \chi'(a)\chi''(a)$$

and $\wp$ divides $(\chi''(a)-1)$, $\wp$ also divides $\sum_{a\in M_n,\ \deg a<\deg P}\chi'(a)(\chi''(a)-1)$. Therefore $\wp$ divides $\sum_{a\in M_n,\ \deg a<\deg P}\chi'(a)$, and since $\phi'=\chi'$, it also divides $\wp|\sum_{a\in M_n,\ \deg a<\deg P}\phi'(a)$. Reversing the above argument shows that $\wp$ divides $L(1,\phi)$. Since $(|\ G_n'\ |,|\ G_n''\ |)=1$, the number of conjugacy classes of characters ϕ of G_n with $\phi'=\chi'$ is the same as the number of conjugacy classes of G_n''. By definition, this number is e_n. So the exponent of p dividing $\prod_{\phi'=\chi'}L(1,\phi)$ is at least $e_nd_{\chi'}$. Now by grouping all characters ϕ of G_n such that $L(1,\phi)$ is divisible by $\wp$ first into conjugacy classes and then according to their components ψ', we get the bound for h_n^-.

The proof for h_n^+ in part 1 is similar, replacing $\sum_{a\in M_n}\chi(a)$ by $\sum_{a\in M_n}\deg(a)\chi(a)$. Note that we have included the trivial character in the definition of a^+ to incorporate the p-powers from the non-trivial real characters χ with trivial χ' (Theorem 2.4.(1)). Proofs of the remaining parts of the theorem are all based on the observation that if p divides $h_n^{\mp}$, then $a^{\mp}\neq 0$. □

We now give a description of the number e_n in the theorem. Recall that we have the decomposition of $G_n=(\mathbb{F}_q[T]/(P(T))^n)^\times$ into $G_n'\times G_n''\cong G_n'\times\prod_{i=1}^m G_n^{(i)}$ with $G_n'\cong(\mathbb{F}_q[T]/(P(T)))^\times$ of order $q^{\deg P}-1$ and $G_n^{(i)}$ cyclic of order $p^{g_n^{(i)}}$ such that $g_n^{(1)}\geq g_n^{(2)}\geq\cdots\geq g_n^{(m)}$. For a fixed integer i with $1\leq i\leq g_n^{(1)}$, define $c_i=\#\{g_n^{(k)}\mid g_n^{(k)}\geq i,\ 1\leq k\leq g_n^{(1)}\}$, and

$$e_n^{(i)}=p^{(i-1)c_i+\sum_{g_n^{(k)}<i}g_n^{(k)}}\frac{p^{c_i}-1}{p^{i-1}(p-1)}.$$

The integers c_i depend on n also, but we omit the index for n so that the notation does not get too complicated.

Proposition 3.1. *The number of conjugacy classes of characters on G_n'' of order p^i is $p^{e_n^{(i)}}$. Therefore, $e_n=\sum_{i=1}^{g_n^{(i)}}e_n^{(i)}$.*

Proof. By the definition of c_i, the number of elements of G_n'' of order less or equal to p^i is $p^{ic_i}p^{\sum_{g_n^{(k)}<i}g_n^{(k)}}$ and the number of elements of G_n'' of order less or equal to p^{i-1} is $p^{(i-1)c_i}p^{\sum_{g_n^{(k)}<i}g_n^{(k)}}$. This shows that the number of elements of G_n'' of order exactly p^i is $p^{(i-1)c_i+\sum_{g_n^{(k)}<i}g_n^{(k)}}(p^{c_i}-1)$. This is also the number of characters on G_n'' with order p^i. There are p^i-p^{i-1} elements in every conjugacy class of characters of order p^i. Therefore, the number of conjugacy classes of characters on G_n'' with order exactly p^i is

$$p^{(i-1)c_i+\sum_{g_n^{(k)}<i}g_n^{(k)}}\frac{p^{c_i}-1}{p^{i-1}(p-1)},$$

as claimed. □

To get a simpler expression for the lower bound of p-powers dividing h_n^-, we need to know more about the structure of the related group $(\mathbb{F}_q[T]/(P^n))^\times$. Let $w_1,\cdots,w_r$ be a basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$. Let t_n be the smallest integer t such that $n<p^t$ and let p^{d_n} be the exact power of p dividing n. For each $0\leq i<t_n$, write $n=u_ip^i+v_i, 0\leq v_i<p^i$. Thus $v_i=0$ for $0\leq i\leq d_n$, $v_i>0$ for $d_n<i<t_n-1$ and $u_i=0$ for $i=t_n$. Here we omit the index of n in u_i and v_i to simplify the notation.

Proposition 3.2. *Let $G_n'' \cong G_n^{(1)} \times \cdots \times G_n^{(m)}$ be the decomposition of G_n'' into a product of cyclic p-groups with orders $g_n^{(1)} \geq \cdots \geq g_n^{(m)}$. Let $q = p^r$ and let $s = r \deg P$. For any integer i with $1 \leq i \leq g_n^{(1)}$, the number of $G_n^{(j)}$ with order exactly p^i is*

$$\begin{cases} s(u_{i-1} - 2u_i + u_{i+1}) & \text{for } i < d_n, \\ s(u_{i-1} - 2u_i + u_{i+1} + 1) & \text{for } i = d_n, \\ s(u_{i-1} - 2u_i + u_{i+1} - 1) & \text{for } i = d_n + 1, \\ s(u_{i-1} - 2u_i + u_{i+1}) & \text{for } i > d_n + 1. \end{cases}$$

Proof. First assume $\deg P = 1$. Since $(\mathbb{F}_q[T]/(P^n))^\times \cong (\mathbb{F}_q[T]/(T^n))^\times$ in this case, we can assume that $P(T) = T$. We will show that the elements $1 + w_j T^k,\ 1 \leq j \leq r,\ 1 \leq k < n, p \nmid k$ form a basis for the group G''. First show that they are independent. Assume that there are integers $c(j,k) > 0$ for some j and k, with $p \nmid k$ such that $(1 + w_j T^k)^{c(j,k)} \not\equiv 1 \pmod{T^n}$ and such that

$$\prod_{j,k}{}' (1 + w_j T^k)^{c(j,k)} = 1 \pmod{T^n}.$$

Here $\prod'$ indicates the product over the terms j, k with $c(j,k) > 0$. Write $c(j,k) = b(j,k)d(j,k)$ with $b(j,k) \geq 1$ a p-power and $d(j,k) > 1,\ p \nmid d(j,k)$. Using the identity $(1+x)^p = 1 + x^p$, we could rewrite the product as

$$\prod_{j,k}{}' (1 + w_j^{b(j,k)} T^{kb(j,k)})^{d(j,k)} = 1 \pmod{T^n}.$$

Since $p \nmid k$ in the product, $k_1 b(j_1, k_1) \neq k_2 b(j_2, k_2)$ if $p \nmid k_1, p \nmid k_2$ and $k_1 \neq k_2$. Thus we could choose $k_0 b(j_0, k_0)$ to be the smallest and take the product

$$\prod_{j,\ k_0 b(j,k_0) = k_0 b(j_0,k_0)}{}' (1 + w_j^{b(j,k_0)} T^{k_0 b(j,k_0)})^{d(j,k_0)}$$

to consist of those factors with $kb(j,k) = k_0 b(j_0, k_0)$ minimal; hence $k = k_0$. By assumption

$$(1 + w_j^{b(j,k_0)} T^{k_0 b(j,k_0)})^{d(j,k_0)} \not\equiv 1 \pmod{T^n};$$

hence $b(j_0, k_0) < n$. On the other hand, expanding the product in the equation above, we get

$$1 + \left(\sum_j{}' d(j,k_0) w_j^{b(j_0,k_0)} \right) T^{k_0 b(j_0,k_0)} + \text{higher powers of T} \equiv 1 \pmod{T^n}.$$

Raising to the p-th power gives an automorphism of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$; thus $\{w_j^{b(j_0,k_0)}\}$ is still a basis of $\mathbb{F}_q/\mathbb{F}_p$. As $p \nmid d(j,k_0)$, it follows that $(\sum_j{}' d(j,k_0) w_j^{b(j_0,k_0)})$ is non-zero in $\mathbb{F}_q$. Then $T^{k_0 b(j_0,k_0)} = 0$ modulo T^n. So we must have $k_0 b(j_0,k_0) \geq n$. This is a contradiction.

We next prove that, for $q = p^r$, the polynomials $1 + w_j T^k,\ 1 \leq j \leq r,\ 1 \leq k < n, p \nmid k$ generate G_n''. For this we only need to show that they generate a group of order $| G_n'' | = q^{n-1}$. Note that, as G_n'' is a p-group, the order of each $1 + w_j T^k$ is a p-power. With the same notation as introduced before the proposition, a counting

process shows that the number of $1+w_jT^k, 1\le k<n, p\nmid k$ with order $\ge p^i$ is

$$\begin{cases} r(u_{i-1}-1)-r(u_i-1)=r(u_{i-1}-u_i) & \text{for } 1\le i<d_n,\\ r(u_{i-1}-1)-ru_i & \text{for } i=d_n,\\ r(u_{i-1}-u_i) & \text{for } d_n<i<t_n. \end{cases}$$

Thus the number of $1+w_jT^k,\ 1\le j\le r,\ 1\le k<n, p\nmid k$ with order exactly p^i is

$$\begin{cases} r((u_{i-1}-u_i)-(u_i-u_{i+1})) & \text{for } i<d_n,\\ r((u_{i-1}-u_i)-(u_i-1-u_{i+1})) & \text{for } i=d_n,\\ r((u_{i-1}-1-u_i)-(u_i-u_{i+1})) & \text{for } i=d_n+1,\\ r((u_{i-1}-u_i)-(u_i-u_{i+1})) & \text{for } i>d_n+1. \end{cases}$$

Therefore the exponent of p for the subgroup of G_n'' generated by

$$\{1+w_jT^k \mid 1\le j\le r,\ 1\le k<n, p\nmid k\}$$

is

$$\begin{aligned} &\sum_{i=1}^{d_n-1} ir((u_{i-1}-u_i)-(u_i-u_{i+1}))+d_nr((u_{d_n-1}-u_{d_n})-(u_{d_n}-1-u_{d_n+1}))\\ &\quad+(d_n+1)r((u_{d_n}-1-u_{d_n+1})-(u_{d_n+1}-u_{d_n+2}))\\ &\quad+\sum_{i=d_n+2}^{h} ir((u_{i-1}-u_i)-(u_i-u_{i+1}))\\ &=r\sum_{i=1}^{d_n}(u_{i-1}-u_i)+r(u_{d_n}-1-u_{d_n+1})+r\sum_{i=d_n+2}^{h}(u_{i-1}-u_i)\\ &=r(u_0-1)=r(n-1). \end{aligned}$$

Hence the subgroup has order $p^{r(n-1)}=q^{n-1}$. This shows that $\{1+w_jT^k \mid 1\le j\le r,\ 1\le k<n, p\nmid k\}$ generates G_n''. Then the proposition follows when $\deg P=1$.

The case when $\deg P>1$ can be reduced to the $\deg P=1$ case by the isomorphism $\mathbb{F}_q[T]/(P^n)\cong(\mathbb{F}_q[T]/(P))[X]/(X^n)$. To prove this isomorphism, let $\mathbb{F}_q(T)_P$ be the completion of the field $\mathbb{F}_q(T)$ at the prime divisor P. Then the field $\mathbb{F}_q(T)_P$ is isomorphic to $\mathbb{F}_{q^{\deg P}}((\pi))$ since it is a local field with the residue field $\mathbb{F}_{q^{\deg P}}$. Let $\mathbb{F}_q[T]\hookrightarrow\mathbb{F}_{q^{\deg P}}[[\pi]]$ be the natural embedding, which is also a ring homomorphism. We claim that this natural embedding induces an isomorphism from the quotient ring $\mathbb{F}_q[T]/(P^n)$ to the quotient ring $\mathbb{F}_{q^{\deg P}}[[\pi]]/(\pi^n)$. It is easy to see that it induces a ring homomorphisms on the quotient rings. Thus we need only to show that it is one-to-one since these are finite rings. Let Q and Q' be two polynomials in $\mathbb{F}_q[T]$ and let $\bar{Q}$ and $\bar{Q}'$ be their images in $\mathbb{F}_{q^{\deg P}}[[\pi]]$. If $\bar{Q}$ and $\bar{Q}'$ lie in the same class of $\mathbb{F}_{q^{\deg P}}[[\pi]]/(\pi^n)$, then $\pi^n\mid\bar{Q}-\bar{Q}'=\overline{Q-Q'}$. Thus P^n divides $(Q-Q')$. Therefore, Q and Q' lie in the same class of the quotient group $\mathbb{F}_q[T]/(P^n)$. Now the proof is completed. □

Theorem 3.4. *The lower bounds for the p-parts of $h_n^{\mp}=h^{\mp}(\mathbf{k}(P^n))$ in Theorem 3.3 are further bounded below by* $\dfrac{a^{\mp}}{p-1}\dfrac{q^{(n-1)\deg P}-1}{n}$.

Remark. The exponent of p in the theorem can be rewritten as

$$\left(\frac{a^{\mp}}{n(p-1)q^{\deg P}}\right)q^{n\deg P}-\frac{a^{\mp}}{n(p-1)}.$$

This can be regarded as an analog of Iwasawa's theorem for the exponent of p dividing the class numbers of finite field extensions from a $\mathbb{Z}_p$-extension of a number field. Note that, unlike in the number field case, it is possible here that the p-part of the relative class number h_n^- increases exponentially as n grows. There are examples (Section 4) where the prime p divides at least one non-real character; therefore the number a^- in this theorem is non-zero.

Proof of Theorem 3.4. To get this bound, we need a second description of $e_n^{(i)}$, the number of conjugacy classes of characters on G_n'' of order exactly p^i.

For a fixed integer n, as in Proposition 3.2 we define t_n to be the smallest integer t such that $n < p^t$ and let p^{d_n} be the highest power of p dividing n. For each $0 \le i < t_n$, write $n = u_i p^i + v_i, 0 \le v_i < p^i$. Thus $v_i = 0$ for $0 \le i \le d_n$, $v_i > 0$ for $d_n < i < t_n - 1$ and $u_i = 0$ for $i = t_n$. Let $q = p^r$ and $s = r \deg P$. We show in the proof of Proposition 3.2 that the number of $G_n^{(j)}$ with order $\ge p^i$ is

$$\alpha_i = \alpha_{n,i} = \begin{cases} s(u_{i-1} - 1) - s(u_i - 1) = s(u_{i-1} - u_i) & \text{for } 1 \le i < d_n, \\ s(u_{i-1} - su_i - 1) & \text{for } i = d_n, \\ s(u_{i-1} - u_i) & \text{for } d_n < i < t_n. \end{cases}$$

To find $e_n^{(i)}$ we compute the number of characters on G_n'' of order exactly p^i, which is the same as the number of elements of G_n'' of order exactly p^i because of the isomorphism $\widehat{G_n''} \cong G_n''$. For this we compute the order of the subgroup $G_n[i]$ of G_n'' consisting of elements with order less or equal to p^i. For each factor $G_n^{(j)}$ in the decomposition $G_n'' \cong \prod_{j=1}^{g_n^{(1)}} G_n^{(j)}$, define $G_n^{(j)}[i] = G_n^{(j)} \cap G_n[i]$. Then $G_n''/G_n[i] \cong \prod_j G_n^{(j)}/(G_n^{(j)}[i])$. For a fixed integer $k \ge i$, the number of cyclic factors $G_n^{(j)}$ of G_n'' with order p^k is $\alpha_k - \alpha_{k+1}$, so the number of cyclic factors $G_n^{(j)}/(G_n^{(j)}[i])$ of $G_n''/G_n[i]$ with order p^{k-i} is also $\alpha_k - \alpha_{k-1}$. Thus the exponent of p for the order of $G_n''/G_n[i]$ are

$$\begin{aligned} &\sum_{k>i} (k-i)(\alpha_k - \alpha_{k+1}) \\ &\quad = \quad (\alpha_{i+1} - \alpha_{i+2}) + 2(\alpha_{i+2} - \alpha_{i+3}) + \cdots \\ &\quad = \quad \sum_{k>i} \alpha_k \\ &\quad = \quad \begin{cases} s(u_i - 1) & \text{if } i < d_n, \\ su_i & \text{if } i \ge d_n. \end{cases} \end{aligned}$$

Therefore the order of $G_n[i]$ is

$$\begin{cases} p^{s(n-u_i)} & \text{if } i < d_n, \\ p^{s(n-u_i-1)} & \text{if } i \ge d_n. \end{cases}$$

Thus the elements of G_n'' and hence of $\widehat{G_n''}$ of order exactly p^i is

$$\begin{cases} p^{sn}(p^{-su_i} - p^{-su_{i-1}}) & \text{if } i < d_n, \\ p^{sn}(p^{-s(u_i-1)} - p^{-su_{i-1}}) & \text{if } i = d_n, \\ p^{sn}(p^{-s(u_i-1)} - p^{-s(u_{i-1}-1)}) & \text{if } i > d_n. \end{cases}$$

Since there are $p^{i-1}(p-1)$ elements in each conjugacy class of characters of order p^i, the number of conjugacy classes of elements of order p^i is

$$e_i = \begin{cases} \frac{p^{sn}}{p^{i-1}(p-1)}(p^{-su_i} - p^{-su_{i-1}}) & \text{if } i < d_n, \\ \frac{p^{sn}}{p^{i-1}(p-1)}(p^{-s(u_i-1)} - p^{-su_{i-1}}) & \text{if } i = d_n, \\ \frac{p^{sn}}{p^{i-1}(p-1)}(p^{-s(u_i-1)} - p^{-s(u_{i-1}-1)}) & \text{if } i > d_n. \end{cases}$$

Now the lower bound of the p-part of $h_n^{\mp}$ in Theorem 3.3 can be expressed as

$$\begin{aligned} a^{\mp}e_n &= a^{\mp}\sum_{i=1}^{g_n^{(1)}} e_n^{(i)} \\ &\geq a^{\mp}\sum_{i=1}^{g_n^{(1)}} \frac{p^{i-1}}{p^{g_n^{(1)}-1}} e_n^{(i)} \\ &= \frac{a^{\mp}\, p^{sn+1-g_n^{(1)}}}{p-1}\left[\sum_{i=1}^{d_n-1}(p^{su_i} - p^{su_{i-1}}) + (p^{s(u_{d_n}-1)} - p^{su_{d_n-1}}) \right. \\ &\qquad \left. + \sum_{i=d_n+1}^{h}(p^{s(u_i-1)} - p^{s(u_{i-1}-1)})\right] \\ &= \frac{a^{\mp}p^{sn+1-g_n^{(1)}}}{p-1}(p^{-s} - p^{-su_0}) \\ &= a^{\mp}p^{1-g_n^{(1)}}\frac{p^{s(n-1)}-1}{p-1} \\ &\geq \frac{a^{\mp}}{p-1}\frac{p^{s(n-1)}-1}{n} \end{aligned}$$

since $p^{g_n^{(1)}} \geq n \geq p^{g_n^{(1)}-1}$. This finishes the proof. □

4. Some data and remarks

We provide some examples and data in this section and use them to comment on the results obtained in earlier sections.

Table 1 shows the data obtained by using the formulas (1.2) and (1.5) and the PARI package. We assume that the polynomial P is of degree one; thus can assume $P(T) = T$, p is the number of elements in the constant field and h^+ and h^- represent the real part and relative part of class number of the ring $\mathbf{k}(P^n)$, respectively. One can see that both h_n^+ and h_n^- grow very fast and even for small values of p and n they already approach the limit that the computer can handle. Because of this nature of the class numbers, we could only get their values for first few n and p even though the formulas and the computer program are effectively computable in theory. With the results we obtained in this paper, we plan to improve the present computer program by removing those factors which are known to appear. By collecting more data this way, we should be able to get further insight on the behavior of those primes which do not divide $p-1$. We would like to take this chance to thank Dominique Bernardi for making the PARI package available to us and to thank David Alden for his help in loading the PARI Library for us.

TABLE 1. Class Numbers of $\mathbf{k}(P^n)$, $\deg P = 1$

n	p	h_n^+	h_n^-
1	p	1	1
2	3	1	2^2
2	5	1	$2^8 \cdot 41$
2	7	1	$2^9 \cdot 3^6 \cdot 13^2 \cdot 118147$
2	11	1	$2^{10} \cdot 3^5 \cdot 5^{10} \cdot 241^2 \cdot 19031 \cdot 34231^2 \cdot$
			$19767211 \cdot 1788286391$
3	3	$2^2 \cdot 7^2$	$2^8 \cdot 7$
3	5	$2^4 \cdot 71^4$	$2^{64} \cdot 3^8 \cdot 11^4 \cdot 41^3 \cdot 61^2 \cdot 101 \cdot 401 \cdot 701 \cdot 821$
4	3	$2^2 \cdot 7^2 \cdot 19^2 \cdot 109^2 \cdot 307^2$	$2^{26} \cdot 7 \cdot 181 \cdot 379 \cdot 523$
5	3	$2^{18} \cdot 7^{15} \cdot 13^2 \cdot 19^6 \cdot 37^4$	$2^{80} \cdot 7^3 \cdot 13 \cdot 17^2 \cdot 19^5 \cdot 31^2 \cdot 37 \cdot 73 \cdot 79$
		$\cdot 109^6 \cdot 307^4 \cdot 577^2$	$\cdot 109^2 \cdot 181 \cdot 379 \cdot 523 \cdot 3511 \cdot 5779 \cdot 6823$

Examples and remarks.

Example 4.1. Choose $p = 5$, $P(T) = T^2 + T + 1$ and $n = 1$. It can be checked that $T+2$ is a generator of $(\mathbb{F}_p[T]/(P))^\times$ and the monic polynomials can expressed as $T+2 = (T+2)^1$, $T+1 = (T+2)^{20}$, $T+3 = (T+2)^3$, $T = (T+2)^{16}$, $T+4 = (T+2)^{17}$, $1 = (T+2)^0$. Let χ be the character on $(\mathbb{F}_p[T]/(P))^\times$ of order 4. Then $\chi(T+2) = \zeta_4$, a primitive 4th root of unity. Thus

$$\begin{aligned} L(1,\chi) &= \sum_{a \in M} \chi(a) = \zeta_4 + \zeta_4^{20} + \zeta_4^3 + \zeta_4^{16} + \zeta_4^{17} + \zeta_4^0 \\ &= \zeta_4 + 1 + \zeta_4^3 + 1 + \zeta_4 + 1 = \zeta_4 + 3. \end{aligned}$$

Since $(\zeta_4 + 3) = (1 + \zeta_4)(2 - \zeta_4)$ and $(2 - \zeta_4)$ is a prime of $\mathbb{Q}(\zeta_4)$ above 5, it follows from Equation (1.5) that 5 divides h^-. This shows that Theorem 2.3.(3) and 2.3.(4) are no longer true if the degree of P is greater than 1. It also provides an example that $a^- \neq 0$ in Theorem 3.4.

Example 4.2. When $p = 3$, $P(T) = T^3 + 2T + 2$ and $h_1^+ = 19683 = 3^9$. This shows that part 3 and 4 of Theorem 2.4 is no longer true if $\deg P > 1$.

Examples 4.1 and 4.2 also provide cases when the exponents of p dividing the relative and real parts of the class number have exponential growth as n goes to infinity, i.e., the analog of the μ-invariant from Iwasawa is non-zero. On the other hand, it is also possible that the invariants $a^\mp$ in Theorem 3.3 and Theorem 3.4 are zero, as shown in the next two examples.

Example 4.3. Take $p = 3$, $P(T) = T^2 + 1$. Then $h_1^- = 64$, which is prime to p.

Example 4.4. Take $p = 3$, $P(T) = T^3 + T^2 + 2$. Then $h_1^+ = 16589$, which is prime to p.

From Theorem 2.3, if $p \nmid h_1^-$, then $p \nmid h_n^-$. Thus Example 4.3 provides an example of $h \nmid h_n^-$. Examples 4.2 and 4.4 also show that in part 2 of Theorem 2.4, when $p \mid \deg P$ and $n = 1$, it is possible that $p \mid h_1^+$ for some P, while $p \nmid h_1^+$ for some other P.

References

[Ca] L. Carlitz, *On certain functions connected with polynomials in the Galois field*, Duke Math. J. **1** (1935), 137-168.

[F-W] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math. **109** (1979), 377-395. MR **81a:**12005

[G-R] S. Galovich and Rosen, *Units and class groups in cyclotomic function fields*, J. Number Theory **14** (1982), 156-184. MR **84b:**12008

[G-K] R. Gold and H. Kisilevsky, *On geometric $\mathbb{Z}_p$-extensions of function fields*, Manuscripta Math. **62** (1988), 145-161. MR **90e:**11160

[Ha] D. Hayes, *Explicit class field theory in global function fields*, in "Studies in Algebra and Number Theory" (G.C Rota, Ed.), Academic Press, San Diego (1979). MR **81d:**12011

[Iw] K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. Math. **76** (1962), 171-179. MR **27:**4806

[Iw2] K. Iwasawa, *On p-adic L-functions*, Ann. Math. **89** (1969), 198-205. MR **42:**4522

[Sh] L. Shu, *Narrow ray class fields and partial zeta-functions*, preprint, 1994.

[Th] D. Thakur, *Iwasawa theory and cyclotomic function fields*, Proceedings of Iwasawa theory and arithmetic geometry, 1993, Tempe, Arizona. MR **95g:**11054

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210

Current address: Department of Mathematics and Computer Science, Rutgers University, Newark, New Jersey 07102

E-mail address: liguo@andromeda.rutgers.edu

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210

Current address: 228 Paseo del Rio, Moraga, California 94556

E-mail address: shul@wellsfargo.com