Gauss' congruence from Dirichlet's class number formula and generalizations

Glenn J. Fox, Jerzy Urbanowicz and Kenneth S. Williams

Dedicated to Professor Andrzej Schinzel on the occasion of his 60th birthday

Abstract. Let d denote the discriminant of a quadratic field. Let n be the number of distinct prime factors of d. Let χ_d and $h(d)$ denote the character and class number of the field respectively. Let B_{k,χ_d} denote the generalized Bernoulli number attached to χ_d. It is shown in an elementary manner how Gauss' congruence for imaginary quadratic fields $h(d) \equiv 0 \pmod{2^{n-1}}$ can be deduced from Dirichlet's formula for $h(d)$. We also generalize the Gauss congruence to 2-integral rational numbers $(B_{k,\chi_d}/k)$. We prove that $(B_{k,\chi_d}/k) \equiv 0 \pmod{2^{n-1}}$ if $\chi_d(-1) = (-1)^k$. This is a further application of an identity proved in [10] expressing short character power sums of any length in terms of generalized Bernoulli numbers. The first application of the identity to classical problems was due to Schinzel, Urbanowicz and van Wamelen [9].

1991 Mathematics Subject Classification: 11L26, 11R11, 11R29, 11S40.

Key words and phrases: imaginary quadratic field, class number, Dirichlet's class number formula, Gauss' congruence, generalized Bernoulli number, short character power sum.

1. Preliminaries

Let d be the discriminant of a quadratic field. Let $h(d)$ and χ_d denote the class number and the character of this field respectively. It is convenient on occasion to allow $d = 1$ in which case χ_d is the primitive trivial character. Together with $d = 1$, these numbers d are the so-called fundamental discriminants. As a consequence of his theory of genera for imaginary quadratic fields, Gauss obtained algebraically the congruence

$$h(d) \equiv 0 \pmod{2^{n-1}}, \tag{1}$$

Research of the second author was supported by State Committee for Scientific Research of Poland (KBN) grant 2 P03A 036 15, while that of the third was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

where n is the number of distinct prime factors of d ($d < 0$), see for example [1, p. 247], [4, p. 227], [6, p. 133]. Dirichlet showed analytically that

$$h(d) = \frac{w(d)}{2(2-\chi_d(2))} \sum_{r=1}^{[|d|/2]} \chi_d(r), \tag{2}$$

where

$$w(d) = \begin{cases} 6, & \text{if } d = -3, \\ 4, & \text{if } d = -4, \\ 2, & \text{if } d < -4, \end{cases}$$

see for example [1, p. 346], [7, p. 325]. We show in an elementary manner how Dirichlet's formula (2) can be made to yield Gauss' congruence (1). We accomplish this by putting (2) into a form (see Theorem 1) from which (1) can be deduced by induction on n. The proof of Theorem 1 is based on three elementary lemmas. The first gives a congruence modulo a power of 2 for $\phi(|d|)$, where ϕ is Euler's phi function. The second evaluates a sum which occurs in the proof of Theorem 1. The third puts (2) into a more general form for use in the proof of Theorem 1. Before the lemmas we give some elementary observations. The detailed proofs of the lemmas are left to the reader.

As d is the discriminant of a quadratic field, we have $d \equiv 1 \pmod 4$, $d \equiv 8 \pmod{16}$ or $d \equiv 12 \pmod{16}$. Moreover, we have

$$d = \prod_{p|d} p^*,$$

where the prime discriminant p^* corresponding to the prime $p|d$ is given by

$$p^* = (-1)^{(p-1)/2} p,$$

if p is odd, and

$$2^* = \begin{cases} 8, & \text{if } d \equiv 8 \pmod{32}, \\ -8, & \text{if } d \equiv 24 \pmod{32}, \\ -4, & \text{if } d \equiv 12 \pmod{16}. \end{cases}$$

Write $2^* = 1$ if $d \equiv 1 \pmod 4$. If $d < 0$, we have

$$|d/2^*| \equiv \begin{cases} 3 \pmod 4, & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 8 \pmod{32}, \\ 1 \pmod 4, & \text{if } d \equiv 12 \pmod{16} \text{ or } d \equiv 24 \pmod{32}. \end{cases}$$

Let u denote the number of distinct prime divisors of d which are congruent to 1 modulo 4 and v the number of distinct prime divisors of d which are congruent to 3 modulo 4, so that

$$u + v = \begin{cases} n, & \text{if } d \equiv 1 \pmod 4, \\ n-1, & \text{if } d \equiv 0 \pmod 4, \end{cases}$$

and

$$v \equiv \begin{cases} 1 \pmod 2, & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 8 \pmod{32}, \\ 0 \pmod 2, & \text{if } d \equiv 12 \pmod{16} \text{ or } d \equiv 24 \pmod{32}. \end{cases}$$

Lemma 1. *Let d be the discriminant of an imaginary quadratic field. Let n denote the number of distinct prime divisors of d and u the number of prime divisors of d which are congruent to 1 modulo 4. Then*

$$\phi(|d|) \equiv \begin{cases} 0 \pmod{2^{n+u}}, & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 12 \pmod{16}, \\ 0 \pmod{2^{n+1+u}}, & \text{if } d \equiv 8 \pmod{16}. \end{cases}$$

Moreover if $u = 0$ then

$$\phi(|d|) \equiv \begin{cases} 2^n \pmod{2^{n+1}}, & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 12 \pmod{16}, \\ 2^{n+1} \pmod{2^{n+2}}, & \text{if } d \equiv 8 \pmod{16}. \end{cases}$$

Proof. The proof is straightforward by an inspection of cases. We apply the observations made before the formulation of the lemma. □

Lemma 2. *If N is a positive integer with $N \geq 3$ then*

$$\sum_{\substack{k=1 \\ (k,N)=1}}^{[N/2]} 1 = \frac{\phi(N)}{2}.$$

Proof. For $1 \leq k \leq N$ we have $(k, N) = 1$ if and only if $(N - k, N) = 1$. Hence the lemma follows at once. □

Lemma 3. *Let d be the discriminant of an imaginary quadratic field and let e be the discriminant of a quadratic field such that $e|d$. Then*

$$\sum_{\substack{k=1 \\ (k,d)=1}}^{[|d|/2]} \chi_e(k) = \begin{cases} (2 - \chi_e(2)) \dfrac{2}{w(e)} \left\{ \prod_{p|(d/e)} (1 - \chi_e(p)) \right\} h(e), \\ \qquad \text{if } e < 0 \text{ and } (d/e) \text{ is odd}, \\ 0, \qquad \text{otherwise}. \end{cases}$$

Proof. Denote by S the sum on the left hand side of the above equation. We have

$$S = \sum_{1 \leq k \leq |d|/2} \chi_e(k) \sum_{f|(k,d/e)} \mu(f) = \sum_{f|(d/e)} \mu(f) \sum_{\substack{1 \leq k \leq |d|/2 \\ f|k}} \chi_e(k)$$

(here as usual μ denotes the Möbius function). Replacing k by fg in the inner sum, we obtain

$$S = \sum_{f|(d/e)} \mu(f) \chi_e(f) \sum_{1 \leq g \leq |(d/e)/f||e|/2} \chi_e(g).$$

Therefore, in view of

$$\sum_{1 \leq g \leq [|(d/e)/f|/2]|e|} \chi_e(g) = 0$$

we obtain

$$S = \sum_{f|(d/e)} \mu(f)\chi_e(f) \sum_{[|(d/e)/f|/2]|e|<g\leq|(d/e)/f||e|/2} \chi_e(g).$$

If $(d/e)/f$ is even the inner sum vanishes. Thus

$$S = \sum_{\substack{f|(d/e)\\ 2\nmid(d/e)/f}} \mu(f)\chi_e(f) \sum_{1\leq h\leq|e|/2} \chi_e\left(\frac{(|(d/e)/f|-1)}{2}|e|+h\right).$$

But $\chi_e(\lambda|e|+h) = \chi_e(h)$ for any integer λ so

$$S = \Big\{ \sum_{\substack{f|(d/e)\\ 2\nmid(d/e)/f}} \mu(f)\chi_e(f)\Big\}\Big\{\sum_{1\leq h\leq|e|/2} \chi_e(h)\Big\}. \tag{3}$$

Next we determine the left hand sum in the above product.

If (d/e) is odd then $(d/e)/f$ is odd for all $f|(d/e)$ and

$$\sum_{\substack{f|(d/e)\\ 2|(d/e)/f}} \mu(f)\chi_e(f) = 0.$$

If (d/e) is even, as (d/e) is the discriminant of a quadratic field, we have $(d/e) = 2^\alpha t$, where $\alpha = 2$ or 3 and t is odd. Writing $f = 2^\beta g$, where g is odd and $0 \leq \beta \leq \alpha - 1$, we see that

$$\sum_{\substack{f|(d/e)\\ 2|(d/e)/f}} \mu(f)\chi_e(f) = \Big\{\sum_{\beta=0}^{\alpha-1} \mu(2^\beta)\chi_e(2)^\beta\Big\}\Big\{\sum_{g|t}\mu(g)\chi_e(g)\Big\}.$$

Hence and from a product expansion property of multiplicative functions, we deduce that

$$\sum_{\substack{f|(d/e)\\ 2\nmid(d/e)/f}} \mu(f)\chi_e(f) = (1-\chi_e(2))\prod_{p|t}(1-\chi_e(p)) = \prod_{p|(d/e)}(1-\chi_e(p)),$$

$$\begin{aligned}\sum_{\substack{f|(d/e)\\ 2\nmid(d/e)/f}} \mu(f)\chi_e(f) &= \sum_{f|(d/e)} \mu(f)\chi_e(f) - \sum_{\substack{f|(d/e)\\ 2|(d/e)/f}} \mu(f)\chi_e(f)\\ &= \begin{cases} \prod_{p|(d/e)} (1-\chi_e(p)), & \text{if } (d/e) \text{ is odd},\\ 0, & \text{if } (d/e) \text{ is even.}\end{cases}\end{aligned}$$

Now to prove Lemma 3 it suffices to make use of the above equation, formula (3), Dirichlet's formula (2) and the trivial equality

$$\sum_{1\leq h\leq|e|/2} \chi_e(h) = 0$$

which holds for $e > 0$. □

We remark that when $e = d$ the formula of Lemma 3 reduces to (2). Throughout the paper, as usual we denote by $\omega(n)$ the number of distinct prime divisors of an integer n ($n \neq 0$).

Theorem 1. *Let d be the discriminant of an imaginary quadratic field. Then*

$$\sum_{\substack{e|d \\ e<0 \\ (d/e)\equiv 1 \,(\mathrm{mod}\, 4)}} (-1)^{\omega(e)-1}(2-\chi_e(2))\frac{2}{w(e)}\Big\{\prod_{\substack{p|d \\ p\nmid e}}(1-\chi_e(p))\Big\}h(e)$$
$$= \frac{\phi(|d|)}{2} - \sum_{\substack{k=1 \\ (k,d)=1}}^{[|d|/2]}\Big\{\prod_{p|d}(1-\chi_{p^*}(k))\Big\},$$

where e runs through fundamental discriminants dividing d such that $e < 0$ and $(d/e) \equiv 1 \,(\mathrm{mod}\, 4)$.

Proof. From a product expansion property of multiplicative functions and Lemmas 2 and 3 we obtain

$$\sum_{\substack{k=1 \\ (k,d)=1}}^{[|d|/2]}\Big\{\prod_{p|d}(1-\chi_{p^*}(k))\Big\} = \sum_{\substack{k=1 \\ (k,d)=1}}^{[|d|/2]} 1 + \sum_{\substack{e|d \\ e\neq 1}}(-1)^{\omega(e)}\sum_{k=1}^{[|d|/2]}\chi_e(k)$$
$$= \frac{\phi(|d|)}{2} + \sum_{\substack{e|d \\ e<0 \\ (d/e)\equiv 1 \,(\mathrm{mod}\, 4)}} (-1)^{\omega(e)}(2-\chi_e(2))\frac{2}{w(e)}\Big\{\prod_{\substack{p|d \\ p\nmid e}}(1-\chi_e(p))\Big\}h(e)$$

and the theorem follows. □

2. Gauss' congruence from Dirichlet's class number formula in an elementary manner

Before proving Gauss' congruence we make some preliminary observations. Regarding the product in the left hand side of the equation of Theorem 1, we note that

$$\prod_{\substack{p|d \\ p\nmid e}}(1-\chi_e(p)) \equiv 0 \,(\mathrm{mod}\, 2^{\omega(d)-\omega(e)}). \tag{4}$$

Similarly, for the sum on the right hand side of the equation of Theorem 1, we have

$$\sum_{\substack{k=1 \\ (k,d)=1}}^{[|d|/2]}\Big\{\prod_{p|d}(1-\chi_{p^*}(k))\Big\} \equiv 0 \,(\mathrm{mod}\, 2^{\omega(d)}). \tag{5}$$

We now discuss briefly the case when d ($d < 0$) has exactly one prime factor. Then we have the classical congruence

$$h(d) \equiv 1 \pmod 2.$$

An algebraic proof of this congruence is given in [4, p. 187]. See also [6, p. 135]. In this case $d = -4$, -8 or $-p$, where p is a prime $\equiv 3 \pmod 4$. It is well known that $h(-4) = h(-8) = 1$. In the remaining case the above congruence follows from formula (2) easily. Indeed, if $d = -p$ we have $w(d) = 2$ if $p > 3$, and $w(3) = 6$, $2 - \chi_d(2) = 3$, resp. 1, if $p \equiv 3$, resp. $7 \pmod 8$, and

$$\sum_{r=1}^{(p-1)/2} \chi_d(r) \equiv \sum_{r=1}^{(p-1)/2} 1 = (p-1)/2 \equiv 1 \pmod 2.$$

We are now ready to deduce Gauss' congruence (1) from Dirichlet's class number formula (2).

Theorem 2. *Let d be the discriminant of an imaginary quadratic field. Then*

$$h(d) \equiv 0 \pmod{2^{n-1}},$$

where n is the number of distinct prime factors of d.

Proof. We make use of Theorem 1 which was proved using Dirichlet's formula. We proceed by induction on the number n of prime divisors of the fundamental discriminant d.

If $n = 1$ the congruence of Theorem 2 is trivial. We thus make the inductive hypothesis that $h(e) \equiv 0 \pmod{2^{r-1}}$ whenever e is a negative fundamental discriminant having r distinct prime factors where $r = 1, 2, \ldots, n-1$ and $n \geq 2$. Let d be a negative fundamental discriminant with n prime factors.

First we treat the case when $d \equiv 1 \pmod 4$. In Theorem 1 the terms with $e \neq d$ have $\omega(e) = r$, $1 \leq r \leq n-1$, and are congruent to 0 modulo $2^{n-r} \times 2^{r-1} = 2^{n-1}$ by (4) and the inductive hypothesis. The term with $e = d$ is

$$(-1)^{n-1} \frac{2}{w(d)} \big(2 - \chi_d(2)\big) h(d) = (\text{odd number}) \times h(d).$$

By Lemma 1 and (5) the right hand side of the equation in the Theorem 1 is divisible by 2^{n-1}. Hence $h(d) \equiv 0 \pmod{2^{n-1}}$.

Secondly we treat the case $d \equiv 8 \pmod{16}$. In this case the terms with $e \neq d$ in the equation of Theorem 1 have $\omega(e) = r$, $1 \leq r \leq n-1$, and are divisible by $2 \times 2^{n-r} \times 2^{r-1} = 2^n$ by (4) and the inductive hypothesis. The term with $e = d$ is $(-1)^{n-1} 2h(d)$. By Lemma 1 and (5) the right hand side of the equation of Theorem 1 is divisible by 2^n. Hence $h(d) \equiv 0 \pmod{2^{n-1}}$.

Finally we treat the case $d \equiv 12 \pmod{16}$. Clearly the fundamental discriminants e in the summation on the left hand side of the equation of Theorem 1 contain -4 as one of their prime discriminant factors. The term with $e = -4$ is

$$\prod_{\substack{p|d \\ p\neq 2}} (1 - \chi_e(p)) = \begin{cases} 2^{n-1}, & \text{if } u = 0, \\ 0, & \text{if } u \geq 1. \end{cases}$$

The term with $e = d$ is

$$(-1)^{n-1} 2h(d).$$

The remaining terms in the sum each contribute by (4) and the inductive hypothesis

$$\pm 2(\text{multiple of } 2^{n-\omega(e)})(\text{multiple of } 2^{\omega(e)-1}) = \text{multiple of } 2^n.$$

Hence the left hand side of the equation of Theorem 1 is

$$\begin{cases} (-1)^{n-1}2h(d) + 2^{n-1} + k2^n, & \text{if } u = 0, \\ (-1)^{n-1}2h(d) + k2^n, & \text{if } u \geq 1, \end{cases}$$

for some integer k. By Lemma 1 and (5) the right hand side of the equation of Theorem 1 is

$$\begin{cases} 2^{n-1} + l2^n, & \text{if } u = 0, \\ l2^n, & \text{if } u \geq 1, \end{cases}$$

for some integer l. Hence $h(d) \equiv 0 \pmod{2^{n-1}}$. Gauss' congruence (1) now follows by the principle of mathematical induction. □

3. Character power sums in terms of Bernoulli numbers

It follows from Dirichlet's class number formula that

$$h(d) = -B_{1,\chi_d} \quad (d < -4),$$

where $B_{k,\chi}$ denotes the generalized Bernoulli number attached to χ (see [15, Chapter 4] for details).

Let F denote a real quadratic field with the discriminant d and let O_F be the ring of integers in F. Let K_2 be the Milnor functor and $k_2(d)$ denote the order of the finite group K_2O_F. The corresponding formula for $k_2(d)$ is

$$k_2(d) = B_{2,\chi_d} \quad (d > 8). \tag{6}$$

It is a special case of a famous conjecture of Birch and Tate, proved by Wiles, see [16, p. 499].

It is well known that $k_2(d)$ for positive d is always divisible by 4. Using Gauss' theory of genera Browkin and Schinzel in [2] obtained algebraically the congruence

$$(k_2(d)/2) \equiv 0 \pmod{2^{n-1}}, \tag{7}$$

where d is the discriminant of a real quadratic field having n distinct prime factors.

We recall that for $d \neq -4$ the numbers $(B_{m,\chi_d}/m)$ $(m \geq 1)$ are 2-integral. In fact, these numbers are always integers unless $d = -4$ or $d = \pm p$, where p is an odd prime number such that $2m/(p-1)$ is an odd integer, in which case they have denominator 2 or p (for details see [3] or [8]). The left hand side of the congruences (1), resp. (7) is equal to $(B_{m,\chi_d}/m)$ for $m = 1$, resp. 2. By analogy, one could expect that these congruences are special cases of a more general corresponding congruence for the generalized Bernoulli numbers attached to quadratic characters $(B_{m,\chi_d}/m)$ $(m \geq 1,\ \chi_d(-1) = (-1)^m)$. The main result of the paper is Theorem 6 giving a congruence of this type.

It follows from (6) that

$$k_2(d) = \frac{4w_2(d)}{\chi_d(2) - 4} \sum_{r=1}^{[d/2]} \chi_d(r) r, \tag{8}$$

where

$$w_2(d) = \begin{cases} 5, & \text{if } d = 5, \\ 2, & \text{if } d = 8, \\ 1, & \text{otherwise,} \end{cases}$$

see [12]. Formula (8) for $k_2(d)$ corresponds to formula (2) for $h(d)$, which yields the identities of Lemma 3 and Theorem 1, and in consequence Gauss' congruence. Thus one could expect that there should exist some corresponding identities for $k_2(d)$ implying Browkin and Schinzel's congruence (7). In this paper we find such identities. In fact, we find identities of a more general form, for the generalized Bernoulli numbers (Theorems 3, 4 and 5). Theorems 3, 4 and 5 are further consequences of an identity proved in [10], expressing short character power sums of any length in terms of generalized Bernoulli numbers.

Let χ be a Dirichlet character modulo M and let N be a multiple of M. For any integer $r > 1$ prime to N and any natural number m we have the following formula from [10]

$$mr^{m-1} \sum_{0<a<(N/r)} \chi(a) a^{m-1} = -B_{m,\chi} r^{m-1} + \frac{\bar{\chi}(r)}{\phi(r)} \sum_{\psi} \bar{\psi}(-N) B_{m,\chi\psi}(N), \tag{9}$$

where the last sum is over all Dirichlet characters ψ modulo r. Here for a Dirichlet character χ, we have

$$B_{m,\chi}(X) = \sum_{k=0}^{m} \binom{m}{k} B_{k,\chi} X^{m-k}.$$

Thus we have

$$mr^{m-1} \sum_{0<a<(N/r)} \chi(a) a^{m-1} = -B_{m,\chi} r^{m-1} + \frac{\bar{\chi}(r)}{\phi(r)} \sum_{k=0}^{m} \binom{m}{k} N^{m-k} \sum_{\psi} \bar{\psi}(-N) B_{k,\chi\psi}.$$

Note that if the character χ modulo T is induced from a character χ' modulo some divisor of T then we have

$$B_{m,\chi} = B_{m,\chi'} \prod_{p|T} \left(1 - \chi'(p)p^{m-1}\right), \tag{10}$$

where the product is over all primes p dividing T. For more details see [10].

Formula (9) if N odd and $r = 2, 4, 8$ together with formula (10) gives some identities for the generalized Bernoulli numbers corresponding to those in Lemma 3. The case $m = 1$ is much simpler than the other cases. For $m \geq 2$ we also need shorter character power sums.

If χ is a Dirichlet character modulo M and N is a multiple of M, then for $m \geq 0$ we set

$$B^{[N]}_{m,\chi} = B_{m,\chi} \prod_{p|(N/M)} \left(1 - \chi(p)p^{m-1}\right).$$

Moreover, we write

$$B^{[N]}_{m,\chi}(X) = \sum_{k=0}^{m} \binom{m}{k} B^{[N]}_{k,\chi} X^{m-k}.$$

Set $B^{[N]}_{m} = B^{[N]}_{m,\chi_1}$, $B^{[N]}_{m}(X) = B^{[N]}_{m,\chi_1}(X)$ for any integer $N > 1$.

Lemma 4. *Let χ be a Dirichlet character modulo M and let N be an odd positive multiple of M. Then for any natural number m we have the following formulae:*

(a)
$$m2^{m-1} \sum_{\substack{0<a<(N/2)\\(a,N)=1}} \chi(a)a^{m-1} = \left(\bar{\chi}(2) - 2^m\right) B^{[N]}_{m,\chi} + \bar{\chi}(2)\left(B^{[2N]}_{m,\chi}(N) - B^{[2N]}_{m,\chi}\right),$$

(b)
$$m2^{2m-2} \sum_{\substack{0<a<(N/4)\\(a,N)=1}} \chi(a)a^{m-1} = \left(\frac{\bar{\chi}(4) - \bar{\chi}(2)2^{m-1} - 2^{2m-1}}{2}\right) B^{[N]}_{m,\chi} + \frac{\bar{\chi}(4)}{2}\left(\left(B^{[2N]}_{m,\chi}(N) - B^{[2N]}_{m,\chi}\right) - \chi_{-4}(N) B^{[4N]}_{m,\chi_{-4}\chi}(N)\right),$$

(c)
$$m2^{3m-3} \sum_{\substack{0<a<(N/8)\\(a,N)=1}} \chi(a)a^{m-1} = \left(\frac{\bar{\chi}(8) - \bar{\chi}(4)2^{m-1} - 2^{3m-1}}{4}\right) B^{[N]}_{m,\chi} + \frac{\bar{\chi}(8)}{4}\left(\left(B^{[2N]}_{m,\chi}(N) - B^{[2N]}_{m,\chi}\right) - \chi_{-8}(N) B^{[8N]}_{m,\chi_{-8}\chi}(N) - \chi_{-4}(N) B^{[4N]}_{m,\chi_{-4}\chi}(N) + \chi_{8}(N) B^{[8N]}_{m,\chi_{8}\chi}(N)\right).$$

Proof. N is odd and so we can make use of formula (9) for $r = 2, 4$ and 8, respectively. Then we have

$$m2^{m-1} \sum_{0<a<(N/2)} \chi(a)a^{m-1} = (\bar{\chi}(2) - 2^m)B_{m,\chi} + \bar{\chi}(2)\Big(B_{m,\chi}^{[2M]}(N) - B_{m,\chi}^{[2M]}\Big),$$

and

$$m2^{2m-2} \sum_{0<a<(N/4)} \chi(a)a^{m-1} = \left(\frac{\bar{\chi}(4) - \bar{\chi}(2)2^{m-1} - 2^{2m-1}}{2}\right)B_{m,\chi} + \frac{\bar{\chi}(4)}{2}\Big((B_{m,\chi}^{[2M]}(N) - B_{m,\chi}^{[2M]}) - \chi_{-4}(N)B_{m,\chi_{-4}\chi}(N)\Big),$$

and

$$\begin{aligned} m2^{3m-3} \sum_{0<a<(N/8)} \chi(a)a^{m-1} &= \left(\frac{\bar{\chi}(8) - \bar{\chi}(4)2^{m-1} - 2^{3m-1}}{4}\right)B_{m,\chi} \\ &+ \frac{\bar{\chi}(8)}{4}\Big((B_{m,\chi}^{[2M]}(N) - B_{m,\chi}^{[2M]}) - \chi_{-8}(N)B_{m,\chi_{-8}\chi}(N) \\ &\qquad - \chi_{-4}(N)B_{m,\chi_{-4}\chi}(N) + \chi_8(N)B_{m,\chi_8\chi}(N)\Big). \end{aligned}$$

Now it is sufficient to replace the character χ modulo M in the above formulae by a character modulo N induced by χ and Lemma 4 follows immediately. □

4. The main results

We are now ready to deduce the main results of the paper. First we prove some identities for the generalized Bernoulli numbers corresponding to that in Theorem 1 (Theorems 3, 4, 5). Next we deduce the main congruence of the paper (Theorem 6) for the numbers $(B_{m,\chi_d}/m)$ for d odd, divisible by 4, or divisible by 8 from Theorems 3, 4, or 5 respectively. We will proceed by induction on the pairs (m, n), where n is the number of distinct prime factors of d.

Theorem 3. *Let m be a natural number and let d be an odd discriminant of a quadratic field. Then we have*

$$\begin{aligned} &\sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)}(\chi_e(2) - 2^m)\frac{B_{m,\chi_e}^{[d]}}{m} + \sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)}\chi_e(2)\left(\frac{B_{m,\chi_e}^{[2d]}(|d|) - B_{m,\chi_e}^{[2d]}}{m}\right) \\ &= 2^{m-1}\Bigg(\sum_{\substack{0<a<(|d|/2) \\ (a,d)=1}} a^{m-1}\Big\{\prod_{p|d}(1 - \chi_{p^*}(a))\Big\} - \sum_{\substack{0<a<(|d|/2) \\ (a,d)=1}} a^{m-1}\Bigg), \end{aligned}$$

where e ($e \neq 1$) runs through fundamental discriminants dividing d.

Proof. Denote by S the left hand side of the equality of Theorem 3. By Lemma 4(a) we have

$$S = 2^{m-1}\Big(\sum_{e|d}\mu(e)\sum_{\substack{0<a<(|d|/2)\\(a,d)=1}}\chi_e(a)a^{m-1} - \sum_{\substack{0<a<(|d|/2)\\(a,d)=1}}a^{m-1}\Big)$$
$$= 2^{m-1}\Big(\sum_{\substack{0<a<(|d|/2)\\(a,d)=1}}a^{m-1}\sum_{e|d}\mu(e)\chi_e(a) - \sum_{\substack{0<a<(|d|/2)\\(a,d)=1}}a^{m-1}\Big).$$

Now the theorem follows from a product expansion property of multiplicative functions. □

Theorem 4. *Let m be a natural number and let d be an odd discriminant of a quadratic field. Then we have*

$$\sum_{\substack{e|d\\e\neq 1}}(-1)^{\omega(e)}(1-\chi_e(2)2^{m-1}-2^{2m-1})\frac{B^{[d]}_{m,\chi_e}}{m}$$
$$+\sum_{\substack{e|d\\e\neq 1}}(-1)^{\omega(e)}\Big(\frac{B^{[2d]}_{m,\chi_e}(|d|)-B^{[2d]}_{m,\chi_e}}{m}-\frac{\chi_{-4}(|d|)B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m}\Big)$$
$$=2^{2m-1}\Big(\sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}a^{m-1}\Big\{\prod_{p|d}(1-\chi_{p^*}(a))\Big\}-\sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}a^{m-1}\Big),$$

where e $(e\neq 1)$ runs through fundamental discriminants dividing d.

Proof. Denote by S the left hand side of the equality of Theorem 4. By Lemma 4(b) we have

$$S = 2^{2m-1}\Big(\sum_{e|d}\mu(e)\sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}\chi_e(a)a^{m-1} - \sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}a^{m-1}\Big)$$
$$= 2^{2m-1}\Big(\sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}a^{m-1}\sum_{e|d}\mu(e)\chi_e(a) - \sum_{\substack{0<a<(|d|/4)\\(a,d)=1}}a^{m-1}\Big).$$

Now the theorem follows from a product expansion property of multiplicative functions. □

Theorem 5. *Let m be a natural number and let d be an odd discriminant of a quadratic field. Then we have*

$$\sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} (\chi_e(2) - 2^{m-1} - 2^{3m-1}) \frac{B^{[d]}_{m,\chi_e}}{m}$$

$$+ \sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \chi_e(2) \times \left(\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m} - \frac{\chi_{-4}(|d|) B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m} \right.$$

$$\left. - \frac{\chi_{-8}(|d|) B^{[8d]}_{m,\chi_{-8}\chi_e}(|d|)}{m} + \frac{\chi_8(|d|) B^{[8d]}_{m,\chi_8\chi_e}(|d|)}{m} \right)$$

$$= 2^{3m-1} \left(\sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} a^{m-1} \left\{ \prod_{p|d} (1 - \chi_{p^*}(a)) \right\} - \sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} a^{m-1} \right),$$

where e ($e \neq 1$) runs through fundamental discriminants dividing d.

Proof. Denote by S the left hand side of the equality of Theorem 5. By Lemma 4(c) we have

$$S = 2^{3m-1} \left(\sum_{e|d} \mu(e) \sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} \chi_e(a) a^{m-1} - \sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} a^{m-1} \right)$$

$$= 2^{3m-1} \left(\sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} a^{m-1} \sum_{e|d} \mu(e) \chi_e(a) - \sum_{\substack{0<a<(|d|/8) \\ (a,d)=1}} a^{m-1} \right).$$

Now the theorem follows from a product expansion property of multiplicative functions. □

The proof of the main theorem (Theorem 6) is based on Theorems 3, 4, 5 and five lemmas (Lemmas 5, 6, 7, 8 and 9). In Lemma 5 we prove an elementary congruence. In Lemma 6 we give an extension (probably already known) of the von Staudt-Clausen theorem for Bernoulli numbers. These two lemmas together with Lemma 7 and 8 imply Lemma 9. Theorems 3, 4, 5 and Lemma 9 give Theorem 6.

Lemma 5. *Let $N > 1$ be a squarefree odd natural number. Then for an even integer $m \geq 2$ we have*

$$N \prod_{p|N} (1 + p + \cdots + p^{m-2}) \equiv (-1)^{\omega(N)} \pmod{2^{\operatorname{ord}_2 m}}.$$

Moreover, if every prime p dividing N satisfies $p \equiv 3 \pmod 4$ then the above congruence holds modulo $2^{\operatorname{ord}_2 m + 1}$.

Proof. We note that for any $p|N$ we have the congruence

$$p\left(1+p+\cdots+p^{m-2}\right) \equiv -1 \pmod{2^{\operatorname{ord}_2 m+\operatorname{ord}_2(p+1)-1}}. \tag{11}$$

This congruence yields the lemma at once.

The task is now to prove congruence (11). Indeed, for u odd we have

$$u^m \equiv 1 \pmod{2^{\operatorname{ord}_2 m+\operatorname{ord}_2(u^2-1)-1}}. \tag{12}$$

It follows from the equation

$$u^m = 1+\sum_{k=1}^{m/2} \frac{m/2}{k}\binom{(m/2)-1}{k-1}(u^2-1)^k$$

because

$$k \operatorname{ord}_2(u^2-1) \geq \operatorname{ord}_2 k + \operatorname{ord}_2(u^2-1),$$

if $k \geq 1$.

Thus we obtain

$$p\left(1+p+\cdots+p^{m-2}\right) = \frac{p^m-1}{p-1} - 1 \equiv -1 \pmod{2^{\operatorname{ord}_2 m+\operatorname{ord}_2(p+1)-1}}.$$

Hence congruence (11) follows at once. □

Lemma 6 extends the von Staudt-Clausen theorem in case $p=2$. The theorem asserts that for a prime number p satisfying $(p-1)|m$, the rational numbers pB_m are p-integral and

$$pB_m \equiv -1 \pmod{p}. \tag{13}$$

If $(p-1)\nmid m$ then B_m are p-integral, but we will not use this. In the proof of Lemma 6 we apply the power summation formula

$$\sum_{0<a<N} a^{m-1} = \frac{1}{m}\left(B_m(N) - B_m\right), \tag{14}$$

where $m \geq 1$. In the proofs of Lemmas 7 and 8 we make use of the following formula for the generalized Bernoulli polynomials

$$B_{m,\chi}(X+Y) = \sum_{k=0}^{m} \binom{m}{k} B_{k,\chi}(X) Y^{m-k}, \tag{15}$$

which easily follows from the formula

$$B'_{m,\chi}(X) = mB_{m-1,\chi}(X).$$

Lemma 6. *For an even integer $m \geq 4$ we have*

$$2B_m \equiv 1 \pmod{2^{\operatorname{ord}_2 m+1}}.$$

Proof. Let R be a natural number such that $R \equiv 2 \pmod 4$. From formula (14) we obtain

$$(m+1)\sum_{0<a<R} a^m = B_{m+1}(R) - B_{m+1},$$

and hence

$$\frac{Rm(m+1)}{2}\sum_{k=3}^{m+1}\frac{1}{k(k-1)}\binom{m-1}{k-2}(2B_{m+1-k})R^{k-1} + \frac{(m+1)R}{2}(2B_m) \equiv (m+1)\sum_{\substack{0<a<R\\ a\text{ odd}}} a^m \pmod{2^{\operatorname{ord}_2 m+1}}.$$

Therefore by (12) and

$$k-1 \geq \operatorname{ord}_2\big(k(k-1)\big)+1,$$

if $k \geq 3$, we deduce that

$$\frac{(m+1)R}{2}(2B_m) \equiv \frac{(m+1)R}{2} \pmod{2^{\operatorname{ord}_2 m+1}}.$$

This implies Lemma 6 easily. □

Remark. Note that if $m = 2$ the above congruence holds modulo $2^{\operatorname{ord}_2 m}$ only, and if $m \geq 6$ we have $\operatorname{ord}_2(2B_m - 1) = \operatorname{ord}_2 m + 1$.

Lemma 7. *Let $N > 1$ be a squarefree odd natural number having n distinct prime factors. Then for a natural number m we have*

$$\frac{B_m^{[2N]}(1)}{m} \equiv 0 \pmod{2^n},$$

unless $m = 1, 2$ and $p \equiv 3 \pmod 4$ for any $p|N$, in which cases

$$\frac{B_m^{[2N]}(1)}{m} \equiv 2^{n-1} \pmod{2^n}.$$

Proof. If $m = 1$ we have

$$B_1^{[2N]}(1) = B_0^{[2N]} + B_1^{[2N]} = \frac{1}{2}\prod_{p|N}(1-p^{-1}) = \frac{\phi(N)}{2N}$$

and the lemma follows. If $m = 2$ we have

$$\frac{B_2^{[2N]}(1)}{2} = \frac{1}{2}\Big(B_0^{[2N]} + B_2^{[2N]}\Big) = \frac{\phi(N)}{4N}\Big(1 - \frac{1}{3}(-1)^{\omega(N)}N\Big).$$

Denote by u the number of distinct prime divisors of N which are congruent to 1 modulo 4. From now on, the proof will be divided into two cases

(i) $u > 0$,

(ii) $u = 0$.

Case (i). In this case

$$\frac{\phi(N)}{4N} \equiv 0 \pmod{2^{n-1}}$$

and

$$1 - \frac{1}{3}(-1)^{\omega(N)} N \equiv 0 \pmod{2},$$

and hence the lemma follows immediately.

Case (ii). In this case

$$\frac{\phi(N)}{4N} \equiv 2^{n-2} \pmod{2^{n-1}}$$

and

$$1 - \frac{1}{3}(-1)^{\omega(N)} N \equiv 1 + (-1)^{2\omega(N)} \equiv 2 \pmod{4},$$

and hence the lemma follows easily.

If $m \geq 3$ we proceed by induction on m. If $m = 3$ we have

$$\frac{B_3^{[2N]}(1)}{3} = \frac{1}{3}\left(B_0^{[2N]} + 3B_2^{[2N]}\right) = \frac{\phi(N)}{6N}\left(1 - (-1)^{\omega(N)} N\right) \equiv 0 \pmod{2^{n-1}},$$

which gives the lemma.

The subsequent proof is based on the following observation. Putting in (15) $X = 1$ and $Y = -1$ we obtain

$$\frac{B_m^{[2N]}}{m} = \frac{1}{m}\sum_{k=0}^{m}\binom{m}{k} B_k^{[2N]}(1)(-1)^{m-k} = (-1)^m \frac{\phi(N)}{2mN} + (-1)^{m-1}\frac{\phi(N)}{2N}$$
$$+ (-1)^{m-2}(m-1)\frac{B_2^{[2N]}(1)}{2} + \sum_{k=3}^{m}(-1)^{m-k}\binom{m-1}{k-1}\frac{B_k^{[2N]}(1)}{k}.$$

Lemma 7 can be deduced from the above formula inductively if we prove that

$$(-1)^m \frac{B_m^{[2N]}}{m} - \frac{\phi(N)}{2mN} + \frac{\phi(N)}{2N} - (m-1)\frac{B_2^{[2N]}(1)}{2} \equiv 0 \pmod{2^n}. \tag{16}$$

Denote by L the left hand side of the above congruence. For odd m we have

$$L = -\frac{\phi(N)}{2mN} + \frac{\phi(N)}{2N} - (m-1)\frac{B_2^{[2N]}(1)}{2} \equiv \frac{\phi(N)}{2N}\left(1 - \frac{1}{m}\right) \equiv 0 \pmod{2^n}.$$

For m (≥ 4) even we have

$$L = \left(\frac{B_m^{[2N]}}{m} - \frac{\phi(N)}{2mN}\right) + \left(\frac{\phi(N)}{2N} - (m-1)\frac{B_2^{[2N]}(1)}{2}\right).$$

Case (i). In this case

$$\phi(N) \equiv 0 \pmod{2^{n+1}}$$

and we have

$$L \equiv \frac{B_m^{[2N]}}{m} - \frac{\phi(N)}{2mN} \pmod{2^n}.$$

Thus in order to prove (16) it suffices to show that

$$(2B_m)\left(1-2^{m-1}\right)N\prod_{p\mid N}\left(1-p^{m-1}\right)\equiv\phi(N)\,(\operatorname{mod}2^{n+\operatorname{ord}_2 m+1}).$$

The left hand side of the above congruence equals

$$\phi(N)(2B_m)\left(1-2^{m-1}\right)N(-1)^{\omega(N)}\prod_{p\mid N}\left(1+p+\cdots+p^{m-2}\right),$$

and so the congruence follows easily from Lemmas 5 and 6.

Case (ii). In this case we have

$$L\equiv\left(\frac{B_m^{[2N]}}{m}-\frac{\phi(N)}{2mN}\right)+\left(2^{n-1}-2^{n-1}\right)(\operatorname{mod}2^n),$$

and so

$$L\equiv\frac{B_m^{[2N]}}{m}-\frac{\phi(N)}{2mN}\,(\operatorname{mod}2^n).$$

Analysis similar to that in case (i) shows that $L\equiv 0\,(\operatorname{mod}2^n)$. It suffices to make use of Lemmas 5, 6 and the congruence

$$\phi(N)\equiv 2^n\,(\operatorname{mod}2^{n+1}).$$

The congruence of Lemma 6 in this case has the form

$$N\prod_{p\mid N}\left(1+p+\cdots+p^{m-2}\right)\equiv(-1)^{\omega(N)}\,(\operatorname{mod}2^{\operatorname{ord}_2 m+1}).\qquad\square$$

Lemma 8. *Let m be a natural number. Let $N>1$ be an odd squarefree natural number having n distinct prime factors and let $d=-4,\pm 8$. Write $\delta=|d|$. Then we have*

$$\frac{B_{m,\chi_d}^{[\delta N]}(N)}{m}\equiv 0\,(\operatorname{mod}2^n),$$

unless $m=1,2$, $d=-4$ and $p\equiv 3\,(\operatorname{mod}4)$ for any $p\mid N$, in which cases

$$\frac{B_{m,\chi_{-4}}^{[4N]}(N)}{m}\equiv 2^{n-1}\,(\operatorname{mod}2^n).$$

Proof. The proof is straightforward and based on the following observations. For an even integer k ($k\geq 0$) we have

$$B_{k,\chi_{-4}}=0,$$

and for an odd integer k ($k\geq 1$)

$$\frac{1}{k}B_{k,\chi_{-4}}=\frac{1}{2}E_{k-1},$$

where E_k denotes the kth classical Euler number, which is an odd integer.

Moreover, for an integer k ($k \geq 0$) we have

$$B_{k,\chi_{-8}} = 0,$$

if k is even, and

$$B_{k,\chi_8} = 0,$$

if k is odd, and

$$B_{0,\chi_8} = 0.$$

For $k \geq 1$ the numbers

$$\frac{1}{k} B_{k,\chi_{\pm 8}}$$

are rational and 2-integral (see [3] or [8] for more details).

Let δ be a natural number relatively prime to N. For a non-principal Dirichlet character χ modulo δ we have

$$\frac{B^{[\delta N]}_{m,\chi}(N)}{m} = \sum_{\substack{1 \leq k \leq m \\ \chi(-1)=(-1)^k}} \binom{m-1}{k-1} \left\{ \prod_{p \mid N} \left(1 - \chi(p) p^{k-1}\right) \right\} \frac{B_{k,\chi}}{k} N^{m-k}. \tag{17}$$

We first consider the case $d = -4$. If $m = 1$, by virtue of (17), we have

$$\begin{aligned} B^{[4N]}_{1,\chi_{-4}}(N) = B^{[4N]}_{1,\chi_{-4}} &= -\frac{1}{2} \prod_{p \mid N} \left(1 - \chi_{-4}(p)\right) \\ &\equiv \begin{cases} 0 \,(\operatorname{mod} 2^n), & \text{if } u > 0, \\ 2^{n-1} \,(\operatorname{mod} 2^n), & \text{if } u = 0. \end{cases} \end{aligned}$$

(recall that $E_0 = 1$) and the lemma in this case follows. If $m = 2$, by virtue of (17), we have

$$\frac{B^{[4N]}_{2,\chi_{-4}}(N)}{2} = B^{[4N]}_{1,\chi_{-4}} N$$

and similar arguments to those in case $m = 1$ apply.

Denote by u the number of distinct prime divisors of N which are congruent to 1 modulo 4. By virtue of (17) if $d = -4$ and $m \geq 3$ we have

$$\begin{aligned} \frac{B^{[4N]}_{m,\chi_{-4}}(N)}{m} &= -\frac{1}{2} \sum_{\substack{1 \leq k \leq m \\ k \text{ odd}}} \binom{m-1}{k-1} \left\{ \prod_{p \mid N} \left(1 - \chi_{-4}(p) p^{k-1}\right) \right\} E_{k-1} N^{m-k} \\ &\equiv \begin{cases} 2^{n-1} \displaystyle\sum_{\substack{1 \leq k \leq m \\ k \text{ odd}}} \binom{m-1}{k-1} \equiv 0 \,(\operatorname{mod} 2^n), & \text{if } u = 0, \\ 0 \,(\operatorname{mod} 2^n), & \text{if } u > 0 \end{cases} \end{aligned}$$

because

$$1 - \chi_{-4}(p) p^{k-1} \equiv 1 - \chi_{-4}(p) \,(\operatorname{mod} 8)$$

for k odd, and

$$\sum_{\substack{1\le k\le m\\ k\,\mathrm{odd}}}\binom{m-1}{k-1}=2^{m-2}.$$

We now turn to the case $d=\pm 8$. Then, by virtue of (17), we have

$$\frac{B^{[8N]}_{m,\chi_{\pm 8}}(N)}{m}=\sum_{\substack{1\le k\le m\\ k\,\mathrm{odd}}}\binom{m-1}{k-1}\left\{\prod_{p|N}\left(1-\chi_{\pm 8}(p)p^{k-1}\right)\right\}\frac{B_{k,\chi_{\pm 8}}}{k}N^{m-k}$$
$$\equiv 0\,(\mathrm{mod}\,2^n)$$

because

$$\left\{\prod_{p|N}\left(1-\chi_{\pm 8}(p)p^{k-1}\right)\right\}\frac{B_{k,\chi_{\pm 8}}}{k}\equiv 0\,(\mathrm{mod}\,2^n)$$

for any $1\le k\le m$. This completes the proof. □

Lemma 9. *Let m be a natural number. Let $N>1$ be an odd squarefree natural number having n distinct prime factors. Then we have*

$$2^{m-1}\sum_{\substack{0<a<(N/2)\\ (a,N)=1}}a^{m-1}\equiv 2^{2m-1}\sum_{\substack{0<a<(N/4)\\ (a,N)=1}}a^{m-1}$$
$$\equiv 2^{3m-1}\sum_{\substack{0<a<(N/8)\\ (a,N)=1}}a^{m-1}\equiv 0\,(\mathrm{mod}\,2^n),$$

except one case

$$2^{m-1}\sum_{\substack{0<a<(N/2)\\ (a,N)=1}}a^{m-1}\equiv 2^{n-1}\,(\mathrm{mod}\,2^n)$$

if $m=1$ and $p\equiv 3\,(\mathrm{mod}\,4)$ for any $p|N$.

Proof. Denote by u the number of distinct prime divisors of N which are congruent to 1 modulo 4.

In order to prove that

$$2^{m-1}\sum_{\substack{0<a<(N/2)\\ (a,N)=1}}a^{m-1}\equiv 0\,(\mathrm{mod}\,2^n),\tag{18}$$

we make use of Lemma 4(a) for the principal character χ modulo N. Then, by (13) if $p=2$, we have

$$2^{m-1}\frac{B^{[N]}_m}{m}=\frac{2^{m-1}}{2m}\prod_{p|N}\left(1-p^{m-1}\right)\left(2B_m\right)\equiv$$

$$\equiv \begin{cases} 2^{n-1} \pmod{2^n}, & \text{if } m = 2 \text{ and } u = 0, \\ 0 \pmod{2^n}, & \text{otherwise.} \end{cases}$$

Therefore Lemma 4(a) implies the congruence

$$2^{m-1} \sum_{\substack{0<a<(N/2) \\ (a,N)=1}} a^{m-1}$$
$$\equiv \begin{cases} 2^{n-1} + \dfrac{B_m^{[2N]}(N)}{m} \pmod{2^n}, & \text{if } m = 2 \text{ and } u = 0, \\ \dfrac{B_m^{[2N]}(N)}{m} \pmod{2^n}, & \text{otherwise.} \end{cases} \tag{19}$$

We first prove the lemma if $m = 1$ or 2. Then by definition

$$B_1^{[2N]}(N) = B_0^{[2N]} N = \frac{\phi(N)}{2},$$

$$B_2^{[2N]}(N) = B_0^{[2N]} N^2 + B_2^{[2N]} = \frac{\phi(N)}{2}\left(N - \frac{1}{3}(-1)^{\omega(N)}\right),$$

and so

$$\frac{B_m^{[2N]}(N)}{m} \equiv \begin{cases} 0 \pmod{2^n}, & \text{if } u > 0, \\ 2^{n-1} \pmod{2^n}, & \text{if } u = 0. \end{cases} \tag{20}$$

Therefore the lemma if $m = 1$ or 2 follows from (19).

If $m \geq 3$ the proof is based on the following observation. By (15) (when $X = 1$, $Y = N - 1$), we have

$$\frac{B_m^{[2N]}(N)}{m} = \frac{\phi(N)}{2mN}(N-1)^m + \frac{\phi(N)}{2N}(N-1)^{m-1}$$
$$+ (m-1)\frac{B_2^{[2N]}(1)}{2}(N-1)^{m-2} + \sum_{k=0}^{m-3} \binom{m-1}{k} \frac{B_{m-k}^{[2N]}(1)}{m-k}(N-1)^k,$$

and in view of Lemma 7 we conclude that (recall that $N - 1$ is even)

$$\frac{B_m^{[2N]}(N)}{m} \equiv 0 \pmod{2^n}.$$

Therefore congruence (18) follows from (19).

In order to prove the congruence

$$2^{2m-1} \sum_{\substack{0<a<(N/4) \\ (a,N)=1}} a^{m-1} \equiv 0 \pmod{2^n}, \tag{21}$$

we use Lemma 4(b) for the principal character χ modulo N. Then, in view of (13) if $p = 2$, we have

$$2^{2m-1}\frac{B_m^{[N]}}{m} = \frac{2^{2m-1}}{2m}\prod_{p|N}\left(1-p^{m-1}\right)(2B_m) \equiv 0 \,(\mathrm{mod}\, 2^n).$$

Therefore Lemma 4(b) yields

$$2^{2m-1}\sum_{\substack{0<a<(N/4)\\(a,N)=1}} a^{m-1} \equiv \frac{B_m^{[2N]}(N)}{m} - \chi_{-4}(N)\frac{B_{m,\chi_{-4}}^{[4N]}(N)}{m} \,(\mathrm{mod}\, 2^n).$$

Thus congruence (21) follows from Lemma 8 and (20).

In order to prove that

$$2^{3m-1}\sum_{\substack{0<a<(N/8)\\(a,N)=1}} a^{m-1} \equiv 0 \,(\mathrm{mod}\, 2^n), \tag{22}$$

we apply Lemma 4(c) for the principal character χ modulo N. Then, in view of (13) if $p = 2$, we have

$$2^{3m-1}\frac{B_m^{[N]}}{m} = \frac{2^{3m-1}}{2m}\prod_{p|N}\left(1-p^{m-1}\right)(2B_m) \equiv 0 \,(\mathrm{mod}\, 2^n).$$

Therefore Lemma 4(c) together with Lemma 8 and congruence (20) gives

$$2^{3m-1}\sum_{\substack{0<a<(N/8)\\(a,N)=1}} a^{m-1} \equiv -\chi_{-8}(N)\frac{B_{m,\chi_{-8}}^{[8N]}(N)}{m} + \chi_8(N)\frac{B_{m,\chi_8}^{[8N]}(N)}{m} \,(\mathrm{mod}\, 2^n).$$

Now congruence (22) follows from Lemma 8 at once. □

Let m be a natural number. Let D be the discriminant of a quadratic field such that $D \neq -4$ and $\chi_D(-1) = (-1)^m$. Then the rational numbers $(B_{m,\chi_D}/m)$ are 2-integral, see for example [3] or [8]. More precisely, we have $\mathrm{ord}_2\left(B_{m,\chi_{\pm 8}}/m\right) = 0$ and $\mathrm{ord}_2\left(B_{m,\chi_D}/m\right) \geq 1$ if $m \geq 2$ and $D \neq \pm 8$, see [13] for details.

Theorem 6. *Let m be a natural number. Let D be the discriminant of a quadratic field such that $D \neq -4$ and $\chi_D(-1) = (-1)^m$. Assume that χ_D is the corresponding character and n is the number of distinct prime factors of D. Then we have*

$$\frac{B_{m,\chi_D}}{m} \equiv 0 \,(\mathrm{mod}\, 2^{n-1}).$$

Proof. Let d be an odd fundamental discriminant. The proof falls naturally into three cases

(i) $D = d$,

(ii) $D = -4d$,

(iii) $D = \pm 8d$.

In order to prove the congruence of Theorem 6, we proceed by induction on the pairs (m,n) ordered lexicographically, that is,

$$(k,r) \le (m,n)$$

if and only if $k < m$, or $k = m$ and $r \le n$.

If $m = 1$ Theorem 6 follows from Theorem 2. We now make the inductive hypothesis that

$$\frac{B_{k,\chi_e}}{k} \equiv 0 \pmod{2^{n-1}},$$

whenever $1 \le k < m$ $(m \ge 2)$ and $e \ne 1$ is a fundamental discriminant having r distinct prime factors where $1 \le r \le n-1$ $(n \ge 2)$.

Case (i). In this case Theorem 3 together with Lemma 9 gives the congruence

$$\sum_{\substack{e|d \\ e\ne 1}} (-1)^{\omega(e)} (\chi_e(2) - 2^m) \frac{B^{[d]}_{m,\chi_e}}{m} + \sum_{\substack{e|d \\ e\ne 1}} (-1)^{\omega(e)} \chi_e(2) \left(\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m} \right) \equiv 0 \pmod{2^n}. \quad (23)$$

Let us first consider the first sum on the left hand side of the above congruence. If $e = d$ we have

$$(\chi_d(2) - 2^m) \frac{B^{[d]}_{m,\chi_d}}{m} = (\text{odd integer}) \times \frac{B^{[d]}_{m,\chi_d}}{m},$$

and if $e|d$ and $e \ne d$, by the inductive assumption, we have

$$(\chi_e(2) - 2^m) \frac{B^{[d]}_{m,\chi_e}}{m} = (\text{odd integer}) \times \left\{ \prod_{p|(d/e)} (1 - \chi_e(p) p^{k-1}) \right\} \frac{B_{m,\chi_e}}{m}$$
$$= (\text{integer}) \times 2^{\omega(d/e)} \times 2^{\omega(e)-1} = (\text{integer}) \times 2^{n-1}.$$

We now turn to the second sum of the left hand side of congruence (23). It consists of the numbers

$$\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m},$$

where $e|d$ and $e \ne 1$. Therefore the summands of the second sum are up to sign of the form

$$\binom{m-1}{k-1} \frac{B_{k,\chi_e}}{k} (1 - \chi_e(2) 2^{k-1}) \prod_{p|(d/e)} (1 - \chi_e(p) p^{k-1}) |d|^{m-k},$$

where $1 \leq k \leq m-1$. If $k=0$ the summand disappears since

$$B_{0,\chi_e} = 0$$

if $e \neq 1$. Thus, by the inductive assumption, the summands of the second sum are of the form

$$(\text{integer}) \times 2^{\omega(e)-1} \times 2^{\omega(d/e)} = (\text{integer}) \times 2^{n-1}$$

and all these observations together give Theorem 6 in case (i).

Case (ii). In this case $n-1 = \omega(d)$. We make use of Theorem 4 and Lemma 9, which give the congruence

$$\sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \left(1 - \chi_e(2)2^{m-1} - 2^{2m-1}\right) \frac{B^{[d]}_{m,\chi_e}}{m}$$
$$+ \sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \left(\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m} \right) - \chi_{-4}(|d|) \sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \frac{B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m}$$
$$\equiv 0 \pmod{2^{\omega(d)}}.$$

We first consider the first and second sums on the left hand side of the above congruence. The numbers

$$\frac{B^{[d]}_{m,\chi_e}}{m}, \quad \frac{B^{[2d]}_{m,\chi_e}(|d|)}{m}$$

are divisible by $2^{\omega(d)-1}$, this follows from Theorem 6(i). Thus, by virtue of congruence (23), we deduce that

$$\sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \left(1 - \chi_e(2)2^{m-1} - 2^{2m-1}\right) \frac{B^{[d]}_{m,\chi_e}}{m}$$
$$+ \sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \left(\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m} \right) \equiv 0 \pmod{2^{\omega(d)}}.$$

Thus we obtain the congruence

$$\sum_{\substack{e|d \\ e\neq 1}} (-1)^{\omega(e)} \frac{B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m} \equiv 0 \pmod{2^{\omega(d)}}. \tag{24}$$

Let us consider the summands of the sum on its left hand side.

$$\frac{B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m} = \sum_{k=1}^{m} \binom{m-1}{k-1} \left\{ \prod_{p|(d/e)} \left(1 - \chi_{-4}\chi_e(p)p^{k-1}\right) \right\} \frac{B_{k,\chi_{-4}\chi_e}}{k} |d|^{m-k}.$$

(Recall that

$$B_{0,\chi_{-4}\chi_e} = 0.)$$

If $e \neq d$ then, by the inductive assumption, the summands of the sum on the right hand side of the above equation have the form

$$(\text{integer}) \times 2^{\omega(d/e)} \times 2^{\omega(e)} = (\text{integer}) \times 2^{\omega(d)}$$

If $e = d$ the summands of the sum on the left hand side of congruence (24) have up to sign the form

$$\frac{B^{[4d]}_{m,\chi_{-4}\chi_d}(|d|)}{m} = \sum_{k=1}^{m} \binom{m-1}{k-1} \frac{B_{k,\chi_{-4}\chi_d}}{k} |d|^{m-k}.$$

Thus, by the inductive assumption, they are

$$(\text{integer}) \times 2^{\omega(d)} \pm \frac{B_{m,\chi_{-4}\chi_d}}{m}$$

and the theorem in case (ii) follows.

Case (iii). In this case $n-1 = \omega(d)$. We make use of Theorem 5 and Lemma 9, which yield the congruence

$$\begin{aligned}
&\sum_{\substack{e|d\\ e\neq 1}} (-1)^{\omega(e)} \big(\chi_e(2) - 2^{m-1} - 2^{3m-1}\big) \frac{B^{[d]}_{m,\chi_e}}{m} \\
&\quad + \sum_{\substack{e|d\\ e\neq 1}} (-1)^{\omega(e)} \chi_e(2) \left(\frac{B^{[2d]}_{m,\chi_e}(|d|) - B^{[2d]}_{m,\chi_e}}{m} \right) \\
&\quad - \chi_{-4}(|d|) \sum_{\substack{e|d\\ e\neq 1}} (-1)^{\omega(e)} \chi_e(2) \frac{B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m} \\
&\quad - \sum_{\substack{e|d\\ e\neq 1}} (-1)^{\omega(e)} \chi_e(2) \left(\frac{\chi_{-8}(|d|) B^{[8d]}_{m,\chi_{-8}\chi_e}(|d|)}{m} - \frac{\chi_8(|d|) B^{[8d]}_{m,\chi_8\chi_e}(|d|)}{m} \right) \\
&\quad \equiv 0 \pmod{2^{\omega(d)}}.
\end{aligned}$$

We first consider the first, second and third sums on the left hand side of the above congruence. The numbers

$$\frac{B^{[d]}_{m,\chi_e}}{m}, \ \frac{B^{[2d]}_{m,\chi_e}(|d|)}{m}$$

are divisible by $2^{\omega(d)-1}$, this follows from Theorem 6(i), and the numbers

$$\frac{B^{[4d]}_{m,\chi_{-4}\chi_e}(|d|)}{m}$$

are divisible by $2^{\omega(d)}$, this follows from Theorem 6(ii). Thus, by virtue of congruence (23), we conclude that

$$\sum_{\substack{e|d\\ e\neq 1}}(-1)^{\omega(e)}\chi_e(2)\left(\frac{\chi_{-8}(|d|)B^{[8d]}_{m,\chi_{-8}\chi_e}(|d|)}{m}-\frac{\chi_8(|d|)B^{[8d]}_{m,\chi_8\chi_e}(|d|)}{m}\right)$$
$$\equiv 0 \pmod{2^{\omega(d)}}.$$

The summands of the sum on the left hand side of the above congruence have up to sign the form

$$\frac{B^{[8d]}_{m,\chi_{-8}\chi_e}(|d|)}{m}\pm\frac{B^{[8d]}_{m,\chi_8\chi_e}(|d|)}{m}=\pm\sum_{k=1}^{m}\binom{m-1}{k-1}\mathcal{B}(k,e,d)|d|^{m-k},$$

where

$$\mathcal{B}(k,e,d)=\begin{cases}\displaystyle\prod_{p|(d/e)}(1-\chi_{-8}\chi_e(p)p^{k-1})\frac{B_{k,\chi_{-8}\chi_e}}{k}, & \text{if } \chi_e(-1)\neq(-1)^k,\\ \displaystyle\prod_{p|(d/e)}(1-\chi_8\chi_e(p)p^{k-1})\frac{B_{k,\chi_8\chi_e}}{k}, & \text{if } \chi_e(-1)=(-1)^k.\end{cases}$$

(Recall that

$$B_{0,\chi_{\pm 8}\chi_e}=0$$

and

$$\left\{\frac{B_{k,\chi_{-8}\chi_e}}{m}\right\}\times\left\{\frac{B_{k,\chi_8\chi_e}}{m}\right\}=0.) \tag{25}$$

If $e\neq d$ then, by the inductive assumption, the summands of the above sum have the form

$$(\text{integer})\times 2^{\omega(d/e)}\times 2^{\omega(e)}=(\text{integer})\times 2^{\omega(d)}.$$

If $e=d$ the corresponding summand has the form

$$\sum_{k=1}^{m}\binom{m-1}{k-1}\left(\frac{B_{k,\chi_{-8}\chi_e}}{k}\pm\frac{B_{k,\chi_8\chi_e}}{k}\right)|d|^{m-k},$$

and so, by the inductive assumption, this summand is

$$(\text{integer})\times 2^{\omega(d)}+\left(\frac{B_{m,\chi_{-8}\chi_d}}{m}\pm\frac{B_{m,\chi_8\chi_d}}{m}\right).$$

Now the theorem in case (iii) follows from (25) if $e=d$ and $k=m$. □

5. Final remarks

One of the most important properties of the generalized Bernoulli numbers is that they give the values of Dirichlet L-functions at negative integers. Namely, we have $L(1-m,\chi) = -(B_{m,\chi}/m)$, where $m \geq 1$ (see [15, Theorem 4.2]). Thus, we can rewrite the congruence of Theorem 6 in the form

$$L(1-m,\chi_d) \equiv 0 \,(\mathrm{mod}\, 2^{n-1}),$$

where $\chi_d(-1) = (-1)^m$ and d has n distinct prime factors. In particular Gauss' congruence considered in Theorem 2 was proved for the numbers $L(0,\chi_d) = h(d)$ (d negative). It is surprising that as yet no one has deduced Gauss' congruence for positive d using complex analytic methods, that is, from Dirichlet's class number formula, which in this case has the form $L(1,\chi_d) = 2d^{-1/2}h(d)\log\varepsilon$, where ε is the fundamental unit of a quadratic field with the discriminant d. Gauss' congruence for positive d has the form

$$h(d) \equiv \begin{cases} 0 \,(\mathrm{mod}\, 2^{n-1}), & \text{if } N(\varepsilon) = -1, \\ 0 \,(\mathrm{mod}\, 2^{n-2}), & \text{if } N(\varepsilon) = 1, \end{cases}$$

where N denotes the norm.

As usual, the complex and p-adic formulae differ by an Euler factor. The corresponding p-adic formulae for class numbers of quadratic fields are of the form $L_p(1,\chi_d) = 2(1-\chi_d(p)p^{-1})d^{-1/2}h(d)\log_p\varepsilon$ if d positive and $\log_p$ denotes the p-adic logarithm (this is Leopoldt's formula), and $L_p(0,\chi_d\omega_p) = (1-\chi_d(p))h(d)$ if d negative and ω_p is the Teichmüller character at p. Similarly, we have $L_p(1-m,\chi\omega_p^m) = -(1-\chi(p)p^{m-1})(B_{m,\chi}/m)$ if $m \geq 1$. Uehara [11, Lemma 3] found an inductive p-adic formula corresponding to that in Lemma 3. Uehara's formula was proved for any quadratic field. It was noticed by Urbanowicz and Wójcik that Uehara's formula is a special case of a more general inductive formula for the so-called p-adic multilogarithms introduced by Coleman [5]. Let χ be a primitive Dirichlet character modulo $M > 1$ and $\tau(\chi)$ denote the normalized Gauss sum attached to χ. Write $\zeta_M = \exp(2\pi i/M)$. Denoting by $l_{k,p}(s)$ the p-adic multilogarithms, it was proved by Coleman [5] that

$$L_p(k,\chi\omega_p^{1-k}) = (1-\chi(p)p^{-k})\frac{\tau(\chi)}{M}\sum_{n=1}^{M}\bar{\chi}(n)l_{k,p}(\zeta_M^{-n}).$$

Denoting by $l_{k,\infty}(s)$ the complex multilogarithms, we have the well known formula

$$L(k,\chi) = \frac{\tau(\chi)}{M}\sum_{n=1}^{M}\bar{\chi}(n)l_{k,\infty}(\zeta_M^{-n}).$$

Let N be a positive multiple of M such that N/M is a rational squarefree integer prime to M. Uehara's inductive formula in its most general form is

$$\sum_{\substack{k=1\\(k,N)=1}}^{N} \chi(k) l_{k,p}(\zeta_N^k) = (-1)^{\omega(N/M)} \prod_{p|(N/M)} \left(1-\chi(p)p^{1-k}\right) \sum_{\substack{k=1\\(k,M)=1}}^{M} \chi(k) l_{k,p}(\zeta_M^k)$$

(see [14, Lemma 1]). This identity implies many new congruences for the values of $L_p(k, \chi\omega_p^{1-k})$. The most general such congruences were proved in [14] and [17]. One may expect that both Gauss' congruence (for any quadratic field) and its generalization for generalized Bernoulli numbers presented in this paper can be deduced from these congruences. This means that with high probability we should be able to prove Gauss' congruence for any quadratic field using p-adic analytic methods. The related complex problem seems hopeless today.

Acknowledgments. We would like to thank A. Schinzel for reading the paper before publication and his helpful remarks. The second author wishes to express his gratitude to J. Browkin for helpful discussions in the course of writing this paper. We also thank the referees for their suggestions.

References

[1] Borevich, Z.I., Shafarevich, I.R., Number theory. Academic Press, New York 1966.

[2] Browkin, J., Schinzel, A., On Sylow 2-subgroup of K_2O_F for quadratic number fields F. J. Reine Angew. Math. 331 (1982), 104–113.

[3] Carlitz, L., Arithmetic properties of generalized Bernoulli numbers. J. Reine Angew. Math. 202 (1959), 174–182.

[4] Cohn, H., Advanced number theory. Dover, New York 1980.

[5] Coleman, R.F., Dilogarithms, regulators and p-adic L-functions. Invent. Math. 69 (1982), 171–208.

[6] Conner, P.E., Hurrelbrink, J., Class number parity. World Scientific, Singapore 1988.

[7] Hua, L.-K., Introduction to number theory. Springer, Berlin 1982.

[8] Leopoldt, H.W., Eine Verallgemeinerung der Bernoullischen Zahlen. Abh. Math. Sem. Univ. Hamburg 22 (1958), 131–140.

[9] Schinzel, A., Urbanowicz, J., van Wamelen, P., On short sums of the Kronecker symbols. To appear.

[10] Szmidt, J., Urbanowicz, J., Zagier, D., Congruences among generalized Bernoulli numbers. Acta Arith. 71 (1995), 273–278.

[11] Uehara, T., On linear congruences between class numbers of quadratic fields. J. Number Theory 34 (1990), 362–392.

[12] Urbanowicz, J., Connections between $B_{2,\chi}$ for even quadratic characters χ and class numbers of appropriate imaginary quadratic fields, I. Compositio Math. 75 (1990), 247–270. Corrigendum: ibid. 77 (1991), 119–123.

[13] Urbanowicz, J., On some new congruences for generalized Bernoulli numbers, I and II. Publ. Math. Fac. Sci. Besançon, Théorie des Nombres 1990/91.

[14] Urbanowicz, J., Wójcik, A., On linear congruence relations related to 2-adic dilogarithms. Publ. Math. Fac. Sci. Besançon, Théorie des Nombres 1995/96.

[15] Washington, L.C., Introduction to cyclotomic fields. Springer, New York 1997.

[16] Wiles, A., The Iwasawa conjecture for totally real fields. Ann. of Math. (2) 131 (1990), 493–540.

[17] Wójcik, A., Linear congruence relation for 2-adic L-series at integers. Compositio Math. 111 (1998), 289–304.