The class number of an imaginary quadratic field.

Autor(en): **Carlitz, L.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **27 (1953)**

PDF erstellt am: **17.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-21900

The class number of an imaginary quadratic field

By L. Carlitz

1. Introduction. Let $h(D)$ denote the number of classes of properly primitive forms $ax^2 + 2bxy + cy^2$ with $b^2 - ac = -D$, $D > 0$. In his paper [3] Hurwitz expressed the residue (mod p) of $h(D)$ in terms of the coefficients of certain power series; here p is an odd prime divisor of D such that $D \not\equiv 0 \pmod{p^2}$. In some cases the residue was expressed explicitly in terms of Bernoulli numbers.

Let now $h(d)$ denote the class number of the imaginary quadratic field $R(\sqrt{d})$ of discriminant d. (We prefer to use the terminology of quadratic fields rather than quadratic forms in order to stress the analogy with certain other results on the class number of cyclic fields [1]). Let p be an odd prime divisor of d and $n \geq 0$; then we show that for $d < -4$.

$$h(d) \equiv -2c\left(\frac{q}{p}\right) \sum_{1 \leq s < q/2} \left(\frac{q_0}{s}\right) B_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}, \tag{1.1}$$

where $d = (-1)^{(p-1)/2} pq_0$, $q = |q_0|$, (q_0/s) is the Kronecker symbol, $B_k(x)$ is the Bernoulli polynomial of degree $k = \frac{1}{2}(p-1)p^n + 1$ and $c = 1 + \frac{1}{2}p^n$ for $n \geq 1$, while $c = 2$ for $n = 0$. A particularly simple special case of (1.1) is

$$h(-4p) \equiv \tfrac{1}{2}E_{k-1} \pmod{p^{n+1}}, \tag{1.2}$$

where $p \equiv 1 \pmod 4$ and E_{k-1} is an Euler number.

2. Kronecker's symbol. We recall a few properties of Kronecker's symbol (see for example [4, p. 51]). If $d \equiv 0$ or $1 \pmod 4$ and is not a square and if $m > 0$, we define

$$\left(\frac{d}{1}\right) = 1, \left(\frac{d}{p}\right) = 0 \quad (p \mid d),$$

$$\left(\frac{d}{2}\right) = \begin{cases} 1 \,(d \equiv 1 \pmod 8) \\ -1 \,(d \equiv 5 \pmod 8), \end{cases}$$

$$\left(\frac{d}{p}\right) = \text{the Legendre symbol when } p > 2,\ d \not\equiv 0 \pmod p,$$

$$\left(\frac{d}{p_1 \cdots p_r}\right) = \left(\frac{d}{p_1}\right) \cdots \left(\frac{d}{p_r}\right).$$

It follows from the definition that

$$\left(\frac{d}{m}\right) = 0 \quad \text{for} \quad (d, m) > 1 ; \left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right); \tag{2.1}$$

also for odd d we have

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right), \tag{2.2}$$

where the quantity on the right is a Jacobi symbol. Another useful property is

$$\left(\frac{d}{m_1}\right) = \left(\frac{d}{m_2}\right) \quad (m_1 \equiv m_2 (\text{mod} \ \ d)) . \tag{2.3}$$

We shall also require

$$\left(\frac{d}{|d| - m}\right) = \left(\frac{d}{m}\right) \text{sgn } d \quad (m < |d|) . \tag{2.4}$$

It is sometimes convenient to define $\left(\frac{d}{0}\right) = 0$.

Thus it is clear that if d is the discriminant of a quadratic field then $\left(\frac{d}{m}\right)$ is a character (mod d).

The letter p will denote a positive odd prime. We define

$$p_0 = (-1)^{(p-1)/2} p, \tag{2.5}$$

so that $p_0 \equiv 1$ (mod 4). If $p \mid d$ we put

$$d = p_0 q_0, \qquad q = |q_0| . \tag{2.6}$$

It follows that the Kronecker symbols (p_0/m) and (q_0/m) are defined; moreover

$$\left(\frac{d}{m}\right) = \left(\frac{p_0}{m}\right)\left(\frac{q_0}{m}\right). \tag{2.7}$$

Hereafter d will denote the discriminant of an imaginary quadratic field. Hence $d < 0$ and is not divisible by the square of any odd prime.

3. Bernoulli polynomials. We use the notation of Nörlund [5, Chapter 2] for the Bernoulli polynomials. The following formulas will be needed.

$$\sum_{a=0}^{m-1} (x + a)^{n-1} = \frac{B_n(x + m) - B_n(x)}{n}, \tag{3.1}$$

$$B_n(x + y) = \sum_{s=0}^{n} \binom{n}{s} x^{n-s} B_s(y) ; \tag{3.2}$$

$$B_n(1 - x) = (-1)^n B_n(x) . \tag{3.3}$$

In addition we recall a special case of Kummer's congruence [2, Theorem 5]

$$\frac{B_{n+t}(a)}{n+t} \equiv \frac{B_n(a)}{n} \pmod{p^e}, \tag{3.4}$$

where $p^{e-1}(p-1) \mid t, n \not\equiv 0 \pmod{p-1}, n > e$ and the rational number a is integral (mod p). The following divisibility property will also be used.

$$B_m(a) \equiv 0 \pmod{p^r} \quad (p^r \mid m, m \not\equiv 0 \pmod{p-1} \tag{3.5}$$

where again a is integral (mod p).

For some purposes it is convenient to define the Bernoulli function $\bar{B}_m(x)$:

$$\bar{B}_m(x) = \bar{B}_m(x) \qquad (0 \leq x < 1)$$

$$\bar{B}_m(x+1) = B_m(x).$$

Then $\bar{B}_m(x)$ satisfies (3.3) as well as the multiplication formula

$$\sum_{s=0}^{r-1} \bar{B}_m\left(x + \frac{s}{r}\right) = r^{1-m} \bar{B}_m(rx); \tag{3.6}$$

the polynomial $B_m(x)$ also satisfies (3.6).

4. The main result. Let $d < -3$. It is familiar that

$$h(d) = \frac{1}{d} \sum_m m\left(\frac{d}{m}\right), \tag{4.1}$$

where m runs through a complete residue system (mod d). We assume $p \mid d$ and make use of (2.5), (2.6), (2.7). Let $q > 1$. Then (4.1) becomes

$$\begin{aligned} h(d) &= \sum_{r=0}^{p-1} \sum_{s=1}^{q-1} (rq+s)\left(\frac{p_0}{rq+s}\right)\left(\frac{q_0}{rq+s}\right) \\ &= \frac{1}{d} \sum_{s=1}^{q-1} \left(\frac{q_0}{s}\right) \sum_{r=0}^{p-1} (rq+s)\left(\frac{rq+s}{p}\right). \end{aligned} \tag{4.2}$$

Now it follows from

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)p^n/2} \pmod{p^{n+1}}. \tag{4.3}$$

Then using (4.3) we have

$$\sum_{r=0}^{p-1} (rq+s)\left(\frac{rq+s}{p}\right) \equiv \sum_{r=0}^{p-1} (rq+s)^k \pmod{p^{n+1}}, \tag{4.4}$$

where for brevity we put

$$k = \tfrac{1}{2}(p-1)\,p^n + 1\,. \tag{4.5}$$

Then using (3.1) we get

$$\sum_{r=0}^{p-1} (rq+s)^k = q^k \sum_{r=0}^{p-1}\left(r+\frac{s}{q}\right)^k = q^k\,\frac{B_{k+1}\left(p+\frac{s}{q}\right) - B_{k+1}\left(\frac{s}{q}\right)}{k+1}\,. \tag{4.6}$$

In the next place by (3.2)

$$B_{k+1}\left(p+\frac{s}{q}\right) - B_{k+1}\left(\frac{s}{q}\right) = (k+1)\,p B_k\left(\frac{s}{q}\right) + \binom{k+1}{2} p^2 B_{k-1}\left(\frac{s}{q}\right)$$
$$+ \sum_{r=3}^{k+1}\binom{k+1}{r} p^r B_{k-r+1}\left(\frac{s}{q}\right).$$

But it is easily verified that

$$\binom{k+1}{r} p^r B_{k-r+1}\left(\frac{s}{q}\right) \equiv 0 \pmod{p^{n+1}} \quad (r \geq 3)\,.$$

Thus (4.6) becomes

$$\sum_{r=0}^{p-1} (rq+s)^k \equiv q^k\left\{p B_k\left(\frac{s}{q}\right) + \tfrac{1}{2} k p^2 B_{k-1}\left(\frac{s}{q}\right)\right\}$$
$$\equiv pq\left(\frac{q}{p}\right) B_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}\,,$$

where we have used (4.3) and (3.5).

Substituting in (4.4) and (4.2) we therefore get

$$h(d) \equiv -\left(\frac{q}{p}\right)\sum_{s=1}^{q-1}\left(\frac{q_0}{s}\right) B_k\left(\frac{s}{q}\right) \pmod{p^n}\,.$$

Finally using (3.4) this becomes

$$h(d) \equiv -\frac{1}{1-\frac{1}{2}p^{n-1}}\left(\frac{q}{p}\right)\sum_{s=1}^{q-1}\left(\frac{q_0}{s}\right) B_l\left(\frac{s}{q}\right) \pmod{p^n}\,.$$

where $l = \frac{1}{2}(p-1)\,p^{n-1} + 1$. Replacing n by $n+1$ we get

$$h(d) \equiv -\,c\left(\frac{q}{p}\right)\sum_{s=1}^{q-1}\left(\frac{q_0}{s}\right) B_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}\,, \tag{4.7}$$

where k is defined by (4.5) and $c = 1 + \frac{1}{2}p^n$ for $n > 0, c = 2$ for $n = 0$.

In the next place if $p \equiv 1 \pmod 4$, then k is odd so that by (3.3)

$$B_k\left(\frac{q-s}{q}\right) = - B_k\left(\frac{s}{q}\right).$$

Also since $p_0 > 0, q_0 < 0$, so that by (2.4) $\left(\frac{q_0}{q-s}\right) = -\left(\frac{q_0}{s}\right)$.

It follows that

$$\left(\frac{q_0}{q-s}\right) B_k\left(\frac{q-s}{q}\right) = \left(\frac{q_0}{s}\right) B_k\left(\frac{s}{q}\right). \tag{4.8}$$

If $p \equiv -1 \pmod 4$, then k is even and $q > 0$, so that

$$B_k\left(\frac{q-s}{q}\right) = B_k\left(\frac{s}{q}\right), \quad \left(\frac{q_0}{q-s}\right) = \left(\frac{q_0}{s}\right).$$

and again (4.8) follows. Since for q_0 even the value $s = q_0/2$ in (4.7) may be ignored we get

$$h(d) \equiv -2c\left(\frac{q}{p}\right) \sum_{1 \leq s < q/2} \left(\frac{q_0}{s}\right) B_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}, \tag{4.9}$$

where k and c are the same as in (4.7).

5. The case $q = 1$. While (4.9) does not hold for $q = 1$, it is easy to obtain a similar result in that case. We now have $d = -p$, where $p \equiv 3 \pmod 4$. Thus (4.1) becomes

$$h(-p) = -\frac{1}{p} \sum_m m\left(\frac{-p}{m}\right) = -\frac{1}{p} \sum_m m\left(\frac{m}{p}\right).$$

Now

$$\sum_{m=1}^{p-1} m\left(\frac{m}{p}\right) \equiv \sum_{m=1}^{p-1} m^k \equiv \frac{B_{k+1}(p) - B_{k+1}}{k+1} \pmod{p^{n+1}},$$

where k is the same as in (4.5); note that k is even. A little manipulation leads to

$$h(-p) \equiv -B_k \pmod{p^n}. \tag{5.1}$$

In particular for $n = 1$, (5.1) becomes

$$h(-p) \equiv -B_{(p-1)p/2+1} \pmod p,$$

which by (3.4) reduces to

$$h(-p) \equiv -2B_{(p+1)/2} \pmod p. \tag{5.2}$$

6. Some special cases. Returning to (4.9) we consider first the special case $d = -3p, p \equiv 1 \pmod 4$. Thus $q_0 = -3, q = 3$ and (4.9) reduces to

$$h(-3p) \equiv -2c\left(\frac{3}{p}\right) B_k\left(\frac{1}{3}\right) \pmod{p^{n+1}}. \tag{6.1}$$

Since k is odd it does not seem possible to further simplify the right member of (6.1). For $n = 0$, (6.1) becomes

$$h(-3p) \equiv -4\left(\frac{3}{p}\right) B_{(p+1)/2}\left(\frac{1}{3}\right) \pmod p. \tag{6.1$'$}$$

Next for $d = -4p, p \equiv 1 \pmod 4$, $q_0 = -4, q = 4$, so that (4.9) becomes

$$h(-4p) \equiv -2cB_k(\tfrac{1}{4}) \pmod{p^{n+1}}. \tag{6.2}$$

Now we may use the formula [4, p. 29]

$$B_k\left(\frac{1}{4}\right) = -k\frac{E_{k-1}}{4^k} \quad (k \text{ odd}),$$

where E_{k-1} is an Euler number. Since

$$4^k = 2^{2k} = 2^{(p-1)p^n+2} \equiv 4 \pmod{p^{n+1}},$$

it is easily verified that (6.2) gives

$$h(-4p) \equiv \tfrac{1}{2}E_{k-1} \pmod{p^{n+1}}; \tag{6.3}$$

in particular for $n = 0$, we get

$$h(-4p) \equiv \tfrac{1}{2}E_{(p-1)/2} \pmod p. \tag{6.3$'$}$$

For example for $p = 5, h(-20) = 2, E_2 = -1$.

For $d = -5p, p \equiv 3 \pmod 4$, $q = q_0 = 5$, we have

$$h(-5p) \equiv -2c\left(\frac{5}{p}\right)\left\{B_k\left(\frac{1}{5}\right) - B_k\left(\frac{2}{5}\right)\right\} \pmod{p^{n+1}}; \tag{6.4}$$

in particular

$$h(-5p) \equiv -4\left(\frac{5}{p}\right)\left\{B_{(p+1)/2}\left(\frac{1}{5}\right) - B_{(p+1)/2}\left(\frac{2}{5}\right)\right\} \pmod p. \tag{6.4$'$}$$

For $d = -8p$, we have either (*i*) $p \equiv 1 \pmod 4$, $q_0 = -8, q = 8$, or (ii) $p \equiv 3 \pmod 4$, $q_0 = q = 8$. The two possibilities may be combined in the single formula

$$h(-8p) \equiv -2c\left(\frac{2}{p}\right)\left\{B_k\left(\frac{1}{8}\right) + \left(\frac{-1}{p}\right)B_k\left(\frac{3}{8}\right)\right\} \pmod{p^{n+1}}, \tag{6.5}$$

which does not seem to reduce further. Using (3.3) we may however write

$$h(-8p) \equiv -2c\left(\frac{2}{p}\right)\left\{B_k\left(\frac{1}{8}\right) - B_k\left(\frac{5}{8}\right)\right\} \pmod{p^{n+1}}, \tag{6.6}$$

as is easily verified.

We may also mention the case $d = -12p$, where $p \equiv 3 \pmod 4$, $q = q_0 = 12$. Thus (4.9) becomes

$$h(-12p) \equiv -2c\left(\frac{3}{p}\right)\left\{B_k\left(\frac{1}{12}\right) - B_k\left(\frac{5}{12}\right)\right\} \pmod{p^{n+1}}. \tag{6.7}$$

7. Some additional formulas. Formula (4.7) becomes somewhat more symmetrical if we introduce the Bernoulli function $\bar{B}_k(x)$ defined in § 3. For we may now write

$$h(d) \equiv -c\left(\frac{q}{p}\right)\sum_s\left(\frac{q_0}{s}\right)\bar{B}_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}, \tag{7.1}$$

where s runs through a complete residue system (mod q). In the next place, using (3.6), we have

$$\sum_{s=0}^{q-1} \bar{B}_k\left(\frac{s}{q}\right) = q^{1-k}\,\bar{B}_k(0) = q^{1-k}B_k. \tag{7.2}$$

Also

$$q^{1-k} = q^{-(p-1)/2\,p^n} \equiv \left(\frac{q}{p}\right) \pmod{p^{n+1}},$$

so that (7.2) becomes

$$\sum_{s=1}^{q-1} \bar{B}_k\left(\frac{s}{q}\right) \equiv \left\{\left(\frac{q}{p}\right) - 1\right\} B_k.$$

Combining with (7.1) we get

$$h(d) \equiv -2c\left(\frac{q}{p}\right)\sum_s{}' \bar{B}_k\left(\frac{s}{q}\right) + c\left\{1 - \left(\frac{q}{p}\right)\right\} B_k \pmod{p^{n+1}}, \tag{7.3}$$

where the sum is now restricted to such s that $(q_0/s) = 1$. If $p \equiv 1$ (mod 4), so that k is odd, (7.3) reduces to

$$h(d) \equiv -2c\left(\frac{q}{p}\right)\sum_s{}' \bar{B}_k\left(\frac{s}{q}\right) \pmod{p^{n+1}}; \tag{7.4}$$

if $(q/p) = 1$ then (7.4) holds for all p. If q is a prime then (7.3) may also be written in the form

$$h(d) \equiv -c\left(\frac{q}{p}\right)\sum_{s=0}^{q-1}\bar{B}_k\left(\frac{s^2}{q}\right) + cB_k \pmod{p^{n+1}}. \tag{7.5}$$

The last formula suggests that it may be interesting to consider the sum

$$S_k(h, q) = \sum_{s=0}^{q-1}\bar{B}_k\left(\frac{s^2 h}{q}\right) - q^{1-k}B_k \tag{7.6}$$

for arbitrary positive k and q. In particular if q is an odd prime power then it follows from (7.2) and (7.6) that

$$S_k(h, q) = \sum_{s=1}^{q-1}\left(\frac{s}{q}\right)\bar{B}_k\left(\frac{sh}{q}\right) \quad ((h, q) = 1)$$

and therefore

$$S_k(h, q) = \left(\frac{h}{q}\right) S_k(1, q). \tag{7.7}$$

In the next place if $q = p^r, r \geq 3,$ then

$$S_k(1, p^r) = \sum_{b=0}^{p^{r-1}-1} \sum_{a=0}^{p-1} \overline{B}_k\left(\frac{b^2}{p^r} + \frac{2ab}{p}\right)$$

$$= p \sum_{b=0}^{p^{r-2}-1} \overline{B}_k\left(\frac{b^2}{p^{r-2}}\right) + \sum_{\substack{b=0 \\ p+b}}^{p^{r-1}-1} \sum_{a=0}^{p-1} \overline{B}_k\left(\frac{b^2}{p^r} + \frac{2ab}{p}\right)$$

$$= p\{S_k(1, p^{r-2}) + p^{(r-2)(1-k)} B_k\} + p^{1-k} \sum_{\substack{b=0 \\ p+b}}^{p^{r-1}-1} \overline{B}_k\left(\frac{b^2}{p^{r-1}}\right)$$

$$= p\{S_k(1, p^{r-2}) + p^{(r-2)(1-k)} B_k\} + p^{1-k} \sum_{b=0}^{p^{r-1}-1} \overline{B}_k\left(\frac{b^2}{p^{r-1}}\right)$$
$$- p^{1-k} \sum_{b=0}^{p^{r-2}-1} \overline{B}_k\left(\frac{b^2}{p^{r-3}}\right)$$

$$= p\{S_k(1, p^{r-2}) + p^{(r-2)(1-k)} B_k\}$$
$$+ p^{1-k}\{S_k(1, p^{r-1}) + p^{(r-1)(1-k)} B_k\}$$
$$- p^{2-k}\{S_k(1, p^{r-3}) + p^{(r-3)(1-k)} B_k\},$$

so that

$$S_k(1, p^r) = p^{1-k} S_k(1, p^{r-1}) + p S_k(1, p^{r-2}) - p^{2-k} S_k(1, p^{r-3}) + p^{r(1-k)} B_k. \tag{7.8}$$

For $r = 2$, we find that

$$S_k(1, p^2) = p^{1-k} S_k(1, p) + (p - p^{1-k} + p^{2(1-k)}) B_k. \tag{7.9}$$

REFERENCES

[1] *L. Carlitz,* The first factor of the class number of a cyclic field, Candian J. Math., to appear.

[2] *L. Carlitz,* A note on Bernoulli numbers and polynomials of higher order, Proc. Amer. Math. Soc., vol. 3 (1952), pp. 608—613.

[3] *A. Hurwitz,* Über die Anzahl der Klassen binärer quadratischer Formen von negativer Determinante, Acta Math., vol. 19 (1895), pp. 351—384 (= Mathematische Werke, vol. 2, Basel, 1933), pp. 208—235.

[4] *E. Landau,* Vorlesungen über Zahlentheorie, vol. 1, Leipzig, 1927.

[5] *N. E. Nörlund,* Vorlesungen über Differenzenrechnung, Berlin, 1924.

(Received March 23, 1953)