Stanislav Jakubec

On divisibility of the class number of real octic fields of a prime conductor $p = n^4 + 16$ by p

Archivum Mathematicum, Vol. 30 (1994), No. 4, 263--270

Persistent URL: http://dml.cz/dmlcz/107512

ARCHIVUM MATHEMATICUM (BRNO)
Tomus 30 (1994), 263 – 270

ON DIVISIBILITY OF THE CLASS NUMBER OF REAL OCTIC FIELDS OF A PRIME CONDUCTOR p n^4 16 BY p

Stanislav Jakubec

Abstract. The aim of this paper is to prove the following Theorem

Theorem. *Let K be an octic subfield of the field $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ and let $p=n^4+16$ be prime. Then p divides h_K if and only if p divides B_j for some $j=\frac{p-1}{8}, 3\frac{p-1}{8}, 5\frac{p-1}{8}, 7\frac{p-1}{8}$.*

Introduction

K p
K $\mathbf{Q}$, , , ,
K $\mathbf{Q}$ K β_i $\beta_{i+2}-\frac{n^2-1}{4}$

K
K $\mathbf{Q}$
K

$\mathbf{Q}$ ζ_p ζ_p^{-1} p
$\mathbf{Q}$ ζ_p ζ_p^{-1}

K $\mathbf{Q}$
K $\mathbf{Q}$
h_K p n^4 n^3 n^2 n

1991 *Mathematics Subject Classification*: Primary 11R29.

Received September 28, 1993.
Research supported by Slovak Academy of Sciences Grant 363.

Theorem. *Let K be a quintic subfield of the field* $\mathbf{Q}\ \zeta_p \quad \zeta_p^{-1}$ *and let* p $n^4 \quad n^3 \quad n^2 \quad n$. *Let $p > N_0$ be prime. Then p divides h_K if and only if p divides B_j for some j* $\frac{p-1}{5}, \ \frac{p-1}{5}, \ \frac{p-1}{5}, \ \frac{p-1}{5}$.

N_0

$K \quad \mathbf{Q}$

$$F_n\ X \quad X^8 \quad n^2X^7 \quad p- \quad X^6 - \ p \quad n^2\ X^5 - \ p\ n^2 \quad - \quad X^4$$

$$n^2 - p\ n^2 - \quad X^3 \quad p- \quad X^2 \quad p- \ n^2\ X \quad ,$$

$$p \quad n^4 \quad ,$$

$$i \quad \beta_i \quad \beta_{i+2} - \frac{n^2 -}{}.$$

$p, p \equiv$ n K $\mathbf{Q}\ \zeta_p$ n $\mathbf{Q}$ a p σ $\mathbf{Q}\ \zeta_p$ $\sigma\ \zeta_p \quad \zeta_p^a$

$\beta_0 \quad {}_{\mathbf{Q}(\zeta_p)/K}\ \zeta_p \quad \beta_1 \quad \sigma\ \beta_0\ , \beta_2 \quad \sigma\ \beta_1\ , \dots, \beta_{n-1} \quad \sigma\ \beta_{n-2} \quad k \quad \frac{p-1}{n}$ $a^k \equiv g$ p $\beta_0, \beta_1, \dots, \beta_{n-1}$ $K/\mathbf{Q}$

Theorem 1. *There is a number $\pi \in K, \pi | p$ such that*

$N_{K/\mathbf{Q}}\ \pi \quad - \quad {}^n p,$

$\sigma\ \pi \ \equiv g\pi \quad \pi^{n+1}\ ,$

$\beta_0 \equiv k \sum_{i=0}^{n} \frac{1}{(ki)!}\pi^i \quad \pi^{n+1}\ .$

□

$\mathbf{Q}\ X$ $\mathbf{Q}^*\ X$ $f\ X \quad a_0\ /$ $f\ X \quad \lambda_1, \lambda_2, \dots, \lambda_r$

$$s_j \; f \; X \qquad \overline{\lambda_1^j} \quad \overline{\lambda_2^j} \quad \cdots \quad \overline{\lambda_r^j}.$$

U_K K $\varepsilon \in U_K$

$$\varepsilon \equiv a_0 \quad a_1\pi \quad \cdots \quad a_n\pi^n \qquad \pi^{n+1} \; .$$

$a_0 \not\equiv$ p ε
$\varepsilon \not\equiv$ π

$$f \; X \qquad a_0 \quad a_1 X \quad \cdots \quad a_n X^n$$

$$s_j \; \varepsilon \qquad s_j \; f \; X \; .$$

$ii_K \; p$ $i \; \varepsilon$

$$ii_K \; p \qquad \{j, j \quad , \; , \ldots, n - \; , B_{kj} \equiv \qquad p \; \},$$

$$i \; \varepsilon \qquad \{j, j \quad , \; , \ldots, n - \; , s_j \; \varepsilon \; \equiv \qquad p \; \}.$$

Theorem 2. *Let* $K \subset \mathbf{Q} \; \zeta_p \quad \zeta_p^{-1}$, $K \quad \mathbf{Q} \qquad n$, $k \quad \frac{p-1}{n}$ *and let* h_K *be the class number of* K.

Then there holds

If there exist a unit ε *and a number* j *such that* $B_{kj} \equiv \qquad p$ *and* $s_j \; \varepsilon \; \not\equiv \qquad p$, *then* p *divides* h_K.

Let ε *be a unit. Then*

$$p^{ii_K(p)-i(\varepsilon)} | h_K.$$

Lemma 1. *Let* K *be an octic subfield of the field* $\mathbf{Q} \; \zeta_p \quad \zeta_p^{-1}$ *and let* $p \quad n^4$ *be prime. If* $B_j \equiv \qquad p$ *for some* $j \quad \frac{p-1}{8}, \; \frac{p-1}{8}, \; \frac{p-1}{8}, \; \frac{p-1}{8}$, *then* p *divides* h_K.

Proof.

$$\varepsilon \quad \beta_0 \quad \beta_2 - \frac{n^2 -}{}.$$

$k \quad \frac{p-1}{8} \; g \quad a^{\frac{p-1}{8}} \qquad p$

$$\varepsilon \quad \frac{p - n^2}{} \quad \frac{k \qquad g^2}{k}\pi \quad \frac{k \quad - g^2}{k}\pi^3 \quad \frac{k}{k}\pi^4 \quad \frac{k \qquad g^2}{k}\pi^5 \quad \frac{k \quad - g^2}{k}\pi^7 - \; k\pi^8.$$

$s_j \; \varepsilon \; \not\equiv \qquad p \qquad j \qquad , \; , \; ,$

$$g\ X \quad X^8 \quad \frac{g^2}{n^2k}X^7 \quad X^6 \quad \frac{-\ g^2}{n^2\ \ k}X^5 \quad \frac{}{An^2}X^4$$
$$\frac{g^2}{n^2\ \ k}X^3 \quad X^2 \quad \frac{-\ g^2}{n^2\ \ k}X - \frac{}{n^2},$$

A $\left(\frac{p-1}{2}\right)$ $A^2 \equiv -$ p

S_i $g\ X$.

S_i $s_i\ \varepsilon$ $S_i \not\equiv$ p
i , , , S_1 $-\frac{1+g^2}{2n^2(k)!} \not\equiv$ p

$$S_3S_5S_7 \not\equiv \quad p\ .$$

$$x_1 \quad k \quad x_2 \quad \frac{k}{k} \quad x_3 \quad \frac{k}{k} \quad x_4 \quad \frac{k}{k}.$$

$$\varepsilon \quad \frac{p-n^2}{} \quad \frac{k \quad g^2}{k}\pi \quad \frac{k \quad -g^2}{k}\pi^3 \quad \frac{k}{k}\pi^4$$
$$\frac{k \quad g^2}{k}\pi^5 \quad \frac{k \quad -g^2}{k}\pi^7 - \ k\pi^8$$
$$\frac{p-n^2}{} \quad \frac{k \quad g^2}{x_1}\pi \quad \frac{k \quad -g^2}{x_1x_2x_3}\pi^3 \quad \frac{k}{A}\pi^4$$
$$-\ k \quad g^2\ x_1x_2x_3\pi^5 - k \quad -g^2\ x_1\pi^7 - \ k\pi^8$$
$$a_0 \quad a_1\pi \quad a_3\pi^3 \quad a_4\pi^4 \quad a_5\pi^5 \quad a_7\pi^7 \quad a_8\pi^8\ .$$

$$K/\mathbf{Q}\ a_0 \quad a_1\pi \quad a_3\pi^3 \quad a_4\pi^4 \quad a_5\pi^5 \quad a_7\pi^7 \quad a_8\pi^8\ ^3$$
$$\equiv\ a_0^3 \quad F\ a_0, a_1, a_3, a_4, a_5, a_7, a_8\ \ \pi^8$$
$$\equiv\ a_0^3 -\ pF\ a_0, a_1, a_3, a_4, a_5, a_7, a_8 \quad \pi^9\ ,$$

$F\ a_0, a_1, a_3, a_4, a_5, a_7, a_8$ $a_0, a_1, a_3, a_4, a_5, a_7, a_8$
π^8

$$a_0 \quad a_1\pi \quad a_3\pi^3 \quad a_4\pi^4 \quad a_5\pi^5 \quad a_7\pi^7 \quad a_8\pi^8\ ^3.$$

$S_3 \;\; n$

$$a_0^3 - \;\; pF \;\; a_0, a_1, a_3, a_4, a_5, a_7, a_8 \;\; \equiv S_3 \;\; n \qquad \pi^9 \;\; ,$$

$$F \;\; a_0, a_1, a_3, a_4, a_5, a_7, a_8 \;\; \equiv \frac{a_0^3 - S_3 \;\; n}{p} \qquad p \;\; .$$

$$\frac{}{x_1^2 x_2 x_3} \equiv - \;\; n^2 \qquad p \;\; .$$

$$K/\mathbf{Q} \;\; a_0 \quad a_1\pi \quad a_3\pi^3 \quad a_4\pi^4 \quad a_5\pi^5 \quad a_7\pi^7 \quad a_8\pi^8 \;\; ^4.$$

$$\frac{}{x_1^4 x_2^2 x_3^2} \quad \frac{x_2 x_3}{x_1^2} \quad \frac{n^2}{x_1^2 x_2 x_3 A} \equiv \quad n^2 \qquad p \;\; .$$

$$K/\mathbf{Q} \;\; a_0 \quad a_1\pi \quad a_3\pi^3 \quad a_4\pi^4 \quad a_5\pi^5 \quad a_7\pi^7 \quad a_8\pi^8 \;\; ^5.$$

$$\frac{}{x_1^4} - \frac{n^2}{x_1^4 x_2^2 x_3^2} \quad \frac{}{x_1^2 x_2 x_3 A} \quad \frac{n^2 x_2 x_3}{x_1^2} \equiv \quad - n^2 \qquad p \;\; .$$

$$\frac{}{x_1^4} \equiv - \quad A \qquad p \;\; ,$$

$$\frac{}{x_1^2 x_2 x_3} \equiv A \;\; - \;\; n^2 \qquad p \;\; ,$$

$$\frac{n^2}{x_1^4 x_2^2 x_3^2} \equiv - \;\; - \;\; n^2 \quad {}^2 \equiv \quad n^2 \qquad p \;\; .$$

$$g\ X \quad X^8 \quad \frac{g^2}{n^2x_1}X^7 \quad X^6 \quad \frac{-\ g^2}{n^2x_1x_2x_3}X^5 \quad \frac{}{An^2}X^4$$

$$\frac{g^2\ x_1x_2x_3}{n^2}X^3 \quad X^2 \quad \frac{-\ g^2\ x_1}{n^2}X - \frac{}{n^2}.$$

$S_3 \equiv \quad p$

$$S_3 \quad -\frac{g^2\ ^3}{n^6x_1^3} - \quad \frac{-\ g^2}{n^2x_1x_2x_3} \equiv \quad p\ .$$

$n^4 \equiv - \quad p \quad g^2\ ^4 \equiv - \quad p \quad -\ g^2 \quad g^2 \equiv \quad p$

$$\frac{}{x_1^4} \quad \frac{}{x_1^2x_2x_3} \equiv \quad p\ .$$

$$— - \quad A \quad A - n^2 \quad \equiv \quad p\ .$$

$n^2 \quad \equiv \quad p \quad\quad p \quad n^4$

$g\ X \quad S_5 \not\equiv \quad p \quad S_7 \not\equiv \quad p$

□

Lemma 2. *Let* $p \quad n^2 \quad , n \equiv \quad$. *Then* $B_{\frac{p-1}{4}}B_{3\frac{p-1}{4}} \not\equiv \quad p\ .$

Proof.

$$X^4 \quad nX^3 - \quad X^2 - nX \quad ,$$

$$\beta_0 - \frac{n-}{}, \quad \mathbf{Q}\ \beta_0 \quad \mathbf{Q} \quad .$$

$$\beta_0 - \frac{p-}{} \equiv \frac{p-n}{} \quad \frac{k}{x_1}\pi \quad \frac{k}{A}\pi^2 - kx_1\pi^3 - k\pi^4 \quad \pi^5\ ,$$

$$k \quad \frac{p-}{} \quad x_1 \quad k \quad A \quad \left(\frac{p-}{}\right).$$

$$g\ X \quad X^4 \quad \frac{}{x_1}X^3 \quad \frac{}{nA}X^2 - \frac{x_1}{n}X - \frac{}{n}.$$

$$\frac{}{x_1^2} \equiv - \ nA \qquad p \ .$$

$$S_1 \not\equiv \qquad p \quad S_2 \equiv \qquad p \quad S_3 \not\equiv \qquad p \ .$$

$B_{\frac{p-1}{4}} \equiv \qquad p \qquad B_{3\frac{p-1}{4}} \equiv \qquad p$
$p \qquad h_K \quad K \quad \mathbf{Q} \qquad p \qquad h_K$
$B_{\frac{p-1}{4}} B_{3\frac{p-1}{4}} \not\equiv \qquad p$ □

$K \qquad \mathbf{Q} \ \zeta_p \quad \zeta_p^{-1} \quad K \quad \mathbf{Q} \quad n$
E_j

Lemma 3. *The prime number p divides h_K if and only if $E_{i\frac{p-1}{n}}$ $p-th$ power for some i $\ ,\ ,\ldots n-\ $. If $E_{i\frac{p-1}{n}}$ $p-th$ power, then $B_{i\frac{p-1}{n}} \equiv \qquad p\ .$*

Proof.

$$\varepsilon_i \qquad \frac{}{p-} \sum_{a=1}^{p-1} \omega^{-1} \ a \ \sigma_a \in \mathbf{Z}_p \ G \quad , \qquad .$$

$$i \not\equiv \qquad \frac{p-1}{n} \qquad \varepsilon_i U_K / U_K^{p^n}$$

$$U_K / U_K^{p^n} \qquad \bigoplus_{j=1}^{n-1} \varepsilon_{j\frac{p-1}{n}} U_K / U_K^{p^n} .$$

□

$$B_{\frac{p-1}{8}} B_{3\frac{p-1}{8}} B_{5\frac{p-1}{8}} B_{7\frac{p-1}{8}} \not\equiv \qquad p \qquad p$$
$h_K \qquad B_{\frac{p-1}{2}} \not\equiv \qquad p \qquad p \qquad h_K$
$B_{\frac{p-1}{2}} \equiv \qquad p \qquad p \qquad h_K \qquad B_{\frac{p-1}{8}} B_{3\frac{p-1}{8}} B_{5\frac{p-1}{8}} B_{7\frac{p-1}{8}} \not\equiv$
$p \qquad B_{\frac{p-1}{4}} B_{3\frac{p-1}{4}} \not\equiv \qquad p \qquad E_{i\frac{p-1}{2}} \quad p$
$E_{i\frac{p-1}{2}} \in \mathbf{Q} \ \sqrt{p} \qquad n$
$p \qquad \mathbf{Q} \ \sqrt{p}$
$h \ \mathbf{Q} \ \sqrt{p} \quad < p$

Theorem 3. *Let K be an octic subfield of the field $\mathbf{Q}\ \zeta_p \quad \zeta_p^{-1}$ and let $p \quad n^4$ be prime. Then p divides h_K if and only if p divides B_j for some $j \quad \frac{p-1}{8}, \quad \frac{p-1}{8}, \quad \frac{p-1}{8}, \quad \frac{p-1}{8}$.*

$$p <$$

$$B_{j\frac{p-1}{8}} \equiv \quad p \quad j \quad , \; , \; , \; , \; .$$

$p <$

$$B_{j\frac{p-1}{5}} \equiv \quad p \quad j \quad , \; , \; , \; ,$$

p $\quad B_{52324} \equiv$

$$/ \; n^4 \quad n^3 \quad n^2 \quad n \quad .$$

References

[1] Buhler, J. P., Crandall, R. E. and Sompolski, R. W., *Irregular primes to one million*, Math. Comp. **59** no. 200 (1992), 717-722.

[2] Darmon, H., *Note on a polynomial of Emma Lehmer*, Math. Comp. **56** no. 44 (1991), 795-800.

[3] Gras, M. N., *Sur les corps cubiques cycliques dont l'anneau des entiers est monogene*, Ann. Sci. Univ. Besancon Math.(3) no. 6, 1-26.

[4] Gras, M. N., *Table numerique du nombre de classes et de unites des extensions cycliques reelles de degre 4 de Q*, Publ. Math. Besancon, fasc. 2 (1977/1978), 1-26, 1-53.

[5] Gras, M. N., *Familles d'unites dans les extensions cycliques reelles de degre 6 de Q*, Publ. Math. Besancon (1984/1985-1985/1986).

[6] Gras, M. N., *Special units in real cyclic sextic fields*, Math.Comp. **48** (1987), 341-355.

[7] Jakubec, S., *The congruence for Gauss's period*, Journal of Number Theory **48** (1994), 36-45.

[8] Jakubec, S., *On the Vandiver's conjecture*, Abh. Math. Sem. Univ. Hamburg **64** (1994), 105-124.

[9] Lazarus, A. J., *Gaussian periods and units in certain cyclic fields*, Proceedings of AMS **115**, 961 - 968.

[10] Lecxacheux, O., *Unites d'une famille de corps cycliques reeles de degre 6 lies a la coube modulaire* $X_1(13)$, J. Number Theory **31** (1989), 54-63.

[11] Lehmer, E., *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535-541.

[12] Metsankyla, T., *A class number congruence for cyclotomic fields and their subfields*, Acta Arith. **23** (1973), 107-116.

[13] Moser, C., *Nombre de classes d'une extension cyclique reelle de* **Q***, de degre 4 ou 6 et de conducteur premier*, Math. Nachr. **102** (1981), 45-52.

[14] Moser, C., Payan, J. J., *Majoration du nombre de classes d'un corps cubique cyclique de conducteur premier*, J.Math. Soc. Japan **33** (1981), 701-706.

[15] Schoof, R., Washington, L. C., *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543-556.

[16] Shanks, D., *The simplest cubic fields*, Math. Comp. **28** (1974), 1137-1152.

[17] Shen, Y. Y., *Unit groups and class numbers of real cyclic fields*, TAMS **326** (1991), 179-209.

[18] Washington, L. C., *Introduction to Cyclotomic Fields*, Springer-Verlag 83.

Stanislav Jakubec
Matematický ústav SAV
Štefánikova 49
814 73 Bratislava, SLOVAK REPUBLIC