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

ON DIVISIBILITY OF THE CLASS NUMBER OF REAL OCTIC FIELDS OF A PRIME CONDUCTOR $\mathbf{p = n^4 + 16}$ BY $\mathbf{p}$

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

In the papers [3], [4], [5], [6], [11], [16], fields K of a prime conductor p of the degree $[K : \mathbf{Q}] = 2, 3, 4, 5, 6$, such that translations of Gaussian periods are units, and in the case $[K : \mathbf{Q}] = 8$ the field K has units $\beta_i + \beta_{i+2} - \frac{n^2-1}{4}$, were investigated. In paper [9], these results were generalized also to a non-prime conductor.

In the papers [2], [10], [15], [16], [17], these results are applied on investigation of various questions connected with the class number and group units of the field K. For example, R. Schoof and L.C. Washington in [15] proved that in the case $[K : \mathbf{Q}] = 5$ the roots of the polynomial given in [11] generate the group of units of the field K.

One can show [13],[14] that the primes dividing the class numbers of the subfields of $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ of degrees 2,3,4 or 6 are less than p. This implies that the subfields of $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ of degree 2,3,4 or 6, will never give rise to counterexamples of Vandiver's conjecture.

For this reason, the cases $[K : \mathbf{Q}] = 5; 8$ are interesting. As concerns the case $[K : \mathbf{Q}] = 5$, the necessary and sufficient condition for divisibility of the class number h_K for $p = n^4 + 4n^3 + 15n^2 + 25n + 25$ is given in [8].

This condition is the following:

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 $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$ and let $p=n^4+5n^3+15n^2+25n+25$. Let $p>N_0$ be prime. Then p divides h_K if and only if p divides B_j for some $j=\frac{p-1}{5},\ 2\frac{p-1}{5},\ 3\frac{p-1}{5},\ 4\frac{p-1}{5}$.*

Note that N_0 is an absolute constant. Its calculation is posible on the basis of the proof of Lemma 6 of [8].

The aim of this paper is to prove an analogical Theorem for the case $[K:\mathbf{Q}]=8$.

* * *

We start from the paper by E. Lehmer [11] where it is proved that the following polynomials

$$F_n(X)=X^8+2n^2X^7+(p-28)X^6-(p+14n^2)X^5-(p(n^2+3)-70)X^4+$$

$$+(14n^2-p(n^2-4))X^3+(5p-28)X^2+(p-2n^2)X+1, \tag{1}$$

$$\text{where } p=n^4+16,$$

have the roots

$$\Theta_i=\beta_i+\beta_{i+2}-\frac{n^2-1}{4}.$$

Further, the results of [7],[8] are used.

Let $p, p\equiv 1 \pmod n$ be prime and let K be a subfield of the field $\mathbf{Q}(\zeta_p)$ of the degree of n over $\mathbf{Q}$. Let a be a primitive root modulo p.We consider the automorphism σ of the field $\mathbf{Q}(\zeta_p)$ such that $\sigma(\zeta_p)=\zeta_p^a$.

Later we denote:

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

The numbers $\beta_0,\beta_1,\dots,\beta_{n-1}$ are called Gaussian periods and as it is known they are the integral normal basis of $K/\mathbf{Q}$.

In [7], the following Theorem is proved.

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

(i) $N_{K/\mathbf{Q}}(\pi)=(-1)^n p$,

(ii) $\sigma(\pi)\equiv g\pi \pmod{\pi^{n+1}}$,

(iii) $\beta_0\equiv k\sum\limits_{i=0}^{n}\frac{1}{(ki)!}\pi^i \pmod{\pi^{n+1}}$.

□

From the paper [8] we take denotations and Theorem 2.

Let $\mathbf{Q}[X]$ be a ring of polynomials. Let $\mathbf{Q}^*[X]$ be a multiplicative semigroup of the polynomials $f(X)$ where $a_0\neq 0$.

Let $f(X)$ have roots $\lambda_1,\lambda_2,\dots,\lambda_r$.

Denote
$$s_j(f(X)) = \frac{1}{\lambda_1^j} + \frac{1}{\lambda_2^j} + \cdots + \frac{1}{\lambda_r^j}.$$
Let U_K be the group of units of the field K. Let $\varepsilon \in U_K$
$$\varepsilon \equiv a_0 + a_1\pi + \cdots + a_n\pi^n \pmod{\pi^{n+1}}.$$
Then $a_0 \not\equiv 0 \pmod p$, which follows from the fact that ε is a unit and hence $\varepsilon \not\equiv 0 \pmod \pi$.

Consider the polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Define
$$s_j(\varepsilon) = s_j(f(X)).$$
Define the numbers $ii_K(p)$ and $i(\varepsilon)$ as follows.
$$ii_K(p) = \#\{j, j = 1, 2, \ldots, n-1, B_{kj} \equiv 0 \pmod p\},$$
$$i(\varepsilon) = \#\{j, j = 1, 2, \ldots, n-1, s_j(\varepsilon) \equiv 0 \pmod p\}.$$
In [8], the following Theorem is proved.

Theorem 2. *Let $K \subset \mathbf{Q}(\zeta_p + \zeta_p^{-1}), [K : \mathbf{Q}] = n$, $k = \frac{p-1}{n}$ and let h_K be the class number of K.*

Then there holds

(i) *If there exist a unit ε and a number j such that $B_{kj} \equiv 0 \pmod p$ and $s_j(\varepsilon) \not\equiv 0 \pmod p$, then p divides h_K.*

(ii) *Let ε be a unit. Then*
$$p^{ii_K(p)-i(\varepsilon)} | h_K.$$

* * *

Now we shall prove the main Theorem of this paper.

Lemma 1. *Let K be an octic subfield of the field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ and let $p = n^4 + 16$ be prime. If $B_j \equiv 0 \pmod p$ for some $j = \frac{p-1}{8}, 3\frac{p-1}{8}, 5\frac{p-1}{8}, 7\frac{p-1}{8}$, then p divides h_K.*

Proof. Put
$$\varepsilon = \beta_0 + \beta_2 - \frac{n^2-1}{4}.$$
Let $k = \frac{p-1}{8}$; $g = a^{\frac{p-1}{8}} \pmod p$.

By the Theorem 1 we have:
$$\varepsilon = \frac{p-n^2}{4} + \frac{k(1+g^2)}{k!}\pi + \frac{k(1-g^2)}{(3k)!}\pi^3 + \frac{2k}{(4k)!}\pi^4 + \frac{k(1+g^2)}{(5k)!}\pi^5 + \frac{k(1-g^2)}{(7k)!}\pi^7 - 2k\pi^8.$$
By the Theorem 2, it is enough to prove that $s_j(\varepsilon) \not\equiv 0 \pmod p$ for $j = 1, 3, 5, 7$.

Denote

$$g(X) = X^8 + \frac{1+g^2}{2n^2k!}X^7 + 0X^6 + \frac{(1-g^2)}{2n^2(3k)!}X^5 + \frac{1}{An^2}X^4$$
$$+ \frac{1+g^2}{2n^2(5k)!}X^3 + 0X^2 + \frac{1-g^2}{2n^2(7k)!}X - \frac{1}{n^2}\,,$$

where $A = \left(\frac{p-1}{2}\right)!$, hence $A^2 \equiv -1 \pmod p$.

Let

$$S_i = \text{ sum of i-th powers of roots of polynomial } g(X).$$

Clearly $S_i = s_i(\varepsilon)$. Hence it is enough to prove that $S_i \not\equiv 0 \pmod p$ for $i = 1, 3, 5, 7$. Clearly $S_1 = -\frac{1+g^2}{2n^2(k)!} \not\equiv 0 \pmod p$.

We shall prove that

$$S_3S_5S_7 \not\equiv 0 \pmod p.$$

Denote

$$x_1 = k!;\ x_2 = \frac{(2k)!}{(k)!};\ x_3 = \frac{(3k)!}{(2k)!};\ x_4 = \frac{(4k)!}{(3k)!}.$$

Then

$$\begin{aligned}
\varepsilon &= \frac{p-n^2}{4} + \frac{k(1+g^2)}{k!}\pi + \frac{k(1-g^2)}{(3k)!}\pi^3 + \frac{2k}{(4k)!}\pi^4 \\
&\quad + \frac{k(1+g^2)}{(5k)!}\pi^5 + \frac{k(1-g^2)}{(7k)!}\pi^7 - 2k\pi^8 \\
&= \frac{p-n^2}{4} + \frac{k(1+g^2)}{x_1}\pi + \frac{k(1-g^2)}{x_1x_2x_3}\pi^3 + \frac{2k}{A}\pi^4 \\
&\quad - k(1+g^2)x_1x_2x_3\pi^5 - k(1-g^2)x_1\pi^7 - 2k\pi^8 \\
&= a_0 + a_1\pi + a_3\pi^3 + a_4\pi^4 + a_5\pi^5 + a_7\pi^7 + a_8\pi^8\,.
\end{aligned}$$

The following congruence holds

$$\begin{aligned}
&\mathrm{Tr}_{K/\mathbf{Q}}(a_0 + a_1\pi + a_3\pi^3 + a_4\pi^4 + a_5\pi^5 + a_7\pi^7 + a_8\pi^8)^3 \\
&\quad \equiv 8a_0^3 + 8F(a_0, a_1, a_3, a_4, a_5, a_7, a_8)\pi^8 \\
&\quad \equiv 8a_0^3 - 8pF(a_0, a_1, a_3, a_4, a_5, a_7, a_8) \pmod{\pi^9}\,,
\end{aligned}$$

where $F(a_0, a_1, a_3, a_4, a_5, a_7, a_8)$ is a polynomial in $a_0, a_1, a_3, a_4, a_5, a_7, a_8$, obtained as a coefficient by π^8 in the

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

Denote by $S_3(n)$ the sum of 3-th powers of roots of polynomial (1).

The following congruence holds

$$8a_0^3 - 8pF(a_0, a_1, a_3, a_4, a_5, a_7, a_8) \equiv S_3(n) \pmod{\pi^9},$$

and hence

$$8F(a_0, a_1, a_3, a_4, a_5, a_7, a_8) \equiv \frac{8a_0^3 - S_3(n)}{p} \pmod{p}.$$

After all necessary calculations we get the congruence

$$\frac{1}{x_1^2 x_2 x_3} \equiv -2n^2 + 8 \pmod{p}.$$

Analogously we calculate

$$\mathrm{Tr}_{K/\mathbf{Q}}(a_0 + a_1\pi + a_3\pi^3 + a_4\pi^4 + a_5\pi^5 + a_7\pi^7 + a_8\pi^8)^4.$$

Then we obtain the following congruence

$$\frac{1}{x_1^4 x_2^2 x_3^2} + \frac{2x_2x_3}{x_1^2} + \frac{24n^2}{x_1^2 x_2 x_3 A} \equiv 256n^2 + 640 \pmod{p}.$$

Analogously we calculate

$$\mathrm{Tr}_{K/\mathbf{Q}}(a_0 + a_1\pi + a_3\pi^3 + a_4\pi^4 + a_5\pi^5 + a_7\pi^7 + a_8\pi^8)^5.$$

Then we obtain the following congruence

$$\frac{1}{x_1^4} - \frac{6n^2}{x_1^4 x_2^2 x_3^2} + \frac{384}{x_1^2 x_2 x_3 A} + \frac{4n^2 x_2 x_3}{x_1^2} \equiv 512(8 - n^2) \pmod{p}.$$

From it follows that

(2) $$\frac{1}{x_1^4} \equiv -1024A \pmod{p},$$

(3) $$\frac{1}{x_1^2 x_2 x_3} \equiv A(-2n^2 + 8) \pmod{p},$$

(4) $$\frac{6n^2}{x_1^4 x_2^2 x_3^2} \equiv -(-2n^2 + 8)^2 \equiv 32n^2 \pmod{p}.$$

Obviously

$$g(X)=X^8+\frac{1+g^2}{2n^2x_1}X^7+0X^6+\frac{(1-g^2)}{2n^2x_1x_2x_3}X^5+\frac{1}{An^2}X^4+$$
$$+\frac{(1+g^2)x_1x_2x_3}{2n^2}X^3+0X^2+\frac{(1-g^2)x_1}{2n^2}X-\frac{1}{n^2}.$$

(i) $S_3\equiv 0 \pmod p$

$$S_3=-\frac{(1+g^2)^3}{8n^6x_1^3}-3\frac{1-g^2}{2n^2x_1x_2x_3}\equiv 0 \pmod p.$$

Clearly
$n^4\equiv -16 \pmod p$, $(1+g^2)^4\equiv -4 \pmod p$, $(1-g^2)(1+g^2)\equiv 2 \pmod p$.
Hence

$$\frac{1}{32x_1^4}+\frac{3}{x_1^2x_2x_3}\equiv 0 \pmod p.$$

Using (2),(3) we have

$$\frac{1}{32}(-1024)A+3A(-2n^2+8)\equiv 0 \pmod p.$$

Hence $3n^2+4\equiv 0 \pmod p$. But it is not possible, because $p=n^4+16$.

Using formulas for calculation of the sum of 5th and 7th powers of roots of the polynomial $g(X)$ we have $S_5\not\equiv 0 \pmod p$ and $S_7\not\equiv 0 \pmod p$.

Lemma 1 is proved. □

Lemma 2. *Let $p=n^2+16, n\equiv 1 \pmod 4$. Then $B_{\frac{p-1}{4}}B_{3\frac{p-1}{4}}\not\equiv 0 \pmod p$.*

Proof. According to [11], the polynomial

$$X^4+nX^3-6X^2-nX+1,$$

has a root the translation of Gaussian period

$$\beta_0-\frac{n-1}{4},\text{ where } [\mathbf{Q}(\beta_0):\mathbf{Q}]=4.$$

Analogically as in the proof of Lemma 1 we have

$$\beta_0-\frac{p-1}{4}\equiv\frac{p-n}{4}+\frac{k}{x_1}\pi+\frac{k}{A}\pi^2-kx_1\pi^3-k\pi^4 \pmod{\pi^5},$$

$$\text{where } k=\frac{p-1}{4};\ x_1=k!;\ A=\left(\frac{p-1}{2}\right)!.$$

Let

$$g(X)=X^4+\frac{1}{x_1}X^3+\frac{1}{nA}X^2-\frac{x_1}{n}X-\frac{1}{n}.$$

Analogically as in the proof of Lemma 1 the following congruence can be proved

$$\frac{1}{x_1^2} \equiv -2nA \pmod p.$$

On the basis of this congruence it is easy to prove that

$$S_1 \not\equiv 0 \pmod p; \; S_2 \equiv 0 \pmod p; \; S_3 \not\equiv 0 \pmod p.$$

If there were $B_{\frac{p-1}{4}} \equiv 0 \pmod p$ or $B_{3\frac{p-1}{4}} \equiv 0 \pmod p$, then according to Theorem 2 p divides h_K, $[K : \mathbf{Q}] = 4$. But according to [13] p does not divide h_K, hence $B_{\frac{p-1}{4}} B_{3\frac{p-1}{4}} \not\equiv 0 \pmod p$. □

Let K be a subfield of the field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$, $[K : \mathbf{Q}] = n$. Define the numbers E_j as in ([18] p.155).

Lemma 3. *The prime number p divides h_K if and only if $E_{i\frac{p-1}{n}}$ $=p-th$ power for some $i = 1, 2, \dots n-1$. If $E_{i\frac{p-1}{n}}$ $=p-th$ power, then $B_{i\frac{p-1}{n}} \equiv 0 \pmod p$.*

Proof. Let

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^{-1}(a)\sigma_a \in \mathbf{Z}_p[G] \quad ,\text{(see [18]. p.153)}.$$

Then it holds if $i \not\equiv 0 \pmod{\frac{p-1}{n}}$ then $\varepsilon_i U_K / U_K^{p^n} = 0$ hence

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

The rest of the proof is analogous to the proof in [18]. □

Now we prove that if $B_{\frac{p-1}{8}} B_{3\frac{p-1}{8}} B_{5\frac{p-1}{8}} B_{7\frac{p-1}{8}} \not\equiv 0 \pmod p$ then p does not divide h_K. If $B_{\frac{p-1}{2}} \not\equiv 0 \pmod p$, then clearly p does not divide h_K. Suppose that $B_{\frac{p-1}{2}} \equiv 0 \pmod p$ and p divides h_K. Because $B_{\frac{p-1}{8}} B_{3\frac{p-1}{8}} B_{5\frac{p-1}{8}} B_{7\frac{p-1}{8}} \not\equiv 0 \pmod p$ and $B_{\frac{p-1}{4}} B_{3\frac{p-1}{4}} \not\equiv 0 \pmod p$ (by Lemma 2), we obtain that $E_{i\frac{p-1}{2}} = p$-th power. It is easily to see that $E_{i\frac{p-1}{2}} \in \mathbf{Q}(\sqrt{p})$ and hence by Lemma 3 (for $n = 2$) we have that p divides the class number of qudratic field $\mathbf{Q}(\sqrt{p})$ which is not possible, because $h(\mathbf{Q}(\sqrt{p})) < p$.

By this the following theorem is proved.

Theorem 3. *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 $j = \frac{p-1}{8}$, $3\frac{p-1}{8}$, $5\frac{p-1}{8}$, $7\frac{p-1}{8}$.*

Calculating according to [1], we get that:

1) There does not exist an irregular prime $p < 1000000$ such that

$$B_{j\frac{p-1}{8}} \equiv 0 \pmod p \text{ for some } j = 1, 3, 4, 5, 7.$$

2) There exists only one irregular prime $p < 1000000$ such that

$$B_{j\frac{p-1}{5}} \equiv 0 \pmod p \text{ for some } j = 1, 2, 3, 4,$$

$p = 130811$ and $B_{52324} \equiv 0 \pmod{130811}$. It is easy to see that

$$130811 \neq n^4 + 5n^3 + 15n^2 + 25n + 25.$$

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 $\mathbf{Q}$, 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