Stanislav Jakubec

Computational proof of some theorems on class numbers

Mathematica Slovaca, Vol. 54 (2004), No. 5, 527--533

Persistent URL: http://dml.cz/dmlcz/136913

Math. Slovaca, **54** (2004), No. 5, 527–533

Mathematica Slovaca

COMPUTATIONAL PROOF OF SOME THEOREMS ON CLASS NUMBERS

STANISLAV JAKUBEC

(*Communicated by Sylvia Pulmannová*)

ABSTRACT. In this paper, an explicit form is given for a prime q such that $(h_q^+, p) = 1$.

Introduction

NOTATION.

B_{2i}	Bernoulli number,
$Q_2 = \frac{2^{p-1}-1}{p}$	Fermat quotient,
$\operatorname{rec}(f(X))$	the reciprocal polynomial to the polynomial $f(X)$,
$\operatorname{coeff}(f, X, i)$	the coefficient at X^i,
$\operatorname{resultant}(f, g, x_i)$	the resultant of the polynomials f, g according to the variable x_i.

In this paper we consider the divisibility of the class number h_q^+ of real cyclotomic fields $\mathbf{Q}(\zeta_q + \zeta_q^{-1})$ for primes q such that $q \equiv -1 \pmod{p}$ and $\frac{q-1}{2}$, $\frac{q-3}{4}$ are primes. Let p be a prime which does not satisfy the Wieferich congruence $2^{p-1} \equiv 1 \pmod{p^2}$. We shall show an explicit form for prime q such that $(h_q^+, p) = 1$. The following two theorems will be proved:

THEOREM 1. *Let $d_1, d_2, \dots, d_{\frac{p-9}{2}}$ be odd numbers such that $d_i \not\equiv \pm 1 \pmod{p}$ and $d_i \not\equiv \pm d_j \pmod{p}$. Let $q \equiv -1 \pmod{p}$ and $d_i \mid q+1$ for $i = 1, 2, \dots, d_{\frac{p-9}{2}}$. Then $(h_q^+, p) = 1$ for all p except a finite number.*

Note. All primes p which are exceptions can be determined. There holds

$$\prod p \approx 10^{4000}.$$

2000 Mathematics Subject Classification: Primary 11R29.
Keywords: class number.

THEOREM 2. *Let* $r \equiv 1 \pmod 2$ *be a primitive root modulo* p. *Then the following holds:*

(i) *If* $q = 2kpr^{\frac{p-13}{2}} - 1$, *then* $(h_q^+, p) = 1$ *for all* $p > 127$.

(ii) *If* $q = 2kp \cdot 3^{\frac{p-33}{2}} - 1$ *and* 3 *is a primitive root modulo* p, *then* $(h_q^+, p) = 1$ *for all* p *except for a finite number.*

The proofs of these theorems are based on the following Proposition.

PROPOSITION. *Let*

$$F(X) = Q_2 + \sum_{i=1}^{\frac{p-3}{2}} \frac{(2^{2i}-1)(2^{2i+1}-1)}{2i \cdot 2^{2i}} B_{2i} B_{p-1-2i} X^{2i}.$$

Let the polynomial $F(X)$ *have* $2n$ *different roots in* $\mathbf{Z}/p\mathbf{Z}$. *Let* $q \equiv -1 \pmod p$ *and* $q+1$ *have* n *odd divisors* $d_1, d_2, \dots, d_n$, $d_i \not\equiv \pm 1 \pmod p$, $d_i \not\equiv \pm d_j \pmod p$. *Then there holds* $(h_q^+, p) = 1$.

P r o o f. On the basis of results of [1] and [2] we get that if (h_q^+, p) were equal to p, then there would exist a root $y \in \mathbf{Z}$ of the polynomial $F(X)$ modulo p such that

$$y,\ d_1 y,\ d_2 y,\ \dots,\ d_n y$$

would be roots of $F(X) \bmod p$. Hence $F(X)$ would have $2(n+1)$ roots modulo p

$$\pm y,\ \pm d_1 y,\ \dots,\ \pm d_n y,$$

which is a contradiction. □

Proofs

The proofs of Theorem 1 and Theorem 2 are based on the following procedure for estimation of the number of roots of the polynomial $F(X)$ in $\mathbf{Z}/p\mathbf{Z}$. Suppose that $F(X)$ has $p-3-2m$ different roots modulo p. Consider the polynomial $G(X) = \operatorname{rec}\left(\frac{F(X)}{Q_2}\right)$. The number of roots of $G(X)$ is greater or equal to the number of roots of $F(X)$. To show that $G(X)$ has at most $p-3-2m$ roots modulo p it is enough to prove that the following congruence does not hold:

$$\frac{X^{p-1}-1}{X^{2m}+A_1X^{2m-2}+\dots+A_m}\left(X^{2m-2}+a_1X^{2m-4}+\dots+a_{m-1}\right) \equiv G(X) \pmod p, \tag{1}$$

It is easy to see that if (1) were true, then there would also hold

$$\frac{\operatorname{rec}(X^{p-1}-1)}{\operatorname{rec}(X^{2m}+A_1X^{2m-2}+\cdots+A_m)}\operatorname{rec}(X^{2m-2}+a_1X^{2m-4}+\cdots+a_{m-1}) \equiv \operatorname{rec}(G(X)) \pmod p\,. \tag{2}$$

Consider the congruence (1) modulo X^{4m+2} since $4m+2\le p-1$, hence

$$\frac{-1}{X^{2m}+A_1X^{2m-2}+\cdots+A_m}(X^{2m-2}+a_1X^{2m-4}+\cdots+a_{m-1}) \equiv G(X) \pmod{X^{4m+2}}\,.$$

By the decomposition of the function

$$\frac{1}{X^{2m}+A_1X^{2m-2}+\cdots+A_m}$$

into Taylor series, the inverse element to $X^{2m}+A_1X^{2m-2}+\cdots+A_m$ modulo X^{4m+2} will be determined.

Denote

$$l(X)\equiv\frac{1}{X^{2m}+A_1X^{2m-2}+\cdots+A_m}(X^{2m-2}+a_1X^{2m-4}+\cdots+a_{m-1}) \pmod{X^{4m+2}}\,.$$

Now $l(X)$ is a polynomial in X the coefficients of which are rational functions in

$$A_1, A_2, \ldots, A_m, a_1, a_2, \ldots a_{m-1}\,.$$

The following congruences hold

$$-\operatorname{coeff}(l(X),X,0)\equiv\frac{(2^{p-3}-1)(2^{p-2}-1)}{(p-3)2^{p-3}}\frac{B_2B_{p-3}}{Q_2} \pmod p\,,$$

$$-\operatorname{coeff}(l(X),X,2)\equiv\frac{(2^{p-5}-1)(2^{p-4}-1)}{(p-5)2^{p-5}}\frac{B_4B_{p-5}}{Q_2} \pmod p\,,$$

$$\vdots$$

$$-\operatorname{coeff}(l(X),X,4m)\equiv\frac{(2^{p-3-4m}-1)(2^{p-2-4m}-1)}{(p-3-4m)2^{p-3-4m}}\frac{B_{4m+2}B_{p-3-4m}}{Q_2} \pmod p\,.$$

We shall apply an analogous procedure on the congruence (2). Denote

$$L(X)\equiv\frac{1}{1+A_1X^2+\cdots+A_mX^{2m}}(1+a_1X^2+\cdots+a_{m-1}X^{2m-2}) \;(\text{pmod } X^{4m+2})\,.$$

Now $L(X)$ is a polynomial in X the coefficients of which are polynomials in

$$A_1, A_2, \dots, A_m, a_1, a_2, \dots, a_{m-1}.$$

The following congruences hold

$$\begin{aligned}
\operatorname{coeff}\bigl(L(X), X, 0\bigr) &\equiv 1 \pmod p\,,\\
\operatorname{coeff}\bigl(L(X), X, 2\bigr) &\equiv \frac{(2^2-1)(2^3-1)}{2.2^2}\frac{B_2B_{p-3}}{Q_2} \pmod p\,,\\
\operatorname{coeff}\bigl(L(X), X, 4\bigr) &\equiv \frac{(2^4-1)(2^5-1)}{4.2^4}\frac{B_4B_{p-5}}{Q_2} \pmod p\,,\\
&\vdots\\
\operatorname{coeff}\bigl(L(X), X, 4m\bigr) &\equiv \frac{(2^{4m}-1)(2^{4m+1}-1)}{4m\cdot 2^{4m}}\frac{B_{4m}B_{p-1-4m}}{Q_2} \pmod p\,.
\end{aligned}$$

Denote

$$\begin{aligned}
ll(i) &= \operatorname{coeff}\bigl(l(X), X, 2i-2\bigr)\,,\\
LL(i) &= \operatorname{coeff}\bigl(L(X), X, 2i\bigr) \qquad \text{for} \quad i = 1, 2, \dots, 2m\,.
\end{aligned}$$

Let

$$\begin{aligned}
H(i) &= H_i(A_1, A_2, \dots, A_m, a_1, a_2, \dots, a_{m-1})\\
&= A_m^i\left(LL(i) - \frac{2i+1}{2i}\frac{2^{2i+1}-1}{2^{2i}-2}ll(i)\right).
\end{aligned}$$

If the congruence (1) were true, then there would hold

$$H(i) = H_i(A_1, A_2, \dots, A_m, a_1, a_2, \dots, a_{m-1}) = 0 \qquad \text{for} \quad i = 1, 2, \dots, 2m\,.$$

For a concrete m we construct this system by the program Maple V.

Then we construct resultants

$$R(i) = \operatorname{resultant}\bigl(H(i), H(1), a_1\bigr) \qquad \text{for} \quad i = 2, 3, \dots, 2m\,.$$

Further we construct the resultants of the resultants by a_2, etc.. Finally we construct the resultant R by the variable A_m, $A_m \neq 0$. Suppose that $R \neq 0$.

Conclusion: If the prime number p does not divide R, then the system $H(i) \equiv 0 \pmod p$ does not have a solution, therefore the polynomial $F(X)$ has at most $p-3-2m$ different roots modulo p.

Proof of Theorem 1. We shall prove that the polynomial $F(X)$ has at most $p-9$ roots modulo p, $m = 3$.

$$\begin{aligned}
R(i) &= \operatorname{resultant}\bigl(H(i), H(1), a_1\bigr) \qquad \text{for} \quad i = 2, 3, \dots, 6\,.\\
RR(i,j) &= \operatorname{resultant}\bigl(R(i), R(j), a_2\bigr)\,.
\end{aligned}$$

Denote

$$W(1) = \text{resultant}\big(RR(2,5), RR(2,3), A_1\big)\,,$$
$$W(2) = \text{resultant}\big(RR(3,4), RR(2,3), A_1\big)\,,$$
$$W(3) = \text{resultant}\big(RR(2,4), RR(2,3), A_1\big)\,,$$
$$W(4) = \text{resultant}\big(RR(4,6), RR(2,3), A_1\big)\,.$$
$$T(1) = \text{resultant}\big(W(1), W(2), A_2\big)\,,$$
$$T(2) = \text{resultant}\big(W(3), W(4), A_2\big)\,.$$

Then there holds

$$\gcd\big(T(1), T(2)\big) = K A_3^{531}\,.$$

It follows that for all primes except for a finite number, the polynomial $F(X)$ has at most $p-9$ different roots. Let

$$R = \text{resultant}\left(\frac{T(1)}{A_3^{531}}, \frac{T(2)}{A_3^{531}}\right) \neq 0\,.$$

All primes for which Theorem 1 does not hold are divisors of R. Also other non-zero resultants were found; their gcd (greatest common divisor) being approximately 10^{4000} and this number failed to be decomposed into primes. The program Maple V has not managed the computation of the resultants for $m = 4$.

□

Proof of Theorem 2. Let $q+1$ be divisible by $r^{\frac{p-3}{2}-m}$. If $\big(h_q^+, p\big) = p$, then there exists a root of a polynomial $F(X)$ modulo p, denoted by $\frac{1}{y}$, such that

$$\frac{1}{y}, \frac{1}{y}r, \frac{1}{y}r^2, \dots, \frac{1}{y}r^{\frac{p-3}{2}-m}$$

are roots of $F(X)$. Hence $\text{rec}\Big(\frac{F(X)}{Q_2}\Big)$ has roots

$$y, yr^{-1}, yr^{-2}, \dots, yr^{-\frac{p-3}{2}-m}\,.$$

It follows that we can apply the above described procedure, where

$$X^{2m} + A_1 X^{2m-2} + \dots + A_m = \prod_{i=1}^{m}\big(X^2 - r^{2i}y^2\big)\,.$$

Let $R(i) = \text{resultant}\big(H(i), H(1), a_1\big)$ for $i = 2, 3, \dots, 2m$.

Now we shall construct resultants $K(i)$, $KK(i)$, $KKK(i)$ by the following commands (in Maple V code):

```
K(i) := R(i), KK(i) := R(i), KKK(i) := R(i) for i = 2,3,...,2m.
for j from 2 by 1 to m-1 do
  for i from j+1 by 1 to m+1 do K(i) := resultant(K(i),K(j),a_j) od:od:
for j from 2 by 1 to m-1 do
  for i from j+2 by 1 to m+2 do KK(i) := resultant(KK(i),KK(j+1),a_j) od;od:
for j from 2 by 1 to m-1 do
  for i from j+3 by 1 to m+3 do KKK(i) := resultant(KKK(i),KK(j+2),a_j) od;od:
```

Finally we get three integral polynomials $K(m)$, $KK(m+1)$, $KKK(m+2)$ in y. In all cases we have computed that there holds

$$\gcd\big(K(m), KK(m+1)\big) = K_1 y^{n_1}, \qquad \gcd\big(K(m), KKK(m+2)\big) = K_2 y^{n_2},$$
$$\gcd\big(KK(m+1), KKK(m+2)\big) = K_3 y^{n_3},$$

where $n_1, n_2, n_3, K_1, K_2, K_3$ are natural numbers.

Therefore the polynomial $F(X)$ has at most $p-3-2m$ roots modulo p for all p except for a finite number.

Now put

$$A = \text{resultant}\left(\frac{K(m)}{y^{n_1}}, \frac{KK(m+1)}{y^{n_1}}, y\right) \neq 0,$$
$$B = \text{resultant}\left(\frac{K(m)}{y^{n_2}}, \frac{KKK(m+2)}{y^{n_2}}, y\right) \neq 0.$$

The primes for which the limitation imposed on the number of roots does not hold are divisors of the number

$$C = \gcd(A, B).$$

Now C is a polynomial in r the irreducible factors of which are the following $r^2 \pm r+1$, r^4+1, r^8+1, r^4-r^2+1, $r^4 \pm r^3+r^2 \pm r+1$, $r^6 \pm r^3+1$, $r^8-r^6+r^4-r^2+1$. It is clear that if p divides some from these polynomials (in the value r), then r is not primitive root modulo p. □

The strongest possible generalization of Theorem 2 which can be proved using this method with respect to the inequality $4m+2 \le p-1$ is the following:

THEOREM. *Let $r \equiv 1 \pmod 2$ be a primitive root modulo p. Then the following holds:*

If $q = 2kpr^{[\frac{p}{4}]} - 1$, then $(h_q^+, p) = 1$ for all p except for a finite number.

Finally, we mention the system

$$H(i) = H_i\big(A_1, A_2, \dots, A_m, a_1, a_2, \dots, a_{m-1}\big) = 0, \qquad \text{for} \quad i = 1, 2, \dots, 2m,$$

for $m = 3$ from Theorem 1 and $m = 3$ from Theorem 2.

REFERENCES

[1] JAKUBEC, S.: *On divisibility of the class number* h^+ *of the real cyclotomic fields of prime degree* l, Math. Comp. **67** (1998), 369–398.
[2] JAKUBEC, S.: *Connection between Schinzel's conjecture and divisibility of class number* h_p^+, Acta Arith. **94** (2000), 161–171.

Received February 26, 2004

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
SLOVAKIA

Žilinská univerzita v Žiline
Fakulta prírodných vied
Hurbanova 15
SK-010 26 Žilina
SLOVAKIA

E-mail: jakubec@mat.savba.sk