Conspectus materiae tomi XXIII, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplare jeder Arbeit
Рукописи статьей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXIII (1973)

A class number congruence for cyclotomic fields and their subfields

by

Tauno Metsänkylä (Turku)

1. Introduction. Consider the cyclotomic field $F = Q(\zeta)$ generated by $\zeta = \exp(2\pi i/p)$, where $p = 2m+1$ is a prime > 3. As usual, write the class number of F in the form $H = H_1 H_2$, where H_1 is an integer and H_2 denotes the class number of the maximal real subfield F_0 of F. Carlitz [5] recently derived a congruence

$$(1)\qquad H_1 \equiv H_2 G \pmod{p} \qquad (G \text{ an integer}),$$

thus giving, among other things, a new proof for the known fact (Kummer's theorem) that $H_2 \equiv 0 \pmod{p}$ implies $H_1 \equiv 0 \pmod{p}$. It is remarkable that Carlitz's proof uses, apart from the explicit expression of H, only a few elementary results from the theory of cyclotomic fields.

Borevich and Shafarevich proved Kummer's theorem in [3] by a new p-adic method, due to D. C. Faddeev. In this paper we shall show that this p-adic method easily gives a congruence for H_2, from which we can deduce a congruence of the form (1) (see Theorem 1 and its Corollary). Furthermore, we shall prove that our congruence implies that of Carlitz, and vice versa.

We shall also generalize Theorem 1 to the subfields of F. This generalization yields, as a special case, the well-known congruence connecting the class number and fundamental unit of a real quadratic field (see Section 6).

2. Preliminaries. Recall that the prime factorization of p in F is $p = \mathfrak{p}^{p-1}$, where $\mathfrak{p} = (1-\zeta)$. Let $F_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completion of F. Then Q_p, the p-adic completion of Q, can be embedded in $F_\mathfrak{p}$ in a natural way, and $[F_\mathfrak{p}: Q_p] = [F: Q] = p-1$. Moreover, the automorphisms σ_s $(s = 0, \ldots, p-2)$ of the extension F/Q, defined by

$$\sigma_s(\zeta) = \zeta^{r^s} \qquad (r \text{ a primitive root} \bmod p),$$

can be extended to $F_\mathfrak{p}/Q_p$ in a natural way. (For the proof of these and the following results in this Section, see [3], Chapter 5, Section 6.)

Let us denote by Z the ring of rational integers and by Z_p and $Y_\mathfrak{p}$ the rings of p-adic and $\mathfrak{p}$-adic integers, respectively. Choose the unique prime element λ of $Y_\mathfrak{p}$ satisfying the conditions

$$\lambda^{p-1}+p = 0, \quad \lambda \equiv \zeta-1 \pmod{\lambda^2}$$

and note that the system $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is a fundamental basis of $F_\mathfrak{p}/Q_p$.

Lemma 1. *In $F_\mathfrak{p}$, the maximal subfield whose elements are left fixed by σ_m is the subfield generated by $\{1, \lambda^2, \ldots, \lambda^{p-3}\}$.*

Consider the function $\log\varepsilon$ over the field $F_\mathfrak{p}$. It is defined for all principal units (i.e., for units ε with $\varepsilon \equiv 1 \pmod{\lambda}$) of $Y_\mathfrak{p}$ and satisfies the equation

(2) $$\log(\varepsilon_1\varepsilon_2) = \log\varepsilon_1+\log\varepsilon_2.$$

Lemma 2. *For every unit ε of F_0, ε^{p-1} is a principal unit of $Y_\mathfrak{p}$ and $\log\varepsilon^{p-1}$ can be represented in the form*

$$\log\varepsilon^{p-1} = \sum_{k=1}^{m-1} d_k\lambda^{2k} \quad (d_k \in Z_p).$$

Lemma 3. *Put*

$$L(1+x) = \sum_{n=1}^{p-1}(-1)^{n-1}x^n/n, \quad E(x) = \sum_{n=0}^{p-1}x^n/n!.$$

Then the following congruences hold in the ring $Y_\mathfrak{p}$:

(i) $L(\varepsilon^{p-1}) \equiv \log\varepsilon^{p-1} \pmod{\lambda^p}$ *(ε a unit of F_0),*

(ii) $E(k\lambda) \equiv \zeta^k \pmod{\lambda^p}$ $(k = 1, 2, \ldots)$.

3. Congruences for H_2. The so-called cyclotomic units of F_0 are the units

(3) $$e_i = \sigma_{i-1}(e(\zeta)) \quad (i = 1, \ldots, m-1),$$

where $e(\zeta)$ is the positive unit

$$e(\zeta) = \left\{\frac{1-\zeta^r}{1-\zeta}\cdot\frac{1-\zeta^{-r}}{1-\zeta^{-1}}\right\}^{1/2}.$$

Let $\{\varepsilon_j = \varepsilon_j(\zeta) \mid j = 1, \ldots, m-1\}$ denote a system of positive fundamental units of F_0 and put

(4) $$e_i = \prod_{j=1}^{m-1}\varepsilon_j^{r(i,j)} \quad (i = 1, \ldots, m-1)$$

with $r(i,j) \in Z$. Then it is known that

(5) $$H_2 = |\det(r(i,j))| \quad (i,j = 1, \ldots, m-1).$$

(Cf. [3], pp. 361–362. Our system of cyclotomic units is not the same as the corresponding system in [3] but is more appropriate for generalization.) In what follows we shall assume the sequence of fundamental units to be so chosen that the determinant on the right is positive.

We apply Lemma 2 to the above units. Since every p-adic integer is congruent mod p to some rational integer, we may then write

(6) $$\log e_i^{p-1} \equiv \sum_{k=1}^{m-1} v_{ik}\lambda^{2k} \pmod{\lambda^{p-1}} \quad (i = 1, \ldots, m-1),$$
$$\log \varepsilon_j^{p-1} \equiv \sum_{k=1}^{m-1} w_{jk}\lambda^{2k} \pmod{\lambda^{p-1}} \quad (j = 1, \ldots, m-1)$$

with $v_{ik}, w_{jk} \in Z$. By (4) and (2), this yields

$$\sum_{k=1}^{m-1} v_{ik}\lambda^{2k} \equiv \sum_{k=1}^{m-1}\sum_{j=1}^{m-1} r(i,j)w_{jk}\lambda^{2k} \pmod{\lambda^{p-1}} \quad (i = 1, \ldots, m-1).$$

Hence we have the following "basic" congruence for H_2:

(7) $$\det(v_{ik}) \equiv H_2\det(w_{jk}) \pmod{p} \quad (i, j, k = 1, \ldots, m-1).$$

The computation of the numbers v_{ik} can be accomplished by a procedure completely similar to that in [3], pp. 374–375, by starting from the formulas

$$e_i = \sigma_{i-1}\left(\frac{\zeta^r-1}{\zeta-1}\zeta^{-(r-1)/2}\right) \quad (i = 1, \ldots, m-1).$$

The result is

(8) $$v_{ik} \equiv \frac{B_{2k}(1-r^{2k})r^{2(i-1)k}}{2k(2k)!} \pmod{p} \quad (i, k = 1, \ldots, m-1),$$

where B_{2k} denotes the $2k$-th Bernoulli number in the even suffix notation. Observing that

$$(1-r^2)(1-r^4)\ldots(1-r^{p-3}) \equiv -\tfrac{1}{2} \pmod{p}$$

we therefore get

Theorem 1. *The class number H_2 of F_0 satisfies the congruence*

(9) $$-\tfrac{1}{2}\det(r^{2(i-1)k})\prod_{n=1}^{m-1}\frac{B_{2n}}{2n(2n)!} \equiv H_2\det(w_{jk}) \pmod{p}$$

$(i, j, k = 1, \ldots, m-1)$, *where the w_{jk} are rational integers defined by* (6).

The determinant on the left side of (9), being of Vandermonde type, equals, except for sign, the product of all $r^{2i}-r^{2k}$, where $1 \leqslant i < k \leqslant m-1$. Hence this determinant is not divisible by p.

According to a classical result of Vandiver ([11], see also [10]),

$$H_1 \equiv (-1)^m 2^{1-m} p \prod_{n=1}^{m} B_{(2n-1)p+1} \pmod{p}.$$

Using Kummer's congruence and von Staudt's theorem for Bernoulli numbers ([3]), we may put this relation in the form

$$H_1 \equiv (-1)^{m-1} 2^{1-m} \prod_{n=1}^{m-1} (B_{2n}/2n) \pmod{p}, \tag{10}$$

which combined with (9) gives

COROLLARY. *We have*

$$H_1 \equiv -2^{2-m} H_2 D^{-1} \det\big(-(2k)!\,w_{jk}\big) \pmod{p}, \tag{11}$$

where $D = \det(r^{2(i-1)k})$ $(i, j, k = 1, \ldots, m-1)$.

As mentioned in Introduction, it follows from this congruence that $H_2 \equiv 0 \pmod{p}$ implies $H_1 \equiv 0 \pmod{p}$.

4. Comparison with Carlitz's congruence. Let us suppose that the unit $\varepsilon_j(\zeta)$ is written in the canonical form by means of the basis $\{1, \zeta, \ldots, \zeta^{p-2}\}$ of F, so that $\varepsilon_j(x)$ is a polynomial over Z $(j = 1, \ldots, m-1)$. Write briefly $(\varepsilon_j'/\varepsilon_j)(x)$ for $\varepsilon_j'(x)/\varepsilon_j(x)$, where $\varepsilon_j'(x)$ denotes the derivative of $\varepsilon_j(x)$, and set

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) = \sum_{s=0}^{p-2} c_{js}\sigma_s(\zeta) \qquad (c_{js} \in Z). \tag{12}$$

Carlitz's congruence can now be presented in the form

$$H_1 \equiv -2^{2-m} H_2 D^{-1} \det\Big(\sum_{s=0}^{p-2} c_{js} r^{(2k-1)s}\Big) \pmod{p}$$

$(j, k = 1, \ldots, m-1)$, where D is the determinant defined in the above Corollary. We shall prove the following lemma which indicates that this congruence implies (11), and conversely.

LEMMA 4.

$$-(2k)!\,w_{jk} \equiv \sum_{s=0}^{p-2} c_{js} r^{(2k-1)s} \pmod{p} \qquad (j, k = 1, \ldots, m-1).$$

Proof. Making use of the fact that $\varepsilon_j(\zeta)$ is real, and of Lemma 3(ii), we obtain from (12)

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) \equiv \tfrac{1}{2}\sum_{s=0}^{p-2} c_{js}\big(\sigma_s(\zeta) - \sigma_{m+s}(\zeta)\big) \equiv \tfrac{1}{2}\sum_{s=0}^{p-2} c_{js}\big(E(r^s\lambda) - E(r^{m+s}\lambda)\big)$$
$$\equiv \sum_{k=1}^{m} \big((2k-1)!\big)^{-1} \sum_{s=0}^{p-2} c_{js} r^{(2k-1)s} \lambda^{2k-1} \pmod{\lambda^{p-1}}$$

(here and below j is fixed, $1 \leqslant j \leqslant m-1$). Thus our lemma is proved after we have shown that the definition (6) of w_{jk} implies

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) \equiv -\sum_{k=1}^{m-1} 2k w_{jk} \lambda^{2k-1} \pmod{\lambda^{p-2}}. \tag{13}$$

To verify (13), put

$$\zeta = \sum_{n=0}^{p-2} a_n \lambda^n \qquad (a_n \in Z_p) \tag{14}$$

and denote

$$P(x) = \sum_{n=0}^{p-2} a_n x^n, \qquad R(x) = \varepsilon_j\big(P(x)\big)^{p-1},$$

so that

$$P(\lambda) = \zeta, \qquad R(\lambda) = \varepsilon_j(\zeta)^{p-1}.$$

Obviously, $P(x), R(x) \in Z_p[x]$, and the constant term of $R(x)$ is, by Lemma 2, congruent to $1 \bmod p$. It follows then from the identity

$$(1+x)\frac{d}{dx}L(1+x) = 1 + (-1)^{p-2}x^{p-1}$$

that

$$R(x)\frac{d}{dx}L\big(R(x)\big) = R'(x) + x^{p-1}S(x) + pT(x) \tag{15}$$

with $S(x), T(x) \in Z_p[x]$.

Applying Lemma 3(i) to (6) we may write

$$L\big(\varepsilon_j(\zeta)^{p-1}\big) = \sum_{n=0}^{p-2} b_n \lambda^n \qquad (b_n \in Z_p),$$

where

$$b_{2k} \equiv w_{jk} \pmod{p} \qquad (k = 1, \ldots, m-1)$$

and the other b_n are $\equiv 0 \pmod{p}$. Now, the equation

$$L\big(R(x)\big) = \sum_{n=0}^{p-2} b_n x^n$$

holds for every $\sigma_s(\lambda)$, that is, for $x = \lambda, \lambda\theta, \ldots, \lambda\theta^{p-2}$, where θ is a primitive $(p-1)$-th root of unity. Hence we have the identity

$$L\big(R(x)\big) = \sum_{n=0}^{p-2} b_n x^n + (x^{p-1} + p)F(x)$$

with $F(x) \in Z_p[x]$. After differentiating and setting $x = \lambda$ we get, by (15),

$$(R'/R)(\lambda) \equiv \sum_{k=1}^{m-1} 2kw_{jk}\lambda^{2k-1} \pmod{\lambda^{p-2}}. \tag{16}$$

On the other hand,

$$(R'/R)(\lambda) = (p-1)(\varepsilon_j'/\varepsilon_j)(\zeta)P'(\lambda), \tag{17}$$

where, furthermore,

$$P'(\lambda) = \sum_{n=1}^{p-2} na_n\lambda^{n-1} \equiv \zeta \pmod{\lambda^{p-2}} \tag{18}$$

because $a_n \equiv 1/n! \pmod p$ (see (14) and Lemma 3(ii)). Combining (16), (17), and (18) we obtain the congruence (13).

5. Generalization. We shall generalize Theorem 1 and Lemma 4 to the subfields K of F. It is known (see, e.g., [6], [2]) that the class number of K is of the form $h = h_1h_2$, where h_1 and h_2 are integral factors of H_1 and H_2, respectively, and h_2 is the class number of the maximal real subfield K_0 of K ($h_1 = 1$ if $K = K_0$). In the following we may assume that K is imaginary, since every real subfield of F is contained as a maximal real subfield in some imaginary subfield of F. Let K be of degree $a = 2u$ over Q and put $p-1 = ab$, where b is odd.

The maximal subfield of F being pointwise invariant under the automorphism σ_u is the real field K_0. The following lemma can be proved similarly as Lemma 1.

LEMMA 1A. *In F_p, the maximal subfield whose elements are left fixed by σ_u is the subfield generated by $\{1, \lambda^{2b}, \ldots, \lambda^{2(u-1)b}\}$.*

Using this lemma, one can easily prove

LEMMA 2A. *For every unit ε of K_0, ε^{p-1} is a principal unit of Y_p and $\log\varepsilon^{p-1}$ can be represented in the form*

$$\log\varepsilon^{p-1} = \sum_{k=1}^{u-1} d_k\lambda^{2bk} \quad (d_k \in Z_p).$$

The cyclotomic units of K_0 are the units

$$\eta_i = e_ie_{i+u}\ldots e_{i+(b-1)u} \quad (i = 1, \ldots, u-1),$$

where the e_i are defined by (3) ([6], p. 23). Let $\{\varepsilon_1, \ldots, \varepsilon_{u-1}\}$ denote a system of positive fundamental units of K_0 (this notation may be used without confusion because the fundamental units of F_0 are not needed any more). Writing, by Lemma 2A,

$$\begin{aligned}\log\eta_i^{p-1} &\equiv \sum_{k=1}^{u-1} s_{ik}\lambda^{2bk} \pmod{\lambda^{p-1}} \quad (i = 1, \ldots, u-1),\\ \log\varepsilon_j^{p-1} &\equiv \sum_{k=1}^{u-1} w_{jk}\lambda^{2bk} \pmod{\lambda^{p-1}} \quad (j = 1, \ldots, u-1)\end{aligned} \tag{19}$$

with $s_{ik}, w_{jk} \in Z$, we have then as an analogue of (7) the congruence

$$\det(s_{ik}) \equiv h_2\det(w_{jk}) \pmod p \quad (i, j, k = 1, \ldots, u-1).$$

Indeed, the analogues of (4) and (5) hold in this case, too. (See, e.g., [6]. Note that there is no ambiguity of sign when we assume the sequence of the ε_j to be suitably ordered, or in case $u = 2$, when we assume $\varepsilon_1 > 1$.)

The numbers s_{ik} may be computed by means of (8) as follows:

$$\begin{aligned}\log\eta_i^{p-1} &= \sum_{t=0}^{b-1}\log e_{i+tu}^{p-1} \equiv \sum_{t=0}^{b-1}\sum_{k=1}^{m-1} v_{i+tu,k}\lambda^{2k}\\ &\equiv \sum_{k=1}^{m-1}\sum_{t=0}^{b-1}\frac{B_{2k}(1-r^{2k})}{2k(2k)!}r^{2(i+tu-1)k}\lambda^{2k}\\ &\equiv \sum_{k=1}^{u-1}\frac{B_{2bk}(1-r^{2bk})}{2bk(2bk)!}br^{2(i-1)bk}\lambda^{2bk} \pmod{\lambda^{p-1}}.\end{aligned}$$

Because of

$$(1-r^{2b})(1-r^{4b})\ldots(1-r^{2(u-1)b}) \equiv -1/2b \pmod p$$

we thus arrive at

THEOREM 1A. *The class number h_2 of K_0 satisfies the congruence*

$$-\tfrac{1}{2}b^{-1}\det(r^{2(i-1)bk})\prod_{n=1}^{u-1}\frac{B_{2bn}}{2n(2bn)!} \equiv h_2\det(w_{jk}) \pmod p \tag{20}$$

$(i, j, k = 1, \ldots, u-1)$, where the w_{jk} are rational integers defined by (19).

The following lemma allows one to put (20) in a slightly different form.

LEMMA 4A. *Let the rational integers c_{js} ($j = 1, \ldots, u-1$; $s = 0, \ldots \ldots, p-2$) be determined by the expansions* (12), *written for the fundamental units ε_j of K_0. Then*

$$-(2bk)!\,w_{jk} \equiv \sum_{s=0}^{p-2} c_{js}r^{(2bk-1)s} \pmod p \quad (j, k = 1, \ldots, u-1).$$

Proof. From (12) it can be concluded that

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) \equiv (2b)^{-1}\sum_{s=0}^{p-2}\sum_{t=0}^{2b-1} c_{js} r^{tu}\sigma_{s+tu}(\zeta) \pmod{\lambda^{p-1}}$$

(apply the automorphisms σ_{tu} to the element on the left). The right side of this congruence is, by Lemma 3(ii), congruent mod λ^{p-1} to

$$\sum_{k=1}^{u}\big((2bk-1)!\big)^{-1}\sum_{s=0}^{p-2} c_{js} r^{(2bk-1)s}\lambda^{2bk-1}.$$

On the other hand, it follows from (19) that

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) \equiv -\sum_{k=1}^{u-1} 2bkw_{jk}\lambda^{2bk-1} \pmod{\lambda^{p-2}}.$$

This can be verified similarly as the corresponding congruence (13) in the proof of Lemma 4. Thus Lemma 4A is seen to be true.

Remarks. As in connection with Theorem 1, we find that the determinant on the left side of (20) is not divisible by p. However, Theorem 1A does not imply any result analogous to the Corollary of Theorem 1, since the analogue of (10) is

$$h_1 \equiv (-1)^u 2^{1-u}\prod_{n=1}^{u}\frac{B_{(2n-1)b+1}}{(2n-1)b+1} \pmod{p},$$

provided K is a proper imaginary subfield of F. This congruence has been demonstrated by Carlitz [4].

The author [9] has previously derived some congruences for h_2, by generalizing certain considerations in Carlitz's paper [5]. To see that these congruences agree with the present results one has to observe that the polynomial

$$\psi(x) = p^{-1}\sum_{s=0}^{p-2}(rr_{s-1}-r_s)x^s,$$

where r_s denotes the least positive residue of r^s mod p, is connected with Bernoulli numbers by the congruences

$$2n\psi(r^{2n-1}) \equiv B_{2n}(r^{2n}-1) \pmod{p} \quad (n = 1, \ldots, m-1)$$

(cf. [7], pp. 280–281).

In [9] it is shown that the analogue of Kummer's theorem for proper subfields K of F reads as follows: if $h_2 \equiv 0 \pmod{p}$, then $H_1/h_1 \equiv 0 \pmod{p}$. This could also be proved as an application of Theorem 1A.

6. Application to a real quadratic field. Let $p \equiv 1 \pmod 4$ and choose $a = 4$, whence K_0 is the quadratic field $Q(\sqrt{p})$. In this case (20) reduces to

$$B_m/m! \equiv hw_{11} \pmod{p} \tag{21}$$

where w_{11} is defined by

$$\log\varepsilon^{p-1} \equiv w_{11}\lambda^m \pmod{\lambda^{p-1}},$$

$\varepsilon\ (>1)$ being the fundamental unit of K_0. Let T and U be rational integers such that $\varepsilon = \frac{1}{2}(T+U\sqrt{p})$. Clearly,

$$\varepsilon^{p-1} \equiv 1-(U/T)\sqrt{p} \pmod{\lambda^{p-1}}$$

and so

$$\log\varepsilon^{p-1} \equiv -(U/T)\sqrt{p} \pmod{\lambda^{p-1}}. \tag{22}$$

We may compute $\sqrt{p}$ by the known Gaussian sum formula ([3], p. 349) and by Lemma 3 (ii) as follows:

$$\sqrt{p} = \sum_{s=0}^{p-2}(-1)^s\sigma_s(\zeta) \equiv \sum_{n=0}^{p-1}\frac{\lambda^n}{n!}\sum_{s=0}^{p-2}(-1)^s r^{sn} \equiv -\frac{\lambda^m}{m!} \pmod{\lambda^{p-1}}.$$

By substituting this in (22) we thus obtain

$$w_{11} \equiv U/Tm! \pmod{p},$$

which combined with (21) yields

$$TB_m \equiv hU \pmod{p}.$$

This congruence has been discovered by Kiselev [8] and, independently, by Ankeny, Artin, and Chowla [1]. A proof for it, resembling our proof, is also sketched in [3], pp. 377–378.

References

[1] N. C. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic number fields*, Ann. of Math. 56 (1952), pp. 479–493.

[2] N. C. Ankeny, S. Chowla, and H. Hasse, *On the class number of the maximal real subfield of a cyclotomic field*, J. Reine Angew. Math. 217 (1965), pp. 217–220.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, New York and London 1966.

[4] L. Carlitz, *The first factor of the class number of a cyclic field*, Canad. J. Math. 6 (1954), pp. 23–26.

[5] — *A congruence for the second factor of the class number of a cyclotomic field*, Acta Arith. 14 (1968), pp. 27–34, *Corrigendum*, ibid. 16 (1970), p. 437.

[6] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952.

[7] D. Hilbert, *Theorie der algebraischen Zahlkörper*, Gesammelte Abh. I, New York 1965.

[8] A. A. Kiselev, *An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers* (Russian), Dokl. Akad. Nauk SSSR 61 (1948), pp. 777–779.
[9] T. Metsänkylä, *A congruence for the class number of a cyclic field*, Ann. Acad. Sci. Fenn., Ser. A I 472 (1970), pp. 1–11.
[10] I. Sh. Slavutsky, *The simplest proof of Vandiver's theorem*, Acta Arith. 15 (1969), pp. 117–118.
[11] H. S. Vandiver, *On the first factor of the class number of a cyclotomic field*, Bull. Amer. Math. Soc. 25 (1919), pp. 458–461.

UNIVERSITY OF TURKU
SF-20500 Turku 50, Finland

Received on 16. 2. 1972 (256)

ACTA ARITHMETICA
XXIII (1973)

On pairings of the first $2n$ natural numbers

by

G. B. Huff (Athens, Ga.)

Introduction. In proposing a research problem [2], Mok-Kong Shen and Tsen-Pao Shen noted that the first $2n$ positive integers may be grouped in n pairs, $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$, with $a_i < b_i$ and conjectured that for $n > 2$, there exists a pairing such that the $2n$ numbers $b_i + a_i$ and $b_i - a_i$ are all different. We say that a pairing of any $2n$ distinct positive integers is *acceptable* if these conditions are satisfied.

A program devised by Mr. James C. Fortson for an IBM 360, Model 65, has produced all acceptable pairings of $\{1, 2, \ldots, 2n\}$ for $n < 9$. The printout shows that if $A(n)$ designates the number of acceptable pairings of $\{1, 2, \ldots, 2n\}$, then $A(1) = 1$, $A(2) = 0$, $A(3) = 1$, $A(4) = 8$, $A(5) = 22$, $A(6) = 51$, $A(7) = 342$, and $A(8) = 2669$. This suggests that the difficulty in an existence proof stems from the fact that too many acceptable pairings exist for large values of n and that the problem may be simplified by putting on additional conditions.

M. Slater [4] has suggested that the Shen problem be attacked by requiring that $1 \leqslant a_i \leqslant n$ and conjectured that acceptable pairings satisfying this condition exist except for $n = 2, 3$, or 6. D. A. Klarner [1] noted that the Slater conjecture is related to the "problem of the reflecting queens" and used results of M. Kraitchik to construct all favorable examples for $n = 4, 5, 7$, and 8. J. D. Sebastian [3] used a computer to construct a favorable example in each of the cases $n = 9, 10, 11, \ldots, 27$.

If K_{2n} is a set of $2n$ distinct integers, a *pairing* of K_{2n} is a collection of pairs $\{(a_i, b_i) \mid i \in [1, n]\}$ such that $a_i < b_i$ for all i, $\{a_i, b_i\} \subset K_{2n}$ and each element of K_{2n} occurs in some pair. A pairing such that each of the sets $\{b_i + a_i\}$ and $\{b_i - a_i\}$ is a complete residue system, modulo n, is a good candidate to be acceptable. In this paper the Shen question is given an affirmative answer by studying pairings such that

(*) each of the sets $\{a_i\}, \{b_i\}, \{b_i + a_i\}, \{b_i - a_i\}$ is a complete residue system, modulo n,

and

$$(\#) \qquad b_i \equiv 2a_i, \text{ modulo } n.$$