[7] G. Billing, *Beiträge zur arithmetischen Theorie ebener kubischer Kurven*, Nova Acta Reg. Soc. Scient. Upsaliensis (IV) 9 (1938), p. 1-165.

[8] E. S. Selmer, *The diophantine equation $ax^3+by^3+cz^3=0$*, Acta Math. Stockholm 85 (1951), p. 203-362.

[9] T. Skolem, *Diophantische Gleichungen*, Ergeb. d. Math. 54 (1938).

[10] J. J. Sylvester, *On certain ternary cubic-form equations*, Coll. Papers. (1909) III, p. 312-319 (= Amer. J. Math. 2 (1878), p. 280-285, 357-393 and 3 (1880), p. 58-88, 179-189).

[11] A. Weil, *L'arithmetique sur les courbes algebriques*, Acta Math. Stockholm 52 (1928-9), p. 281-315.

[12] — *Sur un théorème de Mordell*, Bull. des Sci. Math. (2) 54 (1930), p. 182-191.

Reçu par la Rédaction le 3. 10. 1959

ACTA ARITHMETICA
VI (1960)

The cyclotomic numbers of order twelve*

by

A. L. Whiteman (Princeton, N. J.)

1. Introduction. Let p be an odd prime and g a fixed primitive root of p. Let e be a divisor of $p-1$ and put $p-1 = ef$. The cyclotomic number $(i,j) = (i,j)_e$ is the number of values of y, $1 \leqslant y \leqslant p-2$, for which

$$(1.1) \qquad y \equiv g^{es+i}, \quad 1+y \equiv g^{et+j} \pmod{p},$$

where the values of s and t are each selected from the integers $0, 1, \ldots, f-1$. A central problem in the theory of cyclotomy is to find exact formulas for the constants (i,j). Until now complete solutions have been obtained only in the cases $e = 2, 3, 4, 5, 6, 8, 10$ and 16. References to these solutions are given in R. H. Bruck's report [2] on the computational aspects of the problem. Since the publication of [2] two more articles [11], [12] relevant to the subject have appeared.

This paper is concerned with the case $e = 12$. The systematic study of this case was initiated by L. E. Dickson [4]. The foundation for his work is the following theorem ([4], Theorem 12): when $e = 12$, the 144 cyclotomic constants (i,j) depend solely upon the decompositions $p = x^2 + 4y^2$ and $p = A^2 + 3B^2$ of the prime $p = 12f+1$, where $x \equiv 1 \pmod{4}$ and $A \equiv 1 \pmod{6}$. In a number of instances Dickson obtained explicit formulas to illustrate this theorem. Two examples are as follows. If 2 is a cubic residue of p and 3 is a biquadratic residue of p, then

$$(1.2) \qquad 144(0,0)_{12} = p-35-32A-30x \pm 24(A+x) \qquad (f \text{ even}),$$

$$(1.3) \qquad 144(0,2)_{12} = p+1-2A+24B-12x \qquad (f \text{ odd}).$$

The conditions of the theorem determine x and A uniquely and determine y and B uniquely except for sign. The ambiguous sign in (1.2) is

* Research done in part under Contract NSF G-5877 between the National Science Foundation and the University of Southern California, and in part with support from the Institute for Advanced Study.

fixed by the condition that the symbol $(0,0)_{12}$ is an integer. It is clear that the value of $(0,0)_{12}$ does not depend on the choice of the primitive root g. On the other hand the value of $(0,2)_{12}$ is indeterminate. Formula (1.3) means that for some choice of B there is some choice of g such that (1.3) holds.

Dickson's analysis depends upon elaborate computations and is not entirely definitive. In the present investigation a different method is devised, and the first complete solution of the cyclotomic problem in the case $e = 12$ is obtained. The presentation is virtually self-contained. It is proved that the primes have to be divided into twelve classes with different formulas holding for different classes. Moreover, all possible formulas are derived (§ 5) and tabulated (§ 6). The principal new tools are Theorems 1 to 5 in §§ 3 and 4.

Three important applications of the tables in § 6 may now be indicated.

The so-called f-nomial periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$ are given by

$$\eta_k = \sum_{t=0}^{f-1} \exp(2\pi i g^{et+k}/p) \qquad (k = 0, 1, \ldots, e-1).$$

These η's satisfy an irreducible equation of degree e with integral coefficients known as the period equation. In the determinantal form of the period equation (see e. g. [4], p. 398) the entries are cyclotomic numbers of the eth order. Consequently the formulas in § 6 enable one to express the coefficients of the period equation of degree 12 in terms of p, x, y, A, B. However, this matter will not be pursued in the present paper.

For integers a, b, c the problem of determining the number of solutions $N_e(a, b, c)$ of the congruence

$$(1.4) \qquad ax^e + by^e \equiv c \pmod{p} \qquad \big(xy \not\equiv 0 \pmod{p}\big)$$

can be reduced to the problem of determining the number of solutions of (1.1). Hence the tables for $(i, j)_{12}$ may be used to compute corresponding tables for $N_{12}(a, b, c)$. An example of this kind is given at the end of § 6.

In (1.4) it is natural to take $a = 1$, $b = -1$ and ask for what values of p is it true that the number of solutions of (1.4) is the same for every $c \not\equiv 0 \pmod{p}$. This is the problem of residue difference sets and it is solved in § 7 in the case $e = 12$.

2. Cyclotomy. In this section some results from the theory of cyclotomy are presented for convenient reference.

It should be kept in mind that the cyclotomic numbers (i, j) defined in the introduction are functions of g as well as p. For if g is replaced by another primitive root g', then the correspondence between the numbers $(i, j)'$ for g' and the numbers (i, j) for g is given by the equation $(i, j)' = (ri, rj)$, where r is some integer relatively prime to $p-1$ such that $g' \equiv g^r \pmod{p}$.

Clearly $(i, j) = (i', j')$ if $i \equiv i' \pmod{e}$ and $j \equiv j' \pmod{e}$. Furthermore, the following identities are well-known ([1], p. 202-203):

$$(2.1) \qquad (i, j) = (e-i, j-i);$$

$$(2.2) \qquad (i, j) = \begin{cases} (j, i) & (f \text{ even}), \\ (j+\tfrac{1}{2}e, i+\tfrac{1}{2}e) & (f \text{ odd}). \end{cases}$$

Let $\beta = \exp(2\pi i/e)$ be a primitive eth root of unity. For an integer a not divisible by p let $\operatorname{ind} a$ be defined by means of the congruence $g^{\operatorname{ind} a} \equiv a \pmod{p}$. In the theory of cyclotomy the so-called Jacobi sum ([1], p. 122) plays a fundamental role. For each pair of integers m, n this sum is defined by

$$(2.3) \qquad \psi(\beta^m, \beta^n) = \sum_{a+b\equiv 1 (\mathrm{mod}\, p)} \beta^{m \operatorname{ind} a + n \operatorname{ind} b},$$

where a, b run over all pairs of integers in the range $1 \leqslant a, b \leqslant p-1$ satisfying the summation condition. It follows without difficulty from (2.3) (compare [5], (9)) that

$$(2.4) \qquad \psi(\beta^m, \beta^n) = \psi(\beta^n, \beta^m) = (-1)^{nf} \psi(\beta^{-m-n}, \beta^n).$$

Putting $n = 0$ in (2.3) we get also

$$(2.5) \qquad \psi(\beta^m, \beta^0) = \begin{cases} p-2 & (m = 0), \\ -1 & (1 \leqslant m \leqslant e-1). \end{cases}$$

The most important property of (2.3) is the formula ([1], p. 123)

$$(2.6) \qquad \psi(\beta^m, \beta^n)\psi(\beta^{-m}, \beta^{-n}) = p,$$

provided no one of the integers $m, n, m+n$ is divisible by e.

In (2.3) replace m by vn, where v is an integer. Collecting the exponents of β which are in the same residue class modulo e we obtain the following expansion of $\psi(\beta^{vn}, \beta^n)$ into a finite Fourier series (compare [10], Theorem 3):

$$(2.7) \qquad \psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{i=0}^{e-1} B(i, v) \beta^{ni}.$$

The coefficients $B(i, v)$ are Dickson-Hurwitz sums ([10], (6.2)) defined by

$$B(i, v) = \sum_{h=0}^{e-1} (h, i-vh). \tag{2.8}$$

Using (2.1) and (2.2) we may easily prove the following two properties of $B(i, v)$:

$$B(i, v) = B(i, e-v-1), \tag{2.9}$$

and ([1], p. 201)

$$B(i, 0) = \begin{cases} f-1 & (i = 0), \\ f & (1 \leqslant i \leqslant e-1). \end{cases} \tag{2.10}$$

Putting $n = 0$ in (2.7) and using (2.5) we obtain

$$\sum_{i=0}^{e-1} B(i, v) = p-2. \tag{2.11}$$

Let now α denote a root of the equation $\alpha^{p-1} = 1$ and put $\zeta = \exp(2\pi i/p)$. Closely related to the Jacobi sum $\psi(\beta^m, \beta^n)$ is the resolvent of Lagrange ([1], p. 83):

$$\tau(\alpha) = \sum_{a=1}^{p-1} \alpha^{\operatorname{ind} a} \zeta^a. \tag{2.12}$$

Indeed we have the formula ([1], p. 86)

$$\psi(\beta^m, \beta^n) = \tau(\beta^m)\tau(\beta^n)/\tau(\beta^{m+n}) \tag{2.13}$$

when $m+n$ is not divisible by e. We also have the formula ([1], p. 87)

$$\tau(\beta^n)\tau(\beta^{-n}) = (-1)^{nf} p \tag{2.14}$$

if n is not divisible by e.

Jacobi ([7], p. 167) stated without proof the following two deeper properties of (2.12). (i) If p is an odd prime, then

$$\tau(-1)\tau(\alpha^2) = \alpha^{2m}\tau(\alpha)\tau(-\alpha) \qquad (g^m \equiv 2\,(\mathrm{mod}\,p)). \tag{2.15}$$

(ii) If p is a prime $\equiv 1\,(\mathrm{mod}\,3)$, then

$$\tau(\alpha)\tau(\omega\alpha)\tau(\omega^2\alpha) = \alpha^{-3m'} p\,\tau(\alpha^3) \qquad (g^{m'} \equiv 3\,(\mathrm{mod}\,p)), \tag{2.16}$$

where ω is an imaginary cube root of unity. Formulas (2.15) and (2.16) are special cases of a remarkable identity ([3], (0.9)) first proved by Davenport and Hasse.

In the rest of this section we assume that e is even and write $e = 2E$. For later applications we now derive from (2.15) two properties of the Jacobi sum. In (2.15) replace α by β^v, where $1 \leqslant v \leqslant e-1$. Then multiply both members of the resulting equation by $\tau(\beta^{-v+E})/\tau(\beta^{v+E})\tau(\beta^E)$. In view of (2.13) we obtain

$$\psi(\beta^{2v}, \beta^E) = \beta^{2vm}\psi(\beta^v, \beta^{v+E}) \qquad (v \neq E/2, 3E/2), \tag{2.17}$$

$$\psi(\beta^{2v}, \beta^{-v+E}) = \beta^{2vm}\psi(\beta^v, \beta^{-v+E}) \qquad (v \neq E). \tag{2.18}$$

We shall require an extension of (2.11). Put $n = E$ in (2.7). Then by (2.4) and (2.5) the value of $(-1)^{vEf}\psi(\beta^{vE}, \beta^E)$ is -1. Making use of (2.11) we deduce

$$\sum_{i=0}^{E-1} B(2i, v) = \frac{p-3}{2}, \qquad \sum_{i=0}^{E-1} B(2i+1, v) = \frac{p-1}{2} \qquad (e \text{ even}). \tag{2.19}$$

We next define the functions

$$s(i, j) = (i, j)-(i, j+E), \; t(i, j) = (i, j)-(i+E, j). \tag{2.20}$$

Then it follows from (2.2) that

$$t(i, j) = \begin{cases} s(j, i) & (f \text{ even}), \\ s(j+E, i+E) & (f \text{ odd}). \end{cases} \tag{2.21}$$

In § 5 we shall make use of the following lemma.

LEMMA 1. *If e is even and $E = e/2$, then*

$$4(i, j)_e = (i, j)_E + s(i, j) + s(i+E, j) + 2t(i, j). \tag{2.22}$$

Proof. This lemma is an easy consequence of the formula

$$(i, j)_E = (i, j)_e + (i+E, j)_e + (i, j+E)_e + (i+E, j+E)_e.$$

The purpose of the lemma is to provide a transition from the value of $(i, j)_E$ to the value of $(i, j)_e$.

3. Cyclotomy when e is four times an odd prime. The results in this section will enable us in § 5 to express the numbers $(i, j)_{12}$ in terms of p, x, y, A and B. Our procedure is an extension of the method used in another paper [12] to treat the case $e = 10$. We assume, to begin with, that e is divisible by 4, and we put $E = e/2$, $q = e/4$.

Returning to Lemma 1 we see that (2.22) expresses $(i, j)_e$ in terms of $(i, j)_E$ and numbers of the form $s(i, j)$. The evaluation of $s(i, j)$ will be accomplished with the aid of the following theorem.

THEOREM 1. *Let $e = 4q$, where q is an odd prime. If i and j are arbitrary integers, then*

(3.1) $$es(i,j) = S(i,j)+T(i,j)+\sum_{v=0}^{e-1}\big(B(j+iv,v)-B(j+E+iv,v)\big),$$

where $S(i,j)$ and $T(i,j)$ are sums defined as follows:

(3.2) $$S(i,j) = 4\sum_{n=0}^{q-1}\big((i,j+4n)-(i,j+4n+2)\big),$$

(3.3) $$T(i,j) = 4\sum_{m=0}^{q-1}\sum_{n=0}^{q-1}\big((i+4m,j+4n+2)-(i+4m,j+4n)\big).$$

Proof. The starting point of the proof is the relation

(3.4) $$B(j+iv,v) = (i,j)+\sum_{h=1}^{e-1}(h+i,j-vh),$$

which follows from (2.8). In (3.4) sum over $v = 0, 1, \ldots, e-1$ and then replace j by $j+E$. Employing (2.20) we get after subtraction

(3.5) $$es(i,j) = N(i,j)+\sum_{v=0}^{e-1}\big(B(j+iv,v)-B(j+E+iv,v)\big),$$

where we have put

(3.6) $$N(i,j) = \sum_{h=1}^{e-1}\sum_{v=0}^{e-1}\big((h+i,j+E-vh)-(h+i,j-vh)\big).$$

A comparison of (3.1) and (3.5) shows that the remainder of the proof consists in establishing that $N(i,j) = S(i,j)+T(i,j)$. In several portions of the following argument we shall tacitly employ the hypothesis that q is an odd prime. Consider first a fixed value of h in the outer sum in (3.6). For h odd, $h \neq q$, $h \neq 3q$, the numbers vh run over a complete residue system modulo e whenever v does. For $h = q$, the consecutive terms of the sequence $vh (\mathrm{mod}\, e)$ are $0, q, 2q, 3q, 0, q, 2q, 3q, \ldots, 0, q, 2q, 3q$. For $h = 3q$, the consecutive terms are $0, 3q, 2q, q, 0, 3q, 2q, q, \ldots, 0, 3q, 2q, q$. In any event, when h is odd the corresponding contribution of the inner sum in (3.6) to the value of $N(i,j)$ is zero. Suppose next that $h \equiv 2 (\mathrm{mod}\, 4)$, $h \neq 2q$. Then the least positive remainders of the numbers $vh (\mathrm{mod}\, e)$ run twice over the even integers from 0 to $e-2$ in some order. But if $h = 2q$, then the terms in the sequence $vh (\mathrm{mod}\, e)$ are alternately 0 and E. Thus when $h \equiv 2 (\mathrm{mod}\, 4)$ we conclude again that the corresponding contribution of the inner sum in (3.6) to the value of $N(i,j)$ is zero. Finally, suppose that $h \equiv 0 (\mathrm{mod}\, 4)$. Then the least positive residues of the numbers $vh (\mathrm{mod}\, e)$ run four times in some order over the multiples of four between 0 and $e-4$. Since $E \equiv 2 (\mathrm{mod}\, 4)$, it follows that $N(i,j)$ may now be written in the form

$$N(i,j) = 4\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\big((i+4m,j+4n+2)-(i+4m,j+4n)\big).$$

This completes the proof.

In the statement of Lemma 1 there appears the combination $s(i,j)+s(i+E,j)$. In § 5 we shall require a technique for evaluating this sum. Accordingly we derive the following corollary of Theorem 1.

COROLLARY. *If the hypotheses of Theorem 1 are satisfied, then*

(3.7) $$\begin{aligned} &e\big(s(i,j)+s(i+E,j)\big) \\ &\quad = S'(i,j)+T'(i,j)+2\sum_{v=0}^{E-1}\big(B(j+2iv,2v)-B(j+E+2iv,2v)\big), \end{aligned}$$

where

(3.8) $$S'(i,j) = S(i,j)+S(i+E,j), \quad T'(i,j) = T(i,j)+T(i+E,j).$$

Proof. To establish the Corollary we consider the sum in (3.1) and the corresponding sum with i replaced by $i+E$. For a fixed value of v, corresponding summands differ by the factor $(-1)^v$. It is therefore clear that $es(i,j)+es(i+E,j)$ reduces to the right member of (3.7).

We next concern ourselves with the evaluation of $S(i,j)$ and $S'(i,j)$. For this purpose we put

(3.9) $$b(i,v) = B(i,v)-B(i+E,v),$$

and define the functions $C(i,q)$, $D(i,q)$ by means of

(3.10) $$C(i,q) = b(i,q)+b(i,3q), \quad D(i,q) = b(i+q,q)-b(i+q,3q).$$

We shall express $S(i,j)$, $S'(i,j)$ in terms of $C(i,q)$, $D(i,q)$. Our results will enable us, when we specialize to the case $e = 12$ in § 4, to evaluate $T(i,j)$ and $T'(i,j)$ in terms of p, x, y, A, B. Finally, in § 5 we shall also express $b(i,v)$ in terms of p, x, y, A, B.

It is convenient to consider first $S'(i,j)$. We state the following theorem.

THEOREM 2. *Let $q = e/4 = E/2$ be an odd integer. If $S'(i,j)$ is defined by* (3.8), *then*

(3.11) $$S'(i,j) = \begin{cases} (-1)^{(i-j)/2}2C(-i,q) & (i \equiv j (\mathrm{mod}\, 2)), \\ (-1)^{(i-j+1)/2}2D(-i,q) & (i \equiv j+1 (\mathrm{mod}\, 2)), \end{cases}$$

where $C(i,q)$ and $D(i,q)$ are defined in (3.10).

Proof. We shall prove only the first half of (3.11); the second half may be established similarly. It follows easily from (2.2) and (2.8) that for an odd integer v we have

$$B(i,v) = \sum_{h=0}^{e-1}(i-vh,h) \qquad (v \text{ odd}). \tag{3.12}$$

Taking $v = q$ in (3.12) and collecting the values of h which are in the same residue class modulo 4, we get

$$\begin{aligned} B(i,q) = \sum_{n=0}^{q-1}(i,4n)+\sum_{n=0}^{q-1}(i+3q,4n+1)+\sum_{n=0}^{q-1}(i+2q,4n+2)+ \\ +\sum_{n=0}^{q-1}(i+q,4n+3). \end{aligned} \tag{3.13}$$

In an analogous manner we may write down formulas for $B(i,3q)$, $B(i+2q,q)$, $B(i+2q,3q)$ corresponding to (3.13). Substituting the results into $b(-i,q)+b(-i,3q)$ and applying (2.1) we obtain

$$\begin{aligned} 2C(-i,q) = 4\sum_{n=0}^{q-1}\big((i,i+4n)-(i,\ i+4n+2)\big)+ \\ +4\sum_{n=0}^{q-1}\big((i+2q,\ i+2q+4n+2)-(i+2q,\ i+2q+4n)\big). \end{aligned}$$

In view of (3.2) and (3.8) the result stated in the first half of (3.11) now follows at once.

By means of Theorem 2 we next deduce the following theorem for computing $S(i,j)$.

THEOREM 3. *Let $S(i,j)$ be defined by* (3.2), *and let $q = e/4$ be an odd integer. If $j \equiv 0 \pmod 4$, then*

$$S(i,j) = \begin{cases} C(i,q)+(-1)^{i/2}C(-i,q) & (i \text{ even}), \\ C(i,q)+(-1)^{(i+1)/2}D(-i,q) & (i \text{ odd}). \end{cases} \tag{3.14}$$

If $j \equiv 1 \pmod 4$, then

$$S(i,j) = \begin{cases} D(i,q)+(-1)^{i/2}D(-i,q) & (i \text{ even}), \\ D(i,q)+(-1)^{(i-1)/2}C(-i,q) & (i \text{ odd}). \end{cases} \tag{3.15}$$

Proof. Since $S(i,j+2) = -S(i,j)$, the cases in which $j \equiv 2$ or $3 \pmod 4$ reduce to the cases in which $j \equiv 0$ or $1 \pmod 4$. By (2.1) and (3.2) we have

$$S(i,j) = \begin{cases} (-1)^{i/2}S(-i,j) & (i \text{ even}), \\ (-1)^{(i+1)/2}S(-i,j+1) & (i \text{ odd}). \end{cases} \tag{3.16}$$

Theorem 3 follows from (3.8), (3.11) and (3.16).

4. The case $e = 12$. Throughout this section we shall assume that $e = 12$, $E = 6$, $q = 3$. The number β is thus a primitive twelfth root of unity. In (2.7) put $n = 3$, $v = 1$ and $n = 9$, $v = 1$; put also $n = 2$, $v = 2$ and $n = 10$, $v = 2$. Then it is clear that $\psi(\beta^{-3},\beta^{-3})$ and $\psi(\beta^{-4},\beta^{-2})$ are the complex conjugates of $\psi(\beta^3,\beta^3)$ and $\psi(\beta^4,\beta^2)$ respectively. Following Dickson (compare [4], (50), (85)) we now put

$$\psi(\beta^3,\beta^3) = -x+2y\beta^3, \qquad \psi(\beta^4,\beta^2) = -A+B(2\beta^2-1). \tag{4.1}$$

It follows from (2.6) that

$$p = x^2+4y^2 = A^2+3B^2. \tag{4.2}$$

We next make three applications of (2.7) with $n = 3$ and $v = 1, 2, 5$. We get

$$\psi(\beta^3,\beta^3) = (-1)^f\sum_{i=0}^{11}B(i,v)\beta^{3i} \qquad (v = 1, 2 \text{ or } 5). \tag{4.3}$$

Equating real and imaginary parts in (4.1) and (4.3) we obtain for $v = 1, 2$ or 5

$$\begin{aligned} (-1)^{f+1}x = \big(B(0,v)+B(4,v)+B(8,v)\big)- \\ -\big(B(2,v)+B(6,v)+B(10,v)\big), \end{aligned} \tag{4.4}$$

$$\begin{aligned} (-1)^f 2y = \big(B(1,v)+B(5,v)+B(9,v)\big)- \\ -\big(B(3,v)+B(7,v)+B(11,v)\big). \end{aligned} \tag{4.5}$$

Again, putting $n = 2$, $v = 2$ in (2.7) and noting that $\beta^4 = \beta^2-1$ we derive in a similar manner that $A = -a+\frac{1}{2}b$, $B = \frac{1}{2}b$, where

$$\begin{aligned} a = \big(B(0,2)-B(3,2)+B(6,2)-B(9,2)\big)- \\ -\big(B(2,2)-B(5,2)+B(8,2)-B(11,2)\big), \end{aligned} \tag{4.6}$$

$$\begin{aligned} b = \big(B(1,2)-B(4,2)+B(7,2)-B(10,2)\big)+ \\ +\big(B(2,2)-B(5,2)+B(8,2)-B(11,2)\big). \end{aligned} \tag{4.7}$$

Dickson ([4], p. 400) proved that $x = 6f+1-8(1,2)_4$ or $6f-1-8(1,0)_4$ according as f is even or odd. He ([4], p. 409) also showed that $A = 6(0,3)_6-6(1,2)_6+1$. Hence the values of x and A are uniquely determined by (4.2) and the conditions

$$x \equiv 1 \pmod 4, \qquad A \equiv 1 \pmod 6. \tag{4.8}$$

On the other hand y and B are uniquely determined by (4.2) except for sign. For a fixed primitive root g the precise determinations of y and $2B$ are given by (4.5) and (4.7) respectively.

There are additional formulas related to (4.4) and (4.5). Make two applications of (2.7) with $n = 3$ and $v = 3, 4$. By (2.4) and (2.5) we have

$$\sum_{i=0}^{11} B(i,3)\beta^{3i} = \sum_{i=0}^{11} B(i,4)\beta^{3i} = -1. \tag{4.9}$$

Separating real and imaginary parts in (4.9) and then combining the results with (2.19), we find

$$B(0,v)+B(4,v)+B(8,v) = \tfrac{1}{4}(p-5) \qquad (v = 3 \text{ or } 4), \tag{4.10}$$

$$\begin{aligned} B(1,v)+B(5,v)+B(9,v) &= B(2,v)+B(6,v)+B(10,v) \\ &= B(3,v)+B(7,v)+B(11,v) = \tfrac{1}{4}(p-1) \qquad (v = 3 \text{ or } 4). \end{aligned} \tag{4.11}$$

With the results of this section we can compute the sums $T(i,j)$ and $T'(i,j)$ defined in (3.3) and (3.8) respectively. The formulas depend on the residue classes of i and j modulo four. It is convenient to distinguish seven cases as follows.

Case 1: $i \equiv 0 \pmod 4$, $j \equiv 0 \pmod 4$. Case 2: $i \equiv 0 \pmod 4$, $j \equiv 1 \pmod 4$. Case 3: $i \equiv 2 \pmod 4$. Case 4: $i \equiv 1 \pmod 4$, $j \equiv 0 \pmod 4$. Case 5: $i \equiv 1 \pmod 4$, $j \equiv 1 \pmod 4$. Case 6: $i \equiv 3 \pmod 4$, $j \equiv 0 \pmod 4$. Case 7: $i \equiv 3 \pmod 4$, $j \equiv 3 \pmod 4$. We now state

THEOREM 4. *When $e = 12$ the value of the sum $T(i,j)$ defined in* (3.3) *is given by*

$$T(i,j) = \begin{cases} 2+(-1)^f 2x & (\textit{Case } 1), \\ (-1)^{f+1}4y & (\textit{Case } 2), \\ \quad 0 & (\textit{Case } 3), \\ 1+(-1)^{f+1}(x+2y) & (\textit{Cases } 4,\ 7), \\ 1+(-1)^{f+1}(x-2y) & (\textit{Cases } 5,\ 6), \end{cases} \tag{4.12}$$

where x and y are determined by (4.4) *and* (4.5) *respectively.*

Proof. Since $T(i,j+2) = -T(i,j)$, all remaining cases can be reduced to cases covered by the theorem. Let us return to the functions $C(i,q)$, $D(i,q)$ defined in (3.10). Formulas (4.4), (4.5) and (4.10), (4.11) transform into

$$\begin{aligned} C(0,3)+C(4,3)+C(8,3) \\ = -C(2,3)-C(6,3)-C(10,3) = -1+(-1)^{f+1}x. \end{aligned} \tag{4.13}$$

$$\begin{aligned} C(1,3)+C(5,3)+C(9,3) \\ = -C(3,3)-C(7,3)-C(11,3) = (-1)^f 2y. \end{aligned} \tag{4.14}$$

$$\begin{aligned} D(0,3)+D(4,3)+D(8,3) \\ = -D(2,3)-D(6,3)-D(10,3) = (-1)^f 2y, \end{aligned} \tag{4.15}$$

$$\begin{aligned} D(1,3)+D(5,3)+D(9,3) \\ = -D(3,3)-D(7,3)-D(11,3) = -1+(-1)^f x. \end{aligned} \tag{4.16}$$

By (3.2) and (3.3) we have

$$T(i,j) = -S(i,j)-S(i+4,j)-S(i+8,j). \tag{4.17}$$

We now apply Theorem 3 to (4.17) in each of the seven separate cases under consideration. The five assertions of Theorem 4 are consequences of relations (4.13) to (4.16).

The function $T'(i,j)$ defined in (3.8) may now easily be evaluated. We have the following theorem.

THEOREM 5. *If $e = 12$ the value of $T'(i,j)$ is given by*

$$T'(i,j) = \begin{cases} 2+(-1)^{i+f}2x & (j \equiv 0 \pmod 4), \\ (-1)^{i+f+1}4y & (j \equiv 1 \pmod 4)). \end{cases} \tag{4.18}$$

Proof. Since $T'(i,j+2) = -T'(i,j)$ the cases in which $j \equiv 2$ or $3 \pmod 4$ reduce to the cases in which $j \equiv 0$ or $1 \pmod 4$. The theorem follows immediately from (3.8) and (4.12).

5. Evaluation of the numbers $b(i,v)$. We now turn to the question of computing $es(i,j)$ by means of Theorem 1 in the particular case $e = 12$. For this purpose we require the values of the successive terms $b(j+iv, v)$ in the sum in (3.1). We shall derive formulas which express the values of $b(i,v)$, $i, v = 0, 1, \ldots, 11$ in terms of x, y, A, B.

By (2.9) and (3.9) we have at once

$$b(i,v) = b(i,11-v) = -b(i+6,v). \tag{5.1}$$

It therefore suffices to compute $b(i,v)$ for $i, v = 0, 1, 2, 3, 4, 5$.

To begin with, we note that (2.10) implies

$$b(i,0) = \begin{cases} -1 & (i = 0), \\ 0 & (i = 1, 2, 3, 4, 5). \end{cases} \tag{5.2}$$

The results in § 4 yield additional relations. From (4.4) and (4.5) we get

$$b(0,v)-b(2,v)+b(4,v) = (-1)^{f+1}x \qquad (v = 1, 2 \text{ or } 5), \tag{5.3}$$

$$b(1,v)-b(3,v)+b(5,v) = (-1)^f 2y \qquad (v = 1, 2 \text{ or } 5). \tag{5.4}$$

Again, from (4.10) and (4.11) we obtain

$$b(0,v)-b(2,v)+b(4,v) = -1 \qquad (v = 3 \text{ or } 4), \tag{5.5}$$

$$b(1,v)-b(3,v)+b(5,v) = 0 \qquad (v = 3 \text{ or } 4). \tag{5.6}$$

The basis of further analysis is the following lemma concerning the Jacobi sums $\psi(\beta^m, \beta^n)$ defined in (2.3).

Lemma 2. *If $e = 12$ and the number c is defined by means of the equation*

$$c = \psi(\beta^3, \beta)/\psi(\beta^5, \beta), \tag{5.7}$$

then the Jacobi sums satisfy the relations

(i) $\beta^{2m}\psi(\beta, \beta) = \beta^{3m'}\psi(\beta^3, \beta^3)$,

(ii) $\psi(\beta^2, \beta) = (-1)^f c\beta^{3m'}\psi(\beta^4, \beta^2)$,

(iii) $\psi(\beta^3, \beta) = (-1)^f c\beta^{3m'}\psi(\beta^3, \beta^3)$,

(iv) $\psi(\beta^4, \beta) = \beta^{4m}\psi(\beta^4, \beta^2)$,

(v) $\psi(\beta^5, \beta) = (-1)^f\beta^{3m'}\psi(\beta^3, \beta^3)$,

where $g^m \equiv 2 \pmod p$ and $g^{m'} \equiv 3 \pmod p$.

Proof. At the end of the proof we shall show that the number c is actually a fourth root of unity. We first note that $(3|p) = 1$ since $p = 12f+1$ and hence m' is even. Therefore $\beta^{-3m'} = \beta^{3m'}$. Furthermore, $(2|p) = \pm 1$ according as f is even or odd and hence $m \equiv f \pmod 2$. It is convenient first to derive (iv). Noting that $\beta^{6m} = (-1)^f$ and using (2.4) we see that (iv) is a special case of (2.17) with $v = 1$, $E = 6$. We next prove (v). In (2.16) put $\omega = \beta^4$ and $\alpha = \beta$. Then apply (2.14) with $n = 3$. By (2.13) we get (v). To deduce (i) put $v = 5$, $E = 6$ in (2.18). By (v) and (2.4) we obtain (i). To prove (ii) and (iii) we employ the formula

$$\psi(\beta^2, \beta)\psi(\beta^3, \beta^3) = \psi(\beta^3, \beta)\psi(\beta^4, \beta^2), \tag{5.8}$$

which is an immediate consequence of (2.13). Combining (v) with (5.7) and (5.8) we derive (ii) and (iii).

We now prove that c is a fourth root of unity. In (2.18) take $v = 2$, $E = 6$ and compare the result with (iv). We get $\psi(\beta^4, \beta) = \psi(\beta^4, \beta^4)$. By (2.4) and (2.13) this equation transforms into

$$\psi(\beta^3, \beta) = \psi(\beta^5, \beta^3). \tag{5.9}$$

We also find immediately from (2.13) and (2.14) that

$$\psi(\beta^5, \beta)\psi(\beta^3, \beta^3) = \psi(\beta^3, \beta)\psi(\beta^5, \beta^3). \tag{5.10}$$

Combining (5.7), (5.9) and (5.10) we obtain $\psi(\beta^3, \beta^3) = c\psi(\beta^3, \beta)$. Substituting from (iii) into the last equation we get

$$c^2 = (-1)^f\beta^{3m'}, \tag{5.11}$$

which yields the value of c except for sign.

Lemma 2 serves the purpose of dividing the primes $p = 12f+1$ into classes depending on the residue character of 2 modulo p and the residue character of 3 modulo p. From (5.11) it follows that $c = \pm 1$ if f is even and $m' \equiv 0 \pmod 4$, or if f is odd and $m' \equiv 2 \pmod 4$; also $c = \pm\beta^3$ if f is even and $m' \equiv 2 \pmod 4$, or if f is odd and $m' \equiv 0 \pmod 4$. Furthermore, $m \equiv 0, 2$ or $4 \pmod 6$ if f is even, and $m \equiv 1, 3$ or $5 \pmod 6$ if f is odd. Altogether there are twenty-four classes of primes (which will be reduced to twelve essentially different classes in § 6). For each class there is a separate table of formulas of the cyclotomic constants (see the tables in § 6). The sign of c is fixed by means of a criterion formulated in the paragraph immediately preceding (5.13).

We now describe in general terms the way in which Lemma 2 is used to calculate the numbers $b(i, v)$. Since $\beta^4 = \beta^2-1$, the expansion (2.7) of $\psi(\beta^v, \beta)$ may be transformed into

$$(-1)^{vf}\psi(\beta^v, \beta) = \big(b(0,v)-b(4,v)\big)+\big(b(1,v)-b(5,v)\big)\beta+ \\ +\big(b(2,v)+b(4,v)\big)\beta^2+\big(b(3,v)+b(5,v)\big)\beta^3. \tag{5.12}$$

On the other hand, in view of (4.1), Lemma 2 expresses $\psi(\beta^v, \beta)$ as a power of β multiplied by $-x+2y\beta^3$ or $-A+B(2\beta^2-1)$. By equating coefficients of like powers of β we obtain four linear relations among the six numbers $b(i, v)$, $i = 0, 1, 2, 3, 4, 5$. Two more relations are given in (5.3), (5.4) or (5.5), (5.6). These six linear equations in the same number of unknowns are linearly independent and hence determine the unknowns uniquely. It turns out that, in all instances, $b(i, v)$ is expressible as a linear combination with integral coefficients of $1, A, B, x, y$.

To illustrate the method let us consider, for example, the specific case in which $v = 2$, f is even (and hence m is even), $m' \equiv 2 \pmod 4$, $c = -\beta^3$. From equation (ii) of Lemma 2 it is clear that the value of $b(i, 2)$ does not depend on the residue class of $m \pmod 6$. By (4.1) the right member of (ii) reduces to $-2B\beta+(-A+B)\beta^3$. Since the numbers $1, \beta, \beta^2, \beta^3$ are linearly independent over the field of rational numbers, we may equate coefficients of like powers of β in both members of (ii). From (5.12) with $v = 2$ we get thus the four equations: $b(0,2)-b(4,2) = 0$, $b(1,2)-b(5,2) = -2B$, $b(2,2)+b(4,2) = 0$, $b(3,2)+b(5,2) = -A+B$. By (5.3) and (5.4) we have also the two equations: $b(0,2)-b(2,2)+b(4,2) = -x$, $b(1,2)-b(3,2)+b(5,2) = 2y$. Solving the last six equations for $b(i,2)$ we obtain the solutions: $3b(0,2) = -x$, $3b(1,2) = -A-3B+2y$, $3b(2,2) = x$, $3b(3,2) = -2A-2y$, $3b(4,2) = -x$, $3b(5,2) = -A+3B+2y$.

The results obtained by this method may be summarized by means of the following classification of cases. (In order to save space we list under each case the values of $3b(i,v)$, $i = 0,1,2,3,4,5$ written consecutively.)

I_1. $v = 1$, f even, $m' \equiv 0 \pmod 4$, $m \equiv 0 \pmod 6$.
$-3x,\ 4y,\ 0,\ 2y,\ 0,\ 4y.$

I_2. $v = 1$, f even, $m' \equiv 2 \pmod 4$, $m \equiv 0 \pmod 6$.
$x,\ 0,\ 2x,\ -6y,\ -2x,\ 0.$

II_1. $v = 2$, f even, $m' \equiv 0 \pmod 4$, $c = 1$.
$-2A-x,\ 2y,\ -A+3B+x,\ -2y,\ A+3B-x,\ 2y.$

II_2. $v = 2$, f even, $m' \equiv 2 \pmod 4$, $c = \beta^3$.
$-x,\ A+3B+2y,\ x,\ 2A-2y,\ -x,\ A-3B+2y.$

In Case II when c is replaced by $-c$, x and y remain unaltered while A and B change sign.

III_1. $v = 3$, f even, $m' \equiv 0 \pmod 4$, $c = 1$.
$-1-2x,\ 2y,\ 1-x,\ 4y,\ -1+x,\ 2y.$

III_2. $v = 3$, f even, $m' \equiv 2 \pmod 4$, $c = \beta^3$.
$-1+4y,\ x,\ 1+2y,\ 2x,\ -1-2y,\ x.$

In Case III when c is replaced by $-c$, x and y change sign.

IV. $v = 4$, f even, $m \equiv 0 \pmod 6$.
$-1-2A,\ 0,\ 1-A+3B,\ 0,\ 1-1+A+3B,\ 0.$

In Cases I and IV when $m \equiv 0 \pmod 6$ is replaced by $m \equiv 2 \pmod 6$, $3b(i,v)$ is replaced by $3b(i+8,v)$; when $m \equiv 0 \pmod 6$ is replaced by $m \equiv 4 \pmod 6$, $3b(i,v)$ is replaced by $3b(i+4,v)$.

V_1. $v = 5$, f even, $m' \equiv 0 \pmod 4$.
$-3x,\ 4y,\ 0,\ 2y,\ 0,\ 4y.$

V_2. $v = 5$, f even, $m' \equiv 2 \pmod 4$.
$x,\ 0,\ 2x,\ -6y,\ -2x,\ 0.$

For f odd the corresponding formulas are obtained as follows.

I. Replace m by $m+3 \pmod 6$, m' by $m'+2 \pmod 4$, i by $i+6 \pmod{12}$.

II. Replace m' by $m'+2 \pmod 4$, c by $-c$, i by $i+6 \pmod{12}$.

III. Replace m' by $m'+2 \pmod 4$, c by $-c$.

IV. Replace m by $m+3 \pmod 6$.

V. Replace m' by $m'+2 \pmod 4$, i by $i+6 \pmod{12}$.

The formulas for $b(i,3)$ yield the following criterion for determining the sign of c. Let x and y be determined by (4.4) and (4.5). For f even and $m' \equiv 0 \pmod 4$, $c = \pm 1$ according as $3b(1,3) = \pm 2y$; for f even and $m' \equiv 2 \pmod 4$, $c = \pm\beta^3$ according as $3b(1,3) = \pm x$; for f odd and $m' \equiv 0 \pmod 4$, $c = \pm\beta^3$ according as $3b(1,3) = \mp x$; for f odd and $m' \equiv 2 \pmod 4$, $c = \pm 1$ according as $3b(1,3) = \mp 2y$.

Lemma 1 provides a technique for finding constants α, β, γ, δ, ε such that

$$144(i,j)_{12} = p+\alpha A+\beta B+\gamma x+\delta y+\varepsilon$$

for all the cyclotomic numbers $(i,j)_{12}$. We now have on hand all the necessary machinery for making the computations. To illustrate the method we give the derivation of the formula

$$144(3,1)_{12} = p+1+4A-12B+6x+24y, \tag{5.13}$$

which is valid for f odd, $m' \equiv 0 \pmod 4$, $m \equiv 1 \pmod 6$, $c = -\beta^3$. By (2.21) and (2.22) we have $144(3,1)_{12} = 36(3,1)_6+36s(3,1)+36s(9,1)+{}+72s(7,9)$. From Table II in § 6 we obtain $36(3,1)_6 = p+1-2A-6B$. To compute $36s(3,1)+36s(9,1)$ we use the Corollary of Theorem 1. In (3.7) put $i = 3$, $j = 1$. The six consecutive terms in the sum $3\sum_{v=0}^{5} b(1+6v,\ 2v)$ are $0,\ A+3B+2y,\ 0,\ 0,\ x,\ 6y$. By Theorem 2, $3S'(3,1) = -6C(9,3) = 6b(3,2)+6b(3,3) = (-4A+4y)+4x$. By Theorem 5, $3T'(3,1) = -12y$. Finally, to compute $36s(7,9)$ we use Theorem 1. In (3.1) put $i = 7$, $j = 9$. The twelve consecutive terms in the sum $3\sum_{v=0}^{11} b(9+7v,\ v)$ are $0,\ -x,\ A-3B+2y,\ 1-4y,\ 0,\ 2x,\ 6y,\ 1+2A,\ x,\ x,\ 6y,\ 0$. By Theorem 3, $3S(7,9) = 3D(7,3)-3C(5,3) = 3b(4,2)+3b(11,2)+3b(10,3)+3b(11,3) = x+(A-3B+2y)+(1+2y)-x$. By Theorem 4, $3T(7,9) = -3-3x-6y$. Combining the results in this paragraph we get (5.13).

The smallest prime which may be used to check (5.13) is $p = 181$. From Jacobi's Canon Arithmeticus [8] we find that $g = 2$ (the smallest primitive root), $m = 1$, $m' = 56$. Computing x, y, A, B by means of (4.4), (4.5), (4.6), (4.7) we get $x = 9$, $y = -5$, $A = 13$, $B = 2$. We get also $b(1,3) = 3$ so that $c = -\beta^3$. The value of $(3,1)_{12} = 1$. It is now easy to verify (5.13).

We remark finally that in the application of Lemma 1 the value of $t(i,j)$ is sometimes easily obtained. Indeed, by (2.1) $t(i,j)$ is equal to 0 when f is even and $j = E$, and also when f is odd and $j = 0$.

6. Tables of the cyclotomic constants of order twelve. In the application of Lemma 1 for $e = 12$, $E = 6$ the value of $(i,j)_6$ is required. Tables I and II give the values of the cyclotomic numbers of order six for primes $p = 12f+1$. Table I expresses the 36 constants $(i,j)_6$, $i,j = 0,1,\ldots,5$ in terms of 10 where $(i,j)_6$ is in row i and column j.

TABLE I

	0	1	2	3	4	5
0	00	01	02	03	04	05
1	01	05	12	13	14	12
2	02	12	04	14	24	13
3	03	13	14	03	13	14
4	04	14	24	13	02	12
5	05	12	13	14	12	01

The values of the 10 basic constants are expressible in terms of p, A, B and depend on the cubic character of 2 modulo p (compare [4], p. 408-410). These values are given in Table II. As usual, the integer m is selected so that $g^m \equiv 2 \pmod{p}$.

TABLE II

	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
36(0,0)	$p-17-20A$	$p-17-8A+6B$	$p-17-8A-6B$
36(0,1)	$p-5+4A+18B$	$p-5+4A+12B$	$p-5+4A+6B$
36(0,2)	$p-5+4A+6B$	$p-5+4A-6B$	$p-5-8A$
36(0,3)	$p-5+4A$	$p-5+4A-6B$	$p-5+4A+6B$
36(0,4)	$p-5+4A-6B$	$p-5-8A$	$p-5+4A+6B$
36(0,5)	$p-5+4A-18B$	$p-5+4A-6B$	$p-5+4A-12B$
36(1,2)	$p+1-2A$	$p+1-2A-6B$	$p+1-2A+6B$
36(1,3)	$p+1-2A$	$p+1-2A-6B$	$p+1-2A-12B$
36(1,4)	$p+1-2A$	$p+1-2A+12B$	$p+1-2A+6B$
36(2,4)	$p+1-2A$	$p+1+10A+6B$	$p+1+10A-6B$

Precise determinations of A and B are given by the formulas

$$A = 6(0,3)_6-6(1,2)_6+1, \qquad B = (0,1)_6-(0,5)_6-(1,3)_6+(1,4)_6,$$

which follow from Table II itself.

The 144 constants $(i,j)_{12}$ with $i,j = 0,1,\ldots,11$ have at most 31 different values for a given p. Tables III and IV, which follow, summarize the relations between the constants. In these tables the entry in row i and column j is equal to $(i,j)_{12}$. The number 10 is indicated by the letter X and the number 11 by the letter Y.

The author has employed the method described in § 5 to calculate all possible formulas for the $(i,j)_{12}$. These formulas are expressible in terms of p, x, y, A, B where the signs of x and A are such that $x \equiv 1 \pmod 4$ and $A \equiv 1 \pmod 6$. It is convenient to prove at this point that there are essentially twelve different sets of formulas depending on the parity of f, the sextic residue character of 2 modulo p, the biquadratic character of 3 modulo p, and the value of c.

TABLE III

f even

	0	1	2	3	4	5	6	7	8	9	10	11
0	00	01	02	03	04	05	06	07	08	09	0X	0Y
1	01	0Y	12	13	14	15	16	17	18	19	1X	12
2	02	12	0X	1X	24	25	26	27	28	29	24	13
3	03	13	1X	09	19	29	36	37	38	36	25	14
4	04	14	24	19	08	18	28	38	48	37	26	15
5	05	15	25	29	18	07	17	27	37	38	27	16
6	06	16	26	36	28	17	06	16	26	36	28	17
7	07	17	27	37	38	27	16	05	15	25	29	18
8	08	18	28	38	48	37	26	15	04	14	24	19
9	09	19	29	36	37	38	36	25	14	03	13	1X
10	0X	1X	24	25	26	27	28	29	24	13	02	12
11	0Y	12	13	14	15	16	17	18	19	1X	12	01

TABLE IV

f odd

	0	1	2	3	4	5	6	7	8	9	10	11
0	00	01	02	03	04	05	06	07	08	09	0X	0Y
1	10	11	12	13	14	15	07	05	15	19	1X	1Y
2	20	21	22	23	24	19	08	15	04	14	24	2Y
3	30	31	32	30	2Y	1X	09	19	14	03	13	23
4	22	32	42	31	20	1Y	0X	1X	24	13	02	12
5	11	21	31	32	21	10	0Y	1Y	2Y	23	12	01
6	00	10	20	30	22	11	00	10	20	30	22	11
7	10	0Y	1Y	2Y	23	12	01	11	21	31	32	21
8	20	1Y	0X	1X	24	13	02	12	22	32	42	31
9	30	2Y	1X	09	19	14	03	13	23	30	31	32
10	22	23	24	19	08	15	04	14	24	2Y	20	21
11	11	12	13	14	15	07	05	15	19	1X	1Y	10

For any e, f replace g by a new primitive root g^r, where $(r, p-1) = 1$. By (1.1) $(i,j)_e$ becomes $(ri, rj)_e$. By (2.3) $\psi(\beta^m, \beta^n)$ becomes $\psi(\beta^{m\bar{r}}, \beta^{n\bar{r}})$, where $r\bar{r} \equiv 1 \pmod{e}$.

We now return to the particular case $e = 12$, where we have $r = \bar{r}$. For $r = 5$, we deduce from (4.1) that x, y, A are unaltered while B changes sign. Moreover, by (5.7) and (5.9), c is unaltered. The symbol (i, j) becomes $(5i, 5j)$, m is replaced by $-m$ modulo 6, and m' is unaltered modulo 4. Hence, from tables in which $m \equiv 1$ or $2 \pmod 6$ (Tables 1 to 6) we may deduce corresponding tables in which $m \equiv 5$ or $4 \pmod 6$ respectively.

When $r = 7$, x, A, B are unaltered, y changes sign, m is unaltered modulo 6, m' is unaltered modulo 4, and (i, j) becomes $(7i, 7j)$. By (2.4), (2.13), (2.14) and (v) of Lemma 2 we may establish the identity

$$\psi(\beta^5, \beta)\psi(\beta^9, \beta^7) = (-1)^f \beta^{3m'} \psi(\beta^3, \beta)\psi(\beta^{11}, \beta^7).$$

TABLE 1

	f even, $m' \equiv 2 \pmod 4$, $c = \beta^3$, $m \equiv 2 \pmod 6$
144(0,0)	$p-35-2A+12B+48y$
144(0,1)	$p-11+2A+12B+12x-16y$
144(0,2)	$p-11-4A+6x-16y$
144(0,3)	$p-11+22A+12B$
144(0,4)	$p-11+10A-12B-12x$
144(0,5)	$p-11-4A-24B+6x+8y$
144(0,6)	$p-11-10A-12B-16y$
144(0,7)	$p-11+10A-12B-12x$
144(0,8)	$p-11-20A+6x$
144(0,9)	$p-11-10A+12B+32y$
144(0,10)	$p-11+2A+12B+12x-16y$
144(0,11)	$p-11+4A-18x-24y$
144(1,2)	$p+1-4A-6x+8y$
144(1,3)	$p+1+2A-24B+8y$
144(1,4)	$p+1-4A+12B-6x+32y$
144(1,5)	$p+1-8A+12B+6x$
144(1,6)	$p+1+2A+12B+8y$
144(1,7)	$p+1+8A-12B+6x+8y$
144(1,8)	$p+1+8A+12B+6x-16y$
144(1,9)	$p+1-2A-12B+12x$
144(1,10)	$p+1-4A-12B-6x-16y$
144(2,4)	$p+1+8A-12B+6x+8y$
144(2,5)	$p+1-10A+12B-12x-16y$
144(2,6)	$p+1-4A-6x+8y$
144(2,7)	$p+1-4A-6x+8y$
144(2,8)	$p+1+2A+12B+8y$
144(2,9)	$p+1+8A+24B+6x+8y$
144(3,6)	$p+1+2A-16y$
144(3,7)	$p+1+2A-24B+8y$
144(3,8)	$p+1-8A+6x-24y$
144(4,8)	$p+1+16A+12B-18x-24y$

TABLE 2

	f odd, $m' \equiv 0 \pmod 4$, $c = \beta^3$, $m \equiv 1 \pmod 6$
144(0,0)	$p-23-6A-16y$
144(0,1)	$p+1+4A+24B-18x-24y$
144(0,2)	$p+1-2A-24B-12x$
144(0,3)	$p+1+18A+32y$
144(0,4)	$p+1-12A+6x-16y$
144(0,5)	$p+1-2A-24B-12x$
144(0,6)	$p+1-14A+24B+48y$
144(0,7)	$p+1+12A+6x+8y$
144(0,8)	$p+1+6A+12x-16y$
144(0,9)	$p+1-14A$
144(0,10)	$p+1+4A+6x$
144(0,11)	$p+1+6A+12x-16y$
144(1,0)	$p-11+12B+6x+8y$
144(1,1)	$p-11+6A+8y$
144(1,2)	$p+1-12A+6x-16y$
144(1,3)	$p+1+4A-12B+6x-24y$
144(1,4)	$p+1+6A+36B-12x-16y$
144(1,5)	$p+1-12B-6x+8y$
144(1,9)	$p+1-12A+12B+6x+8y$
144(1,10)	$p+1-6A+8y$
144(1,11)	$p+1+4A+6x$
144(2,0)	$p-11+6A+8y$
144(2,1)	$p+1-12B-6x+8y$
144(2,2)	$p-11-12A-6x+8y$
144(2,3)	$p+1-6A+8y$
144(2,4)	$p+1+12A+6x+8y$
144(2,11)	$p+1-24B-6x-16y$
144(3,0)	$p-11+6A-12B-16y$
144(3,1)	$p+1-6x+32y$
144(3,2)	$p+1-2A+12B+12x$
144(4,2)	$p+1+4A+24B-18x-24y$

Therefore c changes sign when f is even and $m' \equiv 2 \pmod 4$ or when f is odd and $m' \equiv 0 \pmod 4$. Otherwise c is unaltered. Hence, from tables in which f is even and $m' \equiv 2 \pmod 4$ or f is odd and $m' \equiv 0 \pmod 4$ (Tables 1, 2, 7, 8) we may deduce corresponding tables in which c is replaced by $-c$.

By compounding the results for $r = 5$ and $r = 7$, results for $r = 11$ may be deduced. We find for $r = 11$ that x, A are unaltered, y, B change sign, m is replaced by $-m$ modulo 6, m' is unaltered modulo 4, (i, j) becomes $(-i, -j)$, and c changes sign under the same circumstances as when $r = 7$.

It was shown in § 5 that the primes have to be divided into twenty-four classes with different formulas holding for different classes. In view of the results in the last three paragraphs it suffices to compile tables for just twelve of these classes (see Tables 1 to 12).

Our results also enable us to condense the tables to a certain extent. Tables 1, 2 contain the formulas for the 31 basic constants. However, in tables in which f is even, $m' \equiv 0 \pmod 4$ or in which f is odd, $m' \equiv 2 \pmod 4$, the formula for $(7i, 7j)$ is the same as the formula for (i, j) except that y is replaced by $-y$. Again, in tables in which $m \equiv 0$ or $3 \pmod 6$

TABLE 3

	f even, $m' \equiv 0 \pmod 4$, $c = 1$, $m \equiv 2 \pmod 6$
144(0,0)	$p-35-26A+12B-36x$
144(0,1)	$p-11+2A+12B+8x+48y$
144(0,2)	$p-11+4A+24B+6x$
144(0,3)	$p-11+14A+12B-4x$
144(0,4)	$p-11+10A-12B$
144(0,5)	$p-11-4A-24B+14x+24y$
144(0,6)	$p-11-2A-12B+12x$
144(0,8)	$p-11-20A-18x$
144(0,10)	$p-11+10A-12B$
144(1,2)	$p+1-2x$
144(1,3)	$p+1-6A+4x$
144(1,4)	$p+1-4A+12B+2x-24y$
144(1,5)	$p+1-4A+12B+2x-24y$
144(1,6)	$p+1+6A-8x$
144(1,7)	$p+1+12A-14x$
144(1,9)	$p+1+2A-24B-4x$
144(1,10)	$p+1-2x$
144(2,4)	$p+1+4A-12B-6x$
144(2,6)	$p+1-8A-12B+6x$
144(2,8)	$p+1-2A+24B$
144(3,6)	$p+1-6A+4x$
144(4,8)	$p+1+28A+12B+18x$

TABLE 4

	f even, $m' \equiv 0 \pmod 4$, $c = -1$, $m \equiv 2 \pmod 6$
144(0,0)	$p-35+22A+12B+12x$
144(0,1)	$p-11+10A-12B$
144(0,2)	$p-11-12A-24B-10x$
144(0,3)	$p-11-2A+12B+12x$
144(0,4)	$p-11+10A-12B$
144(0,5)	$p-11+4A+6x-24y$
144(0,6)	$p-11-18A-12B-4x$
144(0,8)	$p-11-20A-18x$
144(0,10)	$p-11-6A+36B-16x$
144(1,2)	$p+1-8A+6x$
144(1,3)	$p+1-2A-12B-24y$
144(1,4)	$p+1-8A+6x$
144(1,5)	$p+1+4A+12B-6x-24y$
144(1,6)	$p+1-2A+24B$
144(1,7)	$p+1+4A-24B-6x$
144(1,9)	$p+1-2A-12B-24y$
144(1,10)	$p+1+4A+12B-6x+24y$
144(2,4)	$p+1+12A-12B+2x$
144(2,6)	$p+1+12B+14x$
144(2,8)	$p+1+6A+8x$
144(3,6)	$p+1+10A-12x$
144(4,8)	$p+1+4A+12B-6x$

TABLE 5

	f odd, $m' \equiv 2\,(\mathrm{mod}\,4)$, $c = 1$, $m \equiv 1\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-23-14A+12x$
$144(0,1)$	$p+1+12A+14x-24y$
$144(0,2)$	$p+1-2A-24B$
$144(0,3)$	$p+1-6A-4x$
$144(0,4)$	$p+1-20A+24B+6x$
$144(0,5)$	$p+1+6A+8x-48y$
$144(0,6)$	$p+1+10A+24B-36x$
$144(0,8)$	$p+1-2A-24B$
$144(0,10)$	$p+1+4A-18x$
$144(1,0)$	$p-11-4A+24B-14x$
$144(1,1)$	$p-11+2A-12B-8x$
$144(1,2)$	$p+1+2x+24y$
$144(1,3)$	$p+1+2x+24y$
$144(1,4)$	$p+1+2A+24B+4x$
$144(1,5)$	$p+1-4A-12B-2x$
$144(1,9)$	$p+1-4A-12B-2x$
$144(1,10)$	$p+1-6A-4x$
$144(2,0)$	$p-11+10A+12B$
$144(2,2)$	$p-11-8A-12B+6x$
$144(2,4)$	$p+1+16A-6x$
$144(3,0)$	$p-11+14A-12B+4x$
$144(4,2)$	$p+1-8A+24B+18x$

TABLE 6

	f odd, $m' \equiv 2\,(\mathrm{mod}\,4)$, $c = -1$, $m \equiv 1\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-23+2A-4x$
$144(0,1)$	$p+1+4A+24B+6x+24y$
$144(0,2)$	$p+1-2A-24B$
$144(0,3)$	$p+1+10A+12x$
$144(0,4)$	$p+1-4A-24B-10x$
$144(0,5)$	$p+1-2A-24B$
$144(0,6)$	$p+1-38A+24B+12x$
$144(0,8)$	$p+1+14A+24B-16x$
$144(0,10)$	$p+1+4A-18x$
$144(1,0)$	$p-11+4A-6x$
$144(1,1)$	$p-11+10A+12B$
$144(1,2)$	$p+1-8A-6x+24y$
$144(1,3)$	$p+1+4A-12B+6x$
$144(1,4)$	$p+1-2A+12B+24y$
$144(1,5)$	$p+1+4A-12B+6x$
$144(1,9)$	$p+1-8A-6x-24y$
$144(1,10)$	$p+1-2A+12B+24y$
$144(2,0)$	$p-11+2A-12B+8x$
$144(2,2)$	$p-11-16A+12B+14x$
$144(2,4)$	$p+1+8A+2x$
$144(3,0)$	$p-11-2A-12B-12x$
$144(4,2)$	$p+1+16A+24B-6x$

TABLE 7

	f even, $m' \equiv 2\,(\mathrm{mod}\,4)$, $c = \beta^3$, $m \equiv 0\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-35-32A+18x+48y$
$144(0,1)$	$p-11+2A+36B+12x-16y$
$144(0,2)$	$p-11+2A+12B+12x-16y$
$144(0,3)$	$p-11+16A-6x-24y$
$144(0,4)$	$p-11+10A+12B-12x$
$144(0,6)$	$p-11-16A-6x-16y$
$144(0,7)$	$p-11+10A+12B-12x$
$144(0,9)$	$p-11-16A-6x+56y$
$144(1,2)$	$p+1+2A+8y$
$144(1,3)$	$p+1+2A-24B+8y$
$144(1,4)$	$p+1+2A+8y$
$144(1,5)$	$p+1-14A-24y$
$144(1,6)$	$p+1+2A+12B+8y$
$144(1,8)$	$p+1+2A+8y$
$144(1,9)$	$p+1-2A+12B+12x$
$144(1,10)$	$p+1-10A-12B-12x-16y$
$144(2,4)$	$p+1+2A+8y$
$144(2,6)$	$p+1+2A+12B+8y$
$144(3,6)$	$p+1+8A+6x-16y$
$144(4,8)$	$p+1-14A-24y$

TABLE 8

	f odd, $m' \equiv 0\,(\mathrm{mod}\,4)$, $c = \beta^3$, $m \equiv 3\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-23-24A-6x-16y$
$144(0,1)$	$p+1-2A+24B-12x$
$144(0,2)$	$p+1-2A+24B-12x$
$144(0,3)$	$p+1+24A-6x+56y$
$144(0,4)$	$p+1+6A+12x-16y$
$144(0,6)$	$p+1-8A+18x+48y$
$144(0,7)$	$p+1+6A+12x-16y$
$144(0,9)$	$p+1-8A-6x-24y$
$144(1,0)$	$p-11+6A+24B+8y$
$144(1,2)$	$p+1-6A+8y$
$144(1,3)$	$p+1-2A-12B+12x$
$144(1,4)$	$p+1+6A+12B-12x-16y$
$144(1,5)$	$p+1-6A+8y$
$144(1,9)$	$p+1-6A+24B+8y$
$144(1,10)$	$p+1-6A+8y$
$144(1,11)$	$p+1+10A-24y$
$144(2,0)$	$p-11+6A+8y$
$144(2,4)$	$p+1-6A+8y$
$144(3,0)$	$p-11+6x-16y$
$144(4,2)$	$p+1+10A-24y$

the formula for $(5i, 5j)$ is the same as the formula for (i, j) except that B is replaced by $-B$. Consequently, it suffices to list 22 of the 31 basic constants in Tables 3 to 6, 20 of the constants in Tables 7, 8 and 15 of the constants in Tables 9 to 12.

TABLE 9

	f even, $m' \equiv 0\,(\mathrm{mod}\,4)$, $c = 1$, $m \equiv 0\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-35-56A-54x$
$144(0,1)$	$p-11+2A+36B+8x+48y$
$144(0,2)$	$p-11+10A+36B$
$144(0,3)$	$p-11+8A+2x+24y$
$144(0,4)$	$p-11+10A+12B$
$144(0,6)$	$p-11-8A+18x$
$144(1,2)$	$p+1+6A-8x$
$144(1,3)$	$p+1-6A+4x$
$144(1,4)$	$p+1+2A-4x$
$144(1,5)$	$p+1-10A+8x$
$144(1,6)$	$p+1+6A-8x$
$144(2,4)$	$p+1-2A$
$144(2,6)$	$p+1-2A$
$144(3,6)$	$p+1-2x$
$144(4,8)$	$p+1-2A$

TABLE 10

	f even, $m' \equiv 0\,(\mathrm{mod}\,4)$, $c = -1$, $m \equiv 0\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-35-8A-6x$
$144(0,1)$	$p-11+10A+12B$
$144(0,2)$	$p-11-6A-12B-16x$
$144(0,3)$	$p-11-8A+18x+24y$
$144(0,4)$	$p-11+10A+12B$
$144(0,6)$	$p-11-24A+2x$
$144(1,2)$	$p+1-2A$
$144(1,3)$	$p+1-2A-12B-24y$
$144(1,4)$	$p+1-2A-12B+24y$
$144(1,5)$	$p+1-2A$
$144(1,6)$	$p+1-2A+24B$
$144(2,4)$	$p+1+6A+8x$
$144(2,6)$	$p+1+6A+24B+8x$
$144(3,6)$	$p+1+16A-18x$
$144(4,8)$	$p+1-26A-24x$

TABLE 11

	f odd, $m' \equiv 2\,(\mathrm{mod}\,4)$, $c = 1$, $m \equiv 3\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-23-32A+18x$
$144(0,1)$	$p+1+6A+8x-48y$
$144(0,2)$	$p+1-2A+24B$
$144(0,3)$	$p+1+2x-24y$
$144(0,4)$	$p+1-2A+24B$
$144(0,6)$	$p+1+16A-54x$
$144(1,0)$	$p-11+2A+36B-8x$
$144(1,2)$	$p+1+6A+8x$
$144(1,3)$	$p+1-6A-4x$
$144(1,4)$	$p+1+2A+4x$
$144(1,5)$	$p+1-10A-8x$
$144(2,0)$	$p-11+10A+12B$
$144(2,4)$	$p+1-2A$
$144(3,0)$	$p-11+8A-2x$
$144(4,2)$	$p+1-2A$

TABLE 12

	f odd, $m' \equiv 2\,(\mathrm{mod}\,4)$, $c = -1$, $m \equiv 3\,(\mathrm{mod}\,6)$
$144(0,0)$	$p-23-16A+2x$
$144(0,1)$	$p+1-2A+24B$
$144(0,2)$	$p+1-2A+24B$
$144(0,3)$	$p+1+16A+18x-24y$
$144(0,4)$	$p+1+14A-24B-16x$
$144(0,6)$	$p+1-32A-6x$
$144(1,0)$	$p-11+10A+12B$
$144(1,2)$	$p+1-2A$
$144(1,3)$	$p+1-2A-12B-24y$
$144(1,4)$	$p+1-2A-12B+24y$
$144(1,5)$	$p+1-2A$
$144(2,0)$	$p-11+2A-12B+8x$
$144(2,4)$	$p+1-10A+8x$
$144(3,0)$	$p-11-8A-18x$
$144(4,2)$	$p+1+22A-24x$

The following application of the tables is of interest. For integers a, b the number $N_e(a, b)$ of solutions of the congruence $ax^e+by^e \equiv 1 \pmod p$ may be expressed in terms of the cyclotomic numbers $(i, j)_e$

(see e. g. [4], p. 396-399). Hence tables for the numbers $N_e(a, b)$ may be deduced from the corresponding tables for the numbers $(i, j)_e$. We confine ourselves to a single illustrative example. In the special case $a = 1$, $b = 1$ a theorem of Dickson ([4], Theorem 2) states that the number of solutions prime to $p = ef+1$ is $e^2(0,0)$, and the number of all solutions is $2e+e^2(0,0)$. It follows from Table 7 that if 2 is a cubic residue of p and 3 is a quadratic residue (but not a biquadratic residue) of p, then the congruence

$$x^{12}+y^{12} \equiv 1 \,(\mathrm{mod}\, p = 12f+1) \qquad (f \text{ even})$$

has $p-35-32A+18x\pm 48y$ solutions prime to p and $p-11-32A+18x \pm 48y$ solutions in all. Here the coefficient of y is ± 48 according as $c = \pm\beta^3$.

7. Application to residue difference sets. By a difference set having modulus v, order k and multiplicity λ is meant a set of k distinct residues $r_1, r_2, \ldots, r_k \,(\mathrm{mod}\, v)$ such that the congruence $r_i - r_j \equiv d \,(\mathrm{mod}\, v)$ has exactly λ solutions for each $d \not\equiv 0 \,(\mathrm{mod}\, v)$. In [6] there is given a survey of all known difference sets. Residue difference sets are difference sets composed of eth power residues modulo a prime p. Let $p = ef+1$. It is known [9] that there exists no residue difference set for e odd, or for e even and f even. In the remaining case the following criterion ([9], Theorem 3) is applicable: If e is even and $f = (p-1)/e$ is odd, then a necessary and sufficient condition for the set of eth power residues modulo p to form a difference set is that $(i, 0) = (f-1)/e$, $i = 0, 1, \ldots, \frac{1}{2}e-1$, where $(f-1)/e = \lambda$ is the multiplicity of the set.

The tables in § 6 provide data for applying the criterion stated in the previous paragraph. We shall prove the following theorem.

THEOREM 6. *The set of twelfth power residues modulo a prime $p = 12f+1$ cannot form a difference set.*

Proof. To apply the criterion when $e = 12$ and f is odd we have to consider twelve possible cases. In each of the six cases covered by the tables we first sketch a proof that no difference set exists.

Table 2. $(2,0) = (4,0)$ implies $x = -3A$. $144(0,0) = 144(5,0) = p-13$ implies $A = 1$, $y = -1$. Hence $x = -3$ and $p = 13$. This is a degenerate example since the only twelfth power residue modulo 13 is $r = 1$ so that $\lambda = 0$.

Table 5. $(3,0) = (4,0) = (5,0)$ implies $A = 0$.

Table 6. $(2,0) = (3,0) = (4,0) = (5,0)$ implies $x = 0$.

Table 8. $(1,0) = (5,0)$ implies $B = 0$.

Tables 11, 12. $(2,0) = (4,0)$ implies $B = 0$.

To prove the theorem in the remaining six cases we proceed as follows.

The argument in a case where f is odd and $m \equiv 5 \,(\mathrm{mod}\, 6)$ is the same as the argument in the corresponding case where f is odd and $m \equiv 1 \,(\mathrm{mod}\, 6)$ except that $(i, 0)$ is replaced by $(5i, 0)$ and B is replaced by $-B$. In a case where f is odd and $m' \equiv 0 \,(\mathrm{mod}\, 4)$ the argument for $c = -\beta^3$ is the same as the corresponding argument for $c = \beta^3$ except that y is replaced by $-y$. This completes the proof.

A modified residue difference set is one in which zero is counted as a residue. It is known [9] that such difference sets cannot exist for e odd or for e even and f even. Emma Lehmer [9] has proved that if e is even and $f = (p-1)/e$ is odd, then a necessary and sufficient condition for the set of eth power residues and zero to be a difference set is that $1+(0,0) = (i, 0) = (f+1)/e$, $i = 1, 2, \ldots, \frac{1}{2}e-1$, where $(f+1)/e = \lambda$ is the multiplicity of the set. With the aid of this criterion we now prove

THEOREM 7. *The set of twelfth power residues and zero modulo a prime $p = 12f+1$ cannot form a difference set.*

Proof. As in the proof of Theorem 6 we consider twelve possible cases. Except for the analysis of Table 2 the discussion is the same in all of these cases. Turning to table 2 we find that $(2,0) = (4,0)$ implies $x = -3A$. The condition $144+144(0,0) = 144(5,0) = p+11$ implies $A = -11$, $y = 11$. Hence $x = 33$. This leads to the absurd conclusion that p is divisible by 11. The proof is thus complete.

References

[1] P. Bachmann, *Die Lehre von der Kreisteilung*, zweite Aufl., Leipzig und Berlin, 1921.

[2] R. H. Bruck, *Computational aspects of certain combinatorial problems*, The Proceedings of the Symposia in Applied Mathematics, American Mathematical Society, Providence, 6 (1956), p. 31-43.

[3] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1934), p. 151-182.

[4] L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. 57 (1935), p. 391-424.

[5] — *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), p. 363-380.

[6] Marshall Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc. 7 (1956), p. 975-986.

[7] C. G. Jacobi, *Ueber die Kreisteilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math. 30 (1846), p. 166-182; or Gesammelte Werke 6 (1891), p. 254-274.

[8] — *Canon Arithmeticus*, Berlin 1956.

[9] E. Lehmer, *On residue difference sets*, Can. J. Math. 5 (1953), p. 425-432.

[10] A. L. Whiteman, *Finite Fourier series and equations in finite fields*, Trans. Amer. Math. Soc. 74 (1953), p. 78-98.

[11] A. L. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), p. 401-413.

[12] — *The cyclotomic numbers of order ten*, The Proceedings of the Symposia in Applied Mathematics, American Mathematical Society, Providence, 10 (1960), in preparation.

THE INSTITUTE FOR ADVANCED STUDY
and
UNIVERSITY OF SOUTHERN CALIFORNIA

Reçu par la Rédaction le 19. 10. 1959

ACTA ARITHMETICA
VI (1960)

Remarks on number theory III

On addition chains

by

P. Erdös (Budapest)

Consider a sequence $a_0 = 1 < a_1 < a_2 < \ldots < a_k = n$ of integers such that every a_l $(l \geqslant 1)$ can be written as the sum $a_i + a_j$ of two preceding elements of the sequence. Such a sequence has been called by A. Scholz [1] an *addition chain*. He defines $l(n)$ as the smallest k for which there exists an addition chain $1 = a_0 < a_1 < \ldots < a_k = n$.

Clearly $l(n) \geqslant \log n / \log 2$, the equality occurring only if $n = 2^u$. Scholz conjectured that

$$\lim_{n\to\infty} l(n) \frac{\log 2}{\log n} = 1 \tag{1}$$

and A. Brauer [2] proved (1). In fact Brauer proved that

$$l(n) \leqslant \min_{1\leqslant r\leqslant m} \left\{\left(1+\frac{1}{r}\right)\frac{\log n}{\log 2} + 2^r - 2\right\} \tag{2}$$

where $2^m \leqslant n < 2^{m+1}$. From (2) by choosing $r = \left[(1-\varepsilon)\dfrac{\log\log n}{\log 2}\right]$ it follows that

$$l(n) < \frac{\log n}{\log 2} + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right). \tag{3}$$

In the present note I am going to prove that (3) is the best possible. In fact I shall prove the following

Theorem. *For almost all n (i. e. for all n except a sequence of density 0)*

$$l(n) = \frac{\log n}{\log 2} + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right).$$

[1] Jahresbericht der Deutschen Math. Vereinigung 47 (1937), p. 41.

[2] Bull. Amer. Math. Soc. 45 (1939), p. 736-739.