Internat. J. Math. & Math. Sci.
Vol. 10 No. 1 (1987) 113-123

ON THE COMPLEMENTARY FACTOR IN A NEW CONGRUENCE ALGORITHM

PETER HILTON

Department of Mathematical Sciences
University Center at Binghamton
State University of New York
Binghamton, New York 13901 U.S.A.

JEAN PEDERSEN

Department of Mathematics
Santa Clara University
Santa Clara, CA 95053 U.S.A.

(Received April 17, 1986)

ABSTRACT. In an earlier paper the authors described an algorithm for determining the quasi-order, $Q_t(b)$, of t mod b, where t and b are mutually prime. Here $Q_t(b)$ is the smallest positive integer n such that $t^n \equiv \pm 1$ mod b, and the algorithm determined the sign $(-1)^\varepsilon$, $\varepsilon = 0, 1$, on the right of the congruence. In this sequel we determine the complementary factor F such that $t^n - (-1)^\varepsilon = bF$, using the algorithm rather that b itself. Thus the algorithm yields, from knowledge of b and t, a rectangular array

$$\left|\begin{matrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_r \end{matrix}\right|$$

The second and third rows of this array determine $Q_t(b)$ and ε; and the last 3 rows of the array determine F. If the first row of the array is multiplied by F, we obtain a canonical array, which also depends only on the last 3 rows of the given array; and we study its arithmetical properties.

KEY WORDS AND PHRASES. Number theory, quasi-order, algorithm
1980 AMS SUBJECT CLASSIFICATIONS. 10A10, 10A30

0. INTRODUCTION.

Given $t, b \geq 2$, mutually prime, the quasi-order of t mod b, written $Q_t(b)$, is the smallest positive integer k such that $t^k \equiv \pm 1$ mod b. We have described in [HP] two algorithms for determining $Q_t(b)$ and for deciding whether $t^{Q_t(b)} \equiv +1$ mod b or $t^{Q_t(b)} \equiv -1$ mod b. In fact, our algorithms provide us with a residue ε mod 2 such that $t^{Q_t(b)} \equiv (-1)^\varepsilon$ mod b. In this paper, which can be viewed as a sequel to [HP], we give an algorithm for determining the complementary factor F such that

$$t^{Q_t(b)} - (-1)^\varepsilon = bF, \tag{0.0}$$

and study F as a function of t and b. Of course, a conceptually simple algorithm for determining F would be to divide $t^{Q_t(b)} - (-1)^{\varepsilon}$ by b; however, our algorithm is based on a (reduced, contracted) <u>symbol</u> associated with b, and not on knowledge of b itself. This approach enables us to pursue the analysis of <u>canonical symbols</u> in Section 2. Such symbols may be viewed as generating the entire set of symbols.

Let us recall the ψ-algorithm from [HP] and the notion of a symbol. Given t,b as above, we define $\bar{S}$ to be the set of integers a satisfying

$$0 < a \leq \frac{b}{2}, \quad t \nmid a . \tag{0.1}$$

Given $a \in \bar{S}$, we consider the integers $qb + (-1)^{\varepsilon}a$, $\varepsilon = 0$ or 1, where $1 \leq q \leq \frac{t-1}{2}$ if t is odd; $1 \leq q \leq \frac{t}{2}$ if t is even and $\varepsilon = 1$; $1 \leq q \leq \frac{t}{2} - 1$ if t is even and $\varepsilon = 0$. We claim that, whether t is odd or even, there is exactly one value of q in the given ranges such that $t \mid qb + (-1)^{\varepsilon}a$ for some ε. We choose this value of q and thus define a function $a \mapsto a'$, where

$$qb + (-1)^{\varepsilon}a = t^k a', \; k \geq 1, \; t \nmid a' \tag{0.2}$$

Then the function $a \mapsto a'$ is a permutation ψ of $\bar{S}$. We regard ε as a residue mod 2 and define a <u>symbol</u> (or t-<u>symbol</u>)

$$b \left| \begin{matrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_2 \end{matrix} \right| t \tag{0.3}$$

by means of the system of equations

$$q_i b + (-1)^{\varepsilon_i} a_i = t^{k_i} a_{i+1}, \; i = 1,2,\ldots,r, \; a_{r+1} = a_1 . \tag{0.4}$$

Our notation for a symbol is more complete than in [HP], since there we included neither the q_i nor t in the notation.

We recall that $\gcd(b,a_i)$ is independent of i and we call (0.3) <u>reduced</u> if $\gcd(b,a_i) = 1$. We also call (0.3) <u>contracted</u> if there is no repetition among the a_i. The main theorem of [HP] was the following.

<u>Quasi-Order Theorem</u> <u>Let</u> (0.3) <u>be a reduced and contracted symbol</u>. <u>Let</u> $k = \Sigma k_i$, $\varepsilon = \Sigma \varepsilon_i$. <u>Then</u> k <u>is the quasi-order of</u> t <u>mod</u> b <u>and, indeed,</u> $t^k \equiv (-1)^{\varepsilon}$ <u>mod</u> b.

Actually, we have introduced a very slight change into the description of the algorithm compared with [HP]. For there we considered the set S of integers given by $0 < a < \frac{b}{2}$, $t \nmid a$, and the permutation ψ of S. By allowing $a = \frac{b}{2}$ we enlarge S to $\bar{S}$, the enlargement being actual only if b is even, t is odd. But then $\psi(\frac{b}{2}) = \frac{b}{2}$ and we obtain the new symbols

$$b \left| \begin{matrix} \frac{b}{2} & \cdots & \frac{b}{2} \\ 1 & \cdots & 1 \\ 0 & \cdots & 0 \\ \frac{t-1}{2} & \cdots & \frac{t-1}{2} \end{matrix} \right| t \qquad \text{(t odd, b even).} \tag{0.5}$$

We call such symbols <u>trivial</u>, and note that the only reduced and contracted trivial symbol, for a given odd t, is

$$2\;\begin{vmatrix} 1 \\ 1 \\ 0 \\ \frac{t-1}{2} \end{vmatrix}_{\,t} \quad (t\text{ odd}). \tag{0.6}$$

However, this symbol completes the Quasi-Order Theorem, which, in the version in [HP], excluded the case $b = 2$ and hence excluded the trivial fact that the quasi-order of t mod 2 is 1 if t is odd.

We base our algorithm for calculating the complementary factor, in Section 1, on the symbol (0.3) or, equivalently, the equations (0.4). Indeed, we construct a symbol

$$t^k-(-1)^{\varepsilon}\;\begin{vmatrix} A_1 & A_2 & \cdots & A_r \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_r \end{vmatrix}_{\,t} \tag{0.7}$$

from the data of the last 3 rows of (0.3). We show that there is <u>always</u> such a symbol for an arbitrary choice of positive integers $k_1, k_2, \ldots, k_r$; mod 2 residues $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$; and positive integers $q_1, q_2, \ldots, q_r$ subject to the conditions $1 \le q_i \le \frac{t-1}{2}$ if t is odd, $1 \le q_i \le \frac{t}{2}$ if t is even and $\varepsilon_i = 1$;

$$1 \le q_i \le \frac{t}{2} - 1 \text{ if } t \text{ is even and } \varepsilon_i = 0. \tag{0.8}$$

Indeed, there is then a unique symbol (0.7), which we call a <u>canonical</u> symbol. If the symbol (0.3) is given, then the symbols (0.3), (0.7) are related by the rule

$$(t^k - (-1)^{\varepsilon})a_i = bA_i, \tag{0.9}$$

showing that the complementary factor is any of the equivalent ratios $\frac{A_i}{a_i}$. However, since we calculate A_i simply as a function of the last 3 rows of (0.7), we may consider canonical symbols independently of their relation to the computation of the complementary factor. In fact, Section 2 is devoted to such a study of canonical symbols.

Suppose then that we <u>start</u> with a canonical symbol (0.7); such a symbol is not necessarily either reduced or contracted. Let $\gcd(t^k-(-1)^{\varepsilon}, A_i) = d$. Then we obtain from (0.7), by reducing and contracting, a symbol

$$\frac{t^k-(-1)^{\varepsilon}}{d}\;\begin{vmatrix} A_1/d & A_2/d & \cdots & A_s/d \\ k_1 & k_2 & \cdots & k_s \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_s \\ q_1 & q_2 & \cdots & q_s \end{vmatrix}_{\,t} \tag{0.10}$$

and <u>every reduced, contracted</u> t-<u>symbol is so obtained</u>. Writing $b' = \frac{t^k-(-1)^{\varepsilon}}{d}$, we then know that the quasi-order of t mod b' is $k' = k_1+k_2+\ldots+k_s$, and that $t^{k'} \equiv (-1)^{\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_s}$ mod b'.

1. THE COMPLEMENTARY FACTOR

We proceed to solve the set of equations (0.4) (in the 'unknowns' a_i)

$$q_i b + (-1)^{\varepsilon_i} a_i = t^{k_i} a_{i+1}, \quad i = 1,2,\ldots,r \ (a_{r+1} = a_1). \tag{1.1}$$

It will be convenient henceforth to regard the index i as belonging to the set of residues modulo r, so that we may, in practice, use any integer as an index. Now the determinant of the matrix of coefficients in the equations (1.1) is easily seen to be $\pm(t^k - (-1)^{\varepsilon})$, where

$$k = \sum_{i=1}^{r} k_i \ , \quad \varepsilon = \sum_{i=1}^{r} \varepsilon_i \ . \tag{1.2}$$

Thus the set of equations (1.1) has a unique solution, whatever values are given to $k_1,\ldots,k_r$ (subject to the restraint $k_i \geq 1$ stated in the Introduction); $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$; $q_1, q_2, \ldots, q_r$.

Our procedure is to set $B = t^k-(-1)^{\varepsilon}$ and solve the associated system of equations

$$q_i B + (-1)^{\varepsilon_i} A_i = t^{k_i} A_{i+1} \ , \ i = 1,2,\ldots,r \ ; \tag{1.3}$$

then the solution of (1.1) is given by

$$Ba_i = bA_i \ , \ i = 1,2,\ldots,r \tag{1.4}$$

Since the solution of the system (1.3) is unique, it suffices to find numbers $A_1, A_2, \ldots, A_r$ satisfying (1.3). We claim that the following values of these numbers do indeed satisfy (1.3). Thus we set

$$A_i = c_{i1} t^{k-k_{i-1}} + c_{i2} t^{k-k_{i-1}-k_{i-2}} + \ldots + c_{i,r-1} t^{k_i} + c_{ir} \ , \ i = 1,2,\ldots,r, \tag{1.5}$$

where

$$c_{is} = (-1)^{\varepsilon_{i-1}+\varepsilon_{i-2}+\ldots+\varepsilon_{i-s+1}} q_{i-s} \ , \ s = 1,2,\ldots,r. \tag{1.6}$$

To prove our claim, we first note that

$$c_{i1} = q_{i-1} \ , \ c_{ir} = (-1)^{\varepsilon+\varepsilon_i} q_i \ , \ c_{i+1,s+1} = (-1)^{\varepsilon_i} c_{is} \ ; \tag{1.7}$$

hence

$$q_i B + (-1)^{\varepsilon_i} A_i =$$
$$q_i(t^k-(-1)^{\varepsilon}) + (-1)^{\varepsilon_i}(c_{i1} t^{k-k_{i-1}} + c_{i2} t^{k-k_{i-1}-k_{i-2}} + \ldots + c_{i,r-1} t^{k_i} + c_{ir}),$$

while

$$t^{k_i} A_{i+1} = c_{i+1,1} t^k + c_{i+1,2} t^{k-k_{i-1}} + \ldots + c_{i+1,r} t^{k_i}$$
$$= q_i t^k + (-1)^{\varepsilon_i}(c_{i1} t^{k-k_{i-1}} + \ldots + c_{i,r-1} t^{k_i}) \ ,$$

by (1.7). Since, also by (1.7), we see that $q_i(-1)^{\varepsilon} = (-1)^{\varepsilon_i} c_{ir}$, it follows immediately that we have found a solution, and thus the unique solution, of the set of equations (1.3).

We are particularly interested in A_1. We will write A for A_1, so that

$$A = c_1 t^{k_1+\dots+k_{r-1}} + c_2 t^{k_1+\dots+k_{r-2}} + \dots + c_{r-1} t^{k_1} + c_r, \tag{1.8}$$

where

$$c_i = (-1)^{\varepsilon_r+\varepsilon_{r-1}+\dots+\varepsilon_{r-(i-2)}} q_{r-(i-1)} \ . \tag{1.9}$$

We have proved

<u>Theorem 1.1 Let</u>

$$b \left| \begin{matrix} a_1 & a_2 & \dots & a_r \\ k_1 & k_2 & \dots & k_r \\ \varepsilon_1 & \varepsilon_2 & \dots & \varepsilon_r \\ q_1 & q_2 & \dots & q_r \end{matrix} \right| t \qquad k = \sum k_i \ , \ \varepsilon = \sum \varepsilon_i \tag{1.10}$$

<u>be a reduced and contracted symbol</u>. <u>Then</u> k <u>is the quasi-order of</u> t <u>mod</u> b <u>and</u>

$$t^k \equiv (-1)^\varepsilon \ \underline{\text{mod}}\ b;$$

<u>moreover</u>

$$t^k - (-1)^\varepsilon = bF \ , \tag{1.11}$$

<u>where</u> $a_1 F = A$, <u>and</u> A <u>is given by</u> (1.8). <u>More generally</u>, $a_i F = A_i$, <u>where</u> A_i <u>is given by</u>(1.5).

Let us call a contracted symbol <u>normal</u> if $a_1 = 1$. We then have

<u>Corollary 1.2</u> <u>Let the symbol</u> (1.10) <u>be normal</u>. <u>Then the complementary factor</u> F <u>is</u> A <u>itself</u>,

$$t^k - (-1)^\varepsilon = bA \ ,$$

<u>where</u> A <u>is given by</u> (1.8).

<u>Examples</u> (i) Consider the normal symbol

$$641 \left| \begin{matrix} 1 & 5 & 159 & 241 & 25 & 77 & 141 & 125 & 129 \\ 7 & 2 & 1 & 4 & 3 & 2 & 2 & 2 & 9 \end{matrix} \right| 2$$

(of course, with $t = 2$, $\varepsilon_i = 1$, $q_i = 1$). Then $2^{2^5} + 1 = 2^{32} + 1 = 641A$, and

$$A = 2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^{10} + 2^9 - 2^7 + 1 = 6{,}700{,}417.$$

(ii) Consider the normal symbol

$$23 \left| \begin{matrix} 1 & 9 & 11 & 7 & 6 & 8 & 3 & 4 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & 2 & 2 & 1 & 2 & 1 & 1 & 2 & 1 \end{matrix} \right| 5$$

showing that $5^{11} \equiv -1 \bmod 23$. Then

$$5^{11} + 1 = 23A \ .$$

where

$$A = c_1 5^9 + c_2 5^7 + c_3 5^6 + c_4 5^5 + c_5 5^4 + c_6 5^3 + c_7 5^2 + c_8 5 + c_9 ,$$

and

$$\begin{aligned}
c_1 &= q_9 = 1 \\
c_2 &= (-1)^0 q_8 = 2 \\
c_3 &= (-1)^0 q_7 = 1 \\
c_4 &= (-1)^1 q_6 = -1 \\
c_5 &= (-1)^0 q_5 = 2 \\
c_6 &= (-1)^1 q_4 = -1 \\
c_7 &= (-1)^1 q_3 = -2 \\
c_8 &= (-1)^0 q_2 = 2 \\
c_9 &= (-1)^0 q_1 = 2.
\end{aligned}$$

Thus $A = 1953125 + 156250 + 15625 - 3125 + 1250 - 125 - 50 + 10 + 2 = 2122962$.

Of course, as this second example shows, it is frequently quicker, with a calculating device, simply to divide $t^k-(-1)^\varepsilon$ by b to obtain the complementary factor. However we wish to emphasize that we may define integers A_i by means of the equations (1.3), even if no symbol (0.3) had previously been considered. Thus we may specify the sequences $k_1, k_2, \ldots, k_r; \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r; q_1, q_2, \ldots, q_r$ subject to the appropriate constraints, and then set $B = t^k-(-1)^\varepsilon$ and determine the integers $A_1, A_2, \ldots, A_r$ by means of (1.3) or, equivalently,.(1.5). This becomes particularly relevant in view of the following theorem.

Theorem 1.4 *Given the sequences* $k_1, k_2, \ldots, k_r; \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r; q_1, q_2, \ldots, q_r$ *subject to the appropriate constraints, set* $B = t^k-(-1)^\varepsilon$. *Then there exists exactly one symbol*

$$B\left|\begin{matrix} A_1 & A_2 & \cdots & A_r \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_r \end{matrix}\right| t \tag{1.12}$$

and A_i *is given by* (1.5), $i = 1,2,\ldots,r$.

Proof The uniqueness is obvious. Thus the force of the theorem is that (1.12) *is* a symbol, that is, that

$$0 < A_i \le \frac{B}{2} ; \tag{1.13}$$

of course, it is clear from (1.5) that A_i is an integer.

To prove (1.13), we first observe that it is plain from (1.3) that if $A_i \le \frac{B}{2}$ for all i, then $A_i > 0$ for all i. Thus we have only to prove $A_i \le \frac{B}{2}$.

Assume first that t is odd. Then $q_i \le \frac{t-1}{2}$, so that, by (1.5),

$$A_i \le \frac{t-1}{2}(t^{k-1} + t^{k-2} + \ldots + 1) = \frac{t^k-1}{2} \le \frac{B}{2} .$$

Now assume t even. If $t = 2$, then $\varepsilon_i = 1$, $q_i = 1$, so

$$A_i = t^{k-k_{i-1}} - t^{k-k_{i-1}-k_{i-2}} + \ldots + (-1)^r t^{k_i} - (-1)^r > 0$$

Moreover, $B-A_i = 2^{k_i} A_{i+1}$, $k_i \geq 1$, so $A_{i+1} < \frac{B}{2}$, for all i, as required. Thus we may assume $t \geq 4$.

Next we dispose of the case $r = 1$. It is then plain from (1.3) that $A_1 = q_1$. Now if $\varepsilon_1 = 0$, then $q_1 \leq \frac{t}{2} - 1 < \frac{t^k-1}{2}$, while, if $\varepsilon_1 = 1$, then $q_1 \leq \frac{t}{2} < \frac{t^k+1}{2}$. Thus we have disposed of the case $r = 1$, and may assume $r \geq 2$.

Assume $\varepsilon_{i-1} = 0$. Then, by (1.7), $c_{i1} = q_{i-1} \leq \frac{t}{2} - 1$, so that, by (1.5),

$$A_i < (\tfrac{t}{2} - 1)t^{k-1} + (\tfrac{t}{2} + 1)t^{k-2} = \tfrac{1}{2}(t^k - t^{k-1} + 2t^{k-2}) < \tfrac{1}{2}(t^k-1) \leq \tfrac{1}{2} B.$$

Finally, assume $\varepsilon_{i-1} = 1$. Then $c_{i1} \leq \frac{t}{2}$ and $c_{i2} = -q_{i-2}$. Setting $k - k_{i-1} - k_{i-2} = \ell$, we find

$$A_i \leq \tfrac{t}{2}(t^{k-1}) - 1 < \tfrac{1}{2}(t^k-1) \leq \tfrac{1}{2} B, \text{ if } r = 2;$$

$$A_i < \tfrac{t}{2}(t^{k-1}) - t^\ell + (\tfrac{t}{2} + 1)t^{\ell-1} = \tfrac{1}{2}(t^k - t^\ell + 2t^{\ell-1}) < \tfrac{1}{2}(t^k-1) \leq \tfrac{1}{2} B, \text{ if } r \geq 3.$$

Thus the inequality (1.13) is proved in all cases.

We call a symbol (1.12) a canonical symbol. Note that a canonical symbol can be trivial. For if t is odd then the symbol, with k columns,

$$t^k-1 \left|\begin{array}{ccc} \frac{t^k-1}{2} & \cdots & \frac{t^k-1}{2} \\ 1 & \cdots & 1 \\ 0 & \cdots & 0 \\ \frac{t-1}{2} & \cdots & \frac{t-1}{2} \end{array}\right| t$$

is trivial, and is plainly canonical.

Remark If we had obtained (1.12) from the symbol (0.3) the inequalities (1.13) would, of course, have followed immediately from (1.4). However, we now know that such a symbol (1.12) exists (and is unique) for any allowable selection of $k_1, k_2, \ldots, k_r$; $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$; $q_1, q_2, \ldots, q_r$. In the next section we make a more detailed study of canonical symbols.

2. CANONICAL SYMBOLS

We first prove some easily accessible lemmas relating to the canonical symbols (1.12).

Lemma 2.1 In the symbol (1.12), A_i is independent of k_{i-1}.

Proof See (1.5).

Lemma 2.2 Let

$$t^k \pm 1 \left|\begin{array}{cccc} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_r \end{array}\right| t \qquad (2.1)$$

<u>be a non-trivial symbol</u>. <u>Then it is canonical, so that</u> $a_i = A_i$.

<u>Proof</u> By (1.4), $(t^k - (-1)^\varepsilon)a_i = (t^k \pm 1)A_i$. If $\pm 1 \neq -(-1)^\varepsilon$, then

$$t^k \pm 1 \mid 2a_i, \quad \text{(the factor 2 arises if t is odd)}$$

contradicting $0 < a_i < \frac{1}{2}(t^k \pm 1)$.

<u>Remark</u> Notice that we must insist that (2.1) is non-trivial. For, if t is odd,

$$t^k{+}1 \left|\begin{matrix} \frac{t^k+1}{2} & \cdots & \frac{t^k+1}{2} \\ 1 & \cdots & 1 \\ 0 & \cdots & 0 \\ \frac{t-1}{2} & \cdots & \frac{t-1}{2} \end{matrix}\right| t \qquad \text{(k columns)}$$

is a (trivial) non-canonical symbol.

Our next lemma is a portmanteau enunciation on quasi-orders; recall the notation $Q_t(b)$.

<u>Lemma 2.3</u> (i) <u>If</u> $t^k \equiv \pm 1$ <u>mod</u> b, <u>then</u> $Q_t(b) \mid k$.

(ii) <u>If</u> $c \mid b$ <u>then</u> $Q_t(c) \mid Q_t(b)$.

(iii) <u>If</u> (0.3) <u>is a contracted symbol, then</u> $k \mid Q_t(b)$.

(iv) $Q_t(t^k \pm 1) = k$ <u>unless</u> $t = 2$, $k = 2$, <u>when</u> $Q_2(3) = 1$.

<u>Proof</u> (i) Let $Q_t(b) = \ell$, and $k = u\ell + v$, $0 \leq v < \ell$. Then $t^v \equiv \pm t^k \equiv \pm 1$ mod b, so $v = 0$.

(ii) Let $Q_t(b) = k$. Then $t^k \equiv \pm 1$ mod b, so $t^k \equiv \pm 1$ mod c. Apply (i).

(iii) Let $\gcd(b, a_i) = d$, $b = cd$, $a_i = a_i'd$. Then

$$c \left|\begin{matrix} a_1' & a_2' & \cdots & a_r' \\ k_1 & k_2 & \cdots & k_r \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_r \\ q_1 & q_2 & \cdots & q_2 \end{matrix}\right| t$$

is reduced and contracted, so that, by our main theorem, $Q_t(c) = k$. Apply (ii).

(iv) Let $Q_t(t^k \pm 1) = \ell \geq 1$. Then $\ell \leq k$. But, if $\ell < k$, then $k \geq 2$ and so $t^\ell \pm 1 < t^k \pm 1$, except that $2 + 1 = 2^2 - 1$.

<u>Lemma 2.4</u> <u>Let</u>

$$t^k \pm 1 \left|\begin{matrix} a_1 & a_2 & \cdots & a_s \\ \ell_1 & \ell_2 & \cdots & \ell_s \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_s \\ q_1 & q_2 & \cdots & q_s \end{matrix}\right| t \qquad \ell = \sum \ell_i \qquad (2.2)$$

<u>be a contracted symbol</u>. <u>Then</u> $\ell \mid k$.

<u>Proof</u> By Lemma 2.3(iii), $\ell \mid Q_t(t^k \pm 1)$. Thus the result follows from Lemma 2.3(iv).

<u>Theorem 2.5</u> <u>If</u> (2.2) <u>is a non-trivial contracted symbol, it may be expanded to a canonical symbol</u>.

<u>Proof</u> We know by Lemma 2.4 that $\ell \mid k$. Thus we may expand (2.2) to a symbol (2.1) which is also, of course, non-trivial. Apply Lemma 2.2.

It follows that <u>any</u> non-trivial t-symbol for $t^k \pm 1$ may be contracted-expanded to a canonical symbol, so that the first row of the symbol may be computed from the remaining 3 rows by means of formula (1.5).

<u>Example</u> Consider the symbol

$$624 \left| \begin{array}{c} 24 \\ 2 \\ 1 \\ 1 \end{array} \right|_{5}$$

This expands to

$$624 \left| \begin{array}{cc} 24 & 24 \\ 2 & 2 \\ 1 & 1 \\ 1 & 1 \end{array} \right|_{5}$$

which is canonical.

We now proceed to relate canonical symbols for different values of k_i; to this end, we write $A_i(k)$ instead of A_i.

<u>Theorem 2.6</u> <u>Given the canonical symbols</u>

$$t^k-(-1)^{\varepsilon} \left| \begin{array}{cccc} A_1(k) & A_2(k) & \dots & A_r(k) \\ k_1 & k_2 & \dots & k_r \\ \varepsilon_1 & \varepsilon_2 & \dots & \varepsilon_r \\ q_1 & q_2 & \dots & q_r \end{array} \right|_{t} , \qquad (2.3)$$

$$t^{k+1}-(-1)^{\varepsilon} \left| \begin{array}{ccccc} A_1(k+1) & A_2(k+1) & & \dots & A_r(k+1) \\ k_1 & k_2 & \dots & k_{r-1} & k_r+1 \\ \varepsilon_1 & \varepsilon_2 & & \dots & \varepsilon_r \\ q_1 & q_2 & & \dots & q_r \end{array} \right|_{t} , \qquad (2.4)$$

<u>we have</u> $A_1(k) = A_1(k+1)$.

<u>Proof</u> This follows immediately from Lemma 2.1.

The force of this theorem is the following. We start with $b = t^k \pm 1$ and <u>any</u> $a_1 < \frac{b}{2}$ and construct a contracted t-symbol. By Theorem 2.5 we know it may be expanded to a canonical symbol S. If we now replace k by (k+1) and retain the same a_1, the t-symbol we obtain (perhaps not contracted) (i) has the same ε_i as S, (ii) has the same q_i as S, (iii) has the same k_i as S, $1 \leq i \leq r-1$, (iv) has the final k_r increased by 1.

<u>Example</u> As in our previous example, start with

$$5^4-1 = 624 \left| \begin{array}{c} 24 \\ 2 \\ 1 \\ 1 \end{array} \right|_{5}$$

and expand to

$$\begin{array}{r|rr|l} 624 & 24 & 24 & \\ & 2 & 2 & \\ & 1 & 1 & \\ & 1 & 1 & 5 \end{array}$$

Then we know that the symbol with $b = 3124$ is

$$\begin{array}{r|rr|l} 5^5-1 = 3124 & 24 & ? & \\ & 2 & 3 & \\ & 1 & 1 & \\ & 1 & 1 & 5 \end{array}$$

Executing the algorithm shows that the missing entry is 124. This raises the question of whether there is an easier way to compute the top row of the symbol for $t^{k+1} - (-1)^{\varepsilon}$.

To show that there is, suppose the canonical symbol (2.3) given; we describe how to calculate $A_i(k+1)$. Set

$$A_i(k+1) - A_i(k) = \Delta_i(k), \text{ the } i^{th} \text{ difference, } i = 1,2,\dots,r, \tag{2.5}$$

$$\Delta_i(k) = t^{k_i+\dots+k_r}(t-1)\delta_i(k), \quad i = 1,2,\dots,r, \tag{2.6}$$

and call $\delta_i(k)$ the <u>residual</u> i^{th} <u>difference</u>.

<u>Theorem 2.7</u> <u>The residual</u> i^{th} <u>difference</u> $\delta_i(k)$ <u>is given by</u>

$$\delta_1(k) = 0, \quad \delta_{i+1}(k)-(-1)^{\varepsilon_i}\delta_i(k) = q_i t^{k_1+\dots+k_{i-1}}, \quad i = 1,2,\dots,r-1 . \tag{2.7}$$

<u>Proof</u> Since, by Theorem 2.6, $A_1(k+1) = A_1(k)$ it follows immediately that $\delta_1(k) = 0$. We now prove the rest of (2.7). From (1.3),

$$\left.\begin{aligned} q_i(t^{k+1}-(-1)^{\varepsilon}) + (-1)^{\varepsilon_i}A_i(k+1) &= t^{k_i}A_{i+1}(k+1) \\ q_i(t^{k}-(-1)^{\varepsilon}) + (-1)^{\varepsilon_i}A_i(k) &= t^{k_i}A_{i+1}(k) \end{aligned}\right\} \quad i = 1,2,\dots,r-1 .$$

Thus, by subtraction, $q_i t^k(t-1) + (-1)^{\varepsilon_i}\Delta_i(k) = t^{k_i}\Delta_{i+1}(k)$, or, dividing by $t^{k_i+\dots+k_r}(t-1)$,

$$q_i t^{k_1+\dots+k_{i-1}} + (-1)^{\varepsilon_i}\delta_i(k) = \delta_{i+1}(k), \quad i = 1,2,\dots,r-1.$$

<u>Example</u> Consider the canonical symbol

$$\begin{array}{r|rrr|l} 5^5+1 = 3126 & 28 & 1256 & 374 & \\ & 1 & 1 & 3 & \\ & 0 & 1 & 0 & \\ & 2 & 1 & 1 & 5 \end{array}$$

Here $k = 5$; thus, to obtain the canonical symbol associated with 15626, still with $A_1 = 28$, we compute

$$\delta_2(5) = q_1 = 2,\ \delta_3(5) = (-1)^{\varepsilon_2}\delta_2(5) + q_2 t^{k_1} = -2 + 5 = 3\ ,$$

$$\Delta_2(5) = t^{k_2+k_3}(t-1)\delta_2(5) = 5^4\cdot 4\cdot 2 = 5000\ ,$$

$$\Delta_3(5) = t^{k_3}(t-1)\delta_3(5) = 5^3\cdot 4\cdot 3 = 1500\ .$$

We infer the canonical symbol

$$5^6+1 = 15626 \left|\begin{array}{ccc} 28 & 6256 & 1874 \\ 1 & 1 & 4 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{array}\right|_5$$

Theorem 2.7 admits the following convenient corollary.

Corollary 2.8 $A_i(k+\ell) - A_i(k) = \frac{t^\ell - 1}{t-1}(A_i(k+1) - A_i(k))$.

Proof The only change in the last 3 rows of (2.4), compared with (2.3), is the replacement of k_r by k_r+1. Thus it follows from (2.7) that

$$\delta_i(k+1) = \delta_i(k)\ .$$

Thus (2.6) yields

$$\Delta_i(k+1) = t\Delta_i(k)\ ,$$

or
$$A_i(k+2) - A_i(k+1) = t(A_i(k+1) - A_i(k))\ . \tag{2.8}$$

The corollary is an easy consequence of (2.8).

Example We revert to the previous example and take $\ell = 3$. Thus we seek the canonical symbol for 390626 with $A_1 = 28$. We know that $\Delta_2(5) = 5000$, $\Delta_3(5) = 1500$. Thus, by Corollary 2.8,

$$A_2(8) - A_2(5) = 31\ \Delta_2(5) = 155000,$$

$$A_3(8) - A_3(5) = 31\ \Delta_3(5) = 46500\ ,$$

so that the required symbol is

$$5^8+1 = 390626 \left|\begin{array}{ccc} 28 & 156256 & 46874 \\ 1 & 1 & 6 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{array}\right|_5$$

REFERENCES

[HP] HILTON, P. and PEDERSEN, J. The general quasi-order algorithm in number theory, Int. Journ. Math. and Math. Sci. 9 (1986), 245-252.