Pub. Mat. UAB
Vol. 29 Nº 2-3 Nov. 1985

ON GENERALIZED SYMBOLS, ORDERS AND QUASI-ORDERS

Peter Hilton and Jean Pedersen

0. Introduction

In our earlier paper [5] we introduced the notion of a *symbol*

$$b \left| \begin{array}{cccc} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{array} \right| \; ; \qquad (0.1)$$

where b, a_i are odd positive integers with $a_i < \frac{b}{2}$, the *weights* k_i are positive integers, and the a_i satisfy the determining relations

$$b = a_i + 2^{k_i} a_{i+1} \; , \; i = 1,2,\ldots,r \; (a_{r+1} = a_1). \qquad (0.2)$$

The symbol (0.1) is said to be *controlled* by b; further, it is *reduced* if there does not exist s such $s|r$, $s \neq r$, and, for all j,

$$a_{s+j} = a_j \; , \qquad (0.3)$$

$$\text{and} \quad k_{s+j} = k_j \; , \qquad (0.4)$$

In fact, as shown in [5], (0.3) holds for all j if and only if (0.4) holds for all j.

The reduced symbol (0.1) may be regarded as encoding instructions for folding a straight strip of paper to construct arbitrarily good approximations to a regular star $\{\frac{b}{a_1}\}$ -gon, in Coxeter's terminology [1]. Of course, for this purpose we require that b, a_i, be coprime; it is easy to see from (0.2) that $\gcd(b,a_i)$ is independent of i. Indeed, under the coprimality condition it follows that, if we fold down k_r times at A_0 at the top of the tape, the last fold line meeting the bottom of the tape at A_1; then fold up k_1 times at A_1, the last fold line meeting the top of the tape at A_2; then fold down k_2 times at A_2, the last fold line meeting the bottom of the tape at A_3; ..., then the angle at the vertex A_{nr} made by the line $A_{nr}A_{nr+1}$ converges to $\frac{a_1\pi}{b}$ as n tends to infinity.* From this folded tape it is then easy to construct our regular $\{\frac{b}{a_1}\}$ -gon. The details of the construction -- and further refinements to allow for the construction of the most general regular star polygon -- are to be found in [2,3,4].

However, we derived in [5] a purely number-theoretical significance for the *reduced* symbol (0.1); namely, if $d = \gcd(b,a_1)$ then $k = \sum_{i=k}^{r} k_i$ is the *quasi-order* of 2 modulo $\frac{b}{d}$. Here, we understand by the quasi-order of t modulo c, where t, c are coprime positive integers, the smallest integer m such that

$$t^m \equiv \pm 1 \bmod c \ ; \qquad (0.5)$$

---

* This statement does not require the coprimality of b and a_1. However, the Coxeter notation does!

we write the quasi-order as $quo_t(c)$. Moreover, the reduced symbol (0.1) also tells which sign to take in (0.5) if $m = quo_t(c)$ with $t = 2$, $c = \frac{b}{d}$; the positive sign (negative sign) if r is even (odd). It is plain that the quasi-order, furnished with this extra information based on the parity of r, gives us more precise information than the order (of t modulo c).

It is our aim in this paper to generalize the number-theoretical results of [5] to obtain the corresponding relationship between generalized symbols and quasi-orders. By a *generalized symbol* (or *t-symbol*), we understand a symbol (0.1) in which t is a fixed positive integer $\geqslant 2$, b, a_i are positive integers prime to t with $a_i < \frac{b}{t}$ and the relation (0.2) is replaced by

$$b = a_i + t^{k_i} a_{i+1},\ i = 1,2,\ldots,\ r\ (a_{r+1} = a_1) \qquad (0.2_t)$$

We will find that all our results on quasi-order do, in fact, generalize, but there is one fundamental new phenomenon when we consider generalized symbols. For whereas there is, for given odd b, a_1 with $a_1 < \frac{b}{2}$ always a symbol (0.1), there is not always a t-symbol for a given b, a_1 with b prime to t, $b \equiv a_1 \bmod t$, and $a_1 < \frac{b}{t}$. For example with $b = 11$ there is no 3-symbol at all controlled by b, as the reader may easily verify. This new phenomenon obliges us to find a new proof of the main Quasi-Order Theorem; the preparation for this proof is in Section 1 and the proof is given in Section 2. However, it also compels us to acknowledge that, whereas in the case

$t = 2$, the Quasi-Order Theorem actually yields an efficient *algorithm* for computing the quasi-order, this is not apparently the case for general t. However, an algorithm for computing the *order*, by modifying the notion of a t-symbol, is given in Section 3. Such modified t-symbols always exist.

Where a result in [5] is needed here in generalized form and the proof generalizes in straightforward fashion, we have simply quoted the generalized form. Where a result in [5] generalizes in straightforward fashion but we do not need it here, we have simply suppressed it. We should, however, mention that Theorem 3.4(*) of [5] is in this latter category.

We have not discussed the geometrical significance of our generalization; those who have overcome the prejudice against dividing a given angle into t equal parts (where t is not a power of 2) will be in a good position to formulate it, at least insofar as the results of Section 2 are concerned.

However, we make - as yet - no claim that the modified symbols described in Section 3 have any geometrical significance whatsoever! The effects of this modification are two-fold. We gain the advantage, as stated, that a modified t-symbol always exists for a given base t, a given positive integer b prime to t and a given positive integer $a = a_1 < b$ (with $t \nmid a$); but we have to be content with an algorithm producing the order of t modulo b rather than the quasi-order. We are indebted to a conversation with Don Zagier in which this modification was

suggested.

1. The generalized symbols

Throughout this siction, $t \geqslant 2$ is an integer and the t-*symbol*, controlled by b,

$$b \left| \begin{matrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{matrix} \right| \tag{1.1}$$

means that b is a positive integer prime to t, a_i $(i = 1,2,\ldots,r)$ is a positive integer such that

$$a_i \equiv b \bmod t \quad \text{and} \quad 0 < a_i < \frac{b}{t}\,; \tag{1.2}$$

k_i $(i = 1,2,\ldots,r)$ is a positive integer, and the equations

$$b = a_i + t^{k_i} a_{i+1}, \quad i = 1,2,\ldots,r, \quad (a_{r+1} = a_1) \tag{1.3}$$

hold. Just as in [5] we observe the following elementary facts.

$$\gcd(b,a_i) \text{ is independent of } i. \tag{1.4}$$

If $k_1,k_2,\ldots k_r$ is a repeating sequence,
with $k_{i+s} = k_i$, for a fixed $s \mid r$ $(s \neq r)$, (1.5)
then $a_1,a_2,\ldots,a_r$ is a repeating sequence
with $a_{i+s} = a_i$.

The (unique) solutions of equations (1.3) are rational numbers a_i satisfying $0 < a_i < \frac{b}{t}$; if any a_i is an integer, than all a_i are integers $\equiv b \bmod t$. (1.6)

Proposition 1.1 *The equations* (1.3) *have the solutions*

$$Ba_i = bA_i, \tag{1.7}$$

where

$$B = t^k - (-1)^r, k = \sum_{i=1}^{r} k_i \tag{1.8}$$

and

$$A_i = t^{k-k_i-1} - t^{k-k_i-1-k_{i-2}} + \ldots + (-1)^r t^{k_i} - (-1)^r \tag{1.9}$$

In particular,

$$B \begin{vmatrix} A_1 & A_2 & \cdots & A_r \\ k_1 & k_2 & \cdots & k_r \end{vmatrix} \tag{1.10}$$

is a symbol.

We write

$$b \begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_3 & \cdots & k_r \end{bmatrix}$$

if the symbol is *reduced*, that is, if $k_1, k_2, \ldots, k_r$ (and hence also $a_1, a_2, \ldots, a_r$) is not a repeating sequence.

So far, our generalization has been virtually automatic. However, at this point we encounter a difficulty in pursuing the program in [5], namely that, for given b, a_i satisfying

(1.2), no symbol may exist. Indeed, for a given b (and, of course, a given t), there may be no symbol whatsoever controlled by b. Thus we now study this question. We first prove a lemma.

Lemma 1.2 *Any integer* a *may be expressed as*

$$a = c_m t^m + c_{m-1} t^{m-1} + \ldots + c_0, \tag{1.11}$$

where c_j *is an integer satisfying* $|c_j| \leq \frac{t}{2}$.

Proof It plainly suffices to take a positive. Supose $a < t^n$, and consider the integer

$$\bar{a} = \begin{cases} a + \frac{t}{2}(t^{n-1} + t^{n-2} + \ldots + t + 1), & t \text{ even} \\ a + \frac{t-1}{2}(t^{n-1} + t^{n-2} + \ldots + t + 1), & t \text{ odd.} \end{cases}$$

It is easy to see that $\bar{a} < 2t^n$, so that $\bar{a}$ may be written in base t as

$$\bar{a} = b_n t^n + b_{n-1} t^{n-1} + \ldots + b^0, \quad 0 \leq b_j \leq t-1, \ j \leq n-1, \text{ and } 0 \leq b_n \leq 1.$$

Then $a = b_n t^n + c_{n-1} t^{n-1} + \ldots + c_0$, where

$$c_j = \begin{cases} b_j - \frac{t}{2}, & t \text{ even} \\ b_j - \frac{t-1}{2}, & t \text{ odd} \end{cases} \qquad j = 0,1,\ldots,n-1 .$$

Plainly, $|c_j| \leq \frac{t}{2}$; thus, since $|b_n| \leq \frac{t}{2}$, the lemma is

proved.

Remarks (i) If t is odd, the expression (1.11) is unique; if t is even, we lose uniqueness but we prefer to keep (1.11) since it has for us the decisive advantage that then $-a$ has the admissible form

$$-a = -c_m t^m - c_{m-1} t^{m-1} - \ldots - c_0.$$

(ii) If $a \neq 0$ then, of course, we may assume $c_m \neq 0$. In that case it is clear that $c_m > 0$ if and only if $a > 0$.

We now prove the main theorem of this section.

Theorem 1.3 *Let* $b = t^m - 1$, $m \geqslant 2$. *Then* a *appears in a* t*-symbol controlled by* b *if and only if*

$$a = t^{n_q} - t^{n_{q-1}} + \ldots + t^{n_1} - 1, \tag{1.12}$$

where q *is odd and* $m > n_q > \ldots > n_1 > 0$.

Proof Let a have the indicated form and set $k_1 = n_1$, $k_2 = n_2 - n_1$, $\ldots$, $k_q = n_q - n_{q-1}$, $k_{q+1} = m - n_q$. Then $\sum_{i=1}^{q+1} k_i = m$ and, according to (1.8) and (1.10), we have the symbol

$$b \begin{vmatrix} A_1 & A_2 & \ldots & A_{q+1} \\ k_1 & k_2 & \ldots & k_{q+1} \end{vmatrix}, \quad \sum_{i=1}^{q+1} k_i = m, \tag{1.13}$$

with (see (1.9))

$$A_1 = t^{m-k_{q+1}} - t^{m-k_{q+1}-k_q} + \ldots + t^{k_1} - 1$$

$$= t^{n_q} - t^{n_{q-1}} + \ldots + t^{n_1} - 1 = a.$$

We now prove the converse. If $t = 2$, then, dividing (1.12) by $t-1$, we see that (1.12) simply represents an arbitrary odd number $< 2^{n_q}$, so that all odd number $\leqslant 2^{m-1}$ take the form (1.12); and we know such odd numbers are precisely the integers a_i appearing in a symbol controlled by $2^m - 1$. Thus we may assume $t \geqslant 3$.

Let

$$t^m - 1 \left| \begin{array}{ccccc} a_1 & a_2 & \cdot & \cdot & a_r \\ k_1 & k_2 & \cdot & \cdot & k_r \end{array} \right|$$

be a symbol, with $a = a_1$. Then $0 < a < t^{m-1}$ by (1.2), so that, by Lemma 1.2, and Remark (ii),

$$a = a_1 = c_q t^{n_q} + \ldots + c_1 t^{n_1} + c_0, \quad m > n_q > \ldots > n_1 > 0, \tag{1.14}$$

with $|c_j| \leqslant \frac{t}{2}$ and $c_q > 0$. Since, for each i, $1 \leqslant i \leqslant r$, $a_i \equiv t^m - 1 \equiv -1 \mod t$, we infer in particular that $c_0 \equiv -1 \mod t$. But $|c_j| \leqslant \frac{t}{2}$ and $t \geqslant 3$, so $c_0 = -1$. We may obviously now assume that each $c_j \neq 0$ in (1.14).

Now $t^m - 1 = a_1 + t^{k_1} a_2$. Thus, from (1.14)

$$t^m - c_q t^{n_q} - \ldots - c_1 t^{n_1} = t^{k_1} a_2.$$

It follows that $t^{k_1} a_2$ is divisible by t^{n_1} but not by t^{n_1+1}. Since $a_2 \equiv -1 \bmod t$, this implies that $n_1 = k_1$, so that

$$a_2 = t^{m-n_1} - c_q t^{n_q - n_1} - \ldots - c_1. \tag{1.15}$$

Since (1.15) has the same form as (1.14) we now deduce that $c_1 = 1$, $n_2 - n_1 = k_2$ and

$$a_3 = t^{m-n_2+n_1} - t^{m-n_2} + c_q t^{m_q - n_2} + \ldots + c_2.$$

Proceeding in this way we infer that

$$c_j = (-1)^{j+1}$$

and, since $c_q > 0$, q is odd. This proves the theorem

We enunciate two corollaries, the first following from the statement of the theorem, the second from its proof.

Corollary 1.4 *Every symbol controlled by* $t^m - 1$ *arises from a symbol controlled by* $t^{m-1} + t^{m-2} + \ldots + t + 1$ *by multiplication by* $t-1$. *Then* a *appears in a symbol controlled by* $t^{m-1} + t^{m-2} + \ldots + t + 1$ *if and only if* $0 < a < t^{m-2} + \ldots + t + 1$ *and* a, *written in base* t, *consists exclusively of* 1's *and* 0,s *and terminates in* 1.

Corollary 1.5 *Let* $a = a_1$, *given by* (1.12), *appear in the reduced symbol*

$$t^m - 1 \left[\begin{array}{cccc} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{array} \right] \tag{1.16}$$

then, if $k = \sum_{i=1}^{r} k_i$, *we have*

$$k \mid m, \quad r \mid q+1, \tag{1.17}$$

the quotients in (1.17) *being the same.*

To establish Corollary 1.5 we have only to compare (1.16) with (1.13), where $b = t^m - 1$ and $A_1 = a_1$ to infer that (1.16) arises by reducing (1.13). Thus (1.17) follows, the common quotient being the number of times (1.16) is repeated to produce (1.13). Corollary 1.4, in turn has the following consequence which gives us a recharacterization of the integers a discussed in Theorem 1.3.

Corollary 1.6 *Let* $b = t^m - 1$, $m \geq 2$. *Then* a *appears in a t-symbol controlled by* b *if and only if* $a < t^{m-1}$ *and, when written in base* t, a *consists exclusively of* τ's *and* 0's *and terminates in* τ, *where* $\tau = t-1$.

There is a companion theorem to Theorem 1.3, whose proof we need not give.

Theorem 1.7 *Let* $b = t^m + 1$, $m \geq 1$. *Then* a *appears in a t-symbol controlled by* b *if and only if*

$$a = t^{n_q} - t^{n_{q-1}} + \cdots - t^{n_1} + 1, \tag{1.18}$$

where q *is even and* $m > n_q > \ldots > n_1 > 0$.

There is also a companion corollary to Corollary 1.5

Corollary 1.8 *Let* $a = a_1$, *given by* (1.18), *appear in the reduced symbol*

$$t^m + 1 \begin{bmatrix} a_1 & a_2 & \ldots & a_r \\ k_1 & k_2 & \ldots & k_r \end{bmatrix} \tag{1.19}$$

then, if $k = \sum_{i=1}^{r} k_i$, *we have*

$$k \mid m, \quad r \mid q+1, \tag{1.20}$$

the quotients in (1.20) *being the same.*

2. The main theorem

We recall the *quasi-order* of t mod b is the smallest positive integer n such that $t^n \equiv \pm 1 \bmod b$. We write $\mathrm{quo}_t(b)$ for the quasi-order of t mod b. Note that if $k = \mathrm{quo}_t(b)$ then

$$\text{order of } t \bmod b = \begin{cases} k & \text{if } t^k \equiv 1 \bmod b \\ 2k & \text{if } t^k \equiv -1 \bmod b \end{cases} \tag{2.1}$$

We now prove

Theorem 2.1 *Let*

$$b \begin{bmatrix} a_1 & a_2 & \ldots & a_r \\ k_1 & k_2 & \ldots & k_r \end{bmatrix} \tag{2.2}$$

be a reduced t*-symbol controlled by* b *with* $k = \sum_{i=1}^{r} k_i$. *Then* $k \mid \mathrm{quo}_t(b)$. *Moreover,*

(a) *if* r *is even and* $\gcd(b,a_i) \mid (t-1)$, *we conclude that* $\mathrm{quo}_t(b) = k$ *and* $t^k \equiv 1 \bmod b$;

(b) *if* r *is odd and* $\gcd(b,a_i) = 1$, *we conclude that* $\mathrm{quo}_t(b) = k$ *and* $t^k \equiv -1 \bmod b$.

Proof Let $\mathrm{quo}_t(b) = m$. Then there exists a q such that $bq = t^m - \epsilon$, where $\epsilon = \pm 1$. Multiplying (2.2) by q, we have

$$t^m - \epsilon \begin{bmatrix} a_1 q & a_2 q & \cdots & a_r q \\ k_1 & k_2 & \cdots & k_r \end{bmatrix} .$$

It now follows from (1.17) or (1.20) that $k \mid m$.

Now suppose r even. Then, using (1.7,8,9), we infer from (2.2) that

$$(t^k - 1)a_i = bA_i,$$

and $(t-1) \mid A_i$. If $d = \gcd(b,a_i)$, and $d \mid (t-1)$, then

$$\frac{t^k-1}{t-1}\cdot\frac{a_1}{d} = \frac{b}{d}\cdot\frac{A_1}{t-1}, \quad \text{and} \quad \gcd\left(\frac{b}{d}, \frac{a_1}{d}\right) = 1.$$

Thus $\frac{b}{d} \mid \frac{t^k-1}{t-1}$, so that $b \mid t^k - 1$. We conclude that $m \leqslant k$, so that $k = m$ and assertion (a) is proved.

Finally, suppose r odd. Then, using (1.7,8), we infer from (2.2) that

$$(t^k + 1)a_i = bA_i.$$

Thus if $\gcd(b,a_i) = 1$, $b \mid t^k + 1$. We again conclude that $k = m$

and assertion (b) is proved.

Theorem 2.1 has the following corollaries.

Corollary 2.2 *Let*

$$t^m - 1 \left[\begin{array}{ccccc} a_1 & a_2 & . & . & a_r \\ k_1 & k_2 & . & . & k_r \end{array} \right], \quad m \geqslant 2.$$

Then if $k = \sum_{i=1}^{r} k_i$, *we have* $k \mid m$. *If* $\gcd(t^m-1, a_i) = t - 1$, *and if* $m \geqslant 3$, *then* r *is even and* $k = m$.

Proof Since $\mathrm{quo}_t(t^m-1) = m$, unless $t = 2$, $m = 2$, when $\mathrm{quo}_2(3) = 1$ (see Propositon 2.4 below), we know that $k \mid m$ except in this special case. But it is also true in the special case, since then $2^2-1 \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right]$ si the only reduced symbol.

Now if r is even the conclusion follows from Theoreme 2.1(a). Thus it only remains to show that r cannot be odd. Were r odd, we would have (see (1.7,8))

$$(t^m - 1)A_i = (t^k + 1)a_i \ . \tag{2.3}$$

We know that $k \mid m$. If $k = m$, then we conclude easily from (2.3) that

$$t^m - 1 \mid a_i \quad \text{if} \quad t \quad \text{is even;} \quad \frac{t^m - 1}{2} \mid a_i \quad \text{if} \quad t \quad \text{is odd.}$$

Either conclusion is incompatible with $a_i < t^{m-1}$, so that $k \neq m$. Thus $k \leqslant \frac{m}{2}$. Sut since $\gcd(t^m-1, a_i) = t - 1$, we obtain from (2.3) the relation

$$\frac{t^m - 1}{t - 1} \mid t^k + 1 \ . \tag{2.4}$$

But, since $m \geqslant 3$, we have the inequalities

$$\frac{t^m - 1}{t - 1} > t^{m-1} + 1 > t^{\frac{m}{2}} + 1 \geqslant t^k + 1, \quad \text{so that relation}$$

(2.4) is absurd and hence r cannot be odd.

The companion corollary reads as follows, but this time the proof is almost trivial.

Corollary 2.3 *Let*

$$t^m + 1 \left[\begin{array}{ccccc} a_1 & a_2 & . & . & a_r \\ k_1 & k_2 & . & . & k_r \end{array} \right], \quad m \geqslant 1.$$

Then if $k = \sum_{i=1}^{r} k_i$, *we have* $k \mid m$. *If* $\gcd(t^m+1, a_i) = 1$, *then* r *is odd and* $k = m$.

Proof By Proposition 2.4 below, we know that $\text{quo}_t(t^m+1) = m$, so that $k \mid m$. But now Theorem 1. and (1.20) assure us that r is odd so that Theorem 2.1 completes the proof.

We complete the argument, then, with the following proposition.

Proposition 2.4

(a) *Let* $m \geqslant 2$. *Then* $\text{quo}_t(t^m-1) = m$ *unless* $t = 2$, $m = 2$.

(b) *Let* $m \geqslant 1$. *Then* $\operatorname{quo}_t(t^m + 1) = m$.

Proof (a) Certainly $\ell \leqslant m$, where $\operatorname{quo}_t(t^m - 1) = \ell$. If $t^m - 1 \mid t^\ell - 1$ it immediatelly follows that $\ell = m$. If $t^m - 1 \mid t^\ell + 1$, we obtain a contradiction as follows (unless we are in the exceptional case). We have $t^\ell + 1 \leqslant t^m - 1 + 2$. Thus, since $t^m - 1 \geqslant 3$, the relation $t^m - 1 \mid t^\ell + 1$ implies $t^m - 1 = t^\ell + 1$. Certainly, then $\ell \neq m$. But if $\ell \leqslant m-1$, we would have

$$t^{m-1}(t-1) > 2,$$

unless $t = 2$, $m = 2$, and so $t^m - 1 > t^{m-1} + 1 \geqslant t^\ell + 1$, contradicting $t^m - 1 = t^\ell + 1$.

(b) Again $\ell \leqslant m$, where $\operatorname{quo}_t(t^m + 1) = 1$. If $t^m + 1 \mid t^\ell + 1$, it immediately follows that $1 = m$; and it is impossible that $t^m + 1 \mid t^\ell - 1$.

Remark The case $m = 2$ is rightly excluded from the final statement of Corollary 2.2 since we have the reduced symbol

$$t^2 - 1 \quad \begin{bmatrix} t-1 \\ 1 \end{bmatrix} .$$

3. A modification of the generalized symbols; a new algorithm

In this section, we modify the definition of a symbol in order to obtain an algorithm for computing the order of t modulo b, where t is an integer $\geqslant 2$, and b is prime to t. We need a preliminary lemma.

Lemma 3.1 *Let* b *be prime to* t, *and let* a *be an integer such that* $t \nmid a$. *Then, among the integers*

$$qb + a, \quad 1 \leqslant q \leqslant t-1,$$

there exists exactly one, say $q_0 b + a$, *such that* $t \mid q_0 b + a$.

Proof The set $\{q,\ 0 \leqslant q \leqslant t-1\}$ is a complete, irredundant set of residues modulo t. Since b is prime to t, the set $\{qb,\ 0 \leqslant q \leqslant t-1\}$ is also a complete, irredundant set; and so too, therefore, is the set $\{qb + a,\ 0 \leqslant q \leqslant t-1\}$. Since $t \nmid a$, exactly one of the residues $qb + a$, $1 \leqslant q \leqslant t-1$, must be the zero residue.

An *order-symbol, rel* t,

$$b \left|\left| \begin{matrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{matrix} \right|\right| \tag{3.1}$$

is now defined for all b prime to t and all a_i such that $t \nmid a_i$ by the condition

$$q_i b + a_i = t^{k_i} a_{i+1},\ 1 \leqslant q_i \leqslant t-1,\ k_i \geqslant 1,\ i = 1,2,\ldots,r, \tag{3.2}$$

where $a_{r+1} = a_1$. Here q_i has precisely the meaning of q_0 in Lemma 3.1. Notice that, if $t \nmid a_1$, then (3.2) provides a definition of a_2 such that $t \nmid a_2$. Moreover, if $a_1 < b$, then $q_1 b + a_1 < (t-1)b + b = tb$, so $a_2 < b$. Thus (3.2) defines a function $a_1 \longrightarrow a_2$ from the set S of integers $\{a \mid a < b \text{ and } t \nmid a\}$ to itself. It is easy to see -- Lemma 3.2

below -- that this function is a permutation of S, so that, given b prime to t and $a < b$ such that $t \nmid a$, then an order-symbol (3.1) always exists with $a_1 = a$ and this order-symbol is unique up to iteration. We will henceforth only consider order-symbols (3.1) with $a_1 < b$ (so that $a_i < b$ for all* i).

Lemma 3.2 *The function* $a \longrightarrow a'$ *given by* $q_0 b + a = t^k a'$, $k \geqslant 1$, *from the set* S *to itself is a permutation.*

Proof Given $a' < b$, $t \nmid a'$, choose k minimal so that $t^k a' \geqslant b$. Then $k \geqslant 1$, so $t^k a' > b$. Let $t^k a' = q_0 b + a$, $0 \leqslant a < b$ and $q_0 \geqslant 1$. Then $a \neq 0$; for if $a = 0$, then $b \mid t^k a'$, $b \mid a'$, contradicting $a' < b$. Also $q_0 \leqslant t-1$; for if $q_0 \geqslant t$, then $t^k a' \geqslant tb$, so $t^{k-1} a' \geqslant b$, contradicting the minimality of k. Moreover $t \nmid a$; for if $t \mid a$, then $t \mid q_0 b$, $t \mid q_0$ contradicting $1 \leqslant q_0 \leqslant t-1$. Thus $a \longrightarrow a'$ is surjective and hence bijective as a function from S to S.

We now proceed exactly as for generalized symbols, except that we have replaced the defining relation (1.3) by (3.2).

Actually, to set up the analogy, it is easier to permit zero weights in our order-symbol. This means that our *expanded order-symbol*, rel t, is

$$b \left| \begin{array}{cccc} \bar{a}_1 & \bar{a}_2 & \ldots & \bar{a}_s \\ \ell_1 & \ell_2 & \ldots & \ell_s \end{array} \right| \qquad (3.3)$$

---

* Note that this condition replaces the condition $a_1 < \frac{b}{t}$ of (1.2).

where $t \nmid \bar{a}_j$ and the condition

$$b + \bar{a}_j = t^{\ell_j}\, \bar{a}_{j+1},\ f_j \geqslant 0 \tag{3.4}$$

holds for each j, with $\bar{a}_{s+1} = \bar{a}_1$. For example, with $t = 6$, we have the order-symbol

$$7 \left| \begin{matrix} 3 & 4 \\ 1 & 1 \end{matrix} \right|$$

and the expanded order-symbol

$$7 \left| \begin{matrix} 3 & 10 & 17 & 4 & 11 \\ 0 & 0 & 1 & 0 & 1 \end{matrix} \right| .$$

It is obvious how to obtain the order-symbol from the expanded order-symbol. In particular if $\bar{a}_1 = a_1$ in (3.1), (3.3), then $\Sigma k_i = \Sigma \ell_j$; indeed, the sequence of ℓ_j's is just the sequence of k_i's interspersed with zeros.

Now the equations (3.4) have the solution (compare (1.7) through (1.9))

$$\bar{a}_j \bar{B} = b \bar{A}_j, \tag{3.5}$$

where $$B = t^{\ell} - 1, \quad \ell = \Sigma \ell_j \tag{3.6}$$

$$\bar{A}_j = t^{\ell - \ell_{j-1}} + t^{\ell - \ell_{j-1}\ell_{j-2}} + \ldots + t^{\ell_1} + 1 . \tag{3.7}$$

It should now be obvious that our order-symbol yields

the following theorem.

Theorem 3.3 *Let* (3.1) *be reduced* (i.e., *without repetition*), *let* a_1 *be prime to* b *and let* $k=\Sigma k_i$. *Then* k *is the order of* t *modulo* b.

Proof We described and discussed in Lemma 3.2 the bijective function $\psi:S \to S$ such that $\psi(a_i) = a_{i+1}$, $i = 1,2,\ldots, r$ $(a_{r+1} = a_1)$. In the course of the proof we observed that the inverse to ψ, say $\varphi:S \to S$ is defined as follows: given $a' \in S$ choose k minimal such that $t^k a' > b$ and set $t^k a' = q_0 b + a$, $0 \leq a < b$; then $\varphi(a') = a$.

We now rewrite (3.1) 'in skew-reverse notation' as

$$b \left\| \begin{matrix} c_r & c_{r-1} & \cdots & c_2 & c_1 \\ \ell_{r-1} & \ell_{r-2} & & \ell_1 & \ell_r \end{matrix} \right\| , \quad \sum_{i=1} \ell_i = \ell \qquad (3.8)$$

so that $\varphi(c_i) = c_{i+1}$, $i = 1,2,\ldots,r (c_{r+1} = c_1)$ and, for each i, ℓ_i is minimal such that

$$t^{\ell_i} c_i > b, \quad i = 1,2,\ldots,r \qquad (3.9)$$

Then, for some q_i with $1 \leq q_i \leq t-1$,

$$t^{\ell_i} c_i = q_i b + c_{i+1}, \quad i = 1,2,\ldots,r \ (c_{r+1} = c_1). \qquad (3.10)$$

Consider the sequence of $(\ell+1)$ positive integers $s_i < b$,

$$\{c_1, tc_1, \ldots, t^{\ell_1-1} c_1, c_2, tc_2, \ldots, t^{\ell_2-1} c_2, c_3, \ldots, c_r, tc_r, \ldots, t^{\ell_r-1} c_r, c_1\}$$

Then, for each i,

$$s_{i+1} \equiv ts_i \bmod b, \quad s_i \equiv t^{i-1}c_1. \tag{3.11}$$

so that in particular,

$$c_1 \equiv t^{\ell}c_1 \bmod b \tag{3.12}$$

We now make the key claim that for no i except $i = 1, \ell + 1$ do we have $s_i \equiv c_1 \bmod b$. For, since $s_i < b$, the congruence $s_i \equiv c_1 \bmod b$ would imply $s_i = c_1$; but if $s_i = t^j c_m$, $j \geqslant 1$, then $s_1 \neq c_1$ since $t \nmid c_1$; and if $s_i = c_m$, $m \neq 1$, then $s_i \neq c_1$ since our order-symbol (3.8) has no repeats. This establishes our claim, which implies that ℓ is the smallest positive integer n such that $c_1 \equiv t^n c_1 \bmod b$. But since c_1 is prime to b,

$$c_1 \equiv t^n c_1 \bmod b \iff 1 \equiv t^n \bmod b.$$

Thus ℓ is, as claimed, the order of t mod b.

Examples

From the reduced order-symbol, rel 6, 7 $\left|\left|\begin{matrix} 3 & 4 \\ 1 & 1 \end{matrix}\right|\right|$,
we infer that the order of 6 modulo 7 is 2.
From the reduced order-symbol, rel 11, 6 $\left|\left|\begin{matrix} 1 & 5 \\ 1 & 1 \end{matrix}\right|\right|$,
we infer that the order of 11 modulo 6 is 2.
From the reduced order-symbol, rel 11, 50 $\left|\left|\begin{matrix} 21 & 1 & 41 & 31 \\ 2 & 1 & 1 & 1 \end{matrix}\right|\right|$,
we infer that the order of 11 modulo 50 is 5.

REFERENCES

[1] H.S.M. Coxeter, Regular Polytopes, Methuen (1948).

[2] Peter Hilton and Jean Pedersen, Approximating any regular poligon by folding paper: An interplay of geometry, analysis and number theory, Mathematics Magazine, Vol. 56. Nº 3, 141-155 (1983).

[3] ----------, Regular polygons, star polygons and number theory, Coxeter Festschrift, Math. Sem. Giessen 164, 217-244 (1984).

[4] ----------, Folding regular star polygons and number theory, The Mathematical Intelligencer, Vol. 7, No. 1, 15-26 (1985).

[5] ----------, On certain algorithms in the practice of geometry and the theory of numbers, Publicacions, Sec. Mat., U.A.B. Vol. 29, No. 1, 31-64 (1985).

Rebut el 18 de febrer del 1985

Peter Hilton
Department of Mathematical Sciences
SUNY Binghamton
Binghamton, New York 13901

Jean Pedersen
Department of Mathematics
University of Santa Clara
Santa Clara, California 95053

U.S.A.