Internat. J. Math. & Math. Sci
Vol 9 No. 2 (1986) 245-251

THE GENERAL QUASI-ORDER ALGORITHM IN NUMBER THEORY

PETER HILTON

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

JEAN PEDERSEN

Department of Mathematics
Santa Clara University
Santa Clara, California 95051 U.S.A.

(Received November 27, 1985)

ABSTRACT. This paper deals with a generalization of the Binary Quasi-Order Theorem. This generalization involves a more complicated algorithm than $(0.2)_t$. Some remarks are made on relative merits of two dual algorithms called the ψ-algorithm and the ϕ-algorithm. Some illustrative examples are given.

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

0. INTRODUCTION

In [HP3] the authors gave an algorithm for computing the quasi-order of 2 mod b for any odd number b. Here we understand the quasi-order of t mod b, where b,t are mutually prime positive integers, to be the smallest integer k such that $t^k \equiv \pm 1$ modulo b. The algorithm, which also determined whether $t^k \equiv +1$ or $t^k \equiv -1$, was based on a procedure for folding arbitrarily good approximations to regular star polygons (with b sides) from straight strips of paper, developed in [HP1,2].

All the number-theoretical work which accompanied the evolution of the algorithm in [HP1,2,3] suggested that it should be possible to generalize the algorithm from the case of t = 2 to the case of a general positive integer; all that should be lost would be the original geometrical significance. However, the generalization proposed and studied in [HP4] had the serious defect that, though it was a generalization of the Quasi-Order Theorem of [HP3], it was not an algorithm. Let us briefly review the situation to clarify this point.

We introduced in [HP3] the symbol

$$b \begin{vmatrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{vmatrix} , \qquad (0.1)$$

where a_i, b are odd, $a_1 < b/2$, and

$$b = a_i + 2^{k_i} a_{i+1}, \quad i = 1,2,\ldots,r \quad (a_{r+1} = a_1) \qquad (0.2)_2$$

Such a symbol always exists for a given b and $a = a_1$, and is uniquely determined by b and a up to repetition. Then we proved the following theorem in [HP3].

Theorem 0.1 (The Binary Quasi-Order Theorem) If (0.1) is reduced (i.e., $\gcd(b,a_1) = 1$) and contracted (i.e., the symbol involves no repeated a_i) then the quasi-order of 2 mod b is $k = \sum_{i=1}^{r} k_i$, and, in fact, $2^k \equiv (-1)^r \bmod b$.

We chose a proof of this theorem which contained steps of great interest from the geometric (paper-folding) point of view, but which was not the most direct proof available. The generalization we proved in [HP4] was this:

Theorem 0.2 Suppose b prime to t, and $t \nmid a$, and suppose $a_i < b/t$. If the symbol (0.1) means that

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

then, provided (0.1) is reduced and contracted, the quasi-order of t mod b is $k = \sum_{i=1}^{r} k_i$ and $t^k \equiv (-1)^r \bmod b$.

In fact, we proved a refinement of this if r is even, since then we did not require that (0.1) be reduced but merely that $\gcd(b,a_1) \mid (t-1)$.

However, it is no longer true, if $t \geq 3$, that a symbol in the sense of Theorem 0.2 always exists (for example, there is no symbol with t = 3, b = 11, whatever value we give to a_1); and much of the discussion in [HP4] centered on specifying criteria for the existence of a symbol.

In this paper we give a somewhat different generalization of Theorem 0.1, though it is very similar in spirit to Theorem 0.2. This generalization involves a more complicated algorithm than $(0.2)_t$ but it has the compensating merit that it is genuinely an algorithm. The condition $a_i < b/t$ is replaced by $a_i < b/2$ (after all, both are generalizations of the condition $a_i < b/2$, imposed if t = 2!); but now, given any two positive integers b and t, with b prime to t, and given $a = a_1$ not divisible by t, there is always a (modified) symbol (0.1) and a (generalized) quasi-order theorem holds. This is our Theorem 2.2.

In fact, there are two dual (or mutually inverse) algorithms for generating a symbol from b and a. We use one (which we call the ψ-algorithm and which generalizes $(0.2)_2$) to prove that symbols, suitably modified, always exist (for given b,a), and the dual algorithm (which we call the φ-algorithm) to prove the Quasi-Order Theorem. Our impression is that the ψ-algorithm would appeal to an intelligent human being, while the φ-algorithm is much better adapted to the computer.

The paper continues with some remarks on the relation of the proof to arguments given in [HP3,4] and on the relative merits of the two algorithms; and concludes with some illustrative examples.

1. PRELIMINARY RESULTS

Throughout this section, b,t will be fixed coprime positive integers with $t \geq 2$. The following lemma is quite obvious.

Lemma 1.1 Let T be a set of t consecutive integers, and let a be an arbitrary

integer. Then the set

$$\{qb+a,\ q \in T\}$$

of t integers runs through the complete set of residues modulo t.

Proposition 1.2 Suppose $t \nmid a$. Then

(i) if t is odd, the set of integers $\left\{qb+a,\ 1 \le q \le \frac{t-1}{2};\ qb-a,\ 1 \le q \le \frac{t-1}{2}\right\}$ contains precisely one integer divisible by t;

(ii) if t is even, the set of integers $\left\{qb+a,\ 1 \le q \le \frac{t}{2} - 1;\ qb-a,\ 1 \le q \le \frac{t}{2}\right\}$ contains precisely one integer divisible by t.

Proof We will be content to prove case (i). By Lemma 1.1, the set of integers $\left\{qb+a,\ -\frac{t-1}{2} \le q \le \frac{t-1}{2}\right\}$ contains exactly one integer q_0b+a divisible by t; but $q_0 \neq 0$ since $t \nmid a$. If $q_0 > 0$, then this is the integer required by our proposition, since if $t \mid (qb-a)$ then $t \mid (-qb+a)$. If $q_0 < 0$, then $-(q_0b+a)$ is the integer required by our proposition.

Let us write

$$\bar{q}b + (-1)^{\epsilon}a,\ \epsilon = 0 \text{ or } 1, \tag{1.1}$$

for the integer described in Proposition 1.2; thus

$$\left.\begin{array}{ll} 1 \le \bar{q} \le \frac{t-1}{2} & \text{if t is odd} \\ 1 \le \bar{q} \le \frac{t}{2} - 1 & \text{if t is even and } \epsilon = 0 \\ 1 \le \bar{q} \le \frac{t}{2} & \text{if t is even and } \epsilon = 1 \end{array}\right\} \tag{1.2}$$

Further, suppose $b \ge 3$ and let S be the set of positive integers a such that $t \nmid a$ and $a < b/2$. For $a \in S$, it is plain from (1.2) that the integer (1.1) is always positive, so that there exists a maximal k, with $k \ge 1$, such that

$$\bar{q}b + (-1)^{\epsilon}a = t^k a',\quad a \in S,\ a' > 0\ . \tag{1.3}$$

Since k is maximal, $t \nmid a'$. We claim more, namely,

Theorem 1.3 The function $a \mapsto a'$ is a permutation ψ of the set S.

Proof Assume first that t is odd. Then $k \ge 1$ and $t^k a' < \frac{t-1}{2} b + \frac{b}{2} = \frac{tb}{2}$, so that $a' < b/2$ and so $a' \in S$. Thus $a \mapsto a'$ is a function $\psi: S \to S$. It only remains to show that ψ is surjective, since S is a finite set.

Let $a' \in S$ and let k be minimal such that $t^k a' \ge b/2$. Then $k \ge 1$ so that $t^k a' > b/2$. In fact, $t^k a' \neq \frac{n}{2} b$ for any integer n; for if $t^k a' = \frac{n}{2} b$, then $nb = 2t^k a'$, $b \mid 2t^k a'$, $b \mid 2a'$, contradicting $0 < a' < b/2$. Thus $t^k a'$ may be uniquely expressed as

$$t^k a' = qb + (-1)^{\epsilon}a,\ \epsilon = 0,1,\quad 0 < a < b/2,\ q \ge 1. \tag{1.4}$$

We claim that $q \le \frac{t-1}{2}$; for if $q \ge \frac{t+1}{2}$, then $t^k a' > \frac{t+1}{2} b - \frac{b}{2} = \frac{tb}{2}$, so that $t^{k-1}a' > b/2$, contradicting the minimality of k. It is now plain that $t \nmid a$; for if $t \mid a$, then, from (1.4), $t \mid qb$, $t \mid q$, contradicting $1 \le q \le \frac{t-1}{2}$. Thus $a \in S$, and Proposition 1.2(i), together with (1.4), ensures that $\psi(a) = a'$.

A small modification is needed if t is even. Again, in (1.3), $k \ge 1$ and $t^k a' < \frac{t}{2} b$ so that $a' \in S$, and we have a function $\psi: S \to S$. To show that ψ is

surjective we proceed as above as far as (1.4). We now claim that

$$q \leq \frac{t}{2} - 1 \text{ if } \epsilon = 0 \; ; \quad q \leq \frac{t}{2} \text{ if } \epsilon = 1. \tag{1.5}$$

For if $\epsilon = 0$ and $q \geq t/2$, then, from (1.4), $t^k a' > \frac{t}{2} b$, contradicting the minimality of k; and if $\epsilon = 1$ and $q \geq \frac{t}{2} + 1$, then $t^k a' > \left(\frac{t}{2} + 1\right) b - \frac{b}{2} = \frac{t+1}{2} b$, again contradicting the minimality of k. Thus (1.5) is established. Once more we conclude that $t \nmid a$; for if $t \mid a$, then $t \mid q$, and $q \geq 1$ is constrained by (1.5). We involve Proposition 1.2(ii), together with (1.4), to complete the proof of the theorem.

Remark If $t = 2$, then the integer described in Proposition 1.2(ii) is simply b-a. Thus (1.3) yields in this case the rule

$$b - a = 2^k a' \, , \tag{1.6}$$

which was precisely the basis of the algorithm in Theorem 0.1; see $(0.2)_2$. Thus (1.3) provides a generalization of that basis.

2. THE GENERAL QUASI-ORDER ALGORITHM

Let b and t be any two coprime positive integers; define S as in Section 1. Since $\psi: S \to S$ is a permutation, we may start with any $a \in S$ and we will get a cycle

$$a, \ \psi(a), \ \psi^2(a), \ \ldots, \ \psi^r(a) = a \, .$$

Let r be the strict period of the cycle. Then we may write a t-symbol (with $a_1 = a$)

$$b \begin{vmatrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \\ \epsilon_1 & \epsilon_2 & \cdots & \epsilon_r \end{vmatrix} \tag{2.1}$$

where, as in (1.3),

$$\left.\begin{aligned} &\bar{q}_i b + (-1)^{\epsilon_i} a_i = t^{k_i} a_{i+1} \, , \ i = 1,2,\ldots,r, \ a_{r+1} = a_1, \ \epsilon_i = 0 \text{ or } 1 \, , \\ &k_i \geq 1, \text{ and } \bar{q}_i \text{ is constrained as in (1.2)} \, . \end{aligned}\right\} \tag{2.2}$$

Note that (2.1) is contracted, in the sense that there is no repeat among the a_i's. We will not systematically develop the properties of the symbol (2.1) as in [HP3], but will proceed as directly as possible to the main theorem. We first prove an easy lemma.

Lemma 2.1 In the symbol (2.1), $\gcd(b, a_i)$ is independent of i.

Proof This follows immediately from (2.2) and the fact that b,t are mutually prime.

We call the symbol (2.1) reduced if $\gcd(b, a_i) = 1$; notice that this is a change of terminology from [HP3,4]. Now, in (2.1), let $k = \sum_{i=1}^{r} k_i$, $\epsilon = \sum_{i=1}^{r} \epsilon_i$. We prove

Theorem 2.2 (The General Quasi-order Algorithm) Let b and t be any two coprime positive integers. Let the symbol (2.1) be contracted and reduced. Then k is the quasi-order of t mod b. In fact,

$$t^k \equiv (-1)^{\epsilon} \text{ modulo } b. \tag{2.3}$$

Proof In the course of proving Theorem 1.3, we found an explicit form for φ, the inverse of $\psi: S \to S$. Thus $\varphi(a') = a$, where k is minimal such that $t^k a' \geq b/2$ and (1.4) holds; moreover, the value of q in (1.4) is constrained exactly as in (1.2).

We now concentrate on the φ-algorithm, that is, we make (1.4) the fundamental rule for generating a symbol and write (2.1) in 'skew-reverse' notation as

$$b\begin{vmatrix} c_r & c_{r-1} & \cdots & c_2 & c_1 \\ \ell_{r-1} & \ell_{r-2} & \cdots & \ell_1 & \ell_r \\ \eta_{r-1} & \eta_{r-2} & \cdots & \eta_1 & \eta_r \end{vmatrix}$$

(If one were to regard φ, rather than ψ, as the fundamental algorithm, it would be natural to introduce a change in the format of our t-symbol to relate it better to (2.4).) Then $c_i = a_{r+1-i}$; $\ell_i = k_{r-i}$, $i < r$, $\ell_r = k_r$; $\eta_i = \varepsilon_{r-i}$, $i < r$, $\eta_r = \varepsilon_r$. If $\ell = \sum_{i=1}^{r} \ell_i$, $\eta = \sum_{i=1}^{r} \eta_i$, then we must prove that ℓ is the quasi-order of t mod b, and that $t^{\ell} \equiv (-1)^{\eta}$ modulo b. Our defining equation (1.4) now reads

$$t^{\ell_i} c_i = q_i b + (-1)^{\eta_i} c_{i+1}\ , \quad i = 1,2,\ldots,r \quad (c_{r+1} = c_1)\ . \tag{2.4}$$

Consider the sequence of $(\ell+1)$ integers $s_j < b/2$,

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

Then $s_{j+1} \equiv \pm ts_j$ modulo b, for all j. Indeed, $s_{j+1} \equiv ts_j$ modulo b unless $s_j = t^{\ell_i-1}c_i$, $s_{j+1} = c_{i+1}$ and $\eta_i = 1$; in that case, $s_{j+1} \equiv -ts_j$ modulo b. It follows that

$$c_1 \equiv (-1)^{\eta} t^{\ell} c_1 \text{ modulo } b\ . \tag{2.5}$$

We claim that $s_j \not\equiv \pm c_1$ modulo b unless $j = 1$ or $\ell + 1$. For if $s_j \equiv c_1$ modulo b, then, since $0 < s_j,\ c_1 < b/2$, we must have $s_j = c_1$. This is impossible if $s_j = t^n c_i$, $n \geq 1$, since $t \nmid c_1$. It is also impossible if $s_j = c_i$ (unless $i = 1$) since our symbol is contracted. Again if $s_j \equiv -c_1$ modulo b, then $b \mid (s_j + c_1)$ but $0 < s_j + c_1 < b$, which is an obvious contradiction. Thus ℓ is the minimum m such that

$$t^m c_1 \equiv \pm c_1 \text{ modulo } b.$$

But since, by Lemma 2.1, b, c_1 are mutually prime, it follows that ℓ is the minimum m such that $t^m \equiv \pm 1$ modulo b and, from (2.5), that $t^{\ell} \equiv (-1)^{\eta}$ modulo b. This completes the proof.

Remarks (a) If $t = 2$, then $\varepsilon_i = 1$ for all i, so that $\varepsilon = r$. Thus Theorem 2.2 does generalize the binary quasi-order theorem. Of course, the proof given here applies in the special case -- and, indeed, it then reduces to an argument equivalent to that shown to us by Gerald Preston.

(b) Theorem 0.2 may also be proved along the lines of our proof of Theorem 2.2. However, as we mentioned, that theorem had a refinement which our proof does not yield. Namely, it was shown that, if

$$b\begin{vmatrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{vmatrix}\ , \qquad k = \sum_{i=1}^{r} k_i$$

is a t-symbol in the sense of [HP4], that is, satisfying $(0.2)_t$, if it is contracted, and if r is even and $\gcd(b, a_i) \mid (t-1)$, then k is the quasi-order of t modulo b. Our

line of proof of Theorem 2.2 would enable us to conclude that, if $0 < m < k$ then $t^m \not\equiv \pm 1$ modulo b. But we would need to depend on the argument given in [HP4] to conclude that, in fact, $t^k \equiv 1$ modulo b.

(c) We have two dual algorithms for determining the quasi-order of t modulo b, which we are calling the ψ-algorithm and the φ-algorithm; it is a matter of taste and convenience which is used in any particular case. For $t = 2$, the ψ-algorithm seems simpler to handle -- and has, moreover, the merit of being intimately related to the paper-folding algorithm for constructing regular star polygons. For $t \geq 3$ it may well be that the φ-algorithm is sometimes simpler to handle. The φ-algorithm made no appearance in [HP3] and only appeared in [HP4] to prove the Order Theorem [HP4; Theorem 3.3].

3. EXAMPLES

It is illustrative to compare the ψ-algorithm used in this paper with the 'non-algorithm' based on $(0.2)_t$. Let us take the simplest example, $t = 3$. Then, as already stated, we do not always get a symbol in the sense of [HP4] for given b,a. Indeed, with $b = 11$, $a = a_1 = 2$, we have immediately $a_2 = 1$ since $11 = 2 + 3^2.1$; but then we are trapped in a hopeless spin! If we use the ψ-algorithm $\psi(a) = a'$, given by (1.3), then we must take $\bar{q} = 1$, so we simply have to decide, and record, at each stage whether to take $\varepsilon = 0$ or $\varepsilon = 1$; thus our 3-symbol (see (2.1)) is

$$11 \left|\begin{matrix} 2 & 1 & 4 & 5 \\ 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{matrix}\right|$$

We conclude that the quasi-order of 3 mod 11 is 5 and that $3^5 \equiv +1$ mod 11. As a second example of a 3-symbol, let us take $b = 25$, $a = 1$; then our 3-symbol is

$$25 \left|\begin{matrix} 1 & 8 & 11 & 4 & 7 & 2 \\ 1 & 1 & 2 & 1 & 2 & 3 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{matrix}\right|$$

We conclude that the quasi-order of 3 mod 25 is 10 and that $3^{10} \equiv -1$ mod 25.

In these two cases our algorithm yields a cyclic permutation of the entire subset of the set S (see Section 1) consisting of those a prime to b; this, however, is not necessary. With $b = 80$ and $t = 3$, we get the four reduced 3-symbols

$$80 \left|\begin{matrix} 1 \\ 4 \\ 0 \end{matrix}\right| , \quad 80 \left|\begin{matrix} 7 & 29 & 17 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{matrix}\right| , \quad 80 \left|\begin{matrix} 11 & 23 & 19 \\ 1 & 1 & 2 \\ 1 & 1 & 0 \end{matrix}\right| , \quad 80 \left|\begin{matrix} 13 & 31 & 37 \\ 1 & 1 & 2 \\ 0 & 0 & 0 \end{matrix}\right| .$$

Of course, it is quite obvious that the quasi-order of 3 mod 80 is 4 and $3^4 \equiv +1$ mod 80. Perhaps less obvious is the following example of two 11-symbols, with $b = 25$, which show that the quasi-order of 11 mod 25 is 5 and $11^5 \equiv +1$ mod 25.

$$25 \left|\begin{matrix} 1 & 9 & 6 & 4 \\ 1 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{matrix}\right| , \quad 25 \left|\begin{matrix} 2 & 7 & 12 & 8 & 3 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{matrix}\right|$$

Notice that the Ψ-algorithm is really very easy to execute by hand, even without the use of a calculator. The φ-algorithm is, however, more mechanical. Notice, too, that, in executing the Ψ-algorithm we are concerned with the residues mod t, while our conclusions are concerned with residues mod b.

We close with two "classical" applications of our algorithm in case t = 2; of course, as explained in Remark (a) of Section 3, it is then unnecessary to display the ε_i, since they are always 1. First the symbol

$$23 \begin{vmatrix} 1 & 11 & 3 & 5 & 9 & 7 \\ 1 & 2 & 2 & 1 & 1 & 4 \end{vmatrix}$$

shows that the quasi-order of 2 mod 23 is 11 and that $2^{11} \equiv 1 \bmod 23$. Thus the Mersenne number $2^{11} - 1$ is not prime.

Finally, the coup de grâce! The symbol

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

shows that the quasi-order of 2 mod 641 is 32 and that $2^{32} \equiv -1 \bmod 641$. Thus the Fermat number $2^{2^5} + 1$ is not prime. (Incidentally, as explained in [HP3], the symbol contains the information from which the complementary factor 6,700,417 may be derived -- the calculation should take about 3½ minutes by hand!)

Added in proof The interest in this problem among computer scientists is attested by the reference [5].

REFERENCES

[1] HILTON, P. and PEDERSEN, J., Approximating any regular polygon by folding paper: An interplay of geometry, analysis and number theory, Mathematics Magazine, Vol. 56, No. 3, 141-155 (1983).

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

[3] ----------, On certain algorithms in the practice of geometry and the theory of numbers, Publicacions, Sec. Mat., U. A. B., Vol. 29, 1, 31-64 (1985).

[4] ----------, On generalized symbols, orders and quasi-orders, ibid., 2-3, 123-144 (1985).

[5] BRILLHART, J., LEHMER, D.H., SELFRIDGE, J.L., TUCKERMAN, B., and WAGSTAFF, S.S., Factorizations of $b^n \pm 1$, b = 2,3,5,6,7,10,11,12 up to high powers, Contemporary Mathematics, Vol. 22, American Mathematical Society.