Pub. Mat. UAB
Vol. 29 Nº 1 Abril 1985

ON CERTAIN ALGORITHMS IN THE PRACTICE OF GEOMETRY AND THE THEORY OF NUMBERS

Peter Hilton and Jean Pedersen

0. Introduction

We demonstrated in [1] and [3] a systematic method of folding a straight strip of paper, by what we called a *primary folding procedure,* to approximate, to any desired degree of accuracy, a regular convex s-gon and certain regular star s-gons, provided that $s \in F$, the set of *folding numbers.* Here F is defined to be the set of all integers s of the form

$$s = (x,y) = \frac{2^{xy}-1}{2^x-1}, \text{ where } x \geqslant 1,\ y \geqslant 2.$$

Of course, such numbers s are odd.

By introducing *secondary* folds on the strip of paper we showed how it is possible to approximate regular $2^k s$-gons, where $s \in F$ and $k \geqslant 1$ (and we included, for the sake of completeness, the *exact* constructions of the regular 2^k-gons, $k \geqslant 2$).

The only remaining numbers $\geqslant 3$ are those of the form $2^k a$, where a is odd, $\neq 1$ and *not* a folding number and $k \geqslant 0$. However, the method for approximating those regular polygons can be described by a sequence of steps as follows (consult [1] for details).

First, since we know that, for any odd number a, $2^{\Phi(a)} \equiv 1 \bmod a$, where $\Phi(a)$ is the Euler totient function, it follows that a is a factor of some element of F, say s, with $s = a\ell$. We can use the primary folding procedure to obtain a strip of paper suitable for approximating a regular s-gon. If we then introduce k secondary fold lines at each point that would have been a vertex of the regular s-gon, we can use a longer strip of this folded tape to construct a regular 2^ks-gon. We then glue this 2^ks-gon to a piece of paper and fold on the lines connecting every ℓ^{th} vertex to produce the desired 2^ka-gon. In [2] and [3], we introduced an algorithm for finding the optimal $s \in F$ such that $a|s$.

In summary, the above procedures (using primary and secondary folds) provided us, in conjunction with the algorithm referred to above, with a systematic method that could be used to approximate regular convex s-gons for all $s \geqslant 3$. The same procedures produced many regular *star* s-gons, where $s \in F$. In fact, as discussed and proved in [2], for a given $s = (x,y) \in F$, the exact number of star s-gons produced by the primary folding procedure is $\frac{1}{2}\,\Phi(y)xy$. Further, these could be explicitly described.

In [2] we raised the question as to whether by generalizing in a natural way the primary folding, we might be able to avoid the gluing step described above, and also be able to fold *all* regular star polygons. In this paper we answer that question, in the affirmative.

Given a,b odd with $a < \frac{b}{2}$ and a prime to b, we describe in Section 1 a *generalized* primary folding procedure which approximates a regular star $\{\frac{b}{a}\}$-gon. There are, then, very obvious secondary procedures which allow us to remove the restriction that both a and b be odd. The generalization consists in allowing a procedure of arbitrary periodicity. The procedures in previous papers have all been of period 1 or 2.

An interesting aspect of the content of this paper, and the other papers we refer to, is the way the geometry motivates the number theory, and the subsequent interaction between the two topics. Indeed, although the *Quasi-Order Theorem* of Section 2 would stand on its own merits as an interesting piece of number theory, it is hard to imagine how one would have discovered it without the geometric motivation. Moreover, although our generalized primary folding procedure obviates the need to glue a constructed N-gon to a piece of paper in order to construct an M-gon, with $M|N$, the number theory generated by the gluing technique, described in [2] and [3], stands in its own right, and is in no sense superseded by the more sophisticated paper-folding procedures of this articles, nor subsumed in the number theory that arises from those more sophisticated procedures.

In Section 1 we describe the paper-folding procedure which enables us to construct arbitrary star polygons. We have sought, by including this section, to make the entire paper reasonably self-contained, though we are not actually advocating the neglect of our earlier papers on this subject. Section 2 opens with the definition of a symbol

$$b \left| \begin{array}{ccccc} a_1 & a_2 & \cdot & \cdot & a_r \\ \\ k_1 & k_2 & \cdot & \cdot & k_r \end{array} \right| , \qquad (0.1)$$

which may be regarded as encoding the instructions for folding a strip of tape to form a star $\{\frac{b}{a_i}\}$ -gon, with a_i,b odd, and $a_i < \frac{b}{2}$. The "code" is described in a typical case in Section 1 and, in general, in Appendix 1 (Section 4). However, this symbol also constitutes an interesting algorithm for determining the *quasi-order* of 2 mod b, that is, the smallest positive integer ℓ such that $2^\ell \equiv \pm 1$ mod b. Indeed, if a_1 is prime to b, then the quasi-order is $k = \sum_{i=1}^{r} k_i$ and the parity of r determines whether $2^k \equiv 1$ or $2^k \equiv -1$. Of course, the quasi-order, reinforced with the information provided by the parity of r, provides much more information than the order of 2 mod b. Examples are given in Appendix 2 (Section 5) to show how to apply the algorithm to obtain the symbol (0.1) and then how, in a given case, to obtain, from the symbol, the factor complementary to b in $2^k \pm 1$.

In Section 2 we describe the symbols, prove some basic properties, and enunciate the Quasi-Order Theorem. The theorem is proved in Section 3, where we also obtain some refinements of the theorem of further number-theoretical interest. We remark that an independent proof of the Quasi-Order Theorem was shown to us by Gerald Preston. This proof was based on the notion of Hasse functions (see, for example, [4]); however, the direction of proof does not take us through Theorem 2.5, which has an immediate application to paper-folding.

The paper closes with the two appendices already referred to; in the first we go back to the geometrical significance of the symbols, and, in the second, we discuss, as examples, Fermat and Mersenne non-primes.

A feature of the earlier papers [2] and [3] missing from the present paper was the generalization from 'base 2' -- the only base of geometrical interest, since we modestly confine ourselves to *bisecting* angles -- to 'base t', where t is an arbitrary positive integer $\neq 1$. It appears that this generalization leads to interesting difficulties when we try to introduce the analogs of our symbols in base t, since, in this general context, they may fail to exist for a given b. We propose to devote a sequel [6] to the study of generalized symbols and the (generalized) quasi-order problem.

1. How to fold regular star polygons

First we suppose that appropriate *fold*, of *crease*, lines have been made on our straight strip of paper and we describe the actual construction process for folding a $\{\frac{b}{a}\}$-gon[1], where a and b are mutually prime integers with $a < \frac{b}{2}$. Suppose, as illustrated in Figure 1, that we have a straight strip of paper that has creases along straight lines emanating from marked vertices $A_i, i=0,1,\ldots,$ at the top and bottom edges, and that, for a fixed k, those at the particular vertices A_{nk}, $n=0,1,2,\ldots,b$, which are on the top edge, form identical angles $\frac{a}{b}\pi$. Suppose further that these vertices are equally spaced (we describe below how you might obtain such a strip). Figure 1 (a) shows the beginning of the strip. If we fold this strip on $A_{nk}A_{nk+2}$ (as shown in Figure 1(b)) and then on $A_{nk}A_{nk+1}$ (as shown in Figure 1(c)), the direction of the *top edge* of the tape will be rotated through an angle of $2(\frac{a}{b}\pi)$ and the tape will be oriented the same way, with respect to the center of the polygon being delineated by its top edge. We call these two folds through A_{nk}, in that order, a $2(\frac{a}{b}\pi)$-*twist* at A_{nk}, and observe that, if a $2(\frac{a}{b}\pi)$-twist is performed at A_{nk} for $n = 0, 1, 2, \ldots, b-1$, the top edge of the tape will have turned through an angle of $2a\pi$ and the point A_{bk} will then be coincident with A_o. Thus the top edge of the tape will have visited every a^{th} vertex of a bounding regular convex b-gon, and hence determines a regular star $\{\frac{b}{a}\}$-gon.

[1] A closed sequence of b edges that visit, in order, every a^{th} vertex (mod b) of a bounding regular convex b-gon. We include the regular convex b-gon as the special case $a = 1$.

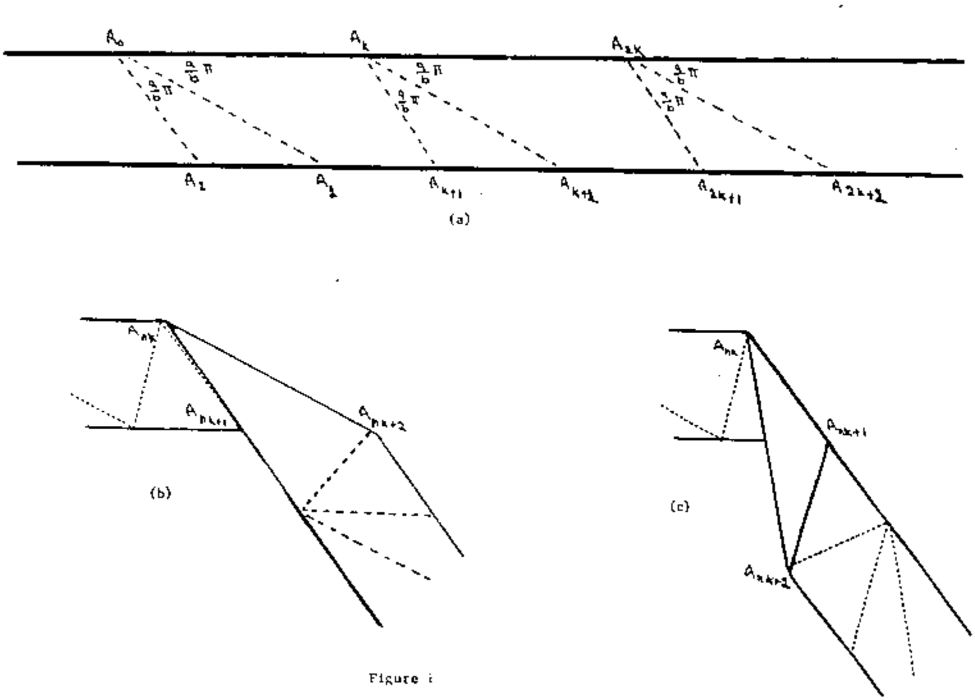


Figure i

We now explain how we obtained the desired crease lines in the strip of tape in the first place. Recall that we are seeking to construct a star $\{\frac{b}{a}\}$-gon where a, b are mutually prime positive integers with $a < \frac{b}{2}$. We assume first that a, b are odd. Thus we wish to have a strip of paper on which the angle $\frac{a}{b}\pi$ appears at regular intervals along the top edge. We designate the direction from left to right as the *forward* direction on the tape. We begin by marking a point A_0 on the top of the tape and making an *initial* crease line going in the downward forward direction from A_0 to A_1 at the bottom of tape, and *assume* that the angle it makes with the top edge is $\frac{a}{b}$; we call this the *putative* angle. The we continue to form new crease lines according to the following four rules:

(1) The first new crease line emanates from the vertex A_1.

(2) Each new crease line goes in the forward direction along the strip of paper.

(3) Each new crease line always *bisects* the angle between the last crease line and the edge of the tape from which it emanates.

(4) The bisection of angles at any vertex continues until a crease line produces a putative angle of the form $\frac{a'}{b}\pi$ where a' is an *odd* number; then the folding stops at that vertex and commences at the intersection point of that last crease line with the other side of the tape.

Let us consider the example $b = 11$, $a = 3$. Then we can see that if we begin with an angle of $\frac{3}{11}\pi$ at A_0 (as shown in Figure 2(a)) and adhere to the above rules we will obtain a strip of tape with the angles and creases (dotted lines) indicated in Figure 2(b). Adhering to the notation for the primary folding procedures in [1], [2] and [3], we could write this more generalized folding procedure as

$$\{d^1u^3d^1u^1d^3u^1\} \ . \qquad (1.1)$$

As before, this notation means that if we begin folding on the strip of paper at the place where there is one crease line sloping *upwards* then the first d^1 refers to the one bisection (producing a line in a downward direction) at A_{10n} (for an = 0,1,2, ...) on the top of the tape; the u^3 refers to the 3 bisections (producing creases in an upward direction) made at the bottom of the tape through A_{10n+1}; etc. However, the folding process is *duplicated* halfway through, so it suffices to write just the first three exponents in (1.1). In fact, we can denote (1.1) even more simply as

$$\{1,3,1\} \tag{1.2}$$

with the understanding that we fold $d^{k_1}u^{k_2}d^{k_3}u^{k_4}\ldots$ with the k_1, k_2, k_3, ... cycling, in order, repeatedly through the values 1, 3, 1, ...

We call (1.1) or (1.2) a primary folding procedure *of period* 3. Note that, in this terminology, the primary folding procedures we have hitherto considered in [1, 2, 3] were all of period 1 ($\{d^n u^n\}$) or period 2 ($\{d^m u^n\}$, $m \neq n$).

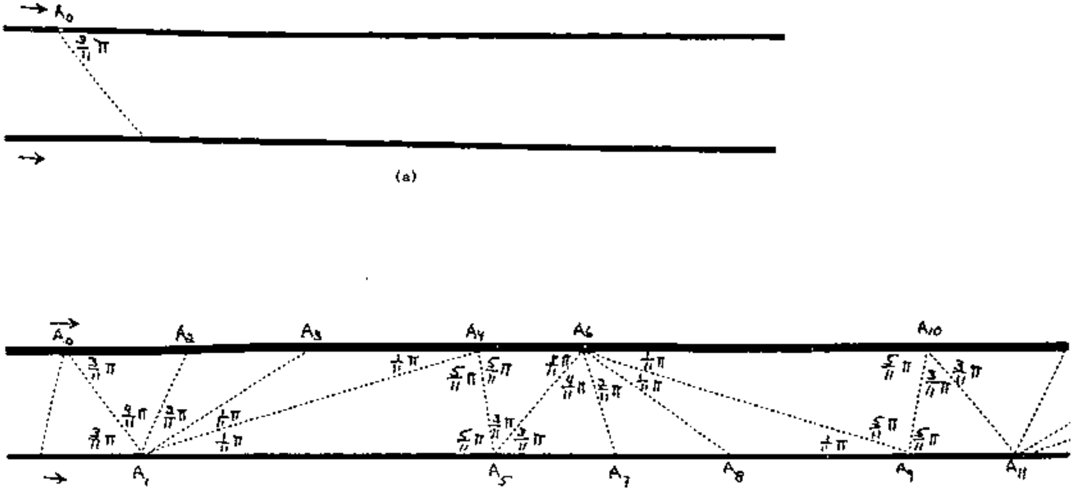
It is easy to see that, starting with any putative angle $\frac{a}{b}\pi$ (a, b odd, mutually prime, $a < \frac{b}{2}$), we will always obtain by our rules a primary folding procedure $k_1, k_2, \ldots, k_r$ which 'produces' this angle. We also note that, starting with the putative angle $\frac{3}{11}\pi$ at the top of the tape, we produced a putative angle $\frac{1}{11}\pi$ at the boton of the tape, then a putative angle $\frac{5}{11}\pi$ at the top of the tape, and so on. Thus if, indeed, our crease lines could have been used to fold a star $\{\frac{11}{3}\}$-gon, they could also have been used to fold a convex 11-gon and a star $\{\frac{11}{5}\}$-gon. This feature of our tape furnished with its crease lines obviously applies in general: other star b-gons will be available to us from the tape yielding the star

$\{\frac{b}{a}\}$-gon.

More still is true; for if there are crease lines enabling us to fold a star $\{\frac{b}{a}\}$-gon, there will be crease lines enabling us to fold star $\{\frac{b}{2^k a}\}$-gons, where $k \geqslant 0$ takes all values such that $2^{k+1}a < b$. Thus effectively we may dispose of the condition that a be odd, although our rules for introducing the crease lies are based on the assumption that a is odd. If a is even, our first step is to write $a = 2^k a_o$, with a_o odd.

One link is still missing in our chain. What is the rela ion of the putative angle to the true angle? It turns out -- the easy proof was given in [2] -- that if we repeat the folding rules, starting at the successive iterates of A_o (thus at $A_0, A_5, A_{10}, \ldots$ in Figure 2(b)), then *the actual angle rapidly converges to the putative angle.* Thus we obtain arbitrarily good approximations to regular star-polygons by starting sufficiently far along the tape. Reverting to our example of the $\{\frac{11}{3}\}$- gon, we showed in [2] that if our initial fold produces an angle of $\frac{1}{6}\pi$ at A_o then the acute angle at A_{10} would differ from $\frac{3}{11}\pi$ by less than

$$\frac{\frac{3}{11}\pi - \frac{1}{6}\pi}{2^{10}} \quad \text{which is about } 0{,}000325$$



(a)

(b)

Figure 2

As pointed out, although we began the folding in Figure 2 with an interest in producing an angle of $\frac{3}{11}\pi$ at equal intervals along the top of the tape we have produced much more. Observe that angles of $\frac{3}{11}\pi$, $\frac{5}{11}\pi$, $\frac{4}{11}\pi$, $\frac{2}{11}\pi$ and $\frac{1}{11}\pi$ appear (to the right of downward sloping transversals wiht equal angles adjacent to them) along the top of the tape. This means that we can use this tape to fold *any* of the star 11-gons. Figure 3 shows the star $\{\frac{11}{4}\}$-gon formed by making a $\frac{4}{11}\pi$-twist at A_{10n+6} (n = 0,1,2,...10). The excess tape that would 'stick out' at each vertex has been folded under to make the resulting model more appealing. It is the top of the tape that delineates the $\{\frac{11}{4}\}$-gon.

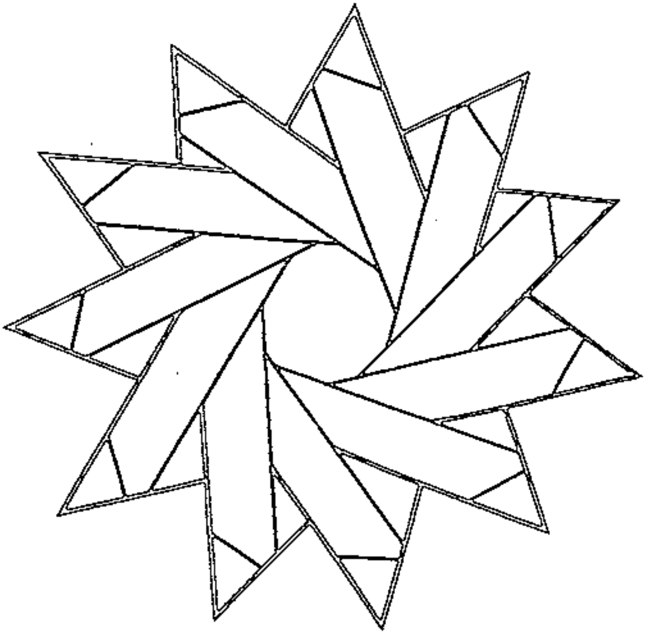


Figure 3

It is also not necessary for b to be odd. For, if a is odd and less than half of b with b even, we can write b as $2^k b'$, where b' is odd. Next carry out the foldind process, seeking an angle of $\frac{1}{b'}\pi$. This tape will always include a sequence of adjacent angles whose sizes are $\frac{1}{b'}\pi, \frac{1}{b'}\pi, \frac{2}{b'}\pi \ldots, \frac{2k-1}{b'}\pi$. It is then always possible to bisect (by secondary folds) the appropiate angle(s) so as to create the desired angles $\frac{a}{b}\pi$, but we will not go into details here, since this would take us from our main purpose. However, we give an example in Figure 4, which illustrates the construction of a $\{\frac{10}{3}\}$-gon where the angle of $\frac{\pi}{5}$ is created first and then this tape is used to get the necessary angle $\frac{3}{10}\pi$. First the tape is folded by a $\{d^2u^2\}$ procedure, which produces angles of $\frac{\pi}{5}$ along the top. Then a secondary fold line is introduced to bisect $A_{4n+1}A_{4n}A_{4n+2}$ for $n = 0,1,\ldots 9$. The construction of the $\{\frac{10}{3}\}$-gon is then completed by performing the $2\ (\frac{3}{10}\pi)$-twist at 10 equally spaced intervals along the top of the tape. The finished $\{\frac{10}{3}\}$-gon appears in Figure 5.

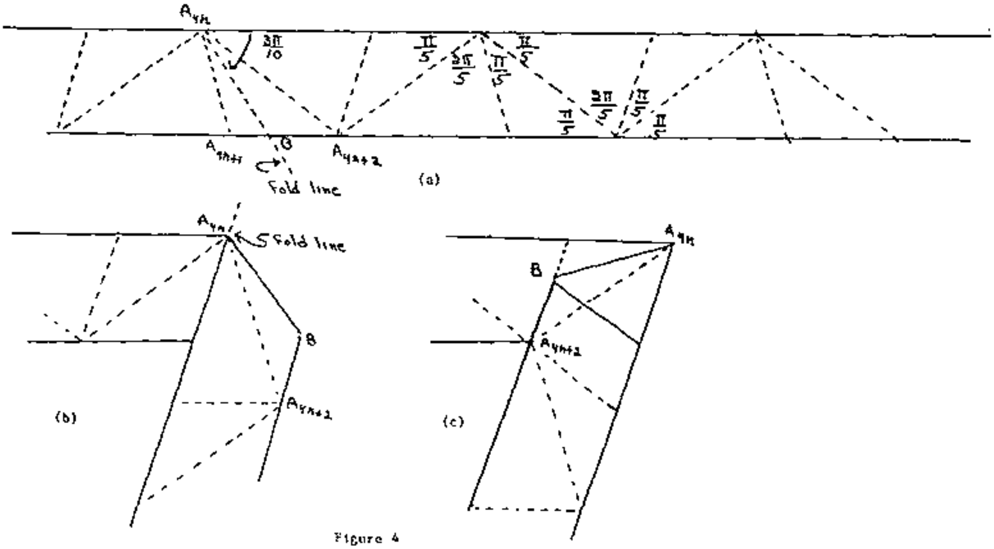


Figure 4

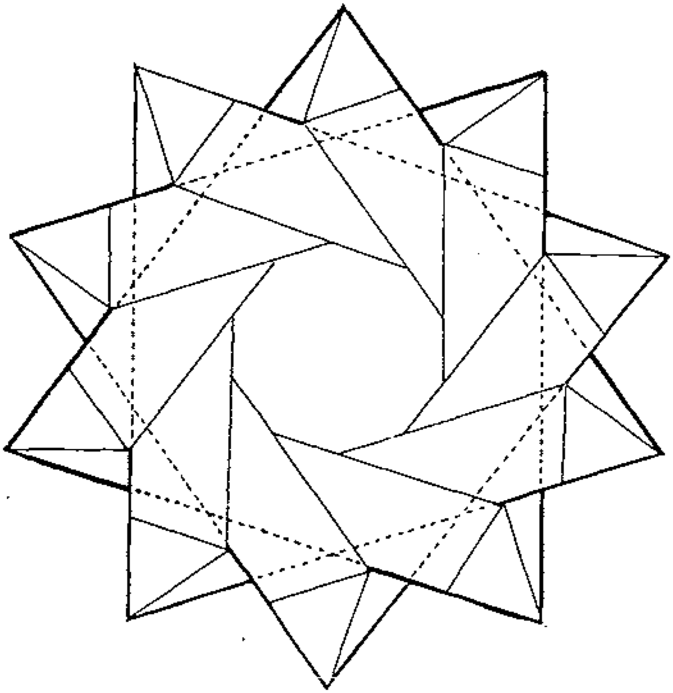


Figure 5

Let us return to the main example of our generalized folding procedure (in which $a = 3$ and $b = 11$) and look at the patterns in the arithmetic of the computations. We change notation in designating the vertices on the tape now, for convenience.[2]

[2] Here we are only interested in folding $\{\frac{b}{a}\}$-gons with a, b odd.

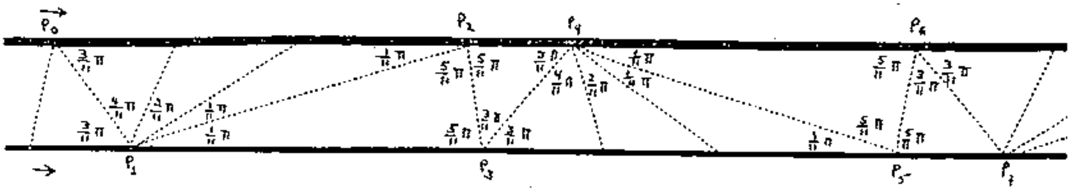


Figure 6

To bring out the relationship between the number of bisections at a vertex and the angle formed at that vertex we now change the labeling of the representative case shown in Figure 2(b) so that it appears as shown in Figure 6. Then we observe that

The angle to the right of P_n where $n =$	is of the form $\frac{a_n}{11}\pi$ where $a_n =$	and the number of bisections at $P_n =$
0	3	3
1	1	1
2	5	1
3	3	3
4	1	1
5	5	1

We could write this in shorthand form (which we will generalize in the next section) as follows:

$$(b=)11 \left| \begin{array}{ccc} (a=)3 & 1 & 5 \\ 3 & 1 & 1 \end{array} \right| \qquad (1.3)$$

As remarked, given any two odd numbers a and b, with

$a < \frac{b}{2}$, there is always a completely determined unique symbol like the one above (we do not need a,b relatively prime). Appropriately interpreted, we can use this symbol to read off the folding procedure that produces the angle of $\frac{a}{b}\pi$ along the top edge of the tape, so that a symbol such (1.3) encodes a folding procedure for producing a star $\{\frac{b}{a}\}$-gon, and also tells us what other star polygons we can obtain from the same tape (of course, for each symbol a diagram similar to Figure 6 can be drawn to illustrate the relative positions of the angles $\frac{a_n}{b}\pi$).

Before we close this section we would like to point out that the folding process described above is the *most efficient* one possible. That is, there could not be any folding procedure of this type that would procuce the required star polygons with fewer folds. It is also optimal from the point of view of "difficulty of execution", for it keeps the number of bisections at each vertex to a minimum. These last comments are explained as follows. If the folding procedure $\{k_1,k_2,\ldots,k_r\}$ produces the angle $\frac{a}{b}\pi$, then (see (2.3) and (2.4) $b \mid 2^k \pm 1$, where $k = \sum_{i=1}^{r} k_i$. If we adopt the procedures described in this section we will have a procedure $\{\ell_1, \ell_2,\ldots,\ell_s\}$ such that $\ell = \sum_{j=1}^{s} \ell_j$ is the *smallest* number m such that $b \mid 2^m \pm 1$, that is, the *quasi-order* of 2 mod b. Moreover, r will be a multiple of s and, suitably cycling the ℓ_j, each k_i is a multiple of ℓ_i.

All these facts are contained in the number-theoretical results of the next two sections.

2. Symbols and the quasi-order of 2 mod b

By the symbol

$$b \left| \begin{matrix} a_1 & a_2 & \dots & a_r \\ \\ k_1 & k_2 & \dots & k_r \end{matrix} \right| \qquad (2.1)$$

we understand that b is an odd positive integer, that a_i is an odd positive integer $< \frac{b}{2}$, $i = 1,2,\dots, r$, and that $k_1, k_2, \dots k_r$ are positive integers such that

$$b = a_i + 2^{k_i} a_{i+1}, \ i = 1,2, \dots ,r, \ a_{r+1} = a_1. \qquad (2.2)$$

Let us agree where convenient, to define a_i for all integers i by making a_i periodic in i, with period r, and similarly for k_i. We note that, given odd positive integers a, b with $a < \frac{b}{2}$, there is always a symbol (2.1) with $a_1 = a$, and that the symbol is unique up to *iteration*; here we say that (2.1) arises by iteration if there exists $s|r$ such that $a_{i+s} = a_i$, $k_{i+s} = k_i$, for all i. A proper iteration, that is, one in which $s \neq r$, is called a *repetition*.

Given $b, k_1, \dots, k_r$, the equations (2.2) have unique solutions, in the "unknowns" a_i, namely

$$Ba_i = bA_i, \ i = 1, 2, \dots, r, \qquad (2.3)$$

where $B = 2^k - (-1)^r,\ k = \sum_{i=1}^{r} k_i,$ (2.4)

and $A_i=2^{k-k_{i-1}} - 2^{k-k_{i-1}-k_{1-2}}+\dots+(-1)^r 2^{k_i}-(-1)^r,\ i=1,2,\dots,r.$ (2.5)

We note, for future use, that A_i *is independent of* k_{i-1}. We also remark that the solutions (2.3) of the equations (2.2) always exist, but that (for a given odd positive integer b) the numbers a_i given by (2.3) may fail to be integers. However, we have immediately

Proposition 2.1 (i) *The solutions of* (2.2) *are rational numbers* a_i *satisfying* $0 < a_i < \frac{b}{2}$;

(ii) *if any* a_i *is an integer, then all* a_i *are odd integers.*

Proof (i) It is clear form (2.4) and (2.5) that B, A_i are odd positive integers. Thus from (2.3), each a_i is a positive rational number. Now $2^{k_i}a_{i+1} = b - a_i < b$, since $a_i > 0$. Since a_{i+1} is positive and $k_i \geqslant 1$, we infer that $a_{i+1} < \frac{b}{2}$. To prove (ii), observe that $a_{i-1} = b - 2^{k_{i-1}}a_i$. Thus if a_i is an integer, a_{i-1} is an odd integer, and the result follows by finite induction.

As an application, consider B, A_i, given by (2.4), (2.5). As already observed, B and A_i are odd positive integers for all i. Moreover, it follows immediately from (2.3) that the solution of the equations $B = x_i + 2^{k_i}x_{i+1}$, $i = 1,2,\dots,r, x_{i+1} = x_1$, is $x_i = A_i$, so that

$$B = A_i + 2^{k_i}A_{i+1}. \qquad (2.6)$$

Thus, by Proposition 2.1,

$$B \left| \begin{matrix} A_1 & A_2 & \cdots & A_r \\ \\ k_1 & k_2 & \cdots & k_r \end{matrix} \right| \qquad (2.7)$$

is a symbol.

We will also need the following elementary propositions; the first is proved in [2].

Proposition 2.2 *In the symbol* (2.1), $\gcd(b,a_i)$ *is independent of* i.

Proposition 2.3 *if, in the symbol* (2.1), $k_i \geqslant n$, *then* $a_{i+1} < \frac{b}{2^n}$.

Proof This is obvious from (2.2).

Proposition 2.4 (Periodicity lemma) *If, in* (2.1), *there exists an* s *such that* $s|r$ *and* $k_{i+s} = k_i$ *for all* i, *then* $a_{i+s} = a_i$ *for all* i.

Proof It is clear from (2.5) that if $k_{i+s} = k_i$ for all i, then $A_{i+s} = A_i$ for all i. The result now follows from (2.3).

The periodicity lemma asserts that if the sequence $k_1, k_2, \ldots, k_r$ is a repeating sequence, then the symbol (2.1) is obtained by the same repetition. If there is no proper repetition, we say that the symbol (2.1) is *reduced* and write

$$b \begin{bmatrix} a_1 & a_2 & \ldots & a_r \\ k_1 & k_2 & \ldots & k_r \end{bmatrix} \qquad (2.8)$$

Then a general symbol (2.1) is obtained by *repeating* a unique reduced symbol; and a reduced symbol (2.8) is obtained by *compressing* a general symbol. Given positive odd integers a and b with $a < \frac{b}{2}$, there is a unique reduced symbol (2.8) with $a_1 = a$.

We come now to our main preliminary result.

Theorem 2.5 *Let* $k_1, k_2, \ldots, k_r$ *be positive integers with* $\sum_{i=1}^{r} k_i = k \geqslant 2$. *Then, for a given odd integer* $a_1 < 2^{k-1}$, *we have*

$$2^k-1 \left| \begin{matrix} a_1a_2\ldots a_r \\ \\ k_1k_2\ldots k_r \end{matrix} \right| \quad \textit{if and only if} \quad 2^{k+1}-1 \left| \begin{matrix} a_1a_2'\ldots a_{r-1}\ a_r' \\ \\ k_1k_2\ldots k_{r-1}\ k_r+1 \end{matrix} \right|$$

In either case, r *is even.*

Proof Assume the left-hand symbol. Then, by (2.3),

$$(2^k - (-1)^r)a_i = (2^k - 1)A_i.$$

If r were odd, we would have $2^k-1|a_i$, an evident contradiction. Thus r is even and $a_i = A_i$, for all i.

We now solve the equations $2^{k+1} - 1 = x_i + 2^{k_i} x_{i+1}$,

where $k'_i = k_i$, $1 \leqslant i \leqslant r-1$, $k'_r = k_r + 1$, so that $\sum_{i=1}^{r} k'_i = k+1 = k'$, say, to obtain (compare (2.6)) $x_i = A'_i$,
with (compare (2.5))

$$A'_i=2^{k'-k'_{i-1}} - 2^{k'-k'_{i-1}-k'_{i-2}} + \dots + (-1)^r 2^{k'_i} - (-1)^r \qquad (2.9)$$

Thus we obtain the symbol

$$2^{k+1} - 1 \left| \begin{matrix} A'_1 & A'_2 & \dots & A'_{r-1} & A'_r \\ \\ k_1 & k_2 & \dots & k_{r-1} & k_r+1 \end{matrix} \right|$$

However, we see from (2.9), recalling that A'_1 is independent of k'_r, that $A'_1 = A_1 = a_1$, establishing the existence of the right-hand symbol of the theorem. The converse is proved similarly.

There is a companion theorem as follows; we need not give an explicit proof.

<u>Theorem 2.5</u>* *Let* $k_1, k_2, \dots, k_r$ *be positive integers with* $\sum_{i=1}^{r} k_i = k \geqslant 1$. *Then, for a given odd integer* $a_1 < 2^{k-1}$, *we have*

$$2^k+1 \left| \begin{matrix} a_1 & a_2 & \dots & a_r \\ \\ k_1 & k_2 & \dots & k_r \end{matrix} \right| \text{ if and only if}$$

$$2^{k+1}+1 \left| \begin{matrix} a_1 & a'_2 & \dots & a'_{r-1} & a'_r \\ \\ k_1 & k_2 & \dots & k_{r-1} & k_r + 1 \end{matrix} \right|$$

In either case, r *is odd.*

We are now ready to state our main theorem.

Quasi-Order Theorem *Let* b *be an odd positive integer, and let* a_i *be an odd positive integer with* $a_i < \frac{b}{2}$ *and a prime to* b. *Then if* $b \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ k_1 & k_2 & \dots & k_r \end{bmatrix}$ *with* $\sum_{i=1}^{r} k_i = k$, *we have*

(i) k *is the minimal* ℓ *such that* $b|2^\ell \pm 1$,

(ii) $b|2^k-1$ *if* r *is even,* $b|2^k+1$ *if* r *is odd.*

We prove this theorem in the next section but we may imme diately anounce the following corollary, relating to the *order* of $2 \bmod b$.

Corollary 2.6 *With the same hypotheses as in the Quasi-Order Theorem, we have*

(i) *if* r *is even, then the order of* $2 \bmod b$ *is* k *and, even if* k *is even,* $2^{k/2} \not\equiv -1 \bmod b$;

(ii) *if* r *is odd, then the order of* $2 \bmod b$ *is* $2k$, *and* $2^k \equiv -1 \bmod b$.

3. Proof of the Main Theorem

We first study a special case of the main theorem and prove

Theorem 3.1 *Let* $\ell \geqslant 2$. *Then if* $2^\ell - 1 \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ \ell_1 & \ell_2 & \dots & \ell_r \end{bmatrix}$, *we have* $\sum_{i=1}^{r} \ell_i \,\Big|\, \ell$.

Proof We argue by induction on ℓ, the case $\ell = 2$ being trivial since $3 \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Thus we assume the theorem for $\ell \geqslant 2$ and prove it for $\ell + 1$. Let

$$2^{\ell+1} - 1 \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ \ell_1 & \ell_2 & \dots & \ell_r \end{bmatrix} \qquad (3.1)$$

If $r=1$ and $\ell_1 = 1$, the conclusion is trivially true. If not, it follows from the periodicity lemma that, for some i, $\ell_i \geqslant 2$. Without real loss of generality we may assume that $\ell_r \geqslant 2$ so that, by Proposition 2.3, $a_1 < 2^{\ell - 1}$. Thus, by our inductive hypothesis, we have

$$2^{\ell} - 1 \begin{bmatrix} a_1 & a_2' & \dots & a_s' \\ k_1 & k_2 & \dots & k_s \end{bmatrix} \qquad (3.2)$$

with $\sum_{i=1}^{s} k_i \,\Big|\, \ell$. By repetition, if necessary, we find the symbol

$$2^{\ell} - 1 \begin{vmatrix} a_1 & a_2' & \dots & a_t' \\ k_1 & k_2 & \dots & k_t \end{vmatrix} \qquad (3.3)$$

with $\sum_{i=1}^{t} k_i = \ell$. By Theorem 2.5 we deduce the symbol

$$2^{\ell+1} - 1 \left| \begin{matrix} a_1 & a''_2 & \dots & a''_{t-1} & a''_t \\ \\ k_1 & k_2 & \dots & k_{t-1} & k_t+1 \end{matrix} \right| \qquad (3.4)$$

Write $k'_i = k_i$, $1 \leqslant i \leqslant t-1$, $k'_t = k_t+1$. Then $\sum_{i=1}^{t} k'_i = \ell+1$.

Compressing, if necessary, we obtain

$$2^{\ell+1} - 1 \begin{bmatrix} a_1 & a''_2 & \dots & a''_u \\ \\ k'_1 & k'_2 & \dots & k'_u \end{bmatrix} \qquad (3.5)$$

with $\sum_{i=1}^{u} k'_i \,\Big|\, (\ell+1)$. By the uniqueness of the reduced symbol, as a function of b and a_o, we infer that (3.5) is identical with (3.1), so that the inductive step is achieved and the theorem is proved.

There is, of course, a companion theorem, with almost identical proof, namely,

<u>Theorem 3.1</u>* *Let* $\ell \geqslant 1$. *Then if*

$$2^{\ell} + 1 \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ \\ \ell_1 & \ell_2 & \dots & \ell_r \end{bmatrix} ,$$

we have $\sum_{i=1}^{r} \ell_i \,\Big|\, \ell$.

<u>Proof of the Quasi-Order Theorem</u> First let

$$b\begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ \\ k_1 & k_2 & \cdots & k_r \end{bmatrix}$$, with no restriction on $\gcd(a_1,b)$.

Let $\sum_{i=1}^{r} k_i = k$ and let k_0 be the minimal ℓ such that $b|2^\ell \pm 1$. If $2^{k_o} \pm 1 = bq$, then, obviously,

$$2^{k_o} \pm 1 \begin{bmatrix} a_1q & a_2q & \cdots & a_rq \\ \\ k_1 & k_2 & \cdots & k_r \end{bmatrix} .$$

Thus, by Theorem 3.1 or 3.1*, $k|k_0$.

Now suppose that a_1 is prime to b. Then, by (2.3) and (2.4),

$$(2^k - (-1)^r)a_i = bA_1.$$

Since b is prime to a_i, we have $b|2^k - (-1)^r$. Since $k|k_0$, the minimality of k_0 implies that $k = k_0$. Moreover it is plain that $b|2^k -1$ if r is even and $b|2^k + 1$ if r is odd.

Remarks (i) Note that we have proved that, if we remove from the hypotheses of the Quasi-Order Theorem the condition that a_1 be prime to b, and if k is *defined* as the minimal ℓ such that $b|2^\ell \pm 1$, then $\sum_{i=1}^{r} k_i | k$. If we write quo(b) for the quasi-order of 2 mod b, then this says that if

$$b\begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ \\ k_1 & k_2 & \cdots & k_r \end{bmatrix}$$, then $\sum_{i=1}^{r} k_i | \text{quo}(b)$. Moreover, the

Quasi-Order Theorem itself tells us that $\sum_{i=1}^{r} k_i = \mathrm{quo}(\frac{b}{d})$, where $d = \gcd(b,a_i)$. Of course, it is obvious on elementary grounds that $\mathrm{quo}(b') \mid \mathrm{quo}(b)$ if $b' \mid b$.

(ii) If we confine attention to odd numbers b of the form $2^\ell \pm 1$, then we immediately infer from what we have proved

<u>Proposition 3.2</u> *If* $\ell \geqslant 3$ *and* $2^\ell - 1 \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ \ell_1 & \ell_2 & \dots & \ell_r \end{bmatrix}$ *with* a_1 *prime to* $2^\ell - 1$, *then* $\sum_{i=1}^{r} \ell_i = \ell$, *and* r *is even.*

<u>Proposition 3.2*</u> *If* $\ell \geqslant 1$ *and* $2^\ell + 1 \begin{bmatrix} a_1 & a_2 & \dots & a_r \\ \ell_1 & \ell_2 & \dots & \ell_r \end{bmatrix}$ *with* a_1 *prime to* $2^\ell + 1$, *then* $\sum_{i=1}^{r} \ell_i = \ell$, *and* r *is odd.*

However, sharper results are available for such odd numbers $2^\ell \pm 1$. To prove these, we first present a combinatorial lemma. We adopt the notion of a *repeating* sequence used in the previous section. (See the remarks following Proposition 2.4).

<u>Lemma 3.3</u> *Let* $k_1, k_2, \dots, k_{r-1}$ *be fixed positive integers*[3]. *Then there exists at most one positive integer* k *such that* $(k_1, k_2, \dots, k_{r-1}, k)$ *is a repeating sequence.*

[3] Note that this lemma really has nothing to do with positive integers. The elements $k_1, k_2, \dots, k_{r-1}, k$ could be drawn from any set.

Proof Suppose $k_1, k_2, \ldots, k_r$ is a repeating sequence with period s; suppose $k'_1, k'_2, \ldots, k'_r$ is a repeating sequence with period t; and let $k_i = k'_i$, $i = 1, 2, \ldots, r-1$. We will prove that $k_r = k'_r$. Let $\ell = \mathrm{lcm}(s,t)$. Since $s | r$, $t | r$, we have $\ell | r$, so $r = \ell u$. If $u > 1$, then $k_r = k_\ell = k'_\ell = k'_r$, so assume $u = 1$, $r = \ell = \mathrm{lcm}(s,t)$. Then $s \nmid t$, since then $r = t$ and a sequence of length t cannot repeat with period t. Likewise $t \nmid s$. Recall that now $r = \mathrm{lcm}(s,t)$.

We now adopt the convention that the indices are residues modulo r, for the sake of simplicity of statement. Let $d = \gcd(s,t) = ms + nt$. Then $r \nmid nt$, $r \nmid ms$, $r \nmid d$, so

$$k_d = k_{nt} = k'_{nt} = k'_r ,$$

and

$$k'_d = k'_{ms} = k_{ms} = k_r .$$

Since $k_d = k'_d$, it follows that $k_r = k'_r$.

We now improve on our Propositions 3.2, 3.2* as follows.

Theorem 3.4 *Fix* a_1 *and let* ℓ *be chosen so that* $2^{\ell-1} > a_1$. *If* $2^\ell - 1 \begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ \ell_1 & \ell_2 & \cdots & \ell_r \end{bmatrix}$, *then, with at most one exceptional value of* ℓ, $\sum_{i=1}^{r} \ell_i = \ell$ *and* r *is even. If* $a_1 = 1$, *the excep-*

tional value is $\ell = 2$. *If* $a_1 > 1$, *the exceptional value, if it occurs, is such that* a_1 *is not prime to* $2^\ell - 1$.

Theorem 3.4* *Fix* a_1 *and let* ℓ *be chosen so that* $2^{\ell-1} > a_1$. *If* $2^\ell + 1 \begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ \ell_1 & \ell_2 & \cdots & \ell_r \end{bmatrix}$, *then, with at most one exceptional value of* ℓ, $\sum_{i=1}^{r} \ell_i = \ell$ *and* r *is odd. The exceptional value, if it occurs, is such that* a_1 *is not prime to* $2^\ell + 1$.

Proof We will be content to prove Theorem 3.4. Let $\bar{\ell}$ be the least ℓ such that $2^{\ell-1} > a_1$. Then we know from Theorem 3.1, by repetition if necessary, that

$$2^{\bar{\ell}} - 1 \begin{vmatrix} a_1 & a_2 & \cdots & a_r \\ \bar{\ell}_1 & \bar{\ell}_2 & \cdots & \bar{\ell}_r \end{vmatrix}, \text{ with } \sum_{i=1}^{r} \bar{\ell}_i = \bar{\ell}. \qquad (3.6)$$

Then, by Theorem 2.5, for any $m \geqslant 0$,

$$2^{\bar{\ell}+m} - 1 \begin{vmatrix} a_1 & a_2' & \cdots & & a_r' \\ \bar{\ell}_1 & \bar{\ell}_2 & \cdots & \bar{\ell}_{r-1} & \bar{\ell}_r + m \end{vmatrix} \qquad (3.7)$$

Now, by Lemma 3.3, the sequence $(\bar{\ell}_1, \bar{\ell}_2, \ldots, \bar{\ell}_{r-1}, \bar{\ell}_r + m)$ repeats for at most one value of m, so that, with this single possible exception,

$$2^{\bar{\ell}+m} - 1 \begin{bmatrix} a_1 & a_2' & \cdots & & a_r' \\ \bar{\ell}_1 & \bar{\ell}_2 & \cdots & \bar{\ell}_{r-1} & \bar{\ell}_r + m \end{bmatrix} \qquad (3.8)$$

Theorem 2.5 also tells us that if (3.8) holds r is even. If

$a_1 = 1$, then $3 \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is exceptional. If $a_1 > 1$, then the proof of the theorem is completed by appeal to the Quasi-Order Theorem.

Remarks. (i) Of course, in the excepcional case $\sum_{i=1}^{r} \ell_i \mid \ell$.

(ii) The smallest number a_1 such that there is no exceptional ℓ, either for $2^{\ell}-1$ or $2^{\ell}+1$, is $a_1 = 19$.

4. Appendix 1: remark on notation, with reference to folding procedures.

Let us start with an example. If we wish to fold an angle of $\frac{19\pi}{63}$, appearing at the top of the tape, then our procedure, given an arbitrary starting line AA_0 on the tape is to fold $d^1u^2d^2u^1$ (see Figure 7).

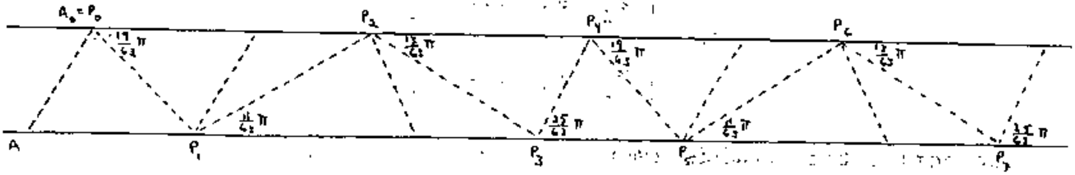


Figure 7

Then the angle $\frac{19\pi}{63}$ appears, to a better and better approximation, at P_0, P_4, P_8, ... Now we have the reduced symbol

$$63 \begin{bmatrix} 19 & 11 & 13 & 25 \\ 2 & 2 & 1 & 1 \end{bmatrix} \qquad (4.1)$$

The entries along the first row, 19, 11, 13, 25, represent the angles appearing sequentially at $P_{4n}, P_{4n+1}, P_{4n+2}, P_{4n+3}$ respectively; however the entries along the second row 2, 2, 1, 1, represent the folding instructions pertaining to $P_{4n+1}, P_{4n+2}, P_{4n+3}, P_{4n}$. This discrepancy suggests that we should consider rewriting the symbol so that the folding instruction at a particular vertex appears immediately below the 'star-number' corresponding to that vertex. This would require us to rewrite (4.1) as, say

$$63 \begin{Bmatrix} 19 & 11 & 13 & 25 \\ 1 & 2 & 2 & 1 \end{Bmatrix} \qquad (4.2)$$

We pass from (4.1) to (4.2) by a cyclic permutation of the folding instructions, bringing the last into the first position. Thus, given a symbol

$$b \begin{vmatrix} a_1 & a_2 & \ldots & a_r \\ k_1 & k_2 & \ldots & k_r \end{vmatrix} \qquad (4.3)$$

we define the *modified symbol* to be

$$b \begin{pmatrix} a_1 & a_2 & \ldots & a_r \\ k_r & k_1 & \ldots & k_{r-1} \end{pmatrix} \qquad (4.4)$$

Now in practice we are given b and a_1 and wish to obtain a (reduced) symbol (4.3). We could, of course, then form the modified symbol (4.4), which encodes the folding instructions and the list of star b-gons which can be folded from the same tape as that used to fold a $\{ \frac{b}{a_1} \}$-gon. If we are impatient to begin the folding we may well wish to find k_r in

(4.4) without going through the entire process of obtaining the (reduced) symbol (4.3). This, however, is easy.

For a symbol is generated by considering the permutation f of the set $S = S_b$ of odd numbers $< \frac{b}{2}$, given by the rule: write $b - a$, for $a \in S$, as $2^k a'$, where a' is an odd number, and set $f(a) = a'$. We would then write, in our symbol,

$$b \left| \begin{matrix} \cdot & \cdot & \cdot & \cdot & a & a' & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & k & \cdot & \cdot & \cdot & \cdot & \cdot \end{matrix} \right|$$

Thus, to determine what appears below a in our modified symbol, we must consider the permutation g inverse to f. Then g is given by the rule: choose ℓ maximal so that $2^\ell a < b$, and set $g(a) = b - 2^\ell a$. This maximal ℓ is then precisely what appears below a in the modified symbol.

The modified symbol has a further aesthetic advantage over the symbol we have used. For, with the modified symbol, the key Theorem 2.5 reads

<u>Theorem 2.5</u> *Let* $k_1, k_2, \ldots, k_r$ *be positive integers with* $\sum_{i=1}^{r} k_i = k \geqslant 2$. *Then for a given odd integer* $a_1 < 2^{k-1}$, *we have*

$$2^k - 1 \begin{pmatrix} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{pmatrix} \quad \textit{if and only if} \quad 2^{k+1} - 1 \begin{pmatrix} a_1 & a_2' & \cdots & a_r' \\ k_1 + 1 & k_2 & \cdots & k_r \end{pmatrix}.$$

Such a reformulation (as also of Theorem 2.5*) is then *immediately* translatable into fold-theoretic language! For it tells us that, if we know how to fold our strip of paper to produce a star $\{\frac{2^k-1}{a}\}$-gon, then, to produce a star $\{\frac{2^{k+1}-1}{a}\}$-gon, we introduce one more fold line precisely at those vertices on the top edge of the tape which are destined to become vertices of our polygon.

5. Appendix 2: a few well-chosen examples

We note that, if

$$b \left[\begin{array}{cccc} a_1 & a_2 & \cdots & a_r \\ k_1 & k_2 & \cdots & k_r \end{array}\right], \quad \sum_{i=1}^{r} k_i = k,$$

with $a_1 = 1$, then, by (2.3),

$$2^k - (-1)^r = bA_1, \tag{5.1}$$

where, by (2.5)

$$A_1 = 2^{\sigma_{r-1}} - 2^{\sigma_{r-2}} + \ldots + (-1)^r 2^{\sigma_1} - (-1)^r, \tag{5.2}$$

with $\sigma_j = \sum_{i=1}^{j} k_i$. (5.3)

Moreover, by our main theorem,

$$k = \text{quo}(b).$$

Let us apply this to case $b = 641$. We obtain, by our algorithm,

$$641 \left[\begin{array}{ccccccccc} 1 & 5 & 159 & 241 & 25 & 77 & 141 & 125 & 129 \\ 7 & 2 & 1 & 4 & 3 & 2 & 2 & 2 & 9 \end{array} \right] \qquad (5.4)$$

Thus we infer, since $k = 32$, $r = 9$, that

$$\text{quo}(641) = 32$$

and, indeed, that $2^{32} + 1 \equiv 0 \bmod 641$.

Moreover, we know from (5.1)

$$2^{32} + 1 = 641A_1,$$

and, from (5.2)

$$\begin{aligned} A_1 &= 2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^{10} + 2^{9} - 2^{7} + 1 \\ &= 6700417. \end{aligned}$$

This is, of course, Euler's famous factorization showing that $2^{2^5} + 1$ is not a (Fermat) prime.[4] Only the paper-folding fanatic would take the view that the principal interest of (5.4) is that it shows how to fold the regular convex 641-gon and certain star 641-gons.

As a second example, consider the symbol

$$23 \left[\begin{array}{cccccc} 1 & 11 & 3 & 5 & 9 & 7 \\ 1 & 2 & 2 & 1 & 1 & 4 \end{array} \right] .$$

Here $k = 11$, $r = 6$, so that

[4] See, for example, the front cover of [5].

$$\mathrm{quo}(23) = 11, \quad 2^{11} - 1 \equiv 0 \bmod 23,$$

and, again by (5.2), the complementary factor is

$$A_1 = 2^7 - 2^6 + 2^5 - 2^3 + 2 - 1 = 89 .$$

Thus $2^{11} - 1 = 23 \cdot 89$ and is not a (Mersenne) prime.

References

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

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

[3] ------------------------, "Folding regular star polygons and number theory", The Mathematical Intelligencer, Vol. 7 (1), 1985 (15 - 26).

[4] K.R. Matthews and A.M. Watts, "A generalization of Hasse's generalization of the Syracuse algorithm", Acta Arithmetica XLIII, 1983 (75 - 83).

[5] Mathematical Intelligencer, Vol. 6. Nº 3, 1984, front cover.

[6] Peter Hilton and Jean Pedersen, "On generalized symbols, orders and quasi-orders" (to appear).

Rebut el 16 d'octubre del 1984

Department of Mathematics
University of Santa Clara
Santa Clara
California 95053
U.S.A.