MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 189
JANUARY 1990, PAGES 345-376

# ON THE MOD 2 RECIPROCATION OF INFINITE MODULAR-PART PRODUCTS AND THE PARITY OF CERTAIN PARTITION FUNCTIONS

RICHARD BLECKSMITH, JOHN BRILLHART, AND IRVING GERST

*Dedicated to the memory of Kurt Mahler*

ABSTRACT. An infinite, modular-part (MP) product is defined to be a product of the form $\prod_{n\in S}(1-x^n)$, where $S=\{n\in \mathbf{Z}^+ : n\equiv r_1,\ldots,r_t \pmod m\}$. Some products of this kind have a mod 2 reciprocal that is also an MP product, while others do not. A complete method is first developed which determines if a given MP product has an MP reciprocal modulo 2 and finds it if it does. Next, a graph-theoretic interpretation of this method is made from which a streamlined algorithm is derived for deciding whether the given MP product is such a reciprocal. This algorithm is then applied to the single-variable Jacobi triple product and the quintuple product to determine the cases when these products have an MP reciprocal (mod 2). When this occurs—and this occurs in infinitely many cases—the parity of the associated partition function can readily be found. A discussion is also made of the probability that a given MP product with modulus $m$ has an MP reciprocal (mod 2).

## 1. INTRODUCTION

In this paper we will be dealing with infinite products of the form

$$\prod_{n\in S}(1-x^n), \tag{1}$$

where $S=\{n\in \mathbf{Z}^+ : n\equiv r_1,\ldots,r_t \pmod m\}$ and $r_1,\ldots,r_t$ are distinct, positive residues of a given modulus $m$. Products of this form will be referred to as "**MP** products" because their exponents are "modular parts." (It should be noted that there are no repeated factors in the MP product defined here.) As in [4, equation (6)], we denote the product in (1) by $(r_1,\ldots,r_t)_m$.

In studying the parity of partition functions, we will be concerned in this paper with:

(i) the partition function $p(S;n)$ generated by the reciprocal of a given MP product, i.e.,

$$\sum_{n=0}^{\infty} p(S;n)x^n = \frac{1}{\prod_{n\in S}(1-x^n)}; \tag{2}$$

Received January 25, 1989; revised April 10, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 05A15, 05A17; Secondary 05-04, 05C05.
*Key words and phrases.* Mod 2 reciprocation, infinite modular-part products, Jacobi triple product, quintuple product.


0025-5718/90 $1.00 + $.25 per page

(ii) computing the mod 2 reciprocal of an MP product and determining if it is an MP product, i.e., whether

$$\frac{1}{\prod_{n\in S}(1-x^n)} \equiv \prod_{n\in S_1}(1-x^n) \pmod 2 \tag{3}$$

for some corresponding modular index set $S_1$;

(iii) the power series expansion of the product in (3), i.e.,

$$\prod_{n\in S_1}(1-x^n) = \sum_{n=0}^{\infty} a_n x^n . \tag{4}$$

When the reciprocal in (3) is MP and the expansion in (4) is known, we are in a position to compute the parity of the partition function, since then

$$p(S; n) \equiv a_n \pmod 2 .$$

(In actual practice we know the expansion in (4) for the set $S_1$ and work backwards through the reciprocal in (3) to obtain the set $S$. Cf. §9.)

Our attention in this paper is directed toward solving the two basic questions raised in (3), namely, does an MP product have a mod 2 reciprocal that is MP, and if it does, what is the reciprocal? In previous papers we have already dealt with a few cases of this problem. In [2, pp. 746-747], the reciprocal was computed using a simple doubling procedure described in §3 below. In another case [3, equation (4)], we found a reciprocal by a method based on an identity of Euler, which is discussed in §4. In the general case, however, either method often continued indefinitely, so it was unclear whether the method itself was inadequate to find the reciprocal, or whether an MP reciprocal just did not exist. (Here and throughout this paper, the term "MP reciprocal" will mean "MP reciprocal (mod 2)".) In those cases where an MP reciprocal actually did exist, we were able to determine this fact and to find the $r_i$ and $m$ in (1) through the use of a heuristic algorithm described in §2. Armed with this information, we could then appropriately modify the particular method to verify the correctness of the heuristically computed reciprocal.

In the general case, such an ad hoc approach was clearly awkward and uninstructive, and it was only when an elaborated form of the Euler reciprocation method of §4 was developed that the reciprocation problem was completely solved. This general algorithm is discussed in §§5 and 7. In §8 we give a streamlined decision algorithm based on the graph-theoretic interpretation of "doubling mod $m$" presented earlier in §6. An application of the second algorithm is made in §9 to determine the conditions under which Jacobi triple products and quintuple products have MP reciprocals modulo 2. It is clear from the results of this section how to obtain parity theorems for partition functions associated with infinitely many of these products. Additional parity results are obtained from eleven identities appearing in [3] and [4] that do not come from the Jacobi triple product or the quintuple product. The paper concludes with a

calculation of the probability that an MP product with an even modulus has an MP reciprocal.

## 2. The Heuristic Pattern Recognition (HPR) algorithm

We begin by establishing a result which shows that the mod 2 reciprocal of any product (not necessarily an MP product) of binomials $1 - x^{a_i}$, where the exponents form an increasing sequence of positive integers, is a product of the same kind. Let $\mathcal{S}$ be the set of all increasing finite or infinite sequences of positive integers. Throughout this paper, the congruences will be understood to be modulo 2.

**Proposition 1.** *For each* $\{a_i\} \in \mathcal{S}$ *there exists a unique* $\{b_i\} \in \mathcal{S}$ *such that*

$$\frac{1}{\prod_i (1 - x^{a_i})} \equiv \prod_j (1 - x^{b_j}).$$

*Proof.* The product $\prod_i (1 - x^{a_i})$ expands uniquely into a power series $1 + \sum_{n=1}^{\infty} \alpha_n x^n$. Since a power series has an inverse if and only if its constant term is a unit, we have

$$\frac{1}{1 + \sum_{n=1}^{\infty} \alpha_n x^n} \equiv 1 + \sum_{n=1}^{\infty} \beta_n x^n.$$

Here the $\beta_n$ are uniquely determined by the Cauchy recursion formula

$$\beta_n \equiv \sum_{i=1}^{n} \alpha_i \beta_{n-i}, \qquad n \geq 1, \quad \beta_0 = 1.$$

Finally, we note that the series $1 + \sum \beta_n x^n$ factors uniquely mod 2 by the greedy algorithm into a product $\prod_j (1 - x^{b_j})$. (See [4, §6, function *DeadEndDegree*].) □

In actual practice the exponents $b_j$ of the reciprocal product can be obtained directly from the $a_i$'s (without the use of intermediate power series) by employing the following equation suggested to us by William D. Blair:

$$\frac{1}{1 - x^t} = \prod_{k=0}^{\infty} (1 + x^{2^k t}). \tag{5}$$

Let $L$ be a fixed positive integer, usually about 1000. Expand $\prod_{a_i \leq L} (1 - x^{a_i})^{-1}$ into a direct product $\prod_{b_j \leq L} (1 - x^{b_j})$ by recursively computing the factors of the partial products:

$$P_k(x) = \prod_{i=1}^{k} \frac{1}{1 - x^{a_i}} \equiv \prod_{t \in S_k} (1 - x^t) \pmod{x^{L+1}, 2}, \quad k \geq 1.$$

Here, $S_1 = \{a_1, 2a_1, \ldots, 2^r a_1\}$, where $2^r a_1 \leq L < 2^{r+1} a_1$. To obtain the next partial product $P_{k+1}(x)$, delete $a_{k+1}$ from $S_k$ to obtain $S_{k+1}$, if $a_{k+1} \in S_k$; otherwise, use (5) to expand $1/(1 - x^{a_{k+1}})$ into factors up to degree $L$ and

append their exponents $a_{k+1}, 2a_{k+1}, 4a_{k+1}, \ldots$ to $S_k$ to form $S_{k+1}$. Note that these latter exponents are not in $S_k$, since $t \in S_k$ for $t > a_k$ if and only if $\frac{t}{2} \in S_k$. In order to avoid sorting the exponents in the reciprocal, we introduce the following characteristic function for $\{a_i\} \in \mathcal{F}$:

$$\chi_n^{(a)} = \begin{cases} 1, & \text{if } n \in \{a_i\}, \\ 0, & \text{otherwise.} \end{cases}$$

Then we can write $\prod_t (1 - x^{a_t}) = \prod_{n=1}^{\infty} (1 - \chi_n^{(a)} x^n)$.

The following algorithm computes $\{\chi_n^{(b)}\}_{n=1}^{L}$ from $\{\chi_n^{(a)}\}_{n=1}^{L}$ for a fixed limit $L$.

**Algorithm.** *Invert*

```
for i = 1 to L do
    χ_i^(b) = 0;
for i = 1 to L do
    if χ_i^(a) = 1 then
    begin
      χ_t^(b) = 1 − χ_t^(b)
      if χ_i^(b) = 1 then
      begin
        k = 2i
        while k ≤ L do
        begin
          χ_k^(b) = 1
          k = 2k
        end
      end
    end.
```

The second step of the HPR method is to search the output sequence $\{\chi_n^{(b)}\}_{n=1}^{L}$ of *Invert* for a pattern which repeats at least once. *Pattern Recognizer* inputs a sequence $\{\chi_n\}_{n=1}^{L}$ of 0's and 1's and outputs the smallest period $m \leq \frac{L}{2}$ such that $\{\chi_n^{(b)}\}_{n=1}^{L}$ repeats; otherwise a 0 is returned.

**Algorithm.** *Pattern Recognizer*

```
for m = 1 to L/2 do
    begin
      n = m + 1
      while n ≤ L and χ_n = χ_{n−m} do
        n = n + 1
      if n > L then return( m )
    end
    return(0).
```

Putting these two algorithms together gives the HPR method, which in brief is:

$$\{\chi_n^{(a)}\}_{n=1}^{L} \to \{\chi_n^{(b)}\}_{n=1}^{L} \to \begin{cases} \{m, r_1, \ldots, r_t\} \\ 0. \end{cases}$$

Note that this algorithm gives the smallest possible modulus $m$.

**Example 1.** Consider the reciprocation of $(1, 5, 6)_6$, with $L = 24$. Table 1 lists the values of $\chi_n^{(b)}$ for $1 \le n \le 24$, as each $1/(1 - x^{a_t})$ is expanded into a product by *Invert*. HPR then recognizes the repeated pattern {1 1 0 1 1 1 1 1 0 1 1 0} in the last row. This suggests that

$$\frac{1}{(0, \pm 1)_6} \equiv (1, 2, 4, 5, 6, 7, 8, 10, 11)_{12},$$

which will be verified in Example 3 of the next section.

TABLE 1

| $a_t$ | | | | | |
|---|---|---|---|---|---|
| 1 | 1 1 0 1 0 | 0 0 1 0 0 | 0 0 0 0 0 | 1 0 0 0 0 | 0 0 0 0 |
| 5 | 1 1 0 1 1 | 0 0 1 0 1 | 0 0 0 0 0 | 1 0 0 0 1 | 0 0 0 0 |
| 6 | 1 1 0 1 1 | 1 0 1 0 1 | 0 1 0 0 0 | 1 0 0 0 1 | 0 0 0 1 |
| 7 | 1 1 0 1 1 | 1 1 1 0 1 | 0 1 0 1 0 | 1 0 0 0 1 | 0 0 0 1 |
| 11 | 1 1 0 1 1 | 1 1 1 0 1 | 1 1 0 1 0 | 1 0 0 0 1 | 0 1 0 1 |
| 12 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 0 1 0 | 1 0 0 0 1 | 0 1 0 1 |
| 13 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 1 1 0 | 1 0 0 0 1 | 0 1 0 1 |
| 17 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 1 1 0 | 1 1 0 0 1 | 0 1 0 1 |
| 18 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 1 1 0 | 1 1 1 0 1 | 0 1 0 1 |
| 19 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 1 1 0 | 1 1 1 1 1 | 0 1 0 1 |
| 23 | 1 1 0 1 1 | 1 1 1 0 1 | 1 0 1 1 0 | 1 1 1 1 1 | 0 1 1 1 |
| 24 | **1 1 0 1 1** | **1 1 1 0 1** | **1 0** 1 1 0 | 1 1 1 1 1 | 0 1 1 0 |

*Remark.* To express the reciprocal of a series $1 + \sum_{n=1}^{\infty} \alpha_n x^n$ as a product $\prod_{j=1}^{\infty}(1 - x^{b_j})$, use the following

**Algorithm.** *Series Invert*

We use the intermediate array $\beta(x) = \sum_{t=0}^{L} \beta_n x^n$.

```
j = 0
β(x) = 1
for n = 1 to L do
    if α_n ≠ β_n then
    begin
        j = j + 1
        b_j = n
        β(x) = β(x)/(1 − x^n), using [2, equation (5)]
    end.
```

## 3. THE DOUBLING METHOD

The following proposition gives two (mod 2) rules used in the doubling method and elsewhere in this work.

**Proposition 2.** *We have*

(6) [*doubling rule*] $(a_1, \ldots, a_r)_n^2 \equiv (2a_1, \ldots, 2a_r)_{2n}$

(7) [*extension rule*] $(a_1, \ldots, a_r)_n = (a_1, \ldots, a_r, a_1 + n, \ldots, a_r + n)_{2n}$.

*Proof.* Equation (6) follows from the congruence

$$\prod_{k=1}^{\infty}(1 - x^{kn+r})^2 \equiv \prod_{k=1}^{\infty}(1 - x^{2kn+2r}).$$

Equation (7) is clear. □

Briefly, this method consists of multiplying the top and bottom of $1/(a_1, \ldots, a_r)_n$ by $(a_1, \ldots, a_r)_n$, then using (6) on the square on the bottom and (7) on the top, canceling as many bottom factors into the top as possible. If some factors remain on the bottom, repeat the process again and again until either all the denominator factors have been canceled into the top or it becomes clear that some factors will never cancel and the process will continue indefinitely.

**Example 2.** This is essentially a "new notation" proof of [2, (18); 3, Table 1]:

$$\frac{1}{(1, 4, 5)_5} = \frac{(1, 4, 5)_5}{(1, 4, 5)_5^2} \equiv \frac{(1, 4, 5, 6, 9, 10)_{10}}{(2, 8, 10)_{10}} = \frac{(1, 4, 5, 6, 9)_{10}(2, 8)_{10}}{(2, 8)_{10}^2}$$
$$\equiv \frac{(1, 2, 5, 8, 9)_{10}(4, 6, 14, 16)_{20}}{(4, 16)_{20}} = (\pm 1, \pm 2, 5)_{10}(\pm 6)_{20}.$$

**Example 3.** The unembellished doubling method often goes into an infinite loop, as the following example shows:

$$\frac{1}{(1, 5, 6)_6} = \frac{(1, 5, 6)_6}{(1, 5, 6)_6^2} \equiv \frac{(1, 5)_6(6, 12)_{12}}{(2, 10, 12)_{12}} \equiv \frac{(1, 5)_6(6)_{12}(2, 10)_{12}}{(4, 20)_{24}} \equiv \cdots.$$

Here the odd integers $(1, 5)_6$ have been separated out, because they play no further part in canceling the even factors in the bottom. Furthermore, it is clear that continuing the procedure will never create any number from $(6)_{12}$ that will cancel numbers on the bottom. The failure of the doubling method to end and produce the reciprocal is a weakness of the method. In this case the reciprocal actually exists, and Example 1 suggests that the reciprocal is $(1, 2, 4, 5, 6, 7, 8, 10, 11)_{12}$. The following proof, in which the top and bottom of the original fraction are first multiplied by $(2, 4, 8, 10)_{12}(6)_6$ and then (6) and (7) are applied, verifies this:

$$\frac{1}{(1, 5, 6)_6} = \frac{(2, 4, 8, 10)_{12}(6)_6}{(1, 5, 7, 11)_{12}(2, 4, 8, 10)_{12}(6)_6^2}$$
$$\equiv \frac{(2, 4, 8, 10, 14, 16, 20, 22)_{24}(6, 12)_{12}}{(1, 2, 4, 5, 7, 8, 10, 11)_{12}(12)_{12}}$$
$$\equiv (1, 2, 4, 5, 6, 7, 8, 10, 11)_{12}.$$

## 4. The Euler reciprocation method

An alternative method of reciprocating is based on the following identity of Euler:

$$\prod_{n=1}^{\infty}(1+x^n)(1-x^{2n-1}) = 1.$$

In our notation this equation implies that

$$(1)_2^2(2)_2 \equiv 1. \tag{8}$$

This identity always allows us to cancel the denominator in a reciprocal product after substituting $(1)_2^2(2)_2$ in an appropriate form for the 1 in the numerator. (We should point out that since the form of (1) does not include multiple factors, we are making a restricted study here that is comparable to one in elementary number theory in which only square-free integers are allowed in the final answer. If this restriction were removed, this paper would immediately reduce to a very simple and short one, since then from (8) any MP product would have an MP reciprocal with at worst squares on some of its factors.)

**Example 4.** This method succeeds in producing the reciprocal for the product in Example 3, where the straightforward doubling method had failed:

$$\frac{1}{(1,5,6)_6} \equiv \frac{(1,3,5)_6^2(2,4,6)_6}{(1,5,6)_6} = (3)_6^2(1,2,4,5)_6$$
$$\equiv (6)_{12}(1,2,4,5)_6 = (\pm 1, \pm 2, \pm 4, \pm 5, 6)_{12}.$$

The following proposition provides a direct way to carry out the first step of the Euler reciprocation. The proof follows easily from (8). We use the brief notation $(X)_m$ for the expression $(x_1, \ldots, x_n)_m$, where $X = \{x_1, \ldots, x_n\}$, and, in later sections, $cX + d$ for the set $\{cx_1 + d, \ldots, cx_n + d\}$.

**Proposition 3.** *For $S \subseteq \mathbf{Z}^+$, let $E(S)$ and $O(S)$ be the sets of even and odd integers in $S$, respectively. Let $m$ be a positive, even integer and $M = \{1, \ldots, m\}$. Then for $A \subseteq M$,*

$$\frac{1}{(A)_m} \equiv (O(M-A))_m^2(O(A) \cup E(M-A))_m. \tag{9}$$

*Note.* To reciprocate a product by this method when $m$ is odd, expand the set of residues by (7) and then use the modulus $2m$, so that the parity of the class determines the parity of the exponent.

The second step of this method is to use (6) on $(O(M-A))_m^2$, producing, say, $(2a_1, \ldots, 2a_r)_{2m}$, and (7) on any terms in $(E(M-A))_m$, which, when expanded, will give a term equal to some $2a_i$. Any expanded term in $(E(M-A))_m$ that is not equal to some $2a_i$ is combined with those in $(O(A))_m$ to form an "inertial" set, i.e., a collection of integers that play no further part in the process. Congruence (6) is then used on the new set of squares and the process is repeated until either no squares are produced and the process ends, or the process seems to continue indefinitely because squares keep appearing.

To illustrate this method, consider:

**Example 5.**

$$\frac{1}{(\pm 1, \pm 10, \pm 11, 12, 24)_{24}} \equiv (\pm 3, \pm 5, \pm 7, \pm 9)_{24}^2 (\pm 1, \pm 2, \pm 4, \pm 6, \pm 8, \pm 11)_{24}$$

$$\equiv (3, 5, 7, 9, 15, 17, 19, 21)_{24}^2 (1, 11, 13, 23, 2, 4, 6, 8, 16, 18, 20, 22)_{24}$$
$$\equiv (1, 2, 4, 8, 11, 13, 16, 20, 22, 23)_{24}$$
$$\times (6, 10, 14, 18, 30, 34, 38, 42)_{48} (6, 18, 30, 42)_{48}$$
$$= (---)_{24} (10, 14, 34, 38)_{48} (6, 18, 30, 42)_{48}^2$$
$$\equiv (---)_{24} (---)_{48} (12, 36, 60, 84)_{96}$$
$$= (---)_{24} (10, 14, 34, 38)_{48} (12, 36)_{48}$$
$$= (1, 2, 4, 8, 11, 13, 16, 20, 22, 23)_{24} (10, 12, 14)_{24}$$
$$= (\pm 1, \pm 2, \pm 4, \pm 8, \pm 10, \pm 11, 12)_{24}.$$

Note the interesting reduction in the modulus from 96 to the final 24.

**Example 6.** In this example, the infinite loop at the end suggests the wrong conclusion.

$$\frac{1}{(\pm 1, \pm 7, \pm 8, 9, 18)_{18}} \equiv (\pm 3, \pm 5)_{18}^2 (\pm 1, \pm 7, 9, \pm 2, \pm 4, \pm 6)_{18}$$
$$\equiv (\pm 1, \pm 2, \pm 4, \pm 7, 9)_{18} (\pm 6, \pm 10)_{36} (\pm 6, \pm 12)_{36} \tag{10}$$
$$= (\pm 1, \pm 2, \pm 4, \pm 7, 9)_{18} (\pm 10)_{36} (\pm 6)_{36}^2 (\pm 12)_{36}.$$

The "squaring" process will continue indefinitely, without finding the reciprocal. The HPR method suggests, however, that the reciprocal is

$$\frac{1}{(\pm 1, \pm 7, \pm 8, 9, 18)_{18}} \equiv (\pm 1, \pm 2, \pm 4, \pm 7, 9)_{18} (\pm 10)_{36}.$$

Comparing this result with the right-hand side of (10) shows the HPR reciprocal agrees exactly with the first factors there. We are thus led to the surprising conclusion that the product of the other factors, $(\pm 6)_{36}^2 (\pm 12)_{36}$, which keeps regenerating squares and forces the process to continue indefinitely, must be congruent to 1. To see that this is true, we note first that (8) implies

$$(k)_{2k}^2 (2k)_{2k} \equiv 1,$$

when $x$ is replaced by $x^k$. It then follows that

$$(1, 5)_6^2 (2, 4)_6 = \frac{(1, 3, 5)_6^2 (2, 4, 6)_6}{(3)_6^2 (6)_6} = \frac{(1)_2^2 (2)_2}{(3)_6^2 (6)_6} \equiv 1.$$

Replacing $x$ by $x^6$ in the above gives $(\pm 6)_{36}^2 (\pm 12)_{36} \equiv 1$. Therefore, in (10) we can replace $(\pm 6)_{36}^2 (\pm 12)_{36}$ by 1, the process comes to an end, and the HPR reciprocal is correct.

**Example 7.** This example shows a more complete algorithm is certainly needed:

$$\begin{aligned}\frac{1}{(1,9,10)_{10}} &\equiv (3,5,7)_{10}^{2}(1,9,2,4,6,8)_{10}\\ &\equiv (1,9)_{10}(6,10,14)_{20}(2,4,6,8,12,14,16,18)_{20}\\ &\equiv (1,9)_{10}(2,10,18)_{20}(6,14)_{20}^{2}(4,8,12,16)_{20}.\end{aligned}$$

Again the process will continue indefinitely, raising the question whether an MP reciprocal exists and the infinite loop is caused by "unity contamination" as in Example 6, or whether an MP reciprocal actually fails to exist. The heuristic method suggests the latter is true by failing to find a modular pattern in the sequence of exponents up to degree $L = 1000$. This will be established in the discussion of the examples preceding Theorem 18. Also see the discussion following Theorem 9.

*Remark.* We note in passing that Example 4 has essentially been done by I. Schur [5, pp. 49–50]. Namely, Schur finds that

$$\frac{1}{(1,5)_6} = \prod_{n=1}^{\infty}(1+x^{3n-1})(1+x^{3n-2}) \equiv (1,2)_3.$$

Hence by Euler's identity, $\frac{1}{(1,5,6)_6} \equiv (1,2)_3(6)_{12}$.

Andrews has generalized Schur's argument to what he calls "Euler pairs": two sets of positive integers $S$ and $T$ such that

$$\prod_{n\in T}\frac{1}{1-x^n} = \prod_{n\in S}(1+x^n).$$

The main result [1, Theorem 1] is that this identity holds if and only if $2S \subseteq S$ (i.e., doubles of elements of $S$ are in $S$) and $T = S - 2S$.

## 5. An analysis of the Euler reciprocation method

The results of this section rest on a careful analysis of the Euler reciprocation method. The starting point of this analysis is the product $(\mathscr{A})_m^2(\mathscr{B})_m$, which comes from canceling the denominator in the Euler method (cf. (9)), that is

$$\frac{1}{(---)_m} \equiv (\mathscr{A})_m^2(\mathscr{B})_m. \tag{11}$$

Let $M = \{1,\ldots,m\}$, $m \geq 2$. Then $\mathscr{A}$ and $\mathscr{B}$ are disjoint subsets of $M$. Although the Euler reciprocation process also implies that $\mathscr{A}$ will contain only odd integers and that $m$ is even, we will not assume these conditions here, because they are not specifically needed in the development that follows. However, we will assume that $\mathscr{A} \neq \varnothing$ and $\mathscr{B} \neq \varnothing$, since this product is already an MP product when $\mathscr{A} = \varnothing$ or will become one after a single use of (6), when $\mathscr{B} = \varnothing$.

**Definition.** For each $a \in M$, let

$$[a]_m = \{x \in M : x \equiv 2^e a \pmod m,\ e \geq 1\}. \tag{12}$$

Note that $e = 0$ is not part of this definition. Moreover, $a \in [a]_m$ if and only if $\nu_2(a) \geq \nu_2(m)$, where $\nu_2(x)$ denotes the highest power of 2 dividing $x$. Also note when $m$ is even that $[\frac{m}{2} + k]_m = [k]_m$, $1 \leq k \leq \frac{m}{2}$.

**Proposition 4.** *Suppose $A_0$ and $B_0$ are disjoint, nonempty subsets of $M$. For each $a \in A_0$, define the* **rank** *of $a$, $\rho(a)$, to be*

$$\rho(a) = \begin{cases} \min\{e \geq 1 : 2^e a \bmod m \notin B_0\}, & \text{if } [a]_m \not\subseteq B_0, \\ \infty, & \text{otherwise.} \end{cases} \tag{13}$$

*Also, for each $e \geq 1$, let*

$$\overline{A}_e = \{2^e a : a \in A_0 \text{ and } \rho(a) = e\}, \tag{14}$$

$$A_e = \{2^e a : a \in A_0 \text{ and } \rho(a) > e\}, \tag{15}$$

*and*

$$B_e = B_{e-1} \cup (B_{e-1} + 2^{e-1} m) \cup \overline{A}_e - A_e. \tag{16}$$

*Then for $e \geq 0$,*

$$(A_e)^2_{2^e m} (B_e)_{2^e m} \equiv (A_0)^2_m (B_0)_m. \tag{17}$$

*Proof.* We begin by establishing the following three results for $e \geq 1$:

(a) $2A_{e-1} = \overline{A}_e \cup A_e$, where $\overline{A}_e \cap A_e = \varnothing$,

(b) $\overline{A}_e \cap B'_e = \varnothing$, where $B'_e = B_{e-1} \cup (B_{e-1} + 2^{e-1} m)$,

(c) $A_e \subseteq B'_e$.

The above results show that $2A_{e-1}$, which is the set obtained from $A^2_{e-1}$ (mod 2), splits into the disjoint sets $\overline{A}_e$ and $A_e$, where the elements of $\overline{A}_e$ do not match any element in $B'_e$ and so do not create a square at the next step, while each of the elements of $A_e$ definitely matches an element in $B'_e$ and so produces a square at the next step.

(a) The definitions of $\overline{A}_e$ and $A_e$ in (14) and (15) imply that

$$\begin{aligned} 2A_{e-1} &= \{2^e a : a \in A_0 \text{ and } \rho(a) > e - 1\} \\ &= \{2^e a : a \in A_0 \text{ and } \rho(a) = e\} \cup \{2^e a : a \in A_0 \text{ and } \rho(a) > e\} \\ &= \overline{A}_e \cup A_e, \quad \text{where clearly } \overline{A}_e \cap A_e = \varnothing \text{ by definition.} \end{aligned}$$

(b) Let $2^e a \in \overline{A}_e$. Since $\rho(a) = e$ by (14), then by (13), $2^e a \neq b + qm$ for any $b \in B_0$ and $q \geq 0$. Thus, $2^e a$ will not match any number in $B'_e$, which is to say, $2^e a \notin B'_e$, unless that number in $B'_e$ was a descendant of some ancestor $2^d a' \in \overline{A}_d$, $1 \leq d \leq e - 1$ ((16) shows such an ancestor can only have entered $B_d$ through $\overline{A}_d$). In this case we would have for some $t \geq 0$ that $2^e a = 2^d a' + (2^d m)t$, so $2^{e-d} a \equiv a' \pmod m$. Since $1 \leq e - d < e = \rho(a)$, then $2^{e-d} a \equiv b' \pmod m$ for some $b' \in B_0$. But then $a' \equiv b' \pmod m$, which contradicts $A_0 \cap B_0 = \varnothing$. Thus, the exception never happens, so $\overline{A}_e \cap B'_e = \varnothing$.

(c) Let $2^e a \in A_e$. Then by (15) there exists a $b \in B_0$ such that $2^e a \equiv b \pmod m$, i.e., $2^e a = b + qm$, where $0 \le q < 2^e$. The form of $b+qm$ indicates it is an element of $B'_e$, so $2^e a$ will match some element in $B'_e$, unless that element is absent because one of its ancestors already matched some element of $A_d$ at a previous level $d$ and was deleted from the set to make a square, i.e., there was a $2^d a' \in A_d$, $1 \le d \le e-1$, so that at level $e$, $2^e a = 2^d a' + (2^d m)t$, or $2^{e-d} a \equiv a' \pmod m$. But since $\rho(a) > e$ by (15) and $1 \le e - d \le \rho(a)$, then there exists $b' \in B_0$ such that $2^{e-d} a \equiv b' \pmod m$. Thus, $a' \equiv b' \pmod m$, which contradicts $A_0 \cap B_0 = \varnothing$. Hence, there is always a match in $B'_e$ for each element in $A_e$, i.e., $A_e \subseteq B'_e$.

Having proved (a)–(c), we now find for $e \ge 1$ that

$$\begin{aligned}(A_{e-1})^2_{2^{e-1}m}(B_{e-1})_{2^{e-1}m} &\equiv (2A_{e-1})_{2^e m}(B'_e)_{2^e m}\\ &= (\overline{A}_e \cup A_e)_{2^e m}[(B'_e - A_e)_{2^e m}(A_e)_{2^e m}]\\ &= (A_e)^2_{2^e m}(B'_e \cup \overline{A}_e - A_e)_{2^e m}\\ &= (A_e)^2_{2^e m}(B_e)_{2^e m}.\end{aligned}$$

Repeated use of this relationship as a reduction step establishes (17). □

We next split each of the sets $\mathscr{A}$ and $\mathscr{B}$ in (11) into two parts whose properties make them central to settling the questions of this investigation. Let

$$\begin{aligned}A &= \{a \in \mathscr{A} : [a]_m \subseteq \mathscr{B}\},\\ A' &= \mathscr{A} - A,\\ B &= \bigcup_{a \in A} [a]_m,\\ B' &= \mathscr{B} - B.\end{aligned} \tag{18}$$

Note that $A$ is also the set of elements in $\mathscr{A}$ with infinite rank. Since $A \cap A' = \varnothing$ and $B \cap B' = \varnothing$, we can immediately write (11) as

$$(\mathscr{A})^2_m(\mathscr{B})_m = (A')^2_m(B')_m\ (A)^2_m(B)_m. \tag{19}$$

We now consider the two pairs of factors on the right-hand side of (19). The nature of the primed pair is readily settled by the next proposition.

**Proposition 5.** $(A')^2_m(B')_m$ *is an MP product* (mod 2).

*Proof.* We use Proposition 4 with $A_0 = A'$ and $B_0 = B'$. Clearly, $\rho(a) < \infty$ for each $a \in A'$. Let $d = \max_{a \in A'} \rho(a)$. Then by (17), $(A')^2_m(B')_m \equiv (B_d)_{2^d m}$, since $A_d = \varnothing$. □

Note that $A = B = \varnothing$ whenever $m$ is odd, so $(\mathscr{A})^2_m(\mathscr{B})_m$ is always MP in this case.

We next introduce some notation which formalizes the doubling and reduction (mod $m$) that appears throughout this work.

**Definition.** The map $\delta_m : M \to M$ is the "doubling, reduction modulo $m$" operator, defined by

$$\delta_m x = 2x \bmod m, \quad \text{for each } x \in M.$$

Observe that the sets $A$ and $B$ in (18) have the basic property that the doubles modulo $m$ of the elements in $A$ and in $B$ again lie in $B$, which, using $\delta_m$, is simply expressed as $\delta_m A \subseteq B$ and $\delta_m B \subseteq B$.

We include the next three propositions to complete the study of the set $B_\infty$ of exponents that occurs in the expansion of the product $(A)_m^2(B)_m \equiv \prod_{n\in B_\infty}(1-x^n)$, regardless of whether $B_\infty$ is an MP set or not.

**Proposition 6.** *Let $A$ and $B$ be disjoint, nonempty subsets of $M$ and assume $\delta_m A \subseteq B$ and $\delta_m B \subseteq B$. Define $\{B_e\}$ recursively for $e \geq 1$ by*

$$B_e = B_{e-1} \cup (B_{e-1} + 2^{e-1}m) - 2^e A, \quad \text{where } B_0 = B. \tag{20}$$

*Then $(A)_m^2(B)_m \equiv \prod_{n\in B_\infty}(1-x^n)$, where $B_\infty = \bigcup_{k=1}^{\infty}\bigcap_{e=k}^{\infty} B_e$.*

*Proof.* We use Proposition 4 with $A_0 = A$ and $B_0 = B$. Since $\rho(a) = \infty$ for each $a \in A$, the sets in (14) and (15) become $A_e = 2^e A$ and $\overline{A}_e = \varnothing$ for $e \geq 1$, so (16) reduces to (20). Let $L$ be any positive integer and choose $k$ large enough so that $2^k > L$. Then for all $e \geq k$, $B_e \cap \{1, \ldots, L\} = B_k \cap \{1, \ldots, L\}$. By (17),

$$(A)_m^2(B)_m \equiv (2^k A)_{2^k m}^2 (B_k)_{2^k m} \equiv (B_k)_{2^k m} \equiv \prod_{n\in B_\infty}(1-x^n) \pmod{x^L, 2}.$$

The proof is completed by letting $L \to \infty$. □

**Definition.** If $X \subseteq M$, then let

$$\{X\}_m = \{x + km : x \in X, k \geq 0\},$$

and

$$\langle X\rangle_m = \{2^e(x+km) : x \in X, \ k \geq 0, \ e \geq 0\}.$$

We say that a set $S \subseteq \mathbf{Z}^+$ is an "MP set" if there exists a modulus $n$ and a set $X$ of residues modulo $n$ such that $S = \{X\}_n$.

**Proposition 7.** *Let $A$ and $B$ be disjoint, nonempty subsets of $M$ and assume $\delta_m A \subseteq B$ and $\delta_m B \subseteq B$. Define $\{B_e\}$ by (20) and put $C = B \cup (B+m) - 2A - 2B$. Then*

$$\bigcup_{k=1}^{\infty}\bigcap_{e=k}^{\infty} B_e = \{B\}_m - \langle A\rangle_m = \langle C\rangle_{2m}.$$

*Proof.* Let $\overline{B} = B \cup (B+m)$ and $B_\infty = \bigcup_{k=1}^{\infty}\bigcap_{e=k}^{\infty} B_e$.

(i) $B_\infty \subseteq \{B\}_m - \langle A\rangle_m$.

Clearly, $B_\infty \subseteq \{B\}_m$, since each $B_e \subseteq \{B\}_m$. It remains to show that $b \in B_\infty$ implies $b \notin \langle A\rangle_m$. We show the contrapositive: $b \in \langle A\rangle_m$ implies $b \notin B_\infty$. Assume $b = 2^e(a_i + mt) = b_0 + 2^e mt$, where $b_0 = 2^e a_i$. By (20), $b_0 \notin B_e$.

This implies $b_0$, $b_0+2^e m \notin B_{e+1}$; $b_0+2^e mv \notin B_{e+2}$ for $v = 0, 1, 2, 3$; etc. Thus, $b_0 + 2^e mt \notin B_{e+k}$ for all $k \geq \log_2 t$, so $b \notin B_\infty$.

(ii) $\{B\}_m - \langle A\rangle_m \subseteq \langle C\rangle_{2m}$.

Let $b \in \{B\}_m - \langle A\rangle_m$. Then $b \equiv b_j + \varepsilon m \pmod{2m}$ for some $b_j \in B$, and some $\varepsilon = 0$ or $1$. Let $\bar{b}_j = b_j + \varepsilon m$. Suppose $\bar{b}_j \equiv 2b_{j'} \pmod{2m}$ for some $b_{j'} \in B$. Since $1 \leq \bar{b}_j$ and $2b_{j'} \leq 2m$, this congruence implies the equation $\bar{b}_j = 2b_{j'}$, and so we have $b = 2b_{j'} + 2mt$ for some nonnegative integer $t$. Write $t = 2t' + \varepsilon'$, $\varepsilon' = 0$ or $1$, and set $\bar{b}_{j'} = b_{j'} + \varepsilon' m$. Then $\bar{b}_{j'} \in \overline{B}$ and $b = 2b'$, where $b' = \bar{b}_{j'} + 2mt'$. Now $b' \in \{B\}_m$, since $b' \equiv b_{j'} \pmod{m}$. It is easy to see that $b' \notin \langle A\rangle_m$; for otherwise, we would have $b = 2b' \in \langle A\rangle_m$, a contradiction. Thus, $b' \in \{B\}_m - \langle A\rangle_m$. If $\bar{b}_{j'} \equiv 2b_{j''} \pmod{2m}$, then we repeat the construction to obtain $b'' \in \{B\}_m - \langle A\rangle_m$ such that $b' = 2b''$, where $b'' = \bar{b}_{j''} + 2mt''$, with $\bar{b}_{j''} \in \overline{B}$. Now $b = 2b' = 4b'' = 8b''' = \cdots$ cannot continue indefinitely, so this process stops, say, after the $e$th stage. Hence, for some $b^{(e)} \in \{B\}_m - \langle A\rangle_m$, we have

$$b = 2^e b^{(e)} = 2^e(\bar{b}_{j(e)} + 2mt(e)), \tag{21}$$

where $t(e)$ is some integer at the $e$th step and $\bar{b}_{j(e)} \in \overline{B}$, but $\bar{b}_{j(e)} \not\equiv 2b_k$ for any $b_k \in B$. Using (21), it follows immediately that $b \in \langle C\rangle_{2m}$ if we can show that $\bar{b}_{j(e)} \in C = \overline{B} - 2A - 2B$. We already have that $\bar{b}_{j(e)} \in \overline{B}$. Also, $\bar{b}_{j(e)} \notin 2B$, for otherwise, there exists a $k$, $1 \leq k \leq s$, such that $\bar{b}_{j(e)} \equiv 2b_k \pmod{2m}$. Finally, the assumption $\bar{b}_{j(e)} \in 2A$ leads to $\bar{b}_{j(e)} = 2a$ for some $a \in A$, which implies $b_{j(e)} + 2mt(e) \in \langle A\rangle_m$, a contradiction. So $\bar{b}_{j(e)} \notin 2A$. Thus, $\bar{b}_{j(e)} \in C$, which completes the proof of (ii).

(iii) $\langle C\rangle_{2m} \subseteq B_\infty$.

This follows easily from

$$\{C\}_{2m} \subseteq B_\infty \tag{22}$$

and

$$b \in B_\infty \implies 2b \in B_\infty, \tag{23}$$

since $\langle C\rangle_{2m}$ is the "smallest" set which contains $\{C\}_{2m}$ and is closed with respect to doubling.

Suppose that (22) is false. Then there exists $c \in C$ and an integer $t \geq 0$ such that $c + 2mt \notin B_\infty$. Since $c + 2mt \in \{B_0\}_m$ (recall $B_0 = B$), there is a least positive integer $k$ for which $c + 2mt \in \{B_{k-1}\}_{2^{k-1}m} - \{B_k\}_{2^k m}$. By (20), $c+2mt = 2^k a+2^k mu$ for some $a \in A$, $u \geq 0$. If $k \geq 2$, then, since $[a]_m \subseteq B$, we have $2^{k-1}a = b_j + mv$ for some $b_j \in B$ and $v \geq 0$. Consequently, $c + 2mt = 2(b_j + (2^{k-1}u + v)m)$, which implies $c \equiv 2b_j \pmod{2m}$. Since both $c$ and $2b_j$ are in the interval $[1, 2m]$, this congruence implies $c = 2b_j$, contradicting the definition of $C$. If $e = 1$, then a similar argument gives the contradiction $c = 2a$. This establishes (22).

To prove (23), assume $b \in B_\infty$ but $2b \notin B_\infty$. Since $\delta_m B \subseteq B$, $2b \in \{B_0\}_m$. So there exists $k \geq 0$ such that $2b \in \{B_k\}_{2^k m}$ but $2b \notin \{B_{k+1}\}_{2^{k+1} m}$. By (20) this means $2b = 2^{k+1}a + 2^{k+1}mt$ for some $a \in A$ and $t \geq 0$. Hence $b = 2^k a + 2^k mt$. If $k = 0$, then $b \equiv a \pmod m$, contradicting $A \cap B = \varnothing$. If $k \geq 1$, then $b \notin B_e$ for all $e \geq k$, contradicting $b \in B_\infty$. □

The next result follows directly from Propositions 6 and 7.

**Proposition 8.** *Let $A$ and $B$ be disjoint, nonempty subsets of $M$ and assume $\delta_m A \subseteq B$ and $\delta_m B \subseteq B$. Then*

$$(A)_m^2 (B)_m \equiv \prod_{n \in \langle C \rangle_{2m}} (1 - x^n),$$

*where $C = B \cup (B + m) - 2A - 2B$.*

*Remark.* No duplication occurs in $\langle C \rangle_{2m}$ in Proposition 8, that is, one can show that $2^e(c + 2kt) = 2^{e'}(c' + 2k't)$ if and only if $e = e'$, $c = c'$, and $k = k'$. Thus, Proposition 8 gives an efficient method for computing the exponent set $B_\infty$ of the product $(A)_m^2 (B)_n \equiv \prod_{n \in B_\infty} (1 - x^n)$ up to any fixed limit $L$.

**Theorem 9.** *Let $A$ and $B$ be disjoint, nonempty subsets of $M$ and assume $\delta_m A \subseteq B$ and $\delta_m B \subseteq B$. Then $(A)_m^2 (B)_m \equiv 1$ if and only if $|A| = |B|$.*

*First proof.* Write $A = \{a_1, \ldots, a_r\}$ and $B = \{b_1, \ldots, b_s\}$ and let $C = \overline{B} - 2A - 2B$ as in Proposition 7. Since $2A$ and $2B$ are disjoint subsets of $\overline{B}$, $|C| = 2|B| - |A| - |B| = s - r$. Thus, $(A)_m^2 (B)_m = \prod_{n \in \langle C \rangle_{2m}} (1 - x^n) = 1 \iff \langle C \rangle_{2m} = \varnothing \iff C = \varnothing \iff s = r$. □

*Second proof.* We use the fact that $f(x) \equiv f(x^2)$ is a necessary and sufficient condition for a product $f(x)$ to be congruent to 1. Suppose $f(x) = (A)_m^2 (B)_m \equiv 1$. Then $f(x) \equiv f(x^2)$, which implies $(A)_m^2 (B)_m \equiv (2A)_{2m}^2 (2B)_{2m}$, or $(2A)_{2m}^2 (B \cup (B + m))_{2m} \equiv (2A)_{2m}^2 (2B)_{2m}$. Canceling equal factors gives $(C)_{2m} \equiv 1$, where $C = B \cup (B + m) - 2A - 2B$. But this is impossible unless $C = \varnothing$, since $C$ has no multiple factors. But then we get $|A| = |B|$. Conversely, if $|A| = |B|$, then $C = \varnothing$, so $(C)_{2m} \equiv 1$, and we simply reverse the steps to get $f(x) \equiv f(x^2)$ or $f(x) \equiv 1$. □

We remark that this second proof could as well have been given before Proposition 6.

In Example 5, $A_0 = \{3, 5, 7, 9, 15, 17, 19, 21\}$, $B_0 = \{1, 2, 4, 6, 8, 11, 13, 16, 18, 20, 22, 23\}$, and $m = 24$. We then find that every element of $A_0$ has finite rank, so in (18), $A = B = \varnothing$, and Proposition 5 implies that $(\mathscr{A})_{24}^2 (\mathscr{B})_{24}$ is an MP product, as we found before. In Example 6, $A_0 = \{3, 5, 13, 15\}$, $B_0 = \{1, 2, 4, 6, 7, 9, 11, 12, 14, 16, 17\}$, and $m = 18$. Then $A = \{3, 15\}$ and $B = \{6, 12\}$ by (18). Since $|A| = |B| = 2$, Theorem 9 implies that $(A)_{18}^2 (B)_{18} \equiv 1$, so the original product is an MP product. In Example 7, $A_0 = \{3, 5, 7\}$, $B_0 = \{1, 2, 4, 6, 8, 9\}$, and $m = 10$. Then $A = \{3, 7\}$ and $B = \{2, 4, 6, 8\}$, so Theorem 9 does not apply. Also,

$C = \overline{B} - 2A - 2B = \{2, 4, 6, 8, 12, 14, 16, 18\} - \{6, 14\} - \{4, 8, 12, 16\} = \{2, 18\}$. Then Proposition 8 implies that $(A)_m^2(B)_m \equiv \prod_{n \in \langle C \rangle_{20}} (1 - x^n)$. In §7, we will show that this latter product is not an MP product. We do this by proving in general (Proposition 13) that $(A)_m^2(B)_m$ is not an MP product, unless $|A| = |B|$, in which case $(A)_m^2(B)_m \equiv 1$.

## 6. The doubling graph $G_m$

We present a graph-theoretical interpretation of doubling modulo $m$. We begin with a graph theory lemma.

**Lemma 10.** *Let $G$ be a connected graph which contains exactly one cycle, and suppose the degree of each vertex is $\leq 3$. Let $T$ be the number of terminal vertices of $G$ (i.e., the vertices of degree 1) and let $N$ be the number of nonterminal vertices of $G$ (i.e., $N = V - T$, where $V$ is the number of vertices). Then $T = N$ if and only if there is no vertex of degree 2.*

*Proof.* Consider the single cycle $\{v_1, \ldots, v_n\}$ in the graph, $n \geq 1$. Each vertex $v_i$ in the cycle is the root of a single tree (possibly just the vertex $v_i$ itself) emanating from that vertex. Thus, $G$ is clearly planar with $F = 2$ faces, one face lying inside the cycle and the other consisting of the rest of the plane. From Euler's formula: $V - E + F = 2$, we have that $V = E$, the number of edges of $G$. Let $N_2 =$ the number of (nonterminal) vertices of degree 2 and $N_3 =$ the number of (nonterminal) vertices of degree 3. Then

$$T + 2N_2 + 3N_3 = \sum_{\text{all } v} \deg v = 2E = 2V = 2(T + N_2 + N_3),$$

which implies $T = N_3$. Since $N_3 = N - N_2$, it easily follows that $T = N$ if and only if $N_2 = 0$. □

For the rest of this section we will assume that our fixed modulus $m$ is even. In what follows it will be useful to utilize the complete **doubling graph** $G_m$ obtained by applying $\delta_m$ to each element of $M$. Its structure is as follows. (Note that the cycles at the top of $G_m$ are determined first by the algorithm, while the odd vertices at the bottom are gotten last.)

Write $m = 2^k m_1$, where $k > 0$ and $m_1$ is odd. Partition $\{1, \ldots, m_1\}$ into disjoint orbits under the operation $\delta_{m_1}$. The set $\{c_1, \ldots, c_t\}$ is an orbit if and only if (i) each $c_i \in \{1, \ldots, m_1\}$, (ii) $\delta_{m_1} c_i \equiv c_{i+1} \pmod{m_1}$, $1 \leq i \leq t-1$, and (iii) $\delta_{m_1} c_t \equiv c_1 \pmod{m_1}$. For each orbit, the top or first row of the associated doubling graph $G_m$ contains the vertices

$$2^k c_1 \; — \; 2^k c_2 \; — \ldots — \; 2^k c_t .$$

Below each vertex $b$ in the top row is the unique vertex $a \in M$ such that $2a \equiv b \pmod{m}$, but $a$ is not in the top row. Starting with this second row, each *even* vertex $b$ branches downward to exactly two vertices $a_1$ and $a_2$ in the third row, which satisfy the linear congruence $2x \equiv b \pmod{m}$. (Note that $a_1 = \frac{b}{2}$ and $a_2 = \frac{b+m}{2}$.) This procedure continues downward until we reach the bottom row where all the vertices are odd. The doubling graphs $G_{10}$, $G_{18}$, and

$G_{24}$ are shown in Figures 1, 2, and 3 below. (The circles drawn around some of the vertices will be referred to later.)

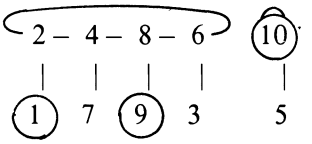



FIGURE 1. $G_{10}$

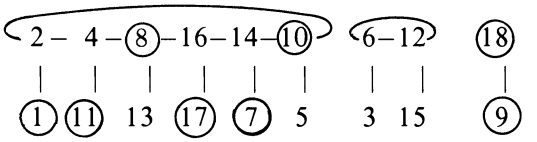



FIGURE 2. $G_{18}$

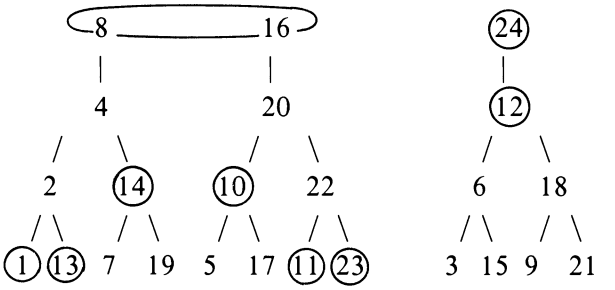



FIGURE 3. $G_{24}$

**Definition.** The notation $x \underset{m}{\sim} y$ means $2^e x \equiv 2^f y \pmod{m}$ for some $e, f \geq 0$.

Clearly, $\underset{m}{\sim}$ is an equivalence relation on $M$.

Let $H$ be a maximal connected subgraph (or component) of $G_m$. The vertices of $H$ form an equivalence class of the relation $\underset{m}{\sim}$. The top row of $H$ is the only cycle of $H$. For each element $v$ in the top row of $H$, the subgraph of $H$ branching downward from $v$ is a binary rooted tree. Now suppose we have two disjoint, nonempty subsets $A$ and $B$ of $M$, where $B = \bigcup_{a \in A} [a]_m$. Then $\delta_m A \subseteq B$, $\delta_m B \subseteq B$, and for each $b \in B$ there is an $a \in A$ such that $b \equiv 2^e a \pmod{m}$, $e \geq 1$. To simplify the discussion of how the elements of $A$ and $B$ lie on the graph $G_m$, we will assume that $A \subseteq H$. (More generally, the elements of $A$ are distributed over several components of $G_m$.) It follows that $B \subseteq H$. For any $a \in A$, the chain $[a]_m$ consists of all the vertices of $H$ directly above $a$, together with the top row of $H$. The set $A \cup B$ and the edges joining any two vertices in $A \cup B$ form a connected subgraph $H_1$ of $H$. No downward path in $H_1$ terminates in a $b \in B$, since, as observed above, every element of $B$ is $\equiv 2^e a \pmod{m}$, $e \geq 1$, for some $a \in A$. Thus, the set of

terminal vertices at the bottom of $H_1$ is exactly the set $A$, and the set of non-terminal vertices is exactly the set $B$. Using Lemma 10, this graph-theoretic interpretation gives us an alternative criterion for the cardinality condition in Theorem 9.

**Proposition 11.** *Let $A$ and $B$ be disjoint, nonempty subsets of $M$, where $B = \bigcup_{a\in A}[a]_m$. Then $|A| = |B|$ if and only if $\deg b = 3$ for every $b \in B$ if and only if for each $b \in B$, the two solutions $x \in M$ of $2x \equiv b \pmod m$ lie in $A \cup B$.*

*Proof.* Let $b \in B$. Since $b$ cannot be a terminal point, we have that $\deg b = 2$ or 3. By Lemma 10, $|A| = |B|$ if and only if $\deg b = 3$ for every $b \in B$ if and only if each of the two elements $x_1$, $x_2$ in $M$ such that $2x_i \equiv b \pmod m$ is in $A \cup B$. □

## 7. Necessary and sufficient conditions for Euler reciprocation

We complete our analysis of the Euler reciprocation method by developing a method for proving the nonexistence of an MP reciprocal.

**Lemma 12.** *Let the decompositon $(\mathscr{A})^2_m(\mathscr{B})_m = (A')^2_m(B')_m\,(A)^2_m(B)_m$ be given, where the sets $A$, $B$, $A'$, and $B'$ are defined by (18). Write $(A)^2_m(B)_m \equiv \prod_{n\in S}(1-x^n)$ and $(A')^2_m(B')_m \equiv \prod_{n\in S'}(1-x^n)$. Then the exponent sets $S$ and $S'$ are disjoint.*

*Proof.* By contradiction. Assume $n \in S \cap S'$. By Proposition 7, $S \subseteq \{B\}_m$, so

$$n = b + mt \tag{24}$$

for some $b \in B$ and $t \geq 0$. By the proof of Proposition 4, $S' \subseteq \{B'\}_m \cup \{2^{\rho(a')}(a' + mt') : a' \in A',\ t' \geq 0\}$. (Here, $\rho$ is the rank for the initial sets $A'$ and $B'$, i.e., $\rho(a') = \min\{e \geq 1 : 2^e a' \bmod m \notin B'\}$.) Now $\{B\}_m \cap \{B'\}_m = \varnothing$ since $B \cap B' = \varnothing$. Thus, $n \notin \{B'\}_m$, which implies

$$n = 2^{\rho(a')}(a' + mt') \tag{25}$$

for some $a' \in A'$ and $t' \geq 0$. Reducing modulo $m$, (24) and (25) yield

$$2^{\rho(a')}a' \bmod m = b. \tag{26}$$

By the definition of rank of $a'$,

$$2^k a' \bmod m \in B' \subseteq \mathscr{B} \tag{27}$$

for $1 \leq k \leq \rho(a') - 1$. Moreover, since $b \in \bigcup_{a\in A}[a]_m$, we have from (26) that

$$2^k a' \bmod m \in B \subseteq \mathscr{B} \tag{28}$$

for $k > \rho(a')$. Relations (26)–(28) prove that $[a']_m \subseteq \mathscr{B}$. By the decompositon in (18), $a' \in A$, contradicting $A \cap A' = \varnothing$. □

**Proposition 13.** *Let $A \subseteq M$ and $B \subseteq \mathrm{Even}(M)$ be nonempty, disjoint subsets. Assume $\delta_m A \subseteq B$, $\delta_m B \subseteq B$, and for each $b \in B$ there exists an*

*$a \in A$ such that $a \underset{m}{\sim} b$. We cannot have $(A)_m^2(B)_m \equiv (D)_n$ for any modulus $n \geq 1$ and any set of residues $\emptyset \neq D \subseteq \{1, \ldots, n\}$.*

*Proof.* The hypotheses imply that $m$ must be even. For if $m$ is odd, then for any $a \in A$, $2^v a \equiv a \pmod{m}$, where $v =$ the order of 2 mod $m$, giving the contradiction $a \in A \cap B$.

*Case* 1. $n = m$.

Assume

$$(A)_m^2(B)_m \equiv (D)_m \tag{29}$$

for some set $\emptyset \neq D \subseteq M$. Note that $D \subseteq B$ since $(A)_m^2(B)_m \subseteq (B)_m$. Let

$$\widehat{A} = \{x \in M : \delta_m x \in B, x \notin B\}.$$

Note that (i) $A \subseteq \widehat{A}$, (ii) $B = \bigcup_{a \in \widehat{A}} [a]_m$ (because $B \subseteq \text{Even}(M)$), and (iii) for all $x \in M$ and all $b \in b$, $\delta_m x = b$ implies $x \in \widehat{A} \cup B$. By Proposition 11, $|\widehat{A}| = |B|$. Let $C = \widehat{A} - A$. Then $C$ is nonempty, for otherwise $A = \widehat{A}$, $|A| = |B|$, and hence $(A)_m^2(B)_m \equiv 1$ by Theorem 9, contradicting (29). Multiply both sides of (29) by $(C)_m^2$ to get

$$(C)_m^2(A)_m^2(B)_m \equiv (C)_m^2(D)_m$$

or

$$(\widehat{A})_m^2(B)_m \equiv (C)_m^2(D)_m$$

or

$$(C)_m^2(D)_m \equiv 1,$$

using Theorem 9 and the fact that $|\widehat{A}| = |B|$. Apply the decomposition (18) to $(C)_m^2(D)_m$, i.e., define

$$C'' = \{c \in C : [c]_m \subseteq D\}, \qquad C' = C - C'',$$
$$D'' = \bigcup_{c \in C''} [c]_m, \qquad D' = D - D''.$$

Write $(C')_m^2(D')_m \equiv \prod_{n \in S'}(1 - x^n)$ and $(C'')_m^2(D'')_m \equiv \prod_{n \in S''}(1 - x^n)$. Since $S'$ and $S''$ are disjoint by Lemma 12, we must have $S' = \emptyset$. By the proof of Proposition 5, $S'$ is a nonempty MP set unless $C' = \emptyset$ and $D' = \emptyset$. This means that $C'' = C$ and $D'' = D$. Thus, $D = \bigcup_{c \in C}[c]_m$. Also, $C \cap D = \emptyset$, since $C \subseteq \widehat{A}$, $D \subseteq B$, and $\widehat{A} \cap B = \emptyset$. By Theorem 9, $|C| = |D|$. By Proposition 11,

$$\forall x \in M \text{ and } \forall d \in D, \qquad \delta_m x = d \implies x \in C \cup D. \tag{30}$$

We derive a contradiction from (30). Pick any $d \in D$. Since $d \in B$, by hypothesis there exists an $a \in A$ such that $a \underset{m}{\sim} d$, say, $2^e a \equiv 2^f d \pmod{m}$, where we can require that $e, f \geq 1$. Let $d' = 2^f d \bmod m$. Then $d' \in D$ since $D$ is closed with respect to $\delta_m$. Write $[a]_m = \{b_1, b_2, \ldots\}$ and let $k$

be the minimum positive index such that $b_k \in D$ ($k$ is well defined since $d' \in [a]_m$). If $k > 1$, then $\delta_m b_{k-1} = b_k$, and so by (30), $b_{k-1} \in C \cup D$. This is a contradiction, for $b_{k-1} \notin C$, since $b_{k-1} \in B$ and $B$ is disjoint from $\hat{A} \supseteq C$, and $b_{k-1} \notin D$ by the minimality of $k$. If $k = 1$, then $\delta a \equiv b_1$, and by (30) we have $a \in C \cup D$, another contradiction: For $a \notin C$ since $A \cap C = \varnothing$, and $a \notin D$ since $D \subseteq B$ and $A \cap B = \varnothing$.

*Case* 2. $n$ is any positive integer.

Let $L = \mathrm{LCM}[m, n]$, and define the sets

$$\overline{A} = \left\{ a + mt : a \in A,\ 0 \le t \le \frac{L}{m} - 1 \right\},$$

$$\overline{B} = \left\{ b + mt : b \in B,\ 0 \le t \le \frac{L}{m} - 1 \right\},$$

and

$$\overline{D} = \left\{ d + nt : d \in D,\ 0 \le t \le \frac{L}{n} - 1 \right\}.$$

We first verify that the hypothesis of Proposition 13 holds for the modulus $L$ and the sets $\overline{A}$, $\overline{B}$, and $\overline{D}$. It is straightforward to show that (i) $\varnothing \neq \overline{A} \subseteq \{1, \ldots, L\}$, (ii) $\varnothing \neq \overline{B} \subseteq \mathrm{Even}(\{1, \ldots, L\})$, (iii) $\overline{A} \cap \overline{B} = \varnothing$, (iv) $\delta_L \overline{A} \subseteq \overline{B}$, and (v) $\delta_L \overline{B} \subseteq \overline{B}$. It remains to verifty that

$$\forall \bar{b} \in \overline{B}\ \exists \bar{a} \in \overline{A} \quad \text{such that} \quad \bar{a} \underset{L}{\sim} \bar{b}. \tag{31}$$

Take any $\bar{b} \in \overline{B}$. Then $\bar{b} \equiv b \pmod m$ for some $b \in B$. By hypothesis, $b \underset{m}{\sim} a$ for some $a \in A$. By the definition of $\sim$, $2^e b \equiv 2^f a \pmod m$ for some integers $e, f \ge 0$. Write $2^e \bar{b} = 2^f a + 2mt$. For any $g \ge 0$ and $x$ (to be chosen later), we have the equivalence

$$2^{e+g} \bar{b} \equiv 2^{f+g}(a + mx) \pmod L \tag{32}$$

if and only if

$$2^{f+g} x \equiv 2^g t \left( \mathrm{mod} \frac{L}{m} \right). \tag{33}$$

Write $\frac{L}{m} = 2^v k$, $k$ odd. Putting $g = v$, congruence (33) holds modulo $2^v$ for any $x$, while modulo $k$, (33) has the solution $x \equiv 2^{-f} t \pmod k$. Thus, (33) has a solution mod $\frac{L}{m}$ and, moreover, we can specify that $0 \le x \le \frac{L}{m} - 1$. Congruence (32), which must hold for these values of $g$ amd $x$, implies that $\bar{b} \underset{L}{\sim} a + mx$. Setting $\bar{a} = a + mx$ establishes (31).

It is easy to show that $(\overline{A})_L = (A)_m$, $(\overline{B})_L = (B)_m$, $(\overline{D})_L = (D)_n$, and hence

$$(\overline{A})_L^2 (\overline{B})_L = (A)_m^2 (B)_m = (D)_n = (\overline{D})_L.$$

Thus we can reduce to Case 1 with the common modulus $L$. □

**Theorem 14.** *Let* $\mathscr{A}$ *and* $\mathscr{B}$ *be disjoint, nonempty subsets of* $M$. *Define* $A, A', B, B'$ *by* (18). *Then* $(\mathscr{A})_m^2(\mathscr{B})_m$ *is an MP product* (mod 2) *if and only if* $|A| = |B|$.

*Proof.* ($\Longleftarrow$) If $|A| = |B|$, then $(A)_m^2(B)_m \equiv 1$ by Theorem 9. Hence

$$(\mathscr{A})_m^2(\mathscr{B})_m = (A')_m^2(B')_m,$$

which is an MP product by Proposition 5.

($\Longrightarrow$) Suppose $(\mathscr{A})_m^2(\mathscr{B})_m$ is an MP product. If $m$ is odd, then $A = \varnothing$ and therefore $B = \varnothing$, so we are done. Assume that $m$ is even. It is clear from (18) that $B \subseteq \text{Even}(M)$. Write $(A)_m^2(B)_m \equiv \prod_{n\in S}(1 - x^n)$ and $(A')_m^2(B')_m \equiv \prod_{n\in S'}(1-x^n)$. Since $S$ and $S'$ are disjoint by Lemma 12, and $S'$ is an MP set by Proposition 5, it follows that $(A)_m^2(B)_m$ is an MP product. This is impossible by Proposition 13, unless $(A)_m^2(B)_m \equiv 1$. By Theorem 9, $|A| = |B|$. □

Proving Theorem 14 completes the analysis of the Euler method and allows us to formulate the following complete, 4-step algorithm for this method.

**The Euler reciprocation algorithm.** *Given a modulus* $m$ *and a set of residues* $U \subseteq M = \{1, \ldots, m\}$. *Determine whether* $\frac{1}{(U)_m}$ *is MP modulo* 2. *If it is, then find the modulus* $n$ *and set of residues* $D \subseteq \{1, \ldots, n\}$ *such that* $\frac{1}{(U)_m} \equiv (D)_n$.

*Step* 1. Extend by (7) to the even modulus $2m$ if $m$ is odd. (We will continue to write "$m$" for both cases.)

*Step* 2. Write $\frac{1}{(U)_m} \equiv (\mathscr{A})_m^2(\mathscr{B})_m$, where $\mathscr{A} = \text{Odd}(M - U)$ and $\mathscr{B} = \text{Odd}(U) \cup \text{Even}(M - U)$.

*Step* 3. Use (18) to define $A, B, A', B'$ in the decomposition

$$(\mathscr{A})_m^2(\mathscr{B})_m = (A)_m^2(B)_m\,(A')_m^2(B')_m.$$

*Step* 4. Does $|A| = |B|$?

If no, then stop: $\frac{1}{(U)_m}$ is not MP. (Proposition 8 may be used to compute the exponent set $B_\infty$ of the reciprocal product $\frac{1}{(U)_m} \equiv \prod_{n\in B_\infty}(1 - x^n)$.)

If yes, then:

Put $A_0 = A'$, $B_0 = B'$ in Proposition 4.
Let $d = \max_{a\in A'} \rho(a)$, where $\rho(a)$ is defined in (13).
Use (14)–(16) to compute $B_d$.
Then $\frac{1}{(U)_m} \equiv (B_d)_{2^d m}$.

Reduce to a smaller modulus if possible. (Use inspection if $2^d m$ is small or else use algorithm *Pattern Recognizer*, described in §2, on the set $B_d$.)

**Definition.** The set $A \subseteq M$ is called **symmetric** with respect to the modulus $m$ if $m - a \in A$ for every $a \in A - \{m\}$.

Alternatively, $A$ is symmetric if and only if for every $a \in A$ there exists an $a' \in A$ such that $a + a' \equiv 0 \pmod m$. Note that $a' \neq a$ unless $a = m$ or $a = \frac{m}{2}$, $m$ even. Observe that for a fixed modulus $m$, symmetry is closed with respect to set-theoretic unions, intersections, differences, and complements ($M - A$).

**Lemma 15.** *Let $A \subseteq M$ be symmetric and suppose for some modulus $n$ and set of residues $A' \subseteq \{1, \ldots, n\}$ that $(A)_m \equiv (A')_n$. Then $A'$ is symmetric with respect to $n$.*

*Proof.* Let $r = \mathrm{LCM}[m, n]$ and let the set of residues (mod $r$) be $A''$. Then clearly $A''$ is symmetric. Dropping to the set $A'$ by reducing to modulus $n$ preserves the symmetry. □

Thus we can say that an MP product $(A)_m$ is symmetric if $A$ is symmetric with respect to $m$. By Lemma 15, this definition is independent of the choice of the modulus and set of residues $A$.

**Theorem 16.** *Assume $(D)_m$ is symmetric and has an MP reciprocal* (mod 2). *Then $\frac{1}{(D)_m}$ is symmetric.*

*Proof.* By using (7), if necessary, we may assume that $m$ is even. It is clear that the sets $M - D$, $\mathrm{Odd}(D)$, and $\mathrm{Even}(M - D)$ are symmetric. Hence, by (9) in Proposition 3, we may write $\frac{1}{(D)_m} \equiv (\mathscr{A})_m^2 (\mathscr{B})_m$, where $\mathscr{A}$ and $\mathscr{B}$ are symmetric. In the decomposition in (18), the sets $A$ and $B$ are symmetric, since the negatives mod $m$ of $[a]_m = \{2a, 2^2 a, \ldots\} \subseteq \mathscr{B}$ must lie in the symmetric set $\mathscr{B}$. It follows that the complement sets $A'$ and $B'$ are symmetric. By Theorem 14, $\frac{1}{(D)_m} \equiv (A')_m^2 (B')_m$. By Proposition 5, $(A')_m^2 (B')_m \equiv (B_d)_{2^d m}$, for some set $B_d$ defined in (16). It is easily checked by induction that the sequence of sets $\{A_e\}$, $\{A'_e\}$, and $\{B_e\}$, in (14), (15), and (16) are symmetric whenever the initial sets $A_0 = A'$ and $B_0 = B'$ are. Hence, $B_d$ is symmetric. □

## 8. The decision algorithm

The previous section gives a method for determining whether a given product $(A)_m$ has an MP reciprocal and for finding it when it does. The method is somewhat lengthy in that we must first apply Proposition 3 to express the reciprocal $\frac{1}{(A)_m}$ as a product $(A_0)_m^2 (B_0)_m$ modulo 2 and then carry out a sequence of detailed set calculations. If the cardinality of $A$ is small in comparison to $m$—which is often the case—then the set $A_0$ will at least contain all of the odd integers in $M - A$, a large set to work with. In this section we present a second algorithm which decides *directly* whether $(A)_m$ has an MP reciprocal, but does not concern itself with finding the MP reciprocal when it exists. The outer loop of this algorithm runs through the elements in $A$, so it is highly efficient when $|A|$ is small. Like the method of the previous section, all arithmetic is performed modulo $m$.

We are now in a position to derive a necessary and sufficient graph-theoretic condition for an MP product *not* to have an MP reciprocal.

**Theorem 17.** *Suppose we are given a positive, even integer $m$ and a set $A \subseteq M$. Put $A^c = M - A$. Then $(A)_m$ has an MP reciprocal* (mod 2) *if and only if there does not exist an $a \in A$ and a number $b \in \mathrm{Odd}(A^c)$ satisfying the three*

*conditions*:

$$\text{(34)} \qquad \begin{aligned} &\text{(i)} \quad [a]_m \subseteq A^c, \\ &\text{(ii)} \quad [b]_m \subseteq A^c, \\ &\text{(iii)} \quad [a]_m \cap [b]_m \neq \varnothing. \end{aligned}$$

*Proof.* (By contradiction.) Let

$$O = \{x \in \mathrm{Odd}(A^c) : [x]_m \subseteq \mathrm{Even}(A^c)\},$$
$$O' = \mathrm{Odd}(A^c) - O,$$
$$E = \bigcup_{x \in O} [x]_m,$$

and

$$E' = (\mathrm{Even}(A^c) - E) \cup \mathrm{Odd}(A).$$

By Proposition 3,

$$\frac{1}{(A)_m} \equiv (O)_m^2 (E)_m (O')_m^2 (E')_m.$$

($\Leftarrow$) Assume that $(A)_m$ has an MP reciprocal and suppose there exists an $a \in A$ and a number $b \in \mathrm{Odd}(A^c)$ satisfying (34). Since $a \notin E \cup O$, we show that this leads to a contradiction of Theorem 14 and Proposition 11 by exhibiting an element $c \in E$ such that $2a \equiv c \pmod m$. Condition (iii) says that $a$ and $b$ are vertices in the same component of $G_m$. Condition (ii) says that $b \in O$ and that all vertices of $G_m$ which branch upward starting from $b$, lie in $E$. Let $[a]_m = \{a_1, a_2, \ldots, a_u, \ldots\}$, where $u$ is the least positive integer such that $a_u \in [b]_m$. (This holds for some $u$ by condition (iii).) We know that $a_u \in E$, so Theorem 14 and Proposition 11 guarantee that $a_{u-1} \in E \cup O$. The case $a_{u-1} \in O$ is clearly impossible, since $a_{u-1}$ is even. Thus, $a_{u-1} \in E$. Continuing, we get that $a_{u-1}, \ldots, a_1 \in E$. Letting $c = a_1$, we arrive at the promised contradiction, since $2a \equiv a_1 \pmod m$, $a_1 \in E$, but $a \notin E \cup O$.

($\Rightarrow$) Assume that $(A)_m$ has no MP reciprocal. By Theorem 14 and Proposition 11, there exist $c \in E$ and $x \in M - (E \cup O)$ such that $2x \equiv c \pmod m$. Now the very fact that $c \in E$ means that $c \equiv 2^e b \pmod m$ for some $b \in O$ and $e \geq 1$. By the definition of $O$, $[b]_m \subseteq E \subseteq A^c$. Since $M = O \dot\cup E \dot\cup O' \dot\cup E' \dot\cup \mathrm{Even}(A)$,[1] the condition $x \notin E \cup O$ implies $x \in O'$ or $x \in \mathrm{Even}(A)$ or $x \in E'$. The first case, $x \in O'$, implies $2x \equiv c \equiv 2b \pmod m$, which leads to the contradiction $[x]_m = [b]_m \subseteq E$. If $x \in \mathrm{Even}(A)$, then $a = x$ and $b$ satisfy (34), so we are done. This leaves the case $x \in E' = (\mathrm{Even}(A^c) - E) \cup \mathrm{Odd}(A)$. If $x \in \mathrm{Odd}(A)$, then we are done by taking $a = x \in A$. So, finally, assume $x \in \mathrm{Even}(A^c) - E$. Then keep halving $x$ until a value $a$ is reached which is either not in $A^c$ or else is odd. If $a \notin A^c$, then we are done, since $a$ and $b$ satisfy (34). If $a$ is odd, then we claim $a \in A$. For if $a \in A^c$, then $[a]_m = \{2a \bmod m, 4a \bmod m, \ldots, x\} \cup [x]_m \subseteq A^c$, which implies $a \in O$, which in turn implies the contradiction $x \in E$. So $a \in A$. □

[1] Here $\dot\cup$ denotes disjoint union.

**Algorithm.** *InvertTest* $(m,\ A = \{a_1, \ldots, a_r\})$.

{Determine whether $(a_1, \ldots, a_r)_m$ has an MP reciprocal (mod 2). The modulus $m$ must be even and $a_i \in M$ must be distinct. Let $A^c = M - A$. The function *InvertTest* will return a 1 if $\frac{1}{(A)_m}$ is an MP set, 0 otherwise.}

Denote by $\nu_2(a)$ the highest power of 2 which divides $a$.

Function *UpSearch* ( $a$ )

{Search $G_m$ for a path entirely in $A^c$ from $a$ up to the top level. If such a path exists, return the element at the top; otherwise return 0 (= false).}

```
begin
    while ν2(a) < ν2(m) do
    begin
        a = δm(a)
        if a ∈ A then return(0)
    end
    return(a)
end.
```

Function *TopSearch* ( *top* )

{Search the top level of $G_m$ for an orbit lying entirely in $A^c$. Return 1 (= true) if such an orbit exists.}

```
begin
    a = top
    repeat
        a = δm(a)
        if a ∈ A then return(0)
    until a = top
    return(1)
end.
```

Function *Branch* ( $a$ )

{ A recursive function which determines whether there exists a path in $A^c$, starting with $a$, down to the bottom of $G_m$.}

```
begin
    if a ∈ R then return(0)
    else if a is odd then return(1)
        else if Branch( a/2 ) then return(1)
            else return(Branch( a/2 + m/2 ))
end.
```

Function *DownSearch* ( *top* )

{Search $G_m$ for a path entirely in $A^c$ from *top* to the bottom.}

```
begin
    first = top
    repeat
        prevtop = top
        top = δm(top)
        second = top/2
        if second = prevtop then second = second + m/2
        if Branch( second ) then return(1)
```

```
    until top = first
    return(0)
end.
begin {InvertTest}
    for i = 1 to r do
    begin
        top = UpSearch(a_i)
        if top > 0 then
            if TopSearch( top ) then
                if DownSearch( top ) then return (0)
    end
    return(1)
end.
```

To show that $(A)_m$ does not have an MP reciprocal, the algorithm searches for a counterexample satisfying (34). For each $a \in A$, *UpSearch* looks for an upward path $\subseteq [a]_m$, lying entirely in the complementary set $A^c = M - A$ and terminating in the element *top* in the top row of $G_m$. *TopSearch* then checks that no element of $A$ lies in the top row. If this is so, then *DownSearch* attempts to find a path in $A^c$, from some element in the top row down to an odd member of $A^c$ in the bottom row of $G_m$. If successful, the pair $a$, $b$ provides the counterexample required by Theorem 17. If unsuccessful for all $a \in A$, then $(A)_m$ has an MP reciprocal.

To illustrate this method, consider Examples 5, 6, and 7 again. In Example 5, we have $m = 24$ and $A = \{1, 10, 11, 12, 13, 14, 23, 24\}$. The $A$ vertices in $G_{24}$ have been circled in Figure 3. Beginning with vertex $a_1 = 1$, *InvertTest* will call function *UpSearch* to find the path $2 - 4 - 8$ entirely in $A^c$ up to $top = 8$. Next, function *TopSearch* will discover that the top row cycle $8 - 16$ lies entirely in $A^c$. *DownSearch*, however, will be unable to find a path, starting at any member of this top row, lying entirely in $A^c$, which branches down to one of the odd vertices 7, 19, 5, or 17 of $A^c$ in the bottom row. Observe that each downward path is successfully blocked by 1, 13, 14, 10, 11, or 23. *InvertTest* will similarly be unsuccessful beginning at any of the other 5 circled vertices in the left component of $G_{24}$. When *InvertTest* begins with $a = 12$ or 24 in the right component, it will be unable to find a path in $A^c$ to the top row, since the only element in the top row, 24, is in $A$. Thus, *InvertTest* will return 1 (= true), indicating that an MP reciprocal exists.

In Example 6, we have circled the vertices in $G_{18}$ for $A = \{1, 7, 8, 9, 10, 11, 17, 18\}$ in Figure 2. Since each of the two components of $G_{18}$ with circled vertices contains an element of $A$ in the top row, *InvertTest* will fail to find a counterexample and will report that $\frac{1}{(A)_{18}}$ is an MP product. (The second component is not involved because no element of $A$ lies in it.)

In Example 7, where the vertices in $G_{10}$ for $A = \{1, 9, 10\}$ are circled in Figure 1, the program (with $a_1 = 1$) immediately finds that $top = 2$. The top row, $2 - 4 - 8 - 6$, lies in $A^c$, and $4 - 7$ is a downward path to $\mathrm{Odd}(A^c)$. Thus, $a = 1$, $b = 7$ provides a counterexample by Theorem 17, and so $(A)_{10}$ has no MP reciprocal.

An immediate application of Theorem 17 is the following result, which completely settles the reciprocation question for odd moduli.

**Theorem 18.** *Let $m$ be odd and $A \subseteq M$. Then $(A)_m$ has an MP reciprocal* (mod 2).

*Proof.* Let $A = \{a_1, \ldots, a_t\}$. We must expand $(a_1, \ldots, a_t)_m$ by (7) to obtain $(a_1, \ldots, a_t, a_1 + m, \ldots, a_t + m)_{2m}$, which has an even modulus. Each component of $G_{2m}$ has 2 rows. For each $i$, the integers $a_i$ and $a_i + m$ lie in one component, since $2 \cdot a_i \equiv 2(a_i + m) \pmod{2m}$, with one of the pair $a_i$, $a_i + m$ always being even, and hence lying in the top row. Thus, condition (i) in (34) can never happen for $a = a_i$ or $a = a_i + m$. Letting $i$ range from 1 to $m$, we find that $\frac{1}{(A)_m}$ is MP. □

## 9. Applications to special products

In this section we will investigate when the following two well-known MP products have MP reciprocals. These are:
Jacobi's Triple Product [4, equation (9)]: For $0 < |l| < k$,

$$(0, \pm(k-l))_{2k} = \sum_{-\infty}^{\infty} (-1)^n x^{kn^2+ln} \tag{35}$$

and the
Quintuple Product [4, equation (20)]: For $0 < 2k < m$,

$$(\pm k, \pm(m-2k), \pm(m-k), m, 2m)_{2m} = \sum_{-\infty}^{\infty} x^{\frac{m}{2}(3n^2+n)}(x^{-3kn} - x^{3kn+k}). \tag{36}$$

First consider the single-variable Jacobi triple product

$$\prod_{j=0}^{\infty}(1 - x^{jm+k})(1 - x^{(j+1)m-k})(1 - x^{(j+1)m}), \qquad 1 \le k < \frac{m}{2},$$

which in our notation is $(\pm k, m)_m$. Without loss of generality, we may assume that $(m, k) = 1$, for if not, then the product can be written as a product in a power of $x$ with a smaller value of $m$.

**Theorem 19.** *Let $m \ge 3$, $1 \le k < \frac{m}{2}$, and $(m, k) = 1$. The Jacobi triple product $(\pm k, m)_m$ has an MP reciprocal* (mod 2) *if and only if* (i) *$m$ is odd,* (ii) *$m = 2^e$, $e \ge 2$, or* (iii) *$m = 6$.*

*Proof.* The case when $m$ is odd was settled in Theorem 18, so assume that $m$ is even. Let us begin with the specified value $k = 1$, so $A = \{1, m-1, m\}$.

*Case* 1. $m = 2^e$, $e \ge 2$.

The doubling graph $G_m$ consists of a single component with only the vertex $m$ at the top. Hence, no path $[x]_m$ lies entirely in $A^c$, i.e., conditions (i) and (ii) of (34) are never satisified, so $\frac{1}{(A)_m}$ is an MP product.

*Case* 2. $m = 6$.

Example 4 verifies that $\frac{1}{(1,5,6)_6}$ is MP.

*Case* 3. $m = 2k$, $k \geq 5$, $k \neq 2^e$.

Here, 1 and $m-1$, being odd, lie in the bottom row of $G_m$. Also, 1 and $m$ are in different components, for otherwise, $1 \underset{m}{\sim} m$ implies $2^e \cdot 1 \equiv 2^f m \equiv 0 \pmod{m}$, which is a contradiction, since $m$ cannot divide a power of 2. Now consider the component $H$ of $G_m$ which contains 1. Then $H$ contains an equal number of odd and even vertices. Since 2, 4, and 8 are three distinct, even vertices of $H$, and $A$ contains only two odd vertices, there exists an odd vertex $b \in H \cap A^c$. The vertices $a = 1$ and $b$ satisfy (34). Hence $\frac{1}{(A)_m}$ is not MP.

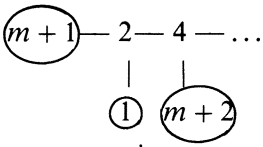
Now consider the case $k > 1$. Observe that the map $\sigma_k : M \to M$, given by $\sigma_k(x) = kx \mod m$, is a permutation, since $(m, k) = 1$. When applied to $G_m$, $\sigma_k$ takes vertices to vertices and preserves adjacency. Hence, $\sigma_k$ is a graph automorphism. Let $A' = \sigma_k(A) = \{k, m-k, m\}$ and $(A^c)' = \sigma_k(A^c) = M - A'$. Then for any pair $(a, b)$ with $a \in A$ and $b \in \mathrm{Odd}(A^c)$ satisfying (34), the elements $a' = \sigma_k(a)$ and $b' = \sigma_k(b)$ satisfy $a' \in A'$, $b' \in \mathrm{Odd}((A^c)')$, and conditions (34). Thus, $(A')_m$ has an MP reciprocal if and only if $(A)_m$ does. □

**Theorem 20.** *The quintuple product* $(\pm k, \pm(m-2k), \pm(m-k), m, 2m)_{2m}$, *where* $0 < 2k < m$, $(k, 2m) = 1$, *and* $m \geq 4$, *has an MP reciprocal* (mod 2) *if and only if* (i) $m$ *is odd,* (ii) $m$ *is* $2 \cdot$ *odd,* (iii) $m = 2^e$, $e \geq 2$, *or* (iv) $m = 12$.

*Proof.* As in the proof of Theorem 19, we can reduce the proof to considering the case when $k = 1$, i.e., we take $A = \{1, m-2, m-1, m, m+1, m+2, 2m-1, 2m\}$.

*Case* 1. $m$ odd.

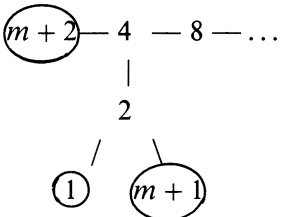
Here, $G_{2m}$ contains the component




The vertex $m+1$ is in the top row, since $m+1$ is even, and it precedes 2 since $2(m+1) \equiv 2 \pmod{2m}$. Thus, condition (i) in (34) fails for the three integers $1, m+1, m+2$. A similar argument works for $2m-1$, $m-1$, and $m-2$. Clearly, the vertices $a = m$ and $a = 2m$ can easily be ruled out as well. Hence, $\frac{1}{(A)_{2m}}$ is MP.

*Case* 2. $m = 2 \cdot \mathrm{odd}$.

Here, $G_m$ contains the component




Since $4 | m+2$, then $m+2$ lies at the top level, which prevents the three vertices $1, m+1$, and $m+2$ in this component from satisfying condition (i) in (34).

A similar argument holds for $m-1$, $m-2$, $2m-1$ and also $m$, $2m$. Thus, $\frac{1}{(A)_{2m}}$ is MP.

*Case* 3. $m = 2^e$, $e \geq 2$.

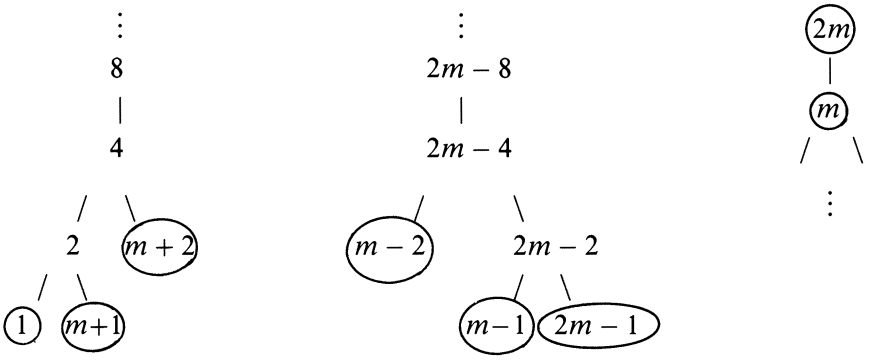
Same argument as in Case 2 in the proof of Theorem 19, since $2m$ is the only vertex at the top of $G_{2m}$.

*Case* 4. $m = 12$.

Verified in Example 15.

*Case* 5. $4|m$, $m \neq 12$, $m \neq 2^e$.

Here $8|2m$. The location in $G_{2m}$ of the 8 residues in $A$ (these are circled) is:




The two subgraphs on the left may or may not be connected, but each is certainly disjoint from the component on the right, since $m \neq 2^e$. Moreover, since $8|m$, both 8 and $2m-8$ are in the fourth row from the bottom, which may or may not be the top level. If 8 is not in the top level, then there must be a path in $A^c$ leading down from 8 to an odd element in $A^c$. In this case, MP reciprocation is impossible by Theorem 17. If 8 is in the top level, then the length of the orbit of 8 is at least two, since $m \neq 2^e$. The entry $2 \cdot 8 \bmod 2m$ will branch down to an odd $b \in A^c$ unless $2 \cdot 8 \equiv 2m - 8 \pmod{2m}$, or equivalently, unless $2m|24$, which has been ruled out in this case. □

Reciprocation of the Jacobi triple product or quintuple product can be used to give infinitely many parity results for the partition functions generated by the reciprocal of certain MP products. Suppose, for instance, that $S = \{n \in \mathbf{Z}^+ : n \equiv r_1, \ldots, r_t \pmod{m}\}$ and $p(S; n)$ is the partition function generated by

$$\prod_{n \in S} \frac{1}{1-x^n} = \sum_{n=0}^{\infty} p(S; n) x^n. \tag{37}$$

In some cases we can compute $p(S; n) \pmod 2$ from (37) by reciprocating the product on the left modulo 2. Whenever this reciprocal turns out to be a product whose expansion we know, such as the Jacobi triple product or quintuple product, we can expand this product and equate coefficients in the power series modulo 2. (Although we could work out some general classes of parity results, we will not do this here.) For example, suppose $A = \{\pm 1, \pm 2, \pm 4, \pm 5, 6\}$,

$m = 12$, $S = \{A\}_m$ and $\frac{1}{(A)_{12}} = \sum_{n=0}^{\infty} p(S; n)x^n$. We know from Example 4 that $\frac{1}{(1,5,6)_6} \equiv (A)_{12}$, so the Jacobi triple product gives

$$\sum_{n=0}^{\infty} p(S; n)x^n = \frac{1}{(A)_{12}} \equiv (1, 5, 6)_6 \equiv \sum_{-\infty}^{\infty} x^{3k^2+2k} = 1 + \sum_{k=1}^{\infty} (x^{k(3k-2)} + x^{k(3k+2)}).$$

It follows then that $p(S; n)$ is odd if and only if $n = k(3k \pm 2)$, $k \geq 0$.

In addition to the parity result above for the case $m = 6$ in Theorem 20, we have comparable results when $m = 2^e$, $e \geq 2$, and when $m$ is odd. In particular, when $m = 5$ and $S = \{n : n \equiv \pm(1, 2, 5, 6, 8, 9) \pmod{20}\}$, we learn from Example 2 and (35) that the parity of $p(S; n)$ is odd if and only if $n = \frac{k(5k\pm 3)}{2}$, $k \geq 0$. (See [2, pp. 746–747].)

Example 5 provides another parity result, this time using the quintuple product formula. In this case, let $A = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 10, \pm 11, 12\}$ and $m = 24$. Then by the results in Example 5 and (36) we have

$$\begin{aligned}\sum_{n=0}^{\infty} p(S; n)x^n = \frac{1}{(A)_{24}} &\equiv (1, 10, 11, 12, 13, 14, 23, 24)_{24} \\ &= \sum_{-\infty}^{\infty} x^{6(3k^2+k)}(x^{-3k} - x^{3k+1}) \\ &\equiv \sum_{k=0}^{\infty} (x^{18k^2+3k} + x^{18k^2+9k+1}) + \sum_{k=1}^{\infty} (x^{18k^2-3k} + x^{18k^2-9k+1}).\end{aligned}$$

Thus, $p(S; n)$ is odd for $n \geq 0$ if and only if $n = 0, 1, 18k^2 \pm 3k$ or $18k^2 \pm 9k + 1$ for $k \geq 1$.

TABLE 2

| | $S$ | $p(S; n)$ is odd exactly when | Reference |
|---|---|---|---|
| 1. | $n \not\equiv 0, \pm(2, 12, 14), 16 \pmod{32}$ | $n = k^2$ or $2k^2$, $k \geq 0$ | [3,Th. 1(a)] |
| 2. | $n \not\equiv 0, \pm(4, 6, 10), 16 \pmod{32}$ | $n = k^2 - 1$ or $2k^2 - 1$, $k \geq 1$ | [3,Th. 1(b)] |
| 3. | $n \not\equiv 0, \pm 5 \pmod{12}$ | $n = k^2$ or $3k^2$, $k \geq 0$ | [3,Th. 3(a)] |
| 4. | $n \not\equiv 0, \pm 1 \pmod{12}$ | $n = k^2 - 1$ or $3k^2 - 1$, $k \geq 1$ | [3,Th. 3(b)] |
| 5. | $n \not\equiv 0, \pm(3, 4, 8, 9) \pmod{24}$ | $n = 2k(k + 1)$ or $6k(k + 1) + 1$, $k \geq 0$ | [4, (26)] |
| 6. | $n \equiv \pm(1, 2, 8, 9), 10 \pmod{20}$ | $n = k^2$ or $5k^2$, $k \geq 0$ | [4, (32)] |
| 7. | $n \equiv \pm(3, 4, 6, 7), 10 \pmod{20}$ | $n = k^2 - 1$ or $5k^2 - 1$, $k \geq 1$ | [4, (33)] |
| 8. | $n \equiv \pm(1, 3, 7, 9), 10 \pmod{20}$ | $n = k(k + 1)$ or $5k(k + 1) + 1$, $k \geq 0$ | [4, (41)] |
| 9. | $n \equiv \pm(1, 2, 5), 6 \pmod{12}$ | $n = 0, 1,$ or $(3k \pm 1)^2$, $k \geq 1$ | [4, p. 312] |
| 10. | $n \equiv \pm 8, 16 \pmod{32}$ | $n = (2k - 1)^2 - 1$, $k \geq 1$ | [4, p. 313] |
| 11. | $n \equiv \pm(3, 6, 12, 15), 18 \pmod{36}$ | $n = 0$ or $(3k \pm 1)^2 - 1$, $k \geq 1$ | [4, p. 314] |

In Table 2 we give other parity results for the partition functions derived from the eleven expansions proved in [3] and [4]. These results differ from those using (35) or (36). (Cf. (2).) Note that the classes in $S$ above were obtained by Euler reciprocation of the products appearing in the referenced equations. (The

reciprocation for 1. and 2. has already appeared in [3, Theorems 2(a),(b)].) To prove 6., for example, observe that identity (32) in [4] gives the congruence

$$(0, \pm 1)_{10}(\pm 12)_{40}(\pm 4)_{20} \equiv 1 + \sum_{n=1}^{\infty}(x^{n^2} + x^{5n^2}).$$

Applying Euler reciprocation to the left-hand side, we obtain

$$\begin{aligned}
&\frac{1}{(0, \pm 1)_{10}(\pm 12)_{40}(\pm 4)_{20}} \\
&\quad \equiv (\pm 1)_{10}(\pm 3, \pm 5, \pm 7, \pm 13, \pm 15, \pm 17)^2_{40}(\pm 2, \pm 6, \pm 8, \pm 14, \pm 18)_{40} \\
&\quad = (\pm 1)_{10}(\pm 3, \pm 5, \pm 7)^2_{20}(\pm 2, \pm 6, \pm 8, \pm 14, \pm 18)_{40} \\
&\quad \equiv (\pm 1)_{10}(\pm 6, \pm 10, \pm 14)_{40}(\pm 2, \pm 6, \pm 8, \pm 14, \pm 18)_{40} \\
&\quad = (\pm 1)_{10}(\pm 2, 10)_{20}(\pm 8)_{40}(\pm 6)^2_{20} \\
&\quad \equiv (\pm 1)_{10}(\pm 2, 10)_{20}(\pm 8)_{40}(\pm 12)_{40} \\
&\quad = (\pm 1, \pm 2, \pm 8, \pm 9, 10)_{20}.
\end{aligned}$$

(We made a few short cuts, by halving the modulus of the square terms, when possible. The strict Euler reciprocation algorithm terminates at modulus 160 and then reduces to the final modulus 20.)

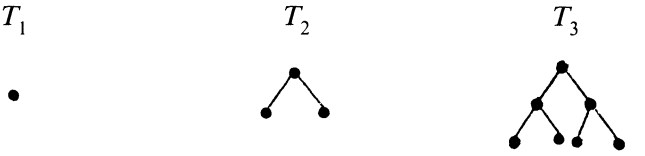
## 10. Some probabilistic considerations

In Theorem 18 we proved that MP products with an odd modulus always have an MP reciprocal. In the case of even moduli, it is not true that all MP products have MP reciprocals. For example, it is easily checked that $(1)_{2n}$ has no MP reciprocal for $n \geq 2$. It is of interest, then, to get some idea of how often MP products with even moduli do not lead to parity results because the reciprocation in (3) fails. Alternatively, we give in Table 3 below the number of "successes", i.e., the number and percentage of the $2^m$ subsets $A$ of $M$ for

TABLE 3

| $m$ | Successes | % | Symmetric | Symmetric Successes | % |
|---|---|---|---|---|---|
| 2 | 4 | 100.0 | 4 | 4 | 100.0 |
| 4 | 14 | 87.5 | 8 | 8 | 100.0 |
| 6 | 56 | 87.5 | 16 | 16 | 100.0 |
| 8 | 218 | 85.2 | 32 | 30 | 93.8 |
| 10 | 968 | 94.5 | 64 | 56 | 87.5 |
| 12 | 3052 | 74.5 | 128 | 112 | 87.5 |
| 14 | 13456 | 82.1 | 256 | 232 | 90.6 |
| 16 | 57074 | 87.1 | 512 | 474 | 92.6 |
| 18 | 225904 | 86.2 | 1024 | 928 | 90.6 |
| 20 | 868924 | 82.9 | 2048 | 1744 | 85.2 |
| 22 | 4190216 | 99.9 | 4096 | 3976 | 97.1 |
| 24 | 12442132 | 74.2 | 8192 | 6540 | 79.8 |
| 26 | 67092488 | 99.9 | 16384 | 16136 | 98.5 |
| 28 | 192697400 | 71.8 | 32768 | 29680 | 90.6 |
| 30 | 793659328 | 73.9 | 65536 | 54208 | 82.7 |

which $\frac{1}{(A)_m}$ is an MP product for $m = 2, 4, 6, \ldots, 30$. The table also lists the number and percentage of successes when $A$ is symmetric. (For completeness, we assume the empty product and its reciprocal are MP.) The data in Table 3, which was initially computed by exhaustive search, can also be obtained from a probabilistic, graph-theoretic argument as follows. First, let $T_n$ be the full binary rooted tree with $2^n - 1$ vertices, where the length from the root to each terminal vertex is exactly $n - 1$.




Now two-color the vertices of $T_n$, say, using red and green. Let $z_n$ count the number of colorings of $T_n$ so that no path exists from the root to a terminal vertex *lying entirely in red vertices.* Greg Manning has shown

**Proposition 21** [Manning]. *The number* $z_n$ *satisfies the recursion*

$$z_n = z_{n-1}^2 + 2^{2^n-2}, \qquad z_0 = 0. \tag{38}$$

*Proof.* If the root of $T_n$ is green, then there are $2^{2^n-2}$ ways to color the remaining $2^n - 2$ vertices. Now suppose the root is red. Remove the root from $T_n$, obtaining $T_n'$, a forest of two trees isomorphic to $T_{n-1}$. By independence of the two trees, the number of ways to color $T_n'$ so that no red path extends from either root to a terminal vertex is $z_{n-1}^2$. □

From Proposition 21 we readily obtain the initial values: $z_1 = 1$, $z_2 = 5$, $z_3 = 89$, and $z_4 = 24305$.

We return to the problem of computing the probability that algorithm *InvertTest* will succeed for any arbitrary subset $A \subseteq M$ for a given modulus $m$. We take advantage of the fact that the probabilities of success for the components of $G_m$ are independent and therefore can be multiplied together to give the probability of success for the entire graph. Note that the probability calculation for each component $H$ of $G_m$ depends only on the number of 2's that divide $m$ and the length of the orbit in the top row of $H$. Let $n =$ the number of rows in $H$ and $k =$ the number of elements in the top row. The parameters $n$ and $k$ uniquely determine the probability of success, i.e., the probability that a subset $A$ of $H$, chosen at random, has the property that no pair $a \in A$, $b \in \mathrm{Odd}(A^c)$ satisfies (34). Let $S(n, k)$ count the number of successes and $F(n, k)$ count the number of failures. Then the probability $P(n, k)$ of success is $S(n, k)/2^{2^{n-1}k}$.

We calculate $F(n, k)$, the number of ways we can choose a subset $A$ of the vertices of $H$ so that there exists a counterexample $a \in A$, $b \in \mathrm{Odd}(A^c)$ satisfying (34). Let the vertices in $A$ be green, say, and those in $A^c$ be red. To construct a counterexample, we are forced to color the entire top row of $H$ red, i.e., the top row must lie in $A^c$. If this top row of $H$ is removed, then the remaining forest $H'$ will have $k$ trees, each isomorphic to $T_{n-1}$. There

are $2^{(2^{n-1}-1)k}$ ways to color the vertices of $H'$. Conditions (i) and (iii) of (34) are automatically satisfied, provided $A \neq \varnothing$, since, given any coloring, we can work our way down $H'$, remaining in red vertices (in $A^c$), until we eventually come to some green vertex $a \in A$. We need only count the number of ways to satisfy condition (ii) of (34), which requires that a red path exists from a root of one of the trees $T_{n-1}$ down to a terminal vertex. By the independence of the $k$ trees and Proposition 21, the number of ways that such a red path fails to exist is $z_{n-1}^k$. Thus,

$$F(n, k) = 2^{(2^{n-1}-1)k} - z_{n-1}^k - 1. \tag{39}$$

(We subtract 1 to exclude the case where all vertices are red.) It follows that

$$S(n, k) = 2^{2^{n-1}k} - 2^{(2^{n-1}-1)k} + z_{n-1}^k + 1. \tag{40}$$

Using (40) and (38), it is easy to verify the following formula for the probability $P(n, k)$:

$$P(n, k) = 1 - \frac{1}{2^k} + \frac{u_{n-1}^k}{2^k} + \frac{1}{2^{2^{n-1}k}} \tag{41}$$

where

$$u_n = (u_{n-1}^2 + 1)/2, \quad u_0 = 0. \tag{42}$$

By independence, the total number of successes for a modulus $m$ is the product of $S(n, k)$ for each component $H$ of $G_m$. For example, one finds that $G_{28}$ has three components, whose top rows have orbit lengths of size 3, 3, and 1. By (40), $S(3, 3) = 2^{12} - 2^9 + 5^3 + 1 = 3710$ and $S(3, 1) = 14$. Thus, the probability of success for $G_{28}$ is

$$\frac{(3710)^2 14}{2^{28}} = \frac{192697400}{268435456} = 71.8\%,$$

in agreement with Table 3.

As another example, the graph $G_{22}$ consists of two components, one with the ten elements 2, 4, 8, 16, 10, 20, 18, 14, 6, 12, forming a cycle in the top row, and the other with only 22 in the top row. For the first component, $S(2, 10) = 2^{20} - 2^{10} + 2 = 1047554$, while $S(2, 1) = 4$. By Theorem 17 and the independence of the events for the two components, the number of subsets of $M$ which have MP reciprocals is $S(2, 10)S(2, 1) = 4190216$, the value given in the the second column of Table 3. The percentage of successes is thus $\frac{4190216}{4194304} = 99.9\%$. Such a high percentage will always occur when $m = 2p$, where $p$ is a prime having 2 as a primitive root. Then $G_{2p}$ also has a two component graph with two lines, where the ratio of successes to the total number is

$$\frac{S(2, p-1)S(2, 1)}{2^{2p}} = \frac{2^{2p} - 2^{p+1} + 8}{2^{2p}} = 1 - \frac{1}{2^{p-1}} + \frac{1}{2^{2p-3}}.$$

The data in Table 3 were computed using Algorithm *InvertTest* on an IBM-compatible AT personal computer. In every case, the numbers agree with the

values obtained using (40). This provides an excellent check on the program. Finally, we mention that a similar theoretical analysis could be made to verify the number of symmetric successes given in Table 3.

## ACKNOWLEDGMENTS

We would like to thank William D. Blair for formula (5), which improved our previous algorithm *Invert*. We would also like to thank Greg Manning, a graduate student currently at Northern Illinois University, for the recursive formula (38), a key tool in analyzing the probability of success of Algorithm *InvertTest*. Finally, we thank the referee for the remark at the end of Section 4.

## BIBLIOGRAPHY

1. G. E. Andrews, *Two theorems of Euler and a general partititon theorem*, Proc. Amer. Math. Soc. **20** (1969), 499–502.
2. R. Blecksmith, J. Brillhart, and I. Gerst, *A computer-assisted investigation of Ramanujan pairs*, Math. Comp. **46** (1986), 731–749.
3. ——, *Parity results for certain partition functions and identities similar to theta function identities*, Math. Comp. **48** (1987), 29–38.
4. ——, *Some infinite product identities*, Math. Comp. **51** (1988), 301–314.
5. I. Schur, *Zur additiven Zahlentheorie*, Sitzungsberichte der Preussischen Akademie der Wissenschaften; Physikalisch-Mathematische Klasse, 1926, 488–495; Collected Works, Springer-Verlag, New York, 1973, 43–50.

DEPARTMENT OF MATHEMATICAL SCIENCES, NORTHERN ILLINOIS UNIVERSITY, DEKALB, ILLINOIS 60115

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ARIZONA, TUCSON, ARIZONA 85721

DEPARTMENT OF APPLIED MATHEMATICS AND STATISTICS, SUNY AT STONY BROOK, STONY BROOK, NEW YORK 11794