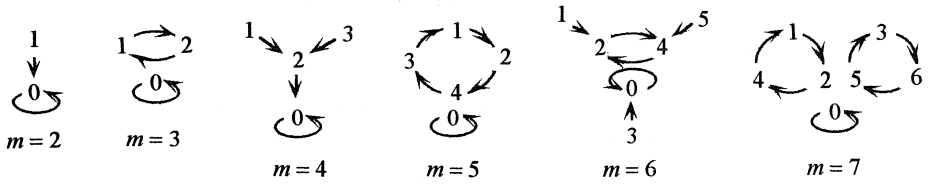
CYCLES IN DOUBLING DIAGRAMS MOD *m*

Amos Ehrlich
School of Education, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel
(*Submitted May 1992*)

1. INTRODUCTION, NOTATIONS, AND A THEOREM

By "doubling diagram mod m" we mean the directed graph whose vertices are 0 and the natural numbers less than m, with directed arcs (arrows) from each vertex x to $2x$ reduced modulo m.



I gave pages with the diagrams for m's from 2 to 31 to a group of students, and asked them to find regularities. This took place at the School of Education of Tel Aviv University, in an elective course for non-mathematicians, intended to improve their ideas about mathematics. The students recognized some known phenomena (see [1]), including the fact that, for an odd m, all the vertices are arranged in cycles. Suzanah Erseven, a prospective English teacher, examined the *numbers* of cycles in the diagrams for the odd m's, and found that the sequence of these numbers consists of two even numbers and two odd numbers, alternately. Her discovery is reformulated here as Theorem 1. Its proof is the central topic of this paper.

Notations: In the following, the variable m will denote the modulus of the diagram, and will be limited to odd numbers.

$L(m)$ is the number of vertices in the cycle of 1,

$C(m)$ is the number of cycles with vertices that are relatively prime to m, and

$T(m)$ is the total number of cycles in the doubling diagram modulo m, including the cycle of 0.

$\varphi(n)$ is the Euler function (number of natural numbers less than and relatively prime to n).

A number m will be called "O.K." if it agrees with the following theorem.

Theorem 1: $m \equiv \pm 1 \pmod 8 \Rightarrow T(m)$ is an odd number.
$m \equiv \pm 3 \pmod 8 \Rightarrow T(m)$ is an even number.

2. PROOF OF THEOREM 1

The proof of Theorem 1 will emerge from some propositions and results. Let us start with these.

Since a chain of n arrows leads from x to x iff $x \cdot 2^n \equiv x \pmod m$, that is, iff $m | x(2^n - 1)$, it follows that

I. $L(m)$ is the minimal n such that $m|2^n-1$, and it divides any other n with this property.

II. If x is prime to m, then its cycle is also of length $L(m)$ (and all the vertices in this cycle are relatively prime to m).

III. The length of any cycle in the doubling diagram mod m divides $L(m)$. [$m|2^{L(m)}-1$ hence $m|x(2^{L(m)}-1)$ hence $L(m)$ arrows from x end at x.]

IV. $C(m)\cdot L(m)=\varphi(m)$. (This follows from II.)

Since $2x\equiv y \pmod m \Leftrightarrow 2kx\equiv ky \pmod{km}$, it follows that

V. If we multiply by k the values of the vertices of a cycle in the doubling diagram mod m, we get a cycle in the doubling diagram mod km.

VI. $L(m)|L(km)$. (This results from III and V.)

Proposition 1: For every prime number $p\neq 2$, $L(p^{n+1})$ is equal to either $p\cdot L(p^n)$ or $L(p^n)$.

Proof: Denote $L(p^n)$ by λ. Then $p^n|2^\lambda-1$, that is, $2^\lambda\equiv 1 \pmod{p^n}$, hence $2^\lambda\equiv 1 \pmod p$, and so are all of the powers of 2^λ. From this, it follows that $1+2^\lambda+2^{2\lambda}+\cdots+2^{(p-1)\lambda}$ is divisible by p, and therefore $2^{\lambda p}-1$, which is the product of this sum and $2^\lambda-1$, is divisible by p^{n+1}. By this and by II we have that $L(p^{n+1})|\lambda p$, and by VI we have that $\lambda|L(p^{n+1})$. □

Remark a: Let $k=(2^\lambda-1)/p^n$. Then

$$\begin{aligned}1+2^\lambda+2^{2\lambda}+\cdots+2^{(p-1)\lambda} &= 1+(kp^n+1)+(kp^n+1)^2+\cdots+(kp^n+1)^{(p-1)}\\ &= p+kp^n\cdot(1+2+\cdots+(p-1))+p^{2n}\cdot(\cdots)\\ &= p+kp^n\cdot p\cdot(p-1)/2+p^{2n}\cdot(\cdots).\end{aligned}$$

The second term on the extreme right side is divisible by p^2 (even for $n=1$, since $p\neq 2$), so the total sum is not a multiple of p^2. Therefore, if $2^\lambda-1$ is divisible by p^n but not by p^{n+1}, then $2^{\lambda p}-1$ is divisible by p^{n+1} but not by p^{n+2}. From this one gets that if, for some n, $L(p^{n+1})\neq L(p^n)$, then $L(p^{n+1})\neq L(p^n)$ for all bigger n's.

Remark b: Computer runs show that, for all prime numbers up to 100,000, there are just two cases where $L(p^{n+1})=L(p^n)$. These are $L(1093^2)=L(1093)=364$ and $L(3511^2)=L(3511)=1755$.

Remark c: A theorem similar to Proposition 1 together with Remark a, but (still?) without examples as in Remark b, was proved by Wall [2] for the length of the period of the Fibonacci series reduced mod m.

Lemma 1: If $m=p$ is O.K., so is $m=p^n$.

Proof: $\varphi(p^{n+1})=p^{n+1}-p^n=p\cdot\varphi(p^n)$. From this, together with IV and Proposition 1, it follows that $C(p^{n+1})$ is either equal to $C(p^n)$ or else p times greater. In any case, they are both even or both odd numbers.

By V, the vertices in the doubling diagram mod p^{n+1} that are the multiples of p form a sub-diagram congruent to the diagram mod p^n, that is, they form $T(p^n)$ cycles. So $T(p^{n+1})=T(p^n)+C(p^{n+1})$.

If $p \equiv \pm 1 \pmod 8$, then so is every p^n. In this case $T(p)$ is an odd number (we've assumed $m = p$ is O.K.), so $C(p)$ is an even number (they differ just by the cycle of 0); hence, all the $C(p^n)$'s are even numbers and, therefore, all the $T(p^n)$'s are odd numbers.

If $p \equiv \pm 3 \pmod 8$, then $p^2 \equiv 1, p^3 \equiv \pm 3, p^4 \equiv 1$, and so on. In this case $T(p)$ is an even number, so $C(p)$ is an odd number; hence, all the $C(p^n)$'s are odd numbers and, therefore, the $T(p^n)$'s are even numbers and odd numbers, alternately. □

Proposition 2: If m_1 and m_2 are relatively prime to each other and to 2, then

$$L(m_1 \cdot m_2) = \text{l.c.m.}(L(m_1), L(m_2)).$$

Proof: $2^x - 1 | 2^{xy} - 1$ (the quotient is a sum of a geometric sequence). By I it follows that both m_1 and m_2 divide $2^{\text{l.c.m.}(L(m_1), L(m_2))} - 1$, and so does their product. Hence, $L(m_1 \cdot m_2)$ divides $\text{l.c.m.}(L(m_1), L(m_2))$. Their equality follows from VI. □

Remark: Wall [2] proves a similar theorem for the lengths of periods of the Fibonacci sequence reduced mod m (not limited to odd numbers). But this does not point at a special similarity between the Fibonacci sequence and the geometric sequence 1, 2, 4, ... In [3] I suggested a generalization of both Wall's theorem and Proposition 2. Let $a(i)$ be any sequence such that reducing its elements modulo m gives, for some m's, a periodic sequence (the period does not have to start at the very beginning). Let $P(m)$ be the length of the period, and let m_1 and m_2 be *any* two numbers for which P is defined. Then $P(\text{l.c.m.}(m_1, m_2)) = \text{l.c.m.}(P(m_1), P(m_2))$. This result, like Theorem 1, emerged from a suggestion of a student of mine (in a mathematics club for high school students).

Proposition 3: If m_1 and m_2 are prime to each other and to 2 and different from 1, then $C(m_1 \cdot m_2)$ is an even number.

Proof: Let us recall two properties of the Euler φ function: (a) If n_1 and n_2 are relatively prime, then $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$. (b) If $n \neq 2$, then $\varphi(n)$ is an even number.

Now,

$$\begin{aligned} C(m_1 \cdot m_2) &= \varphi(m_1 \cdot m_2) / L(m_1 \cdot m_2) \\ &= \varphi(m_1) \cdot \varphi(m_2) / \text{l.c.m.}(L(m_1), L(m_2)) \\ &= \varphi(m_1) / L(m_1) \cdot \varphi(m_2) / L(m_2) \cdot \text{g.c.d.}(L(m_1), L(m_2)) \\ &= C(m_1) \cdot C(m_2) \cdot \text{g.c.d.}(L(m_1), L(m_2)). \end{aligned}$$

At least one of the last three factors is an even number since, if $C(m)$ is an odd number, then $L(m)$, which equals $\varphi(m) / C(m)$, is an even number. □

Lemma 2: If m_1 and m_2 are as in Proposition 3 and are both O.K., then so is $m = m_1 \cdot m_2$.

Proof: By V, those vertices in the diagram mod m that are multiples of m_1 form $T(m_2)$ cycles, and the multiples of m_2 form $T(m_1)$ cycles. Together they form $T(m_1) + T(m_2) - 1$ cycles, since the cycle of 0 is the only one that is counted both in $T(m_1)$ and in $T(m_2)$.

Let us partition the other vertices into classes in the following way: For each pair d_1 and d_2 that are *proper* divisors of m_1 and m_2, respectively, let us form the class of all the vertices that are

multiples of $d_1 \cdot d_2$ but not of any greater factor of m. We are going to show that the elements of such a class form an even number of cycles. Indeed, if we divide the elements of the class by $d_1 \cdot d_2$, we get the vertices of the doubling diagram modulo m_1 / d_1 and m_2 / d_2 satisfy the conditions of Proposition 3.

It follows that $T(m)$ is an even number $\Leftrightarrow T(m_1) + T(m_2) - 1$ is an even number $\Leftrightarrow$ just one of $T(m_1), T(m_2)$ is an even number $\Leftrightarrow$ just one of m_1, m_2 is $\equiv \pm 3 \pmod 8 \Leftrightarrow m \equiv \pm 3 \pmod 8$. □

Lemma 3: Every prime number $p \neq 2$ is O.K.

Proof: p divides $2^{p-1} - 1$. Therefore, it divides either $2^{(p-1)/2} - 1$ or $2^{(p-1)/2} + 1$.

If p divides $2^{(p-1)/2} + 1$, then $(p-1)/2$ arrows of the diagram mod p lead from 1 to -1 (more precisely, to $p - 1$). In one turn around the cycle of 1, the number of arrows from 1 to -1 is equal to the number of arrows from -1 to 1, so $(p-1)/2$ arrows make an odd number of half-turns around this cycle [that is, $(p-1)/2$ = an odd number $\cdot L(p)/2$]. Since $C(p) = (p-1)/L(p) = ((p-1)/2)/(L(p)/2)$, it is an odd number and since, for a prime p, $T(p) = C(p) + 1$, it follows that in our case $T(p)$ is an even number.

If p divides $2^{(p-1)/2} - 1$, then $(p-1)/2$ arrows lead from 1 to 1, hence $(p-1)/2$ is a multiple of $L(p)$, hence $C(p) = (p-1)/L(p)$ is an even number, so $T(p)$ is an odd number.

To complete our proof, we have to show that $p | 2^{(p-1)/2} - 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$.

Corollary 2.28 (or Theorem 3.1a) in Niven-Zuckerman [4], with $a = 2$, says that p divides $2^{(p-1)/2} - 1$ iff there is a solution for $x^2 \equiv 2 \pmod p$. Problem 10 on page 73 (solved by the last part of Theorem 3.3) says that $x^2 \equiv 2 \pmod p$ has a solution iff $p \equiv \pm 1 \pmod 8$. □

Proof of Theorem 1: By Lemma 3, Lemma 1, and Lemma 2. □

3. ANOTHER POINT OF VIEW AND ANOTHER THEOREM

An exercise in long division in base 2 will show that $L(m)$ is the length of the period of the binacy fraction for $1/m$. Moreover, $C(m)$ is the number of classes of fractions-in-lower-terms with the denominator m and with binary expansions whose periods are equal to each other up to a cyclic permutation, while $T(m)$ may be described in the same way, omitting the words "in-lower-terms."

The analog of Theorem 1 for the base 10 is the following:

Theorem 2: Let m be relatively prime to 10, and consider the number of different periods in the decimal expansions of fractions with the denominator m. This number is an odd number iff $m \equiv \pm 1$ or ± 3 or ± 9 or $\pm 27 \pmod{40}$.

The proof is similar to that of Theorem 1 with some self-evident modifications, but two additional lemmas are needed. For convenience, I am going to write "m is like 1" for $m \equiv \pm 1$ or ± 3 or ± 9 or $\pm 27 \pmod{40}$, and "m is like 7" for $m \equiv \pm 7$ or ± 11 or ± 17 or $\pm 19 \pmod{40}$.

Lemma 4: The product of two numbers like 1 and the product of two numbers like 7 are like 1; the product of a number like 1 and a number like 7 is like 7.

Proof: By checking the different cases. □

The next lemma is needed for the last half of the proof of the base-10 version of Lemma 1.

Lemma 5: Let m be a natural number prime to 10. For each integer i from 0 to $(m-1)/2$, let us write r_i for the residue of $10i$ when reduced mod m, and let n be the number of r_i's that are greater than $m/2$. With this notation, n is an even number iff m is like 1.

Proof: Numerical checks show that the lemma holds for every $m < 50$. We have to demonstrate that, if the lemma holds for some $m > 10$, then it holds also for $m+40$. Let us assume $m \geq 11$.

Consider the sequence 0, 10, 20, ..., $5m - 5$. Reducing its elements modulo m to get their r_i's consists of five stages: In the first stage we subtract $0 \cdot m$, in the second stage $1 \cdot m$, and so on until the fifth stage, where we subtract $4m$'s. Each stage starts by yielding an r_i of one digit, followed by all the other numbers less than m, which end with that digit. (The fifth stage is not interrupted by the end of the sequence, since adding 10 to the last element gives a number $> 5m$.)

The r_i's we get in this way are different from each other, since m is relatively prime to 10, so they consist of all the integers from 0 to $m - 1$, having one of certain five digits for their last digit. Consequently, every ten successive integers in $[0, m-1]$ include exactly five r_i's.

Replacing m by $m' = m+40$ does not change the above-mentioned set of five digits since, if $10i - jm = r$ with $1 \leq (m-1)/2$ and $j \leq 4$, then $10(i+4j) - jm' = r$ and $i+4j \leq (m'-1)/2$. The set of the r_i's associated with m' that are greater than $m'/2$ include the old r_i's that are greater than $m/2$, plus twenty new r_i's bigger than $m - 1$, less ten r_i's that are between $m/2$ and $m'/2$.

It follows that the n associated with m' is an even number iff the n associated with m is an even number. □

This lemma, together with Theorem 3.2 of [4] (a lemma of Gauss), are used instead of Problem 10 at the end of the proof of the base-10 version of Lemma 3. Theorem 3.2 says, for $a = 10$, that if m is a prime number different from 2 and from 5, then the congruence $x^2 \equiv 10 \pmod{m}$ has a solution iff the n we have defined in Lemma 2 is an even number. Lemma 5 itself now completes the proof.

REFERENCES

1. A. Ehrlich. "Doubling Diagrams." *Math. Teaching* **84** (1978):35-39.
2. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
3. A. Ehrlich. "On the Periods of the Fibonacci Sequence Modulo m." *The Fibonacci Quarterly* **27.1** (1989):11-13.
4. I. Niven & H. S. Zuckerman. *An Introduction to the Theory of Numbers.* 2nd ed. New York: John Wiley, 1968.

AMS Classification Number: 11A99

❖❖❖