CONCERNING THE DIVISORS OF N AND THE EXPONENTS THEY BELONG TO MODULO $(N - 1)$ or $(N + 1)$

Irving Adler
North Bennington, VT 05257
(Submitted June 1987)

1. Definition

A finite set of positive integers is said to have property A if every member of the set is a divisor of the greatest member of the set.

Example: The set of exponents to which numbers prime to m belong modulo m has property A. [The greatest exponent in the set is $\lambda(m)$, and every member of the set is a divisor of $\lambda(m)$. See the propositions listed for reference in Section 3 below.] Let N be any positive integer greater than 3. Let S be the set of exponents to which the numbers prime to $N - 1$ belong modulo $(N - 1)$. Let T be the set of exponents to which the numbers prime to $N + 1$ belong modulo $(N + 1)$. S and T have property A. Let S' and T' be the sets of exponents to which the divisors of N belong modulo $(N - 1)$ and $(N + 1)$, respectively. S' is a subset of S, and T' is a subset of T. For example, if $N = 21$, the numbers less than 20 and prime to it are 1, 3, 7, 9, 11, 13, 17, and 19. The exponents they belong to modulo (20) are, respectively, 1, 4, 4, 2, 2, 4, 4, and 2. Then $S = \{1, 2, 4\}$. The divisors of 21 are 1, 3, 7, and 21. The exponents they belong to modulo (20) are, respectively, 1, 4, 4, and 1. Then $S' = \{1, 4\}$. The numbers less than 22 and prime to it are 1, 3, 5, 7, 9, 13, 15, 17, 19, and 21. The exponents they belong to modulo (22) are, respectively, 1, 5, 5, 10, 5, 10, 5, 10, 10, and 2. Then $T = \{1, 2, 5, 10\}$. The exponents that the divisors of 21 (1, 3, 7, 21) belong to modulo (22) are, respectively, 1, 5, 10, and 2. Then $T' = \{1, 2, 5, 10\}$. The propositions proved in this paper grew out of a search for values of N for which S' and T' also have property A.

2. Origin of the Problem

This problem grew out of the following permutation problem. Let a be any proper divisor of N. N cards in a deck are numbered from 1 to N from the top down and are permuted as follows: Divide the deck into a equal piles and place them side by side in the order of their positions in the deck from the top down. Then pick up the top card from each pile in rotation, starting with the pile that came from the top, until all the cards have been picked up. Question: What is the order of the permutation? That is, how many repetitions of this procedure will restore all the cards to their original positions in the deck? It is not hard to prove that the answer is e repetitions, where e is the exponent that a belongs to modulo $(N - 1)$. (The proof is given in the Appendix.) (For example, for an ordinary deck of playing cards, $N = 52$. If the permutation is done with two piles, $a = 2$. Then $e = 8$, since 8 is the least exponent for which $2^e \equiv 1$ modulo 51.) This fact led to an examination of the set S' defined above. Since the set T' is also well defined for any N, it is natural to examine this set as well. It is immediate that S' or T' has property A if N has a divisor that is a primitive λ-root of $(N - 1)$ or $(N + 1)$,

respectively. Calculation for many values of N shows that there are many cases where S' or T' has property A even when N does not have a divisor that is a primitive λ-root of $(N - 1)$ or $(N + 1)$, respectively. However, there are also values of N for which S' does not have property A. For $N < 26{,}720$, there are 130 values of N for which S' does not have property A. The first ten of these are 572, 1182, 1463, 1953, 2004, 2010, 2338, 2343, 2405, and 3002. (For example, for $N = 572$, $S' = \{1, 57, 114, 190, 285\}$. Since neither 114 nor 190 is a divisor of 285, S' does not have property A.) All 130 of these numbers have the property that they are divisible by three or more different prime numbers. Also, for $N < 5254$, there are 25 values of N for which T' does not have property A. The first ten of these are 1085, 1434, 2354, 2409, 2849, 2975, 3069, 3130, 3138, and 3154. (For example, for $N = 1085$, $T' = \{1, 2, 12, 20, 30\}$. Since neither 12 nor 20 is a divisor of 30, T' does not have property A.) All 25 of these numbers also have the property that they are divisible by three or more different primes. These observations led to the conjecture that if N has at most two different prime divisors, then S' and T' have property A. The purpose of this paper is to prove the conjecture.

3. Definitions and Propositions

For handy reference, we list below the definitions and propositions of elementary number theory that are relevant to this paper.

Definition: If a and m are relatively prime positive integers, and e is the least positive integer such that $a^e \equiv 1 \mod (m)$, then e is said to be the exponent to which a belongs mod (m).

Definition (Euler's ϕ-function)*:* For any positive integer m, $\phi(m)$ is the number of positive integers not greater than m and prime to it.

Proposition 3.0: If $p_1, p_2, \ldots, p_n$ are the different prime divisors of m, then

$$\phi(m) = m(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_n).$$ (see [1], p. 32).

Definition: For any positive integer m, $\lambda(m)$ is defined as follows:

$\lambda(2^a) = \phi(2^a)$ if $a = 0, 1, 2$.

$\lambda(2^a) = (1/2)\phi(2^a)$ if $a > 2$.

$\lambda(p^a) = \phi(p^a)$ if p is an odd prime.

$\lambda(2^a p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}) = M$, where M is the least common multiple of $\lambda(2^a), \lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_n^{a_n})$.

Definition: If a belongs to $\lambda(m)$ modulo m, then a is said to be a primitive λ-root modulo m.

Proposition 3.1: If $(a, b) = 1$, there exist positive integers x, y such that $xa - yb = \pm 1$.

Proposition 3.2: If a and m are any two relatively prime positive integers, the congruence $a^{\lambda(m)} \equiv 1 \mod m$ is satisfied (see [1], p. 54).

Proposition 3.3: If a belongs to d mod m, and $a^n \equiv 1 \mod m$, then d is a divisor of n (see [1], p. 62).

Proposition 3.4: Every modulus m has primitive λ-roots (see [1], p. 72).

Proposition 3.5: If x belongs to the exponent ab modulo m, then x^a belongs to the exponent b (see [2], p. 106).

Proposition 3.6: If x belongs to the exponent a and y belongs to the exponent b modulo m, where $(a, b) = 1$, then xy belongs to the exponent ab (see [2], p. 106).

4. Propositions I and II

Proposition I: If N has the form p^a, where p is a prime number, then S' and T' have property A.

Proof: The following argument is valid for congruences modulo $(N-1)$ or $(N+1)$: Let p belong to e, and let p^r belong to d for any $r \leq a$. Since $p^e \equiv 1$, it follows that $(p^r)^e \equiv 1$. Therefore, by Proposition 3.3, d divides e. Then S' and T' have property A.

Proposition IIA: If N has the form $p^a q^b$, where p and q are different primes, then S' has property A.

Proposition IIB: If N has the form $p^a q^b$, where p and q are different primes, then T' has property A.

The proofs for Propositions IIA and IIB are carried through separately below.

5. Proofs of Some Preliminary Propositions

Before proving Proposition IIA, we prove some preliminary propositions. We consider first the special case where $(a, b) = 1$. Since a and b are relatively prime, then (with appropriate choice of notation, interchanging a and b if necessary) there exist positive integers x and y such that $xa - yb = 1$.

Proposition 5.1: If $(a, b) = 1$, there exist integers x, y such that $0 < x \leq b$ and $0 \leq y < a$ and $xa - yb = 1$.

(1) Can we have $x \leq b$ and $y > a$? If we did, then $b = x + s$ for some $s \geq 0$, and $y = a + r$ for some $r > 0$. Then $ax - (a + r)(x + s) = 1$ yields $-as - rx - rs = 1$, which is impossible.

(2) Can we have $y \leq a$ and $x > b$? If we did, then $a = y + s$ for some $s \geq 0$, and $x = b + r$ for some $r > 0$. Then $(b + r)(y + s) - yb = 1$, and $bs + ry + rs = 1$. This is impossible if $s > 0$. If $s = 0$, $ry = 1$, and hence $r = 1$ and $y = 1$. Then $x = b + 1$, $y = a = 1$. Then this case is possible only if $N = pq^b$. However, with a change of notation, writing p for q and vice versa, and a for b and vice versa, we could have written $N = p^a q$, and use $x = 1$, $y = a - 1$, so that we have $x = b$, $y < a$ [see case (4) below]. Note that y is positive unless $a = 1$, in which case $y = 0$.

(3) If $x > b$ and $y > a$, we can replace x by $x - b$ and y by $y - a$, since

$$(x - b)a - (y - a)b = xa - yb = 1.$$

By repeated application of this procedure, we would ultimately get either case (2) above or case (4) below.

(4) $0 < x \leq b$, and $0 \leq y \leq a$. We can include case (2) in the changed notation ($N = p^a q$, with $x = 1$, $y < a$, and $y = 0$ only if $a = 1$) by permitting y to be 0 if $a = 1$. We cannot have $y = a$, because if $y = a$,

$xa - ba = 1$, $a(x - b) = 1$; thus $a = 1$, $x = b + 1$, contradicting $x \leq b$. If $x = b$, $ba - by = 1$, $b(a - y) = 1$. Then $b = 1$, $y = a - 1$. Consequently, we may always assume x and y such that $0 < x \leq b$ and $0 \leq y < a$.

Proposition 5.2: If $(a, b) = 1$, then S' has property A.

Proof: By Proposition 5.1, $p^y q^x$ is a proper divisor of N. Let e be the exponent to which $p^y q^x$ belongs modulo $(N - 1)$. We now show that if $p^m q^n$ is any proper divisor of N, and it belongs to f modulo $(N - 1)$, then f divides e. We show first that the ordered pairs $(0, 1)$ and $(1, 0)$ are linear combinations (with integral coefficients) of (a, b) and (y, x):

$$a(y, x) - y(a, b) = (0, ax - by) = (0, 1).$$

$$x(a, b) - b(y, x) = (xa - by, 0) = (1, 0).$$

$$(m, n) = m(1, 0) + n(0, 1) = mx(a, b) - mb(y, x) + na(y, x) - ny(a, b)$$
$$= (mx - ny)(a, b) - (mb - na)(y, x).$$

We know that $p^a q^b \equiv 1$ modulo $(N - 1)$ and $(p^y q^x)^e \equiv 1$ modulo $(N - 1)$. Then

$$(p^a q^b)^{e(mx - ny)} \equiv 1 \quad \text{and} \quad (p^y q^x)^{e(mb - na)} \equiv 1.$$

Therefore,

$$(p^a q^b)^{e(mx - ny)} \equiv (p^y q^x)^{e(mb - na)} \bmod (N - 1).$$

Since p and q are prime to $N - 1$, we may divide by the right-hand member. This yields

$$(p^m q^n)^e \equiv 1 \text{ modulo } (N - 1).$$

Therefore, f divides e.

6. Proof of Proposition IIA

We consider now the general case, $N = p^{ga} q^{gb}$, where $(a, b) = 1$ and $g \geq 1$. Let (x, y) be determined such that $xa - yb = 1$, $0 < x \leq b$ and $0 \leq y < a$. Let e be the exponent that $p^y q^x$ belongs to modulo $(N - 1)$. Let $p^r q^s$ be any divisor of N.

$$p = (p^a q^b)^x (p^y q^x)^{-b}. \qquad q = (p^a q^b)^{-y} (p^y q^x)^a.$$

$$p^r = (p^a q^b)^{rx} (p^y q^x)^{-br}. \qquad q^s = (p^a q^b)^{-sy} (p^y q^x)^{as}.$$

Then $p^r q^s = (p^a q^b)^{rx - sy} (p^y q^x)^{as - br}$.

Let f be the least common multiple of g and e. Then

$$(p^r q^s)^f \equiv (p^a q^b)^{f(rx - sy)} (p^y q^x)^{f(as - br)} \equiv 1.$$

If $p^r q^s$ belongs to h modulo $(N - 1)$, it follows that h divides f. To complete the proof, we now show that there exists a divisor of N that belongs to f. In the special case where g is a divisor of e, the result is immediate, since then $f = e$, and $p^y q^x$ belongs to e.

For the completely general situation, we express g and e as products of powers of primes.

$$g = p_1^{a_1} \ldots p_k^{a_k} \quad \text{and} \quad e = p_1^{b_1} \ldots p_k^{b_k},$$

where the set $W = \{p_1, \ldots, p_k\}$ includes all the primes that occur in either g or e. (Some of the a_i and some of the b_i may be zero.) Partition W into two disjoint sets U and V as follows:

$$p_i \in U \text{ if } a_i > b_i, \quad p_i \in V \text{ if } a_i \leq b_i.$$

Let $m = \prod_{p_i \in U} p_i^{a_i}$, $n = \prod_{p_i \in V} p_i^{a_i}$. $g = mn$.

Let $w = \prod_{p_i \in U} p_i^{b_i}$, $z = \prod_{p_i \in V} p_i^{b_i}$. $e = wz$.

Let $m = w = 1$ if U is empty. Let $n = z = 1$ if V is empty.

$p^a q^b$ belongs to mn. Therefore, $(p^a q^b)^n$ belongs to m, by Proposition 3.5.

$p^y q^x$ belongs to wz. Therefore, $(p^y q^x)^w$ belongs to z.

But m and z are relatively prime. Therefore, by Proposition 3.6,

$(p^a q^b)^n (p^y q^x)^w$ belongs to $mz = f$.

Let $J = (p^a q^b)^n (p^y q^x)^w = p^{na+wy} q^{nb+wx}$.

If $w = m = 1$, then $f = e$, which is an element of S'; otherwise, $w < m$, $y < a$, and $x \leq b$. Then

$na + wy < (n + m)a$ and $nb + wx < (n + m)b$.

$m = n$ only if $m = n = 1$, in which case $g = 1$, a case already disposed of.

Assume now that $m \neq n$.

A. If $m > n$, $m = n + d$, $d > 0$. Then $m + n = 2n + d$ and $mn = n^2 + nd$.

If $n > 1$, $mn > m + n$. Then

$$(n + m)a < mna = ga \quad \text{and} \quad (n + m)b < mnb = gb.$$

Then J is a divisor of N.

If $n = 1$, $m = g$ and $w < g$. Then

$$na + wy = a + wy \leq a + wa = a(1 + w) \leq ga.$$

$$nb + wx = b + wx \leq b + wb = b(1 + w) \leq gb.$$

Then J is a divisor of N.

B. If $n > m$, $n = m + d$, $d > 0$. $m + n = 2m + d$, $mn = m^2 + md$.

If $m > 1$, $mn > m + n$. Then, as in A above, J is a divisor of N.

If $m = 1$, then $g = n$, and g divides e, a case dealt with above.

Since J is a divisor of N, and J belongs to f modulo $(N - 1)$, S' has property A.

7. Proofs of Some Preliminary Propositions

Here we prove some preliminary propositions that will be used in the proof of Proposition IIB.

Proposition 7.1: Let $N = p^{ga} q^{gb}$, where $(a, b) = 1$. Then $p^a q^b$ belongs to $2g$ modulo $(N + 1)$.

Proof: $N^2 \equiv 1$ modulo $(N + 1)$. Let $p^a q^b$ belong to m. Then, since $(p^a q^b)^{2g} = 1$, $m = 2g/k$ for some positive integer k. If $k \geq 2$, then $m \leq g$ and $p^{ma} q^{mb} \leq N$, while $(p^a q^b)^m \equiv 1$. This is impossible, since all the numbers $0, 1, 2, \ldots, N$ are noncongruent modulo $(N + 1)$. Therefore, $k = 1$ and $m = 2g$.

Proposition 7.2: If $JJ' = N$, and J belongs to m modulo $(N + 1)$, and J' belongs to n modulo $(N + 1)$, then either both m and n are even and $m = n$ or m is odd and $n = 2m$ or n is odd and $m = 2n$.

Proof: $(JJ')^2 \equiv 1$ modulo $(N + 1)$. Therefore, $[J^m(J')^m]^2 \equiv 1$. Hence, $(J')^{2m} \equiv 1$. Consequently, $2m = kn$ for some positive integer k. Similarly, $2n = mh$ for some positive integer h. Therefore, $hk = 4$. Consequently, $k = 1$, 2, or 4. If $k = 1$, $n = 2m$. If $k = 2$, $m = n$. If $k = 4$, $m = 2n$. If m is even, we have both J^m and $J^m(J')^m$ congruent to 1 modulo $(N + 1)$. Then $(J')^m \equiv 1$ and n divides m. Similarly, if n is even, m divides n. Therefore, if both m and n are even, $m = n$. If m is odd and n is even, then $n = 2m$; if n is odd and m is even, then $m = 2n$. Moreover, m and n cannot both be odd, for if they were it would be necessary that $m = n$. It would follow that $(JJ')^m \equiv 1$, and 2 would be a divisor of m, which is impossible.

Proposition 7.3: If J is a divisor of N and $J'' = NJ$, and J belongs to m modulo $(N + 1)$ and J'' belongs to n, then either both m and n are even and $m = n$, or m is odd and $n = 2m$, or n is odd and $m = 2n$. The proof is similar to the proof of Proposition 7.2.

Proposition 7.4: (Corollary of Propositions 7.2 and 7.3) If J is a divisor of N and $J' = N/J$ and $J'' = NJ$, and the exponent that either J or J' or J'' belongs to is divisible by 4, then all three belong to the same exponent.

8. Proof of Proposition IIB

We consider first the special case where $(a, b) = 1$. By Proposition 5.1, there exist integers x and y such that $xa - yb = 1$, with $0 < x \leq b$ and $0 \leq y < a$, so that $p^y q^x$ is a divisor of N. Let $p^y q^x$ belong to e modulo $(N + 1)$. $p^a q^b$ belongs to 2. Let $p^{a-y} q^{b-x}$ belong to g. Let $p^r q^s$ be any divisor of N. Then, as shown in Section 6,

$$p^r q^s = (p^a q^b)^{rx - sy} (p^y q^x)^{as - br}.$$

Let f be the least common multiple of e and 2. Then $(p^r q^s)^f \equiv 1$. Consequently, the exponent that every divisor of N belongs to is a divisor of f. If e is even, $f = e$. If e is odd, $g = 2e$ by Proposition 7.2. Then $f = g$. In either case, f is an element of T'. Therefore, T' has property A.

If $N = p^{ga} q^{gb}$, where $(a, b) = 1$ and $g > 1$, let (x, y) be determined as before such that $xa - yb = 1$, with $0 < x \leq b$ and $0 \leq y < a$. Again, let $p^y q^x$ belong to e modulo $(N + 1)$. By Proposition 7.1, $p^a q^b$ belongs to $2g$. As shown above, if $p^r q^s$ is any divisor of N,

$$p^r q^s = (p^a q^b)^{rx - sy} (p^y q^x)^{as - br}.$$

Let f be the least common multiple of e and $2g$. Then $(p^r q^s)^f \equiv 1$ modulo $(N + 1)$, and the exponent that each divisor of N belongs to is a divisor of f. To complete the proof, we must show that there exists a divisor of N that belongs to f, so that f would be an element of T'. Express $2g$ and e as products of powers of primes.

$$2g = p_1^{a_1} \cdots p_k^{a_k}, \quad e = p_1^{b_1} \cdots p_k^{b_k},$$

where, as in Section 6, $W = \{p_1, \ldots, p_k\}$ includes all the primes that occur in either $2g$ or e. Define U, V, m, n, w, and z as in Section 6. Then $p^a q^b$ belongs to $mn = 2g$, and $p^y q^x$ belongs to $wz = e$. $(p^a q^b)^n$ belongs to m, and $(p^y q^x)^w$ belongs to z. Then $(p^a q^b)^n (p^y q^x)^w$ belongs to $mz = f$. Let

$$J = (p^a q^b)^n (p^y q^x)^w = p^{na + wy} q^{nb + wx}.$$

If $m = 1$, then $w = 1$, and $f = e$, which is an element of T'. If $m \neq 1$, then $w < m$. Thus,

$$na + wy < (n + m)a \quad \text{and} \quad nb + wx < (n + m)b.$$

(a) Consider first $n, m > 3$. If $n = m = 4$, then $n + m \le (1/2)mn = g$. By induction on m and n separately, it follows that, for all $m, n > 3$,

$$na + wy < ga \quad \text{and} \quad nb + wx < gb.$$

Consequently, J is a divisor of N, and f is an element of T'.

(b) If $m = 3$, then n is even, since $mn = 2g$. Suppose $n \ge 6$. Then, by induction on n, $m + n \le (1/2)mn$, and J is a divisor of N. Similarly, if $n = 3$, then m is even, and if $m \ge 6$, $m + n \le (1/2)mn$, and J is a divisor of N. Therefore, for m or $n = 3$, we have left for consideration only $m = 3$ and $n = 2$, or $m = 3$ and $n = 4$, or $m = 2$ and $n = 3$, or $m = 4$ and $n = 3$. The cases where m or $n = 2$ are considered in (c) and (d) below. If $m = 3$ and $n = 4$, $2g = 12$, and $g = 6$. It follows that $w = 3^0 = 1$. Then

$$na + wy = 4a + y < 5a < ga \quad \text{and} \quad nb + wx = 4b + x \le 5b < gb.$$

Then J is a divisor of N. If $n = 3$ and $m = 4$, $2g = 12$, and $g = 6$. Then $w = 2$ or 1. If $w = 1$,

$$na + wy = 3a + y < 4a < ga \quad \text{and} \quad nb + wx = 3b + x \le 4b < gb.$$

If $w = 2$,

$$na + wy = 3a + 2y < 5a < ga \quad \text{and} \quad nb + wx = 3b + 2x \le 5b < gb.$$

In both cases, then, J is a divisor of N.

(c) If $m = 2$, then $w = 1$, $2g = 2n$, $g = n$, and $e = z$, which is odd. $f = mz = 2e$, which is the exponent that $p^{ga - yq^{gb - x}}$ belongs to. Therefore, f is an element of T'.

(d) If $n = 2$, $m = g$, and m is odd. Therefore, g is odd.

$$w \le (1/3)m = (1/3)g.$$

$$na + wy < 2a + (1/3)ga = (2 + g/3)a.$$

Since $3 \le g$ (because $g > 1$ and is odd), $2 \le 2g/3$. Then

$$na + wy < (2g/3 + g/3)a = ga.$$

Similarly, $nb + wx \le gb$. Consequently, J is a divisor of N.

(e) If $n = 1$, $m = 2g$, and $w \le (1/2)m$. Consider first $w < (1/2)m$. Then

$$w \le (1/4)m = (1/2)g.$$

$$na + wy < a + (1/2)ga = (1 + g/2)a.$$

Since $2 \le g$, $1 \le g/2$. Then

$$na + wy < (g/2 + g/2)a = ga.$$

Similarly, $nb + wx \le gb$. Then J is a divisor of N.

(f) If $w = (1/2)m$, $w = g$ and the only element of U is 2. Consequently, g is a power of 2. Then f, which equals $2gz$, is divisible by 4. $e = wz = gz$. $f = mz = 2gz$, and z is odd. $J = p^{a + gy}q^{b + gx}$. $a + gy < 2ga$ and $b + gx < 2gb$. If

$$a + gy \le ga \quad \text{and} \quad b + gx \le gb,$$

J is a divisor of N. Still to be dealt with is the case where either $a + gy > ga$, or $b + gx > gb$. If $a + gy > ga$, $y > a(g - 1)/g$. Since $xa = by + 1$,

$$xa > ab(g - 1)/g + 1.$$

Thus, $gx > (g - 1)b + g/a$; $b + gx > gb + g/a > gb$. Then $J' = J/N$ is well defined and is a divisor of N. Now, by Proposition 7.4, since $J = J'N$ and f is

divisible by 4, J' belongs to f. Therefore, f is an element of T'. Suppose $b + gx > gb$. Then $x > b(g - 1)/g$. Since $by = xa - 1$,

$$by > ab(g - 1)/g - 1.$$

Then $gy > (g - 1)a - g/b$ and $a + gy > ga - g/b$. If $g \leq b$, $a + gy \geq ga$. Then $J' = J/N$ is well defined, is a divisor of N, and belongs to f. If $g > b$,

$$b + gx < g + gx = g(1 + x) \leq gb \text{ if } x < b.$$

This contradicts the assumption that $b + gx > gb$. Thus, the case $x < b$ cannot occur in this context. If $x = b$, since $ax - by = 1$, $b(a - y) = 1$. Then $b = 1$ and $y = a - 1$. $b + gx = g + 1 > bg$.

$$a + gy = a + g(a - 1) = ga + (a - g) \geq ga \text{ if } a \geq g.$$

Then, as above, $J' = J/N$ is well defined, is a divisor of N, and belongs to f. Now suppose that $g > a$. Recall that $x = b = 1$, and $y = a - 1$. $N = p^{ga}q^g$. p^aq belongs to $2g$, which is divisible by 4. Therefore, $p^{ga-a}q^{g-1}$ belongs to $2g$, which is a power of 2. $p^yq^x = p^{a-1}q$ belongs to gz. Then $p^{ga-g}q^g$ belongs to z, which is odd. Thus, $p^{2ga-g-a}q^{2g-1}$ belongs to $2gz$. Let

$$J'' = p^{2ga-g-a}q^{2g-1}$$

and let

$$J' = J''/N = p^{ga-g-a}q^{g-1}.$$

Assume $a \geq 2$. Then $g(a - 1) - a < 0$ only if $g < a/(a - 1) < 2$. But $g > a \geq 2$. Therefore, for $a \geq 2$, $0 \leq ga - g - a < ga$. Moreover, $0 < g - 1 < g$. Then J' is a divisor of N. Since J'' belongs to $2gz$ which is divisible by 4, J' belongs to $2gz$, which equals f. Then f is an element of T'. What remains to be dealt with now is the case where $a = 1$, $g > 1$. Then we have $N = p^gq^g$. $g = 2^c$ for some $c > 0$. $a = b = 1$, $x = 1$, $y = a - 1 = 0$. $p^aq^b = pq$ belongs to $2g$, and $p^yq^x = q$ belongs to gz. Therefore, q^g belongs to z which is odd. Thus, p^g belongs to $2z$. Let p belong to e'. Then e' divides $2gz$, so that $2gz = e'h$ for some positive integer h. Since $(p^g)^{e'} \equiv 1$, $2z$ divides e', so that $e' = 2zk$ for some positive integer k. Then $2gz = e'h = 2zkh$. Thus, $kh = g$. Consequently, k is a power of 2 such that $1 \leq k \leq g$. Then possible values of e' are $2z$, $4z$, $8z$, ..., gz, $2gz$. If $e' = 2gz$, then $f = e'$, which is an element of T'. If $e' = gz$, then p^g belongs to z, contradicting the fact that p^g belongs to $2z$. So this case cannot arise. If $e' = gz/t$ with $t > 1$, then we would have $p^{gz/t} \equiv 1$, from which it follows that $(p^{gz/t})^t \equiv 1$, which implies that $(p^g)^z \equiv 1$, which implies that $2z$ divides z. Hence, this case too cannot arise.

References

1. R. D. Carmichael. *The Theory of Numbers*. New York: Wiley & Sons, 1914.
2. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover, 1954.

Appendix

Let $b = N/a$. The cards are in a piles, with b cards in each pile. This is equivalent to a rectangular array with a columns and b rows. Consider the card in row h, column k ($h = 1, 2, \ldots, b$; $k = 1, 2, \ldots, a$). Let x designate its original position in the deck. Let $f(x)$ be its new position as a result of the permutation. $x = (k - 1)b + h$. $f(x) = (h - 1)a + k$. Direct calculation shows that

$$f(x) = ax - (a - 1) - (k - 1)(N - 1).$$

Therefore, $f(x) \equiv ax - (a - 1)$ modulo $(N - 1)$. Designate by $f_i(x)$ the position of the card after i repetitions of the permutation. Then, by induction,

$$f^i(x) \equiv a^i x - (a^i - 1) \text{ modulo } (N - 1).$$

It follows that $f^i(x) = x$ if and only if $a^i \equiv 1$ modulo $(N - 1)$.

*****

A GENERAL RECURRENCE RELATION FOR REFLECTIONS IN MULTIPLE GLASS PLATES

Jeffrey A. Brooks
(student)
West Virginia University, Morgantown, WV 26506
(Submitted June 1987)

The number of possible light paths in a stack of two glass plates can be expressed in terms of Fibonacci numbers, as was first pointed out by Moser [1]. If two glass plates are placed together in such a way that each surface can either reflect or transmit light, then the number of distinct paths through the two plates with exactly n internal reflections is F_{n+2}.

Junge and Hoggatt [2] used matrix methods to count reflections in larger numbers of plates. Hoggatt and Bicknell-Johnson [3] used geometric and matrix techniques to count specific sets of reflections. However, these authors did not present a general recurrence relation for the number of distinct light paths with a fixed number of reflections in an arbitrary number of glass plates. Here we shall present such a recurrence relation.

Consider a single ray of light directed into a stack of r glass plates. Let $T_r(n)$ be the number of distinct paths that can be taken by a light ray entering through the top plate, leaving through either the top plate or the bottom plate, and having exactly n internal reflections. Figure 1 illustrates the distinct light paths in two plates with zero, one, two, and three reflections.

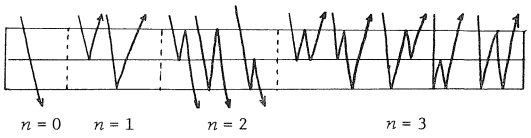

FIGURE 1

As a light ray passes through the stack of plates in a fixed direction, there are a total of r internal surfaces from which it could be reflected. (The surface crossed by the light ray as it enters the stack of plates cannot cause an internal reflection.) Number the reflecting surfaces from 1 to r along the direction of the ray. Figure 2 illustrates this numbering scheme; the path shown consists of reflections from surfaces 2-3-3-2-2.