PERIODICITY OF A COMBINATORIAL SEQUENCE

BJORN POONEN
Student, Harvard College, Cambridge, MA 02138

(Submitted July 1986)

In June 1985, twenty-three other high school students and I trained for the International Mathematical Olympiad in a three-week session hosted by the U.S. Military Academy. There I, along with three classmates (John Dalbec, Jeremy Kahn, and Joseph Keane) and the two coaches (Professor Cecil Rousseau and Gregg Patruno) considered $\omega(n)$, defined as the number of possible outcomes in a race among n horses with multiple ties permitted. This sequence was first studied by A. Cayley [1] as the number of a certain type of tree having $n + 1$ terminal nodes. His results have been extended by the more recent papers of Gross [3] and Good [2].

Before uncovering these three papers, we independently proved eleven results which can be found in [1], page 113, [2], pages 11-14, and [3], pages 5-8. Although we found that Good's statement (p. 13),

$$\left|\omega(n) - \frac{n!}{2(\ln 2)^{n+1}}\right| < \frac{1}{2} \text{ for all } n < 16, \tag{1}$$

could be extended to $n < 17$, the only important new results were my proofs of Good's Conjectures 1-5. These conjectures are concerned with the behavior of the sequence modulo r. To prove these, we need the following lemmas.

Lemma 1: If $n, k \geq 1$, and we define $\omega(0) = 1$, then

$$2^k\omega(n) = \sum_{j=1}^{k-1} 2^{k-j-1}j^n + \sum_{j=0}^{n} k^j\binom{n}{j}\omega(n - j). \tag{2}$$

Proof of Lemma 1: We have, by equation (4) of [2],

$$\begin{aligned} 2^k\omega(n) &= 2^k\sum_{j=1}^{k-1}\frac{j^n}{2^{j+1}} + 2^k\sum_{i=0}^{\infty}\frac{(i+k)^n}{2^{i+k+1}} \\ &= \sum_{j=1}^{k-1} 2^{k-j-1}j^n + \sum_{i=0}^{\infty}\sum_{j=0}^{n}\frac{\binom{n}{j}i^{n-j}k^j}{2^{i+1}} \\ &= \sum_{j=1}^{k-1} 2^{k-j-1}j^n + \sum_{j=0}^{n} k^j\binom{n}{j}\omega(n - j). \end{aligned}$$

Note that, we we let $k = 1$ in Lemma 1, we obtain a relation derived by Cayley ([1], p. 113). Similarly, we can prove

$$2^{-k}\omega(n) = -\sum_{j=0}^{k} 2^{j-k-1}(-j)^n + \sum_{j=1}^{n} (-k)^j \binom{n}{j}\omega(n-j). \tag{3}$$

From Lemma 1, we have the following useful result.

Corollary; If $n, k \geq 1$, then

$$(2^k - 1)\omega(n) \equiv \sum_{j=1}^{k-1} 2^{k-j-1} j^n \pmod{k}. \tag{4}$$

It is interesting to note that the corollary, along with Fermat's Theorem, provides a simple proof of Theorem 5 in [2]. Now we shall use the corollary to prove another lemma.

Lemma 2: For an odd prime p, let $q = p^m$ and $r = p^{m+1}$ be consecutive powers of p. Suppose the sequence $\omega(a), \omega(a+1), \ldots$ modulo r has period c, where c is a multiple of $\phi(q)$. Then

$$0 \equiv \sum_{k=0}^{q-1} 2^{q-k-1}[(g+kp)^c - 1] \pmod{r} \tag{5}$$

for $g = 1, 2, \ldots, p-1$.

Proof: From the corollary to Lemma 1, we find that, for all $n \geq a$,

$$0 \equiv (2^r - 1)[\omega(n+c) - \omega(n)] \equiv \sum_{j=1}^{r-1} 2^{r-j-1} j^n (j^c - 1) \pmod{r}.$$

It follows that for any polynomial $P(j)$ with integral coefficients,

$$\sum_{j=1}^{r-1} 2^{r-j-1} j^n P(j)(j^c - 1) \equiv 0 \pmod{r}.$$

Let $P(j) = 1 - (j-g)^{p-1}$ and let n be a multiple of $\phi(r)$ greater than a. By repeated use of theorems of Fermat and Euler, we make the following sequence of observations concerning the terms of the sum that are nonvanishing (mod r):

$$j \not\equiv 0 \pmod{p},\ j^n \equiv 1 \pmod{r},\ j^c - 1 \equiv 0 \pmod{q},$$
$$j \equiv g \pmod{p},\ P(j) \equiv 1 \pmod{p},\ P(j)(j^c - 1) \equiv j^c - 1 \pmod{r}.$$

Thus, the sum reduces to

$$\sum_{k=0}^{q-1} 2^{r-(g+kp)-1}[(g+kp)^c - 1] \equiv 0 \pmod{r}.$$

Now $r - (g+kp) - 1 \equiv q - g - k - 1 \pmod{p-1}$. Also, since c is a multiple of $\phi(q)$, we have $[(g+kp)^c - 1] \equiv 0 \pmod{q}$. Thus, by Fermat's Theorem, we

may substitute $2^{q-g-k-1}$ for $2^{r-(g+kp)-1}$ in the last equation. Finally, multiplying by 2^g, we obtain

$$\sum_{k=0}^{q-1} 2^{q-k-1}[(g + kp)^e - 1] \equiv 0 \pmod{r}.$$

Now we are ready to prove the theorems.

Theorem 1: Modulo a prime p, the period of the sequence $[\omega(n)]$ is at least $p - 1$. This, along with Good's Theorem 5, implies that the period is exactly $p - 1$.

Proof of Theorem 1: For $p = 2$, the result is clear. If $p \geq 3$, let e be the minimum period. Applying Lemma 2 with $\alpha = 1$ and $q = 0$, and with g a primitive root modulo p, we have

$$0 \equiv 2^{p-1-g}(g^e - 1) \pmod{p}.$$

However, 2^{p-1-g} is not divisible by p, so $g^e - 1$ must be. Since we chose g as a primitive root modulo p, we must have $e \geq p - 1$.

Theorem 1 does *not* imply that, if $\omega(n) \equiv 0 \pmod{p}$, then $n \equiv 0 \pmod{p - 1}$. [A counterexample is $\omega(3) \equiv 0 \pmod{13}$.] Proofs of three of Good's conjectures in [1] depended on this result:

$$\text{GCF}(\omega(n), \omega(n + 1)) = 1, \quad \text{GCF}(\omega(n) - 1, \omega(n + 1) - 1) = 2, \quad \text{and} \quad n \mid \omega(n),$$

for all n. The first is false because $\omega(1090)$, $\omega(1091)$, and $\omega(1092)$ are all divisible by 1093. The second and third are still open.

Theorem 2: If $q = p^m$ with p prime, then for all $n \geq m$,

$$\omega(n + \phi(q)) \equiv \omega(n) \pmod{q}, \tag{6}$$

where ϕ is Euler's totient function.

Proof of Theorem 2: Since $n \geq m$, the terms in the sum given by (4) with j divisible by p will drop out. The result then follows from $j^{n+\phi(q)} \equiv j^n \pmod{q}$, which is Euler's Theorem.

Theorem 2 does not tell us that the period of the sequence $\{\omega(n)\}$ modulo q is exactly $\phi(q)$ for q a power of a prime. We know only that the minimum period must be a factor of $\phi(q)$. Theorem 3 shows that, when q is the power of an odd prime, this fundamental period is no less than $\phi(q)$. To prove this, we need one more lemma.

Lemma 3: For an odd prime p, let $q = p^m$ and $r = p^{m+1}$. Then, for any integer k, $(1 + kp)^{\phi(q)} - 1 = -kq \pmod{r}$.

Proof: By the binomial theorem,

$$(1 + kp)^{\phi(q)} = \sum_{i=0}^{\phi(q)} \binom{\phi(q)}{i} (kp)^i .$$

Let $f(n)$ denote the greatest integer d such that p^d divides n. Then

$$f\left(\binom{\phi(q)}{i} p^i\right) = \sum_{j=\phi(q)-i+1}^{\phi(q)} f(j) - \sum_{j=1}^{i} f(j) + i = f(\phi(q)) - f(i) + i,$$

Since $f(\phi(q) - j) = f(j)$ for any j with $0 < j < \phi(q)$. But if $f(i) > 0$, then

$$i \geqslant p^{f(i)} \geqslant 3^{f(i)} \geqslant f(i) + 2,$$

so $i - f(i) \geqslant 2$ for all $i \geqslant 2$. Also, $f(\phi(q)) = m - 1$, so if we look at the binomial expansion modulo r, all but the first two terms drop out:

$$(1 + kp)^{\phi(q)} - 1 \equiv 1 + \phi(q)(kp) - 1 \equiv -kq \pmod{r}.$$

Theorem 3: Let p be an odd prime. Then, modulo p^m, the sequence

$$\omega(m), \omega(m + 1), \omega(m + 1), \ldots$$

has period exactly $\phi(p^m)$.

Proof of Theorem 3: Theorem 1 proved the case $m = 1$. Now suppose that Theorem 3 holds for a certain m. We shall prove that it must also hold for $m + 1$. Let $q = p^m$, let $r = p^{m+1}$, and let c be the minimum period of the sequence $\{\omega(n)\}$ modulo r. By the inductive hypothesis, $\phi(q)$ is the period modulo q, so c must be a multiple of $\phi(q)$. By Theorem 2, c must be a factor of $\phi(r)$. But $\phi(r) = p\phi(q)$, so c is either $\phi(q)$ or $\phi(r)$.

Suppose $c = \phi(q)$. Applying Lemma 2 with $a = m$ and $g = 1$ yields

$$0 \equiv \sum_{k=0}^{q-1} 2^{q-k-1}[(1 + kp)^c - 1] \equiv \sum_{k=0}^{q-1} 2^{q-k-1}(-kq) \pmod{r},$$

by Lemma 3. Evaluating this sum, we obtain

$$0 \equiv (2^q - q - 1)q \equiv -q \pmod{r} \quad \text{(by Fermat's Theorem)},$$

a contradiction. Thus, $c = \phi(r)$, and the induction is complete.

We now proceed to consider the sequence modulo a power of 2.

Theorem 4: If $1 \leqslant m \leqslant n - 4$, then

$$\omega(n + 2^m) \equiv \omega(n) + 2^{m+4} \pmod{2^{m+5}}. \tag{7}$$

Proof of Theorem 4: Set $k = 2^{m+5}$ in the corollary of Lemma 1. Then $2^k - 1 \equiv -1 \pmod{k}$, so

$$\omega(n + c) - \omega(n) \equiv -\sum_{j=1}^{k-1} 2^{k-j-1} j^n (j^c - 1) \pmod{k}.$$

Now set $c = 2^m$. The terms with even j drop out because 2^{k-j-1} is even and j^n is divisible by 2^{m+4}. The terms with odd $j \leq k - 5$ also drop out since 2^{k-j-1} is divisible by 2^4 and $j^c - 1$ is divisible by 2^{m+1} (by Euler's Theorem). Thus, our sum reduces to

$$\begin{aligned}&\omega(n + c) - \omega(n)\\ &\equiv -2^2(k - 3)^n[(k - 3)^c - 1] - (k - 1)^n[(k - 1)^c - 1] \pmod{k}\\ &\equiv -4(-3)^n(3^c - 1) \pmod{k}.\end{aligned}$$

To show that this is congruent to 2^{m+4} modulo 2^{m+5}, it suffices to prove that 2^{m+2} is the highest power of 2 dividing

$$3^{2^m} - 1 = (3^{2^{m-1}} + 1)(3^{2^{m-2}} + 1) \ldots (3 + 1)(3 - 1).$$

This is true since the second-to-last factor is 4 and each of the other m factors is congruent to 2 modulo 4.

Theorem 5: If $\omega(n)$ is expressed in binary notation as

$$a_{n0} + 2a_{n1} + 2^2 a_{n2} + 2^3 a_{n3} + \ldots,$$

then the sequence a_{mm}, $a_{(m+1)m}$, $a_{(m+2)m}$, ... runs into a cycle whose lengths for $m = 0, 1, 2, 3, \ldots$ are, respectively, 1, 2, 2, 1, 2, 4, 8, ... From this, it follows that, modulo 2^m, the sequence $\omega(m - 1)$, $\omega(m)$, $\omega(m + 1)$, ... has period 1 when $m = 1$, period 2 when $2 \leq m \leq 4$, and period 2^{m-4} when $m \geq 5$. [We define $\omega(0) = 1$.]

Proof of Theorem 5: By Theorem 4 with $m = 1$, if $n \geq 5$, then

$$\omega(n + 1) \equiv \omega(n) \pmod{32},$$

so for $m < 5$, the sequence a_{5m}, a_{6m}, a_{7m}, ... is periodic with period dividing 2. [The period is 1 iff $a_{5m} = a_{6m}$, which we see holds iff $m = 3$, by observing the five least significant binary digits of $\omega(5)$ and $\omega(6)$.] Also, by observing the five least significant binary digits of $\omega(0)$, $\omega(1)$, ..., $\omega(4)$, we see that the periodicity begins with a_{mm} instead of a_{5m} for $m < 5$.

If $m \geq 5$, then in the sequence a_{mm}, $a_{(m+1)m}$, $a_{(m+2)m}$, ... of zeros and ones, the terms are the opposite of what they were, after every 2^{m-4} terms, by Theorem 4. This implies that, after 2^{m-3} terms, the sequence repeats. Hence, the

sequence runs into a cycle whose length is a factor of 2^{m-3} but not of 2^{m-4}. Thus, the period is exactly 2^{m-3}.

Finally, to summarize and extend our results, we have the following:

Theorem 6: Let the prime factorization of $r > 1$ be $2^m p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$. If

$$a = \max\{m - 1, m_1, m_2, m_3, \ldots, m_k\}$$

and

$$b = \text{LCM}(\phi(p_1^{m_1}), \phi(p_2^{m_2}), \ldots, \phi(p_k^{m_k})),$$

then the period of the sequence

$$\omega(a), \omega(a + 1), \omega(a + 2), \ldots \text{ modulo } r$$

is exactly

$$\begin{cases} b, & \text{if } m = 0 \text{ or } 1, \\ \text{LCM}(2, b), & \text{if } 2 \leqslant m \leqslant 4, \\ \text{LCM}(2^{m-4}, b), & \text{if } m \geqslant 5. \end{cases}$$

Note that the period of $\{\omega(n)\}$ modulo r is not the product of the periods modulo its prime power factors, but is, rather, their lowest common multiple. This implies that even when r is odd, the period modulo r is not necessarily $\phi(r)$, although it must be a factor of $\phi(r)$. The smallest example of this is $r = 15$, in which case the period is $\text{LCM}(\phi(3), \phi(5)) = 4$ instead of $\phi(15) = 8$.

Proof of Theorem 6: Let c be the claimed period. If $n \geqslant m - 1$, then

$$\omega(n + c) \equiv \omega(n) \pmod{2^m}$$

by Theorem 5, since c is a multiple of the period of $\{\omega(n)\}$ modulo 2^m. Also, if $n \geqslant m_i$, then

$$\omega(n + c) \equiv \omega(n) \pmod{p_i^{m_i}}$$

by Theorem 3, since c is a multiple of $\phi(p_i^{m_i})$, for $i = 1, 2, \ldots, k$. Hence, if $n \geqslant a$,

$$\omega(n + c) \equiv \omega(n) \pmod{r}.$$

If the actual period d of $\{\omega(n)\}$ modulo r were any smaller than c, then it could not be a multiple of all the necessary periods modulo 2^m and $p_i^{m_i}$, since c is their LCM. Suppose d is not a multiple of the necessary period modulo p^q. Then, for some $n \geqslant a$, $\omega(n + d) \not\equiv \omega(n) \pmod{p^q}$, so

$$\omega(n + d) \not\equiv \omega(n) \pmod{r},$$

a contradiction. Hence, the period given is minimum.

Now that we have finished proving the main theorems, we will conclude with a few applications of Theorem 6 and other miscellaneous results:

(a) $\omega(12k) \equiv \omega(12k + 3) \equiv 0 \pmod{13}$.

(b) $59 | \omega(11)$, so $59 | \omega(58k + 11)$. Dirichlet's Theorem implies that there are infinitely many primes of the form $58k + 11$, so there are infinitely many primes p for which $\omega(p)$ is composite.

(c) $9 \nmid \omega(n)$ for any n, so there seems to be no generalization of $p | \omega(p - 1)$ ([12], p. 23) to powers of odd primes.

(d) For any prime p and any $m \geq 1$, $\omega(p^m) \equiv 1 \pmod{p}$, so if $n | \omega(n)$, n has at least two distinct prime factors.

(e) For odd primes p and q, $pq | \omega(pq)$ iff $p | \omega(q)$ and $q | \omega(p)$. There are no such primes less than 1700, but I conjecture on probabilistic grounds that such primes do exist.

(f) For all n, $\text{GCF}(\omega(n) - 1, \omega(n + 1) - 1)$ has no divisor less than 1700 except 2. Yet, again on probabilistic grounds, I conjecture that there exists n for which $\text{GCF}(\omega(n) - 1, \omega(n + 1) - 1) \neq 2$.

(g) The only r for which the period of $\{\omega(n)\}$ modulo r is exactly $\phi(r)$ are the numbers of the form p^m and $2p^m$, where p is an odd prime, and 4.

ACKNOWLEDGMENTS

I would like to thank the two coaches at the training session, Professor Cecil Rousseau and Gregg Patruno, who suggested that I write this paper, and who provided many helpful comments.

REFERENCES

1. A. Cayley. *Collected Works*, 4:112-15. Cambridge, Mass.: Cambridge University Press, 1891.
2. I. J. Good. "The Number of Orderings of n Candidates When Ties Are Permitted." *The Fibonacci Quarterly 13*, no. 1 (1975):11-18.
3. O. A. Gross. "Preferential Arrangements." *Amer. Math. Monthly 69* (1962): 4-8.

◆◇◆◇◆