JOURNAL OF NUMBER THEORY 25, 308–312 (1987)

Periodicities of Partition Functions and Stirling Numbers modulo p

ALBERT NIJENHUIS AND HERBERT S. WILF*

University of Pennsylvania, Philadelphia, Pennsylvania 19104

Communicated by P. Roquette

Received April 9, 1985; revised February 16, 1986

If $p(n, k)$ is the number of partitions of n into parts $\leqslant k$, then the sequence $\{p(k, k), p(k+1, k),...\}$ is periodic modulo a prime p. We find the minimum period $Q = Q(k, p)$ of this sequence. More generally, we find the minimum period, modulo p, of $\{p(n; T)\}_{n \geqslant 0}$, the number of partitions of n whose parts all lie in a fixed finite set T of positive integers. We find the minimum period, modulo p, of $\{S(k, k), S(k+1, k),...\}$, where these are the Stirling numbers of the second kind. Some related congruences are proved. The methods involve the use of cyclotomic polynomials over $\mathbf{Z}_p[x]$.

1. STATEMENT OF RESULTS

We study the periodicity of counting sequences modulo a prime p. If k is a positive integer, let $p(n, k)$ be the number of partitions of n into parts $\leqslant k$, $(n = 0, 1,...)$.

THEOREM 1. *The sequence* $\{p(n, k) \pmod p\}_{n=0}^{\infty}$ *is periodic. Its minimum period is* $Q = p^{\rho} Q'$, *where* Q' *is the p-free part of* $\operatorname{lcm}\{1, 2,..., k\}$ *and* ρ *is the least integer such that*

$$p^{\rho} \geqslant \sum_{l \geqslant 0} \phi(p^l) \left\lfloor \frac{k}{p^l} \right\rfloor,$$

where ϕ *is Euler's function.*

More generally, let T be a fixed set of positive integers, and let $p(n; T)$ be the number of partitions of n whose parts lie in T, $(n = 0, 1,...)$. For each integer $m \geqslant 1$, we define $\rho(m)$ by $p^{\rho(m)} \mid m$, $p^{\rho(m)+1} \nmid m$. We prove

* Supported in part by U.S. Office of Naval Research.

0022-314X/87 $3.00

THEOREM 2. *Let L' be the p-free part of* $\operatorname{lcm}\{a \mid a \in T\}$, *and let r be the least integer such that*

$$p^r \geqslant \sum_{a \in T} p^{\rho(a)}$$

Then the sequence $\{p(n; T) \pmod p\}_{n \geqslant 0}$ *is periodic of minimum period* $Q = p^r L'$.

The same method yields the following result on the periodicity of the Stirling numbers of the second kind, $S(n, k)$. It refines earlier theorems of Becker and Riordan [1].

THEOREM 3. *Let p be a prime and k be a positive integer. Then the sequence* $\{S(n+k, k) \pmod p\}_{n \geqslant 0}$ *is periodic. The minimum period* $Q = Q(k, p)$ *of the sequence is as follows*:

(a) *if* $1 \leqslant k < p$ *then* $Q(k, p)$ *is the least common multiple of the orders of the residues* $1, 2, \dots, k$ *in the multiplicative group* $\mathbf{Z}_p^* = \mathbf{Z}_p - \{0\}$.

(b) *if* $k \geqslant p$, *then* $Q(k, p) = p^\sigma(p-1)$, *where* $p^\sigma < k \leqslant p^{\sigma+1}$.

2. TOOLS

The cyclotomic polynomials $\{\Phi_n(x)\}_{n=1}^{\infty}$ are defined by the equations

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \qquad (n \geqslant 1).$$

Each $\Phi_m(x)$ is monic, with integer coefficients, and of degree $\phi(m)$.

LEMMA 1. *Let p be prime, m, n integers, $m \neq n$, $p \nmid m$, $p \nmid n$. Then $\Phi_m(x)$ and $\Phi_n(x)$ are relatively prime over $\mathbf{Z}_p[x]$. Further, all $\Phi_m(x)$ are squarefree.*

Proof. Under the hypotheses stated, $\Phi_m(x)\,\Phi_n(x)$ divides $x^{mn} - 1$, which is squarefree. ∎

LEMMA 2. *Let* $f(x) = \sum_{n \geqslant 0} a_n x^n$ *be a formal power series over* $\mathbf{Z}_p$. *Then the coefficient sequence is periodic modulo p with period Q iff* $(1 - x^Q)/f(x) \in \mathbf{Z}_p[x]$. ∎

By the *minimum period*, modulo p, of a polynomial $f(x)$, we mean the least Q such that $f(x)$ divides $x^Q - 1$ in $\mathbf{Z}_p[x]$.

PROPOSITION (Berlekamp [2, p. 151]. *Let* $f(x) = \prod_i f_i(x)^{m_i}$ *be the canonical factorization of the polynomial f, the $f_i(x)$ being irreducible over*

$GF(p^a)$, and of respective periods n_i. Then the period of f is equal to

$$\operatorname{lcm}(n_i)\min\{p^\beta \mid \forall i: p^\beta \geqslant m_i\}. \tag{2.1}$$

We will in fact use the following variant.

THEOREM 4. *Let $f(x)=\prod_i f_i(x)^{m_i}$ be a factorization of the polynomial f, where the f_i are squarefree and pairwise relatively prime (not necessarily irreducible) polynomials, of respective periods n_i. Then the period of f is given by* (2.1).

Proof. For each i, let $f_i=\prod_j g_{i,j}$, where the g's are irreducible. Since each f_i is squarefree, the $g_{i,j}$ are all distinct, for each fixed i. Since the f_i's are relatively prime, in fact all of the $g_{i,j}$ are distinct. Hence the canonical factorization of f is

$$f(x)=\prod_{i,j} g_{i,j}(x)^{m_i}$$

and the result now follows from the proposition above. ∎

3. PROOFS OF THE THEOREMS

Proof of Theorem 2. The period of the sequence is the period of the polynomial

$$\prod_{a\in T}(1-x^a)=\prod_{a\in T}(1-x^{p^{\rho(a)}a'}) \qquad (p\nmid a')$$

$$\equiv\prod_{a\in T}(1-x^{a'})^{p^{\rho(a)}}=\prod_{a\in T}\left\{\prod_{m\mid a'}\Phi_m(x)\right\}^{p^{\rho(a)}}.$$

Each fixed $\Phi_m(x)$ occurs with exponent

$$\gamma_m=\sum_{\substack{a\in T\\ m\mid a'}} p^{\rho(a)}.$$

Since the Φ's are relatively prime, by lemma 1, and squarefree, the result follows from theorem 4. ∎

Proof of Theorem 1. Take $T=\{1,2,\ldots,k\}$ in Theorem 2. ∎

Proof of Theorem 3. The Stirling numbers $S(n,k)$ are the numbers of partitions of a set of n letters into k blocks. They satisfy

$$\sum_{n\geqslant 0} S(n+k,k)\,x^n=\frac{1}{(1-x)(1-2x)\cdots(1-kx)}.$$

Let $k = qp + r$, where $q \geqslant 0$, $0 < r \leqslant p$, and let $F_k(x)$ denote the denominator above. Then

$$F_k(x) \equiv (1-x)^{q+1} \cdots (1-rx)^{q+1}\ (1-(r+1)\,x)^q \cdots (1-(p-1)\,x)^q.$$

Note that the cases $r = p-1$ and $r = p$ yield the same $F_k(x)$. If $q = 0$ and $k < p$ then $Q(k, p) = \mathrm{lcm}(\mathrm{ord}(1),..., \mathrm{ord}(k))$, while $Q(p, p) = Q(p, p-1) = p-1$. If $q \geqslant 1$ then $Q(k, p) = p^\sigma(p-1)$ where $p^{\sigma-1} < q+1 \leqslant p^\sigma$. Since $0 < r/p \leqslant 1$, this is equivalent to $p^{\sigma-1} < q + r/p \leqslant p^\sigma$, or $p^\sigma < k \leqslant p^{\sigma+1}$. ∎

We remark that the minimum period, as given by Theorem 3, and the period that was found in [1], differ only when k is a power of p or $k < p$.

4. Miscellanea

While studying these minimum periods we found some congruences, not directly related to the above, which may have some independent interest. We state them as

THEOREM 5. *If $k+n$ is odd then*

(a) *$S(n, k)$ is divisible by the odd part of k and*

(b) *$s(n, k)$ is divisible by the odd part of $n-1$.*

Remark. $s(n, k)$ is the number of n-permutations that have k cycles.

Proof. If r is an odd divisor of k, then modulo r we have

$$\begin{aligned}\sum_{n \geqslant 0} S(n+k, k)\, x^n &= \frac{1}{(1-x)\cdots(1-kx)} \\ &\equiv \frac{1}{\{(1-x)\cdots(1-(r-1)\,x)\}^{k/r}} \pmod r \\ &= \frac{1}{\{(1-x^2)(1-4x^2)\cdots(1-(r-1)^2\,x^2/4)\}^{k/r}}\end{aligned}$$

which is an even function of x, modulo r. Hence

$$S(n+k, k) \equiv 0 \pmod r$$

if n is odd, r is odd, and $r \mid k$, which is the assertion (a) of the theorem.

The proof of part (b) begins with

$$\sum_{m \geqslant 0} s(n+1, n+1-m)\, u^m = (1+u)(1+2u) \cdots (1+nu)$$

in place of (4.1). Thereafter the argument exactly parallels the above, and is omitted. ∎

References

1. H. W. Becker and J. Riordan, The arithmetic of Bell and Stirling numbers, *Amer. J. Math.* **70** (1948), 385–394.
2. E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill, New York, 1968.