COUNTING THE NUMBER OF SOLUTIONS OF EQUATIONS IN GROUPS BY RECURRENCES

Umberto Cerruti

Dipartimento di Matematica, Università di Torino, Via Carlo Alberto 10, 10123 Torino, Italy
e-mail: cerruti@dm.unito.it

Gabriella Margaria

Dipartimento di Matematica, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy
e-mail: margaria@calvino.polito.it

(*Submitted May 1999-Final Revision September 1999*)

1. THE BASIC THEOREM

Let $G=(G, *, e)$ be a finite group with support $G=\{g_1, g_2, \ldots, g_n\}$, operation $*$ and identity element $g_1=e$. The aim of this paper is to find recurrences for the number $N(T, k, a)$ of solutions of the equation $x_1 * x_2 * \cdots * x_k = a$, where $a \in G$ and the variables x_i are limited to belonging to a given subset T of G. Let θ be the left regular representation of G extended to the group algebra ZG. If $T \subset G$, we pose $\gamma(T)=\sum_{g \in T} g \in ZG$.

We begin with the following basic result.

Theorem 1.1: Given $T \subset G$, let $A=\theta(\gamma(T)) \in Mat(n, Z)$. Then

(a) $N(T, k, g_j)=A_{1,j}^k$.

(b) The sequence $N(T, k, g_j)$, $k \in N$, is linearly recurrent with characteristic polynomial $f(x)$, where $f(x)$ is any polynomial s.t. $f(A)=0$.

Proof:

(a) Let $T=\{g_{i_1}, g_{i_2}, \ldots, g_{i_m}\}$, then

$$(\gamma(T))^k=(g_{i_1}+g_{i_2}+\cdots+g_{i_m})^k=\sum_{j=1}^n N(T, k, g_j) g_j \quad \text{in } ZG.$$

Applying θ on both sides:

$$A^k=\sum_{j=1}^n N(T, k, g_j) \theta(g_j).$$

The first row of $\theta(g_j)$ is $(0, \ldots, 1, \ldots, 0)$ with 1 in the j^{th} place and 0 elsewhere, and the result follows. □

(b) By Theorem 1.6 in [3], the sequence A_{ij}^k (for fixed indices i, j) is linearly recurrent with any polynomial $f(x)$ s.t. $f(A)=0$ and initial values $A_{ij}^0, A_{ij}^1, \ldots, A_{ij}^{m-1}$ [if $\deg(f(x))=m$]. □

Example 1.2: Let $G=S_n$ (the symmetric group of degree n), $T=\{n\text{-}cycles\}$, $a \in T$. By Corollary 4.2 of [5],

$$N(T, k, a)=n!^{-1}(n-1)!^k \sum_{h=0}^{n-1}(-1)^{h(k-1)}\binom{n-1}{h}^{1-k}. \tag{1}$$

We know from Theorem 1.1 that this sequence is recurrent. We now find a characteristic polynomial. If n is odd, collecting some terms, we can rewrite (1) as

$$N(T,k,a)=\sum_{h=0}^{\frac{n-1}{2}} C_h[(-1)^h h!(n-h-1)!]^{k-1}, \tag{2}$$

where the coefficients C_h are rational numbers. From equation (2) and Theorem C.1. of [6], we see that the sequence $N(T,k,a)$ is recurrent with characteristic polynomial of degree $\frac{n+1}{2}$:

$$f_{\text{odd}}(n)=\prod_{h=0}^{\frac{n-1}{2}}(x-(-1)^h h!(n-h-1)!).$$

For example, if $n=7$, $N(T,k,a)$ is linearly recurrent of fourth degree with characteristic polynomial $x^4-612x^3-80928x^2+2073600x+149299200$ and initial values

$$\{1,180,153072,106173504\}.$$

Let us suppose now that n is even. Of course, in this case, when k is even, $N(T,k,a)=0$. We consider the subsequence formed by the terms with k odd, $k=2s+1$. From equation (1), we obtain

$$N(T,2s+1,a)=\sum_{h=0}^{n-1} D_h[[(-1)^h h!(n-h-1)!]^2]^s,$$

which can be rewritten as

$$N(T,2s+1,a)=\sum_{h=0}^{\frac{n}{2}-1} D_h([h!(n-h-1)!]^2)^s.$$

Then the subsequence $N(T,2s+1,a)$, $s=0,1,\ldots$, is recurrent with characteristic polynomial

$$f_{\text{even}}(n)=\prod_{h=0}^{\frac{n}{2}-1}(x-(h!(n-h-1)!)^2)$$

of degree $\frac{n}{2}$. For example, if $n=6$, $N(T,2s+1,a)$ is recurrent of third degree with characteristic polynomial $x^3-15120x^2+10450944x-1194393600$ and initial values

$$\{1,5040,69237504\}.$$

2. SMALLER DEGREE OF RECURRENCE

As we have seen, the sequence $N(T,k,a)$ is always linearly recurrent with degree at most $n=|G|$ for any subset T in which we confine the variables $x_1,x_2,\ldots,x_k$.

Sometimes we can find recurrences of lower degree.

Definition 2.1: A partition $\mathcal{T}=\{T_1,T_2,\ldots,T_m\}$ of G is said to be *closed* if $\forall h,\ k\in\{1,\ldots,m\}$ the set-product T_h*T_k is a disjoint union of elements of $\mathcal{T}$.

We can write

$$\gamma(T_h)*\gamma(T_k)=\sum\lambda_{hk}^s\gamma(T_s)$$

in the algebra ZG, where λ_{hk}^s is the number of solutions of the equation $x*y=g$, where $x\in T_h$, $y\in T_k$, $g\in T_s$. This number does not depend on g itself but only on the fact that $g\in T_s$. Then $\lambda_{hh}^s=N(T_h,2,g)$ with $g\in T_s$. Of course,

$$\underbrace{\gamma(T_h) * \gamma(T_h) * \cdots * \gamma(T_h)}_{k \text{ times}} = \Sigma N(T_h, k, g_s)T_s, \text{ where } g_s \in T_s.$$

We abbreviate $N(T_h, k, g_s)$ to $N(h, k, s)$.

Now let $A_h = \theta(\gamma(T_h))$, $h = 1, \ldots, m$. Then the set $\mathcal{A} = \{A_h : h = 1, \ldots, m\}$ satisfies

$$\sum_{h=1}^{m} A_h = J \text{ where } J \text{ is the all one matrix.} \tag{3}$$

There exist natural numbers λ_{hk}^s s.t.

$$A_h^k = \sum_{s=1}^{m} \lambda_{hk}^s A_s. \tag{4}$$

The numbers λ_{hk}^s are those we are searching for, that is,

$$A_h^k = \sum_{s=1}^{m} N(h, k, s) A_s. \tag{5}$$

If we compute A_h^k, the k^{th} power of A_h, the number $N(h, k, s)$ appears in the places of the first row of A_h^k, where A_s has ones.

Let us define the set of matrices $\mathcal{B}$, $\mathcal{B} = \{B_h : h = 1, \ldots, m\}$, where $(B_h)_{ij} = \lambda_{hi}^j$. By the following theorem, we obtain recurrences of degree lower than $|G|$ when T is an element of a closed partition.

Theorem 2.2: Let $T_h \subset G$ be an element of a closed partition $\mathcal{T}$. Then the sequence $N(T_h, k, g)$, $g \in G$, satisfies a recurrence of degree at most $m = |\mathcal{T}|$ with characteristic polynomial any polynomial $f(x)$ s.t. $f(B_h) = 0$, where the matrix B_h is defined by $(B_h)_{ij} = \lambda_{hi}^j$.

Proof: Again by Theorem 1.6 of [3], it is enough to prove that $N(T_h, n+1, g) = (B_h^n)_{ht}$ for every $h = 1, \ldots, m$ and $n \geq 1$, with $g \in T_t$. We prove this by induction.

For $n = 1$, $N(h, 2, t) = \lambda_{hh}^t = (B_h)_{ht}$.

Let us suppose that $N(h, n, t) = (B_h^{n-1})_{ht}$. Then

$$(A_h)^n = \sum_t N(h, n, t) A_t = \sum_t (B_h^{n-1})_{ht} A_t$$

and

$$\begin{aligned}(A_h)^{n+1} &= \sum_t (B_h^{n-1})_{ht} A_h A_t = \sum_{t,s} (B_h^{n-1})_{ht} \lambda_{ht}^s A_s \\ &= \sum_{t,s} (B_h^{n-1})_{ht} (B_h)_{ts} A_s = \sum_s (B_h^n)_{hs} A_s.\end{aligned}$$

It follows that $(B_h^n)_{hs} = N(h, n+1, s)$ by equation (5) and the independence of the A_s. □

Corollary 2.3: Let G and H be, respectively, a finite group and an automorphism group of G. Let $\mathcal{O} = \{O_1, O_2, \ldots, O_m\}$ be the set of orbits and let $N(h, k, t)$ be the number of solutions of $x_1 * x_2 * \cdots * x_k = g$, with $x_i \in O_h$ and $g \in O_t$. Then $N(h, k, t)$ is linearly recurrent with characteristic polynomial of degree at most m.

Proof: The proof follows from Theorem 2.2 and the fact that $\mathcal{O}$ is a closed partition. □

Remark 2.4:

(a) In the case of Corollary 2.3, the matrices A_h form an association scheme (see [1]), where $A_h^t = A_v$ and A_v is the matrix corresponding to the orbit $O_v = O_h^{-1}$.

(b) The characteristic polynomial can be computed as the minimum polynomial of the matrix B_h.

(c) The set of conjugacy classes is a well-known example with $H = Inn(G)$. The example 1.2 falls in this case, where conjugacy classes are those of n-cycles and transposition. Let us observe that, from Theorem 1.1, we could only suppose a recurrence of degree $n! = |S_n|$. Instead, from Theorem 2.2 and Corollary 2.3, we know that the recurrence degree for equations in S_n with variables constrained in conjugacy classes is at most equal to the number of partitions of n.

3. CYCLIC GROUPS AND RANDOM WALKS ON THE CIRCLE

Let Z_n be the additive cyclic group $Z_n = \{0, 1, \ldots, n-1\}$ and $Z_n^* = Aut(Z_n)$. If $H \le Z_n^*$ acts on Z_n, we get m orbits:

$$O_0 = O(0),\ O_1 = O(1) = H, \ldots, O_i = O(g_i),\ 0 \le i \le m-1,$$

with a set of representatives $\mathcal{R} = \{g_0 = 0, g_1 = 1, g_2, \ldots, g_{m-1}\}$. We know that $\mathcal{T} = \{O(g_i),\ 0 \le i \le m-1\}$ is a closed partition.

Let us now consider the special case $H = \{\pm 1\}$.

If n is odd, we have $\frac{n+1}{2}$ orbits with $\mathcal{R}_{\text{odd}} = \{0, 1, \ldots, \frac{n-1}{2}\}$; if n is even, we have $\frac{n+2}{2}$ orbits with $\mathcal{R}_{\text{even}} = \{0, 1, \ldots, \frac{n}{2}\}$.

Let z be the $n \times n$ circulant matrix with first row $[0, 0, \ldots, 0, 1]$, that is, the permutation matrix corresponding to the n-cycle $(1, 2, \ldots, n)$.

The adjacency matrices of the well-known "polygon scheme" determined by the action of H are:

(a) if r is odd,

$$A_0 = I_n,\ A_k = z^k + z^{-k} \ \text{ for } 1 \le k \le \frac{n+1}{2};$$

(b) if r is even,

$$A_0 = I_n,\ A_{n/2} = z^{n/2},\ A_k = z^k + z^{-k} \ \text{ for } 1 \le k \le \frac{n+2}{2}.$$

We divide the circle in n equal parts labeled $0, 1, \ldots, n-1$.

Let $P(k, a)$ be the probability that we get the vertex a starting from 0 and flipping a coin k times to decide whether to move one step clockwise or counterclockwise. Of course,

$$P(k, a) = \frac{N(O(1), k, a)}{2^k}.$$

Theorem 3.1: Let $g(x) = x^m + b_1 x^{m-1} + \cdots + b_m$ be the characteristic polynomial of B_1.

The sequence $P(0, a), P(1, a), \ldots, P(k, a), \ldots$ is recurrent with polynomial

$$f(x) = x^m + \sum_{h=1}^{m} \frac{b_h}{2^h} x^{m-h}.$$

Proof: From the proof of Theorem 2.2, we know that we find $P(k,a)$ in the first row of $(\frac{1}{2}B_1)^k$. The result follows because, if $g(x)$ is the characteristic polynomial of B_1, then $f(x)$ is the characteristic polynomial of $\frac{1}{2}B_1$. □

Example 3.2: Let $n=7$. The matrix $\frac{1}{2}A_1$ is the double stochastic transition matrix of the Markov chain associated with this random walk (see [4], p. 82).

$$A_1 = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

$C = \frac{1}{2}B_1$ is the stochastic matrix

$$C = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ 1 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

We find $P(k,0)$, that is, the probability that we come back to the origin 0 after k steps, in the place (1, 1) of C^k.

From Theorem 3.1, the sequence $P(k,0)$, $k \in N$, is recurrent with polynomial $x^4 - \frac{1}{2}x^3 - x^2 + \frac{3}{8}x + \frac{1}{8}$ and initial values $\{1, 0, \frac{1}{2}, 0\}$.

This recurrence sequence is convergent to $\frac{1}{7}$; in general, the first row of C^k converges to

$$\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right), \text{ that is, } \forall a \lim_{k\to\infty} P(k,a) = \frac{1}{n}.$$

The polygon scheme is a particular polynomial scheme. Then the matrix B_1 is tridiagonal and has the form

$$B_1 = \begin{Bmatrix} * & 1 & \ldots & 1 & 1 \\ 0 & 0 & \ldots & 0 & 1 \\ 2 & 1 & \ldots & 1 & * \end{Bmatrix} \tag{6}$$

for n odd, and

$$B_1 = \begin{Bmatrix} * & 1 & \ldots & 1 & 2 \\ 0 & 0 & \ldots & 0 & 0 \\ 2 & 1 & \ldots & 1 & * \end{Bmatrix} \tag{7}$$

for n even (see [1] for notation).

Let $B_1^{(n)}$ be the tridiagonal matrix of the polygon scheme with n vertices, and $g_n(x)$ be its minimum polynomial. Then

$$g_n = \prod_{h=0}^{[\frac{n}{2}]}\left(x - 2\cos\frac{2\pi h}{n}\right). \tag{8}$$

We now see that g_n can be computed easily using recurrence.

Theorem 3.3: The sequence $g_n(x)$ is recurrent with polynomial

$$y^4 - xy^2 + 1 \tag{9}$$

and initial values $\{g_0(x), g_1(x), g_2(x), g_3(x)\} = \{0, x-2, x^2-4, x^2-x-2\}$.

Proof:

$$B_1^{(n)} = \begin{Bmatrix} * & c_1 & c_2 & \dots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \dots & a_{d-1} & a_d \\ k & b_1 & b_2 & \dots & b_{d-1} & * \end{Bmatrix}, \tag{10}$$

where $c_1 = c_2 = \cdots = c_{d-1} = 1$, $a_1 = a_2 = \cdots = a_{d-1} = 0$, and $k = 2$, $b_1 = b_2 = \cdots = b_{d-1} = 1$; also, for n odd, $c_d = 1$, $a_d = 1$, $n = 2d+1$, and for n even, $c_d = 2$, $a_d = 0$, $n = 2d$.

Let us consider the sequence

$$F_0(x) = 1,\ F_1(x) = x+1,\ F_i(x) = (x - k + b_{i-1} + c_i)F_{i-1}(x) - b_{i-1}c_{i-1}F_{i-2}(x).$$

Then (see [1], p. 202), $(x-2)F_d(x) = g_n(x)$.

If n is odd, we have

$$F_i = xF_{i-1}(x) - F_{i-2}(x) \tag{11}$$

$\forall i, 2 \le i \le d$, which implies immediately that

$$g_n(x) = xg_{n-2}(x) - g_{n-4}(x), \tag{12}$$

and (9) is proved.

If n is even, (11) holds true $\forall i,\ 2 \le i < d$, but $F_d = (x+1)F_{d-1} - F_{d-2} = xF_{d-1} + F_{d-1} - F_{d-2}$.

Then $(x-2)F_d = (x-2)(xF_{d-1} - F_{d-2}) + (x-2)F_{d-1}$, that is,

$$g_n(x) = g_{n+1}(x) + g_{n-1}(x) \tag{13}$$

with $n = 2d$. Hence,

$$xg_{n-2} - g_{n-4} = x(g_{n-1} + g_{n-3}) - (g_{n-3} + g_{n-5}) = g_{n+1} + g_{n-1} = g_n \tag{14}$$

by (13) and (12). □

Of course, the sequence $g_k(x)$ has a geometrical meaning only if $k \ge 3$; we have extended it adding $g_0(x)$, $g_1(x)$, and $g_2(x)$ by computing the recurrence backward.

Remark 3.4: Let

$$F_d^{\text{even}} = \frac{g_{2d}}{(x-2)} \quad \text{and} \quad F_d^{\text{odd}} = \frac{g_{2d+1}}{(x-2)}.$$

Theorem 3.3 is equivalent to saying that the sequence F_0^{even}, F_1^{even}, ... and F_0^{odd}, F_1^{odd}, ... are both recurrent with characteristic polynomial $y^2 - xy + 1$, with initial values, respectively, $\{1, x+1\}$ and $\{0, x+2\}$.

Theorem 3.5: Let C be the matrix

$$\begin{pmatrix} x+1 & x+2 \\ -1 & -1 \end{pmatrix}. \tag{15}$$

Then the first row of C^d is $[F_d^{\text{odd}}, F_d^{\text{even}}]$ $\forall d \ge 0$.

Proof: The characteristic polynomial of C is y^2-xy+1 which is, by Theorem 3.3, the recurrence polynomial of both F_d^{odd} and F_d^{even}. Then the result follows from Remark 3.4 and Theorem 2.5 of [2], where the ring R is $Z[x]$. □

Corollary 3.6: The first row of $(x-2)C^d$ is $[g_{2d+1}(x), g_{2d}(x)]$ $\forall d \geq 0$.

4. DIHEDRAL GROUP

Let D_n be the group of symmetries of a regular polygon $D_n = \{\rho^k, \tau\rho^k, k = 0, 1, \ldots, n-1\}$, where n is the number of sides of the polygon, ρ is a rotation of $2\pi/n$, and τ is a reflection.

When n is odd, the regular representation θ is a direct sum of irreducible representations:

$$\theta = \psi_1 + \psi_2 + 2\phi_1 + 2\phi_2 + \cdots + 2\phi_{\frac{n-1}{2}},$$

where ψ_1 is the trivial representation, ψ_2 is the alternating representation, and ϕ_l is the two-dimensional representation such that

$$\phi_l(\rho^k) = \begin{pmatrix} \alpha^{lk} & 0 \\ 0 & \alpha^{-lk} \end{pmatrix} \phi_l(\tau\rho^k) = \begin{pmatrix} 0 & \alpha^{-lk} \\ \alpha^{lk} & 0 \end{pmatrix}, \quad \alpha = \exp\frac{2\pi i}{n}.$$

If n is even,

$$\theta = \psi_1 + \psi_2 + \psi_3 + \psi_4 + 2\phi_1 + 2\phi_2 + \cdots + 2\phi_{\frac{n-2}{2}},$$

where $\psi_3(\rho^k) = \psi_4(\rho^k) = (-1)^k$ and $\psi_3(\tau\rho^k) = (-1)^k$, $\psi_4(\tau\rho^k) = (-1)^{k+1}$.

Let us now consider the case of two reflections which generates D_n, τ, and $\tau\rho$, that is, suppose $T = \{\tau, \tau\rho\}$ and $a \in D_n$.

Theorem 4.1:

(a) The sequence $N(T, k, a)$ is recurrent with polynomial

$$p_n(x) = \frac{g_{2n}^2(x)}{x^2-4}. \tag{16}$$

(b) The sequence $p_n(x)$ for $n = 1, 2, \ldots$ is recurrent with polynomial

$$y^4 - y^3x^2 + (2x^2-2)y^2 - x^2y + 1 \tag{17}$$

and initial values $\{x^2-4,\ x^4-4x^2,\ -4+9x^2-6x^4+x^6,\ -16x^2+20x^4-8x^6+x^8,\ -4+25x^2-50x^4+35x^6-10x^8+x^{10}\}$.

Proof:

(a) From the decomposition of θ, if n is even,

$$p_n(x) = x^2(x-2)(x+2)\prod_{h=1}^{\frac{n-2}{2}}\left(x^2 - 4\cos^2\frac{2\pi h}{n}\right)^2, \tag{18}$$

and if n is odd,

$$p_n(x) = (x-2)(x+2)\prod_{h=1}^{\frac{n-1}{2}}\left(x^2 - 4\cos^2\frac{2\pi h}{n}\right)^2. \tag{19}$$

Collecting appropriate terms and using equation (8), we find (16). □

(b) By remark 3.4, $p_n(x) = \frac{x-2}{x+2}(F_n^{\text{even}}(x))^2$. In the ring $Z(x)\frac{x-2}{x+2}$ is constant and the sequence $p_n(x)$ is recurrent with the same recurrence of $(F_n^{\text{even}}(x))^2$. By the same remark $F_n^{\text{even}}(x)$ is recurrent with polynomial $y^2 - xy + 1$ whose companion matrix is

$$C = \begin{pmatrix} 0 & -1 \\ 1 & x \end{pmatrix}.$$

By Theorem 2.6 of [2], $(F_n^{\text{even}}(x))^2$ is recurrent with the characteristic polynomial of the Kronecker product $C \otimes C$, that is, $y^4 - y^3x^2 + (2x^2 - 2)y^2 - x^2y + 1$. □

For example, if $n = 7$, the sequence $N(T, k, e)$ is recurrent with polynomial $-4 + 49x^2 - 196x^4 + 294x^6 - 210x^8 + 77x^{10} - 14x^{12} + x^{14}$ and initial values

$$\{0, 2, 0, 6, 0, 20, 0, 70, 0, 252, 0, 924, 0, 3434\}.$$

We now consider the case of the basic rotation ρ and the reflection τ, that is, $T = \{\rho, \tau\}$ and $a \in D_n$.

Theorem 4.2:

(a) The sequence $N(T, k, a)$ is recurrent with polynomial

$$p_n^{\text{odd}}(x) = \frac{g_n^2}{(x-2)} x^n \tag{20}$$

if n is odd, and

$$p_n^{\text{even}}(x) = \frac{g_n^2}{(x-2)(x+2)} x^n \tag{21}$$

if n is even.

(b) The subsequences p_{2s+1}^{odd} and p_{2s}^{even} are recurrent with polynomial

$$y^4 - y^3x^4 + (2x^6 - 2x^4)y^2 - x^8y + x^8 \tag{22}$$

and initial values, respectively,

$$\{x^2 - 2x, -2x^3 - 3x^4 + x^6, -2x^5 + 5x^6 - 5x^8 + x^{10}, -2x^7 - 7x^8 + 14x^{10} - 7x^{12} + x^{14}\}$$

and

$$\{-4x^6 + x^8, -4x^6 + 9x^8 - 6x^{10} + x^{12}, -16x^{10} + 20x^{12} - 8x^{14} + x^{16},$$
$$-4x^{10} + 25x^{12} - 50x^{14} + 35x^{16} - 10x^{18} + x^{20}\}.$$

Proof:

(a) From the decomposition of θ, we find

$$p_n^{\text{even}}(x) = x(x-2)(x+2)\prod_{h=1}^{\frac{n-2}{2}} x^2\left(x - 2\cos\frac{2\pi h}{n}\right)^2 \tag{23}$$

and

$$p_n^{\text{odd}}(x) = x^2(x-2)\prod_{h=1}^{\frac{n-1}{2}} x^2\left(x - 2\cos\frac{2\pi h}{n}\right)^2. \tag{24}$$

Equations (20) and (21) follow from (8). □

(b) In the ring $Z[x]$, $p_{2s+1}^{\text{odd}}(x)$ is equal to $x(x-2)$ multiplied by $(F_s^{\text{odd}}(x))^2 x^{2s}$. Furthermore, $(F_s^{\text{odd}}(x))^2$ is recurrent by characteristic polynomial $y^4 - y^3x^2 + (2x^2-2)y^2 - x^2y + 1 = u(x)$ and x^{2s} by $y - x^2$. We again use Theorem 2.6 of [2]: the characteristic polynomial of x^2U, where U is the companion matrix of $u(x)$, is precisely $y^4 - y^3x^4 + (2x^6 - 2x^4)y^2 - x^8y + x^8$.

The same holds for $p_{2s}^{\text{even}}(x)$. □

For example, if $n=7$, the sequence $N(T,k,e)$ is recurrent with polynomial $-2x^7 - 7x^8 + 14x^{10} - 7x^{12} + x^{14}$ and initial values

$$\{0,1,0,3,0,10,1,35,9,126,55,462,286,1717\}.$$

If $n=8$, the sequence $N(T,k,e)$ is recurrent with polynomial $-16x^{10} + 20x^{12} - 8x^{14} + x^{16}$ and initial values

$$\{0,1,0,1,0,3,0,10,0,36,0,136,0,528,0,2080,0,8256\}.$$

REFERENCES

1. E. Bannai & T. Ito. *Algebraic Combinatorics.* I. *Association Schemes.* Canada: Benjamin/Cummings Co., 1984.
2. U. Cerruti & F. Vaccarino. "*R*-Algebras of Linear Recurrent Sequences." *J. Algebra* **175** (1995):332-38.
3. U. Cerruti & F. Vaccarino. "Matrices, Recurrent Sequences and Arithmetics." In *Applications of Fibonacci Numbers* **6:**53-62. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1996.
4. K. L. Chung. *Elementary Probability Theory with Stochastic Processes.* New York: Springer Verlag, 1979.
5. D. M. Jackson. "Some Combinatorial Problems Associated with Products of Conjugacy Classes of the Symmetric Group." *J. Comb. Theory* **49** (1987):363-69.
6. T. N. Shorey & R. Tijdeman. *Exponential Diophantine Equations.* Cambridge: Cambridge University Press, 1986.

AMS Classification Number: 11B37

❖❖❖

FERMAT'S BIRTHDAY

August 20, 2001 marks the 400th anniversary of Fermat's birth.