Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 459–473
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Symmetric Pascal matrices modulo p

Roland Bacher[a], Robin Chapman[b]

[a] *Institut Fourier, UMR 5582, Laboratoire de Mathématiques, BP 74, 38402 St. Martin d'Hères Cedex, France*
[b] *School of Mathematical Sciences, University of Exeter, North Park Road, Exeter EX4 4QE, UK*

Received 16 December 2002; received in revised form 3 June 2003; accepted 4 June 2003

Abstract

We give some results concerning determinants and characteristic polynomials modulo p of the symmetric Pascal matrix with coefficients $\binom{i+j}{i} \pmod{p}$, $0 \le i, j < n$.

1. Introduction

This paper presents results and conjectures concerning symmetric matrices associated to Pascal's triangle. We first give a formula for the determinant over **Z** of the reduction modulo 2 with values in $\{0, 1\}$ and of the reduction modulo 3 with values in $\{-1, 0, 1\}$ for such a matrix. We then study the reduction modulo a prime p of the characteristic polynomials of these matrices. Our main results imply a recursive formula for the prime $p = 2$ and a conjectural recursive formula for $p = 3$.

Consider the symmetric matrix $P(n)$ with coefficients

$$p_{i,j} = \binom{i+j}{i}, \qquad 0 \le i, j < n.$$

We call $P(n)$ the *symmetric Pascal matrix* of order n. The entries of $P(n)$ satisfy the recurrence

$$p_{i,j} = p_{i-1,j} + p_{i,j-1}.$$

In [2] the first author studied the determinant of the general matrix with entries satisfying this recurrence.

E-mail addresses: Roland.Bacher@ujf-grenoble.fr (R. Bacher), rjc@maths.ex.ac.uk (R. Chapman).

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2003.06.001

An easy computation yields $P(\infty) = TT^t$ where T is the infinite unipotent lower triangular matrix

$$T = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ \vdots & & & & \ddots \end{pmatrix} = \exp \begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ 0 & 2 & 0 & & \\ & 0 & 3 & 0 & \\ & & & & \ddots \end{pmatrix}$$

with coefficients $t_{i,j} = \binom{i}{j}$. This shows that $\det(P(n)) = 1$ and that $P(n)$ is positive definite for all $n \in \mathbf{N}$. Hence all zeros of the characteristic polynomial $\chi_n(t) = \det(tI(n) - P(n))$ (where $I(n)$ denotes the identity matrix of size n) of $P(n)$ are positive reals. The inverse $P(n)^{-1}$ of $P(n)$ is given by

$$P(n)^{-1} = (T(n)^t)^{-1} T(n)^{-1}$$

and $T(n)^{-1}$ has coefficients $(-1)^{i+j}\binom{i}{j}$, $0 \le i, j < n$. Hence $T(n)$ and $T(n)^{-1}$ are conjugate by an orthogonal matrix, and thus also $P(n)$ and $P(n)^{-1}$ are conjugate. The characteristic polynomial $\chi_n(t)$ therefore satisfies $\chi_n(t) = (-t)^n \chi(1/t)$ and 1 is always an eigenvalue of $P(2n+1)$, cf. [4]. The polynomials $\chi_n(t)$, especially their behaviour modulo primes, will be our main object of study. For convenience, we write I for $I(n)$ whenever the size of the identity matrix is unambiguous.

Define $\overline{P}(n)_2$ with coefficients $(\overline{P}(n)_2)_{i,j} \in \{0, 1\}$ as the reduction modulo 2 of $P(n)$ by setting

$$(\overline{P}(n)_2)_{i,j} = \left(\binom{i+j}{i} \pmod 2\right) \in \{0, 1\}.$$

The Thue–Morse sequence $s(n) = \sum \nu_i \pmod 2$ records the parity of the sum of the binary digits of $n = \sum \nu_i 2^i$. It can also be defined recursively by $s(0) = 0$, $s(2k) = s(k)$ and $s(2k+1) = 1 - s(k)$ (cf. for instance [1]).

Similarly, we define $\overline{P}(n)_3$ with coefficients $(\overline{P}(n)_3)_{i,j} \in \{-1, 0, 1\}$ as the reduction modulo 3 of $P(n)$ by setting

$$(\overline{P}(n)_3)_{i,j} = \left(\binom{i+j}{i} \pmod 3\right) \in \{-1, 0, 1\}.$$

We introduce furthermore the sequence $t(n)$ defined recursively by $t(0) = 0$, $t(3n) = t(n)$, $t(3n+1) = t(n) + 1$, $t(3n+2) = t(n) - 1$. One has $t(n) = \alpha(n) - \beta(n)$ where $\alpha(n) = \#\{j \mid \nu_j = 1\}$ (respectively $\beta(n) = \#\{j \mid \nu_j = 2\}$) count the number of occurrences of digits equal to 1 (respectively to 2) when writing $n = \sum \nu_j 3^j$ (with $\nu_j \in \{0, 1, 2\}$) in base 3.

Theorem 1.1. (i) *The determinant over* $\mathbf{Z}$ *of* $\overline{P}(n)_2$ *is given by*

$$\det(\overline{P}(n)_2) = \prod_{k=0}^{n-1} (-1)^{s(k)}.$$

(ii) *The determinant over* $\mathbf{Z}$ *of* $\overline{P}(n)_3$ *is given by*

$$\det(\overline{P}(n)_3) = \prod_{k=0}^{n-1} (-2)^{t(k)}.$$

In the sequel, we will be interested in the characteristic polynomial $\det(tI - P(n)) \pmod p$ for p a prime number. The next result yields a formula for $n = p^l$ and is of crucial importance in the sequel.

Proposition 1.2. *Given a power* $q = p^l$ *of a prime* p*, the matrix* $P(q)$ *has order 3 over* $\mathbf{F}_p$*. Its characteristic polynomial* $\chi_q(t) = \det(tI(q) - P(q))$ *satisfies*

$$\chi_q(t) \equiv (t^2 + t + 1)^{\frac{q-\epsilon(q)}{3}} (t-1)^{\frac{q+2\epsilon(q)}{3}} \pmod p$$

where $\epsilon(q) \in \{-1, 0, 1\}$ *satisfies* $\epsilon(q) \equiv q \pmod 3$.

In particular, $P(q)$ can be diagonalized over $\mathbf{F}_{p^2}$ except when $p = 3$. For instance, $P(3)$ has a unique Jordan block over $\mathbf{F}_3$.

This proposition (except for the diagonalization part) admits the following generalization:

Theorem 1.3. *When* $q = p^l$ *is a power of a prime* p *and* $0 \le k \le q/2$ *then*

$$\chi_{q-k}(t) \equiv (t^2 + t + 1)^{(q-\epsilon(q))/3-k} (t-1)^{(q+2\epsilon(q))/3-k} \det(t^2 I + P(k)) \pmod p$$

where $\epsilon(q) \in \{-1, 0, 1\}$ *satisfies* $\epsilon(q) \equiv q \pmod 3$.

Theorem 1.3 completely determines the reduction modulo 2 of $\chi_n(t)$ as follows: Define a sequence $\gamma(0) = 0, \gamma(1), \ldots$ recursively by

$$\gamma(2^l - k) = \frac{2^l + 2(-1)^l}{3} - k + 2\gamma(k), \qquad 0 \le k \le 2^{l-1}.$$

Theorem 1.4. *For all* $n \in \mathbf{N}$

$$\chi_n(t) \equiv (t+1)^{\gamma(n)} (t^2 + t + 1)^{\gamma_2(n)} \pmod 2$$

where $\gamma_2(n) = (1/2)(n - \gamma(n))$.

It follows immediately that the matrix $I - P(n)^3$ is nilpotent over $\mathbf{F}_2$ for all $n \in \mathbf{N}$. It would be of interest to investigate the sizes of the Jordan blocks of $I - P(n)^3$ over $\mathbf{F}_2$.

The first terms $\gamma(1), \ldots, \gamma(32)$ and $\gamma_2(1), \ldots, \gamma_2(32)$ are given by

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\gamma(n)$	1	0	3	2	5	0	3	2	5	0	11	6	9	4	7	6
$\gamma_2(n)$	0	1	0	1	0	3	2	3	2	5	0	3	2	5	4	5
n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\gamma(n)$	9	4	15	10	21	0	11	6	9	4	15	10	13	8	11	10
$\gamma_2(n)$	4	7	2	5	0	11	6	9	8	11	6	9	8	11	10	11

The sequence $\gamma(0), \gamma(1), \ldots$ has many interesting arithmetic features. In order to describe them, let us introduce the number $b(n)$ of “blocks” of consecutive ones in the binary expansion of a positive integer n. For instance $667 = (1010011011)_2$ and so $b(667) = 4$. Notice that $b(2n) = b(n)$ and $b(2n+1) = b(n) + 1 - (n \pmod 2)$ (with $n \pmod 2 \in \{0, 1\}$). This, together with $b(0) = 0$, defines the sequence $b(n)$ recursively.

Theorem 1.5. (i) *We have*

$$\gamma(2^l + k) = \frac{2^l + 2(-1)^l}{3} - k + 4\gamma(k)$$

for all $0 \le k \le 2^{l-1}$.

(ii) *We have for* $2^{l-2} \le k \le 2^{l-1}$

$$\gamma(2^l - k) = \gamma(k) + 2\gamma(2^{l-1} - k).$$

(iii) *We have*

$$\gamma(2^l + k) = 1 + \gamma(2^l + k - 1) + 2\gamma(2^l - k) - 2\gamma(2^l + 1 - k)$$

for $1 \le k \le 2^l$.

(iv) *We have, for all* $n \in \mathbf{N}$,

$$\gamma(2n) = n - \gamma(n),$$
$$\gamma(2n-1) = \gamma(2n) + (4^{b(2n-1)} - 1)/3 = n - \gamma(n) + (4^{b(2n-1)} - 1)/3,$$
$$\gamma(2n+1) = \gamma(2n) + (2^{1+2b(n)} + 1)/3 = n - \gamma(n) + (2^{1+2b(n)} + 1)/3.$$

Part (iv) of this theorem gives an alternative recursive definition of the sequence $(\gamma(n))$. Theorem 1.3 seems to have many variants. One is given by the following:

Conjecture 1.6. *For each integer* $k \ge 0$ *there exists a monic polynomial* $c_k(t) \in \mathbf{Z}[t]$ *of degree* $4k$ *such that* $c_k(t) = t^{4k} c_k(t^{-1})$ *with the following property: if* q *is a power of a prime* p, *and* $0 \le k \le q/2$ *then*

$$\chi_{q+k}(t) \equiv (t^2 + t + 1)^{(q-\epsilon(q))/3-k} (t-1)^{(q+2\epsilon(q))/3-k} c_k(t) \pmod p$$

where $\epsilon(q) \in \{-1, 0, 1\}$ *satisfies* $\epsilon(q) \equiv q \pmod 3$.

The first few of these conjectural polynomials $c_k(t)$ are

$$c_0(t) = 1,$$
$$c_1(t) = t^4 - 2t^3 - 2t + 1,$$
$$c_2(t) = t^8 - 6t^7 + 4t^6 - 4t^5 + 15t^4 - 4t^3 + 4t^2 - 6t + 1,$$
$$c_3(t) = (t^4 - 2t^3 - 2t + 1)(t^8 - 16t^7 + 4t^6 - 4t^5 + 40t^4 - 4t^3 + 4t^2 - 16t + 1),$$
$$c_4(t) = t^{16} - 58t^{15} + 288t^{14} - 240t^{13} + 393t^{12} - 1440t^{11} + 836t^{10} - 902t^9 + 2376t^8 - 902t^7 + \cdots - 58t + 1,$$
$$c_5(t) = c_1(t)(t^{16} - 196t^{15} + 2112t^{14} - 792t^{13} + 1290t^{12} - 10560t^{11} + 2768t^{10} - 2972t^9 + 17424t^8 - 2972t^7 + \cdots - 196t + 1).$$

For $p = 2$, it follows from Theorem 1.4 and assertion (i) in Theorem 1.5 that if $c_k(t)$ exists then

$$c_k(t) \equiv (\det(tI + P(k)))^4 \pmod 2.$$

Computations suggest:

Conjecture 1.7. *We have*

$$c_k(t) \equiv (t+1)^{3k} \det(tI + P(k)) \pmod 3.$$

This conjecture, together with Theorem 1.3 yields conjectural recursive formulas for the reduction modulo 3 of $\chi_n(t) = \det(tI(n) - P(n))$ as follows: Set $\chi_0(t) = 1$ and $\chi_1(t) = 1 - t$. For $n = 3^l \pm k > 1$ with $0 \le k < 3^l/2$ the characteristic polynomial $\chi_n(t) \pmod 3$ is then conjecturally given by

$$\begin{array}{ll} (t-1)^{3^l - 3k} \det(t^2 I + P(k)) & \text{if } n = 3^l - k, \\ (t-1)^{3^l - 3k}\,(t+1)^{3k} \det(tI + P(k)) & \text{if } n = 3^l + k. \end{array}$$

In particular, all roots of $\chi_n(t)$ modulo 3 should be of multiplicative order a power of 2 in the algebraic closure of $\mathbf{F}_3$.

We conclude finally by mentioning a last conjectural observation:

Conjecture 1.8. *Given a prime-power* $q = p^l \equiv 2 \pmod 3$, *we have*

$$\chi_{(q+1)/3}(t) \equiv (t+1)^{(q+1)/3} \pmod p$$

and

$$\chi_{(2q-1)/3}(t) \equiv (t+1)^{(q+1)/3}\,(t-1)^{(q-2)/3} \pmod p.$$

Remark 1.9. (i) The matrix $C = P((q+1)/3) + I((q+1)/3)$ for $q = p^l \equiv 2 \pmod 3$ a prime-power, appears to have a unique Jordan block of maximal length over $\mathbf{F}_p$. If so, the rows of $C^{(q+1)/6}$ generate a self-dual code over $\mathbf{F}_p$.

(ii) Given a prime-power $q = p^l \equiv 2 \pmod 3$ as above we set $n = (2q+2)/3$ and $k = (2q-1)/3$. We conjecture that the characteristic polynomial of the matrix $\tilde{P}_k(n)$ with coefficients

$$\tilde{p}_{i,j} = \binom{i+j+2k}{i+k}, \qquad 0 \le i, j < n$$

satisfies $\det(tI - \tilde{P}_k(n)) \equiv (1+t)^n \pmod p$.

Remark 1.10. In [3, Theorems 32 and 35] Krattenthaler gives evaluations of determinants related to ours, namely of $\det(\omega I + Q(n))$ where ω is a sixth root of unity, and $Q(n)$ has entries $\binom{2\mu+i+j}{j} (0 \le i, j < n)$.

The sequel of this paper is organized as follows:

Section 2 is devoted to autosimilar matrices. Such matrices generalize the matrices $\overline{P}(\infty)_2$, $\overline{P}(\infty)_3$ and their properties imply easily Theorem 1.1.

Section 3 contains proofs of Proposition 1.2 and Theorem 1.3.

Section 4 contains proofs of Theorems 1.4 and 1.5.

2. Autosimilar matrices

Let $b > 1$ be a natural integer. An infinite matrix M with coefficients $m_{i,j}$ $(i, j \geq 0)$ in an arbitrary commutative ring is *b-autosimilar* if $m_{0,0} = 1$ and if

$$m_{s,t} = \prod_i m_{\sigma_i,\tau_i}$$

where the indices $s = \sum \sigma_i b^i$, $t = \sum \tau_i b^i$ are written in base b, that is, $\sigma_i, \tau_i \in \{0, \dots, b-1\}$ for all $i = 0, 1, 2, \dots$.

We denote by $M(n)$ the finite sub-matrix of M with coefficients $m_{i,j}$, $0 \leq i, j < n$. A b-autosimilar matrix M is *non-degenerate* if the determinants

$$\det(M(n))$$

are invertible for $n = 2, \dots, b$.

Theorem 2.1. *Let $b \geq 2$ be an integer and let M be a b-autosimilar matrix which is non-degenerate. One has then a factorization*

$$M = LDU$$

where L, D, U are b-autosimilar and where L is unipotent lower-triangular, D is diagonal and U is unipotent upper-triangular.

Corollary 2.2. *Given a non-degenerate b-autosimilar matrix M one has*

$$\det(M(n)) = \prod_{m=0}^{n-1} d_m$$

where $d_0 = 1$,

$$d_m = \det(M(m+1))/\det(M(m))$$

for $m = 1, \dots, b-1$ and

$$d_m = \prod_{j \geq 0} d_{\mu_j}, \qquad m = \sum \mu_j b^j, \ \mu_j \in \{0, 1, \dots, b-1\}$$

for $m \geq b$.

Remark 2.3. In general, one can compute determinants of arbitrary b-autosimilar matrices over a field K by applying Corollary 2.2 to the b-autosimilar matrix obtained from a generic perturbation of the form

$$M_t(b) = (1-t)M(b) + tP(b)$$

(where $P(b)$ is a matrix such that $M_t(b)$ becomes non-degenerate) and working over the rational function field $K(t)$.

Proof of Theorem 2.1. The non-degeneracy of M implies that

$$M(b) = L(b)D(b)U(b)$$

where $L(b)$ and $U(b)$ are unipotent lower and upper triangular matrices and the diagonal matrix $D(b)$ has entries $d_{0,0} = 1$ and $d_{k,k} = \det(M(k+1))/\det(M(k))$ for $k = 1, \dots, b-1$. Extending $L(b)$, $D(b)$ and $U(b)$ in the unique possible way to infinite b-autosimilar matrices L, D and U we have

$$\begin{aligned}(LDU)_{s,t} &= \sum_k L_{s,k} D_{k,k} U_{k,t} \\ &= \sum_{k=\sum \kappa_i b^i} \prod_i L_{\sigma_i,\kappa_i} D_{\kappa_i,\kappa_i} U_{\kappa_i,\tau_i} \\ &= \prod_i \sum_{\kappa_i=0}^{b-1} L_{\sigma_i,\kappa_i} D_{\kappa_i,\kappa_i} U_{\kappa_i,\tau_i} \\ &= \prod_i m_{\sigma_i,\tau_i} = m_{s,t}\end{aligned}$$

for all $s = \sum \sigma_i b^i, t = \sum \tau_i b^i \in \mathbf{N}$. $\square$

The identity

$$\det(M(n)) = \det(D(n))$$

implies immediately Corollary 2.2.

2.1. *Binomial coefficients modulo a prime p*

Let p be a prime number. Writing p-adically $n = \sum_{i\geq 0} \nu_i p^i$ and using the existence of the Frobenius automorphism for fields of characteristic p we get

$$(1+x)^n = \prod_{i\geq 0} (1+x)^{\nu_i p^i} \equiv \prod_{i\geq 0} (1+x^{p^i})^{\nu_i} \pmod p.$$

This implies immediately the congruence

$$\binom{n}{k} \equiv \prod_i \binom{\nu_i}{\kappa_i} \pmod p$$

where $k = \sum_{i\geq 0} \kappa_i p^i$ and allows (for small primes) an efficient computation of binomial coefficients (mod p).

This equality shows that the infinite matrices $\overline{P}(\infty)_2$ and $\overline{P}(\infty)_3$ with coefficients in $\{0, 1\}$ (respectively in $\{-1, 0, 1\}$) obtained by reducing the symmetric Pascal matrix modulo 2 (respectively modulo 3) are 2− (respectively 3−) autosimilar.

For $p = 2$ we have

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

which yields $d_0 = 1, d_1 = -1$ and Corollary 2.2 implies now assertion (i) of Theorem 1.1.

Remark 2.4. One can show that the inverse of the integral matrix $\overline{P}(n)_2$ considered in Theorem 1.1 has all its coefficients in $\{-1, 0, 1\}$ for all n.

For $p = 3$ we have

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

This shows that $\det(\overline{P}(n)_3)$ (over $\mathbf{Z}$) equals $(-2)^{a-b}$ where a and b are the number of digits 1 and 2 needed in order to write all natural integers $< n$ in base 3. This is the statement of assertion (ii) of Theorem 1.1.

3. Proofs of Proposition 1.2 and Theorem 1.3

Proof of Proposition 1.2. Let R be a commutative ring, and let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, R).$$

Then A determines a (graded R-algebra) automorphism ϕ_A of $R[X, Y]$ via $\phi_A(X) = aX + bY$ and $\phi_A(Y) = cX + dY$, or alternatively

$$\begin{pmatrix} \phi_A(X) \\ \phi_A(Y) \end{pmatrix} = A \begin{pmatrix} X \\ Y \end{pmatrix}.$$

It is easy to see that $\phi_A \circ \phi_B = \phi_{BA}$. Each ϕ_A restricts to an R-module automorphism of the homogeneous polynomials $R[X, Y]_{n-1}$ of degree $n - 1$. Let $A^{(n)}$ denote the matrix of this endomorphism with respect to the basis $X^{n-1}, X^{n-2}Y, X^{n-3}Y^2, \ldots, Y^{n-1}$, that is

$$\begin{pmatrix} \phi_A(X^{n-1}) \\ \phi_A(X^{n-2}Y) \\ \phi_A(X^{n-3}Y^2) \\ \vdots \\ \phi_A(Y^{n-1}) \end{pmatrix} = A^{(n)} \begin{pmatrix} X^{n-1} \\ X^{n-2}Y \\ X^{n-3}Y^2 \\ \vdots \\ Y^{n-1} \end{pmatrix}.$$

Then $A^{(n)} \in \mathrm{GL}(n, R)$ and $(AB)^{(n)} = A^{(n)}B^{(n)}$. (Another way of expressing this is to say that $A^{(n)}$ is the $(n-1)$-th symmetric power of A.)

Let us specialize to the case $R = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ and $n = p^l$. In this case $A^{(n)} = I$ if and only if A is a scalar matrix. The matrix

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

yields $A^{(n)} \equiv P(p^l) \pmod{p}$. Since $A^3 = -I$, the matrix $A^{(n)}$ has order 3.

Let us first compute the multiplicities of the three eigenvalues of $P = P(p) \pmod{p}$ over $\overline{\mathbf{F}}_p$.

The easy congruence $\binom{2k}{k} \equiv \binom{(p-1)/2}{k}(-4)^k \pmod p$ for p an odd prime and $0 \le k \le (p-1)/2$ shows

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k} \left(\frac{-x}{4}\right)^k \equiv (1+x)^{(p-1)/2} \pmod p$$

and yields $\mathrm{tr}(P) \equiv (-3)^{(p-1)/2} \equiv \epsilon(p) \pmod p$ (where $\epsilon(p) \in \{-1, 0, 1\}$ satisfies $\epsilon(p) \equiv p \pmod 3$) by quadratic reciprocity.

Since the characteristic polynomial for P has antisymmetric coefficients ($\alpha_k = -\alpha_{p-k}$) the two eigenvalues $\neq 1$ of P have equal multiplicity r. Lifting into non-negative integers $\le (p-1)/2$ the solution of the linear system $-r + (p-2r) \equiv \mathrm{tr}(P) \pmod p$ now yields the result.

The case $p = 2$ is easily solved by direct inspection.

The formula for $P(p^l)$ is now a straightforward consequence of the fact the $P(p^l)$ is the l-fold Kronecker product $P \otimes P \otimes \cdots \otimes P$ of $P = P(p)$ with itself. All eigenvalues of $P(p^l) \pmod p$ are third roots of 1 over $\mathbf{F}_{p^2}$. Their multiplicities in the characteristic polynomial $\chi_{p^l}(t) \pmod p$ can be computed as above by remarking that $\mathrm{tr}(P(p^l)) = (\mathrm{tr}(P(p)))^l$. $\square$

Remark 3.1. Recall that we have (with the notations of the above proof) $P = P(n) = A^{(n)} \pmod p$ for $n = p^l$ and introduce $L = L(n) = B^{(n)} \pmod p$ and $\tilde{L} = \tilde{L}(n) = C^{(n)} \pmod p$ where

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$

It is straightforward to check that L and $\tilde{L}$ have coefficients

$$l_{i,j} = (-1)^i \binom{i}{j} \pmod p \qquad \text{and} \qquad \tilde{l}_{i,j} = (-1)^j \binom{i}{j} \pmod p$$

for $0 \le i, j < n$.

Then $A^3 = -I$, but $(-I)^{(n)}$ is the identity. Hence $P^3 = I$. Also $C^2 = I$ and $CAC = A^{-1}$. It follows that A and C generate a dihedral group of order 12, containing $-I$. Hence $A^{(n)} = P$ and $C^{(n)} = \tilde{L}$ generate a dihedral group of order 6.

Proof of Theorem 1.3. Using Proposition 1.2, we can rewrite the equation to be proved as

$$(t^3-1)^k \det(tI - P(q-k)) \equiv \det(tI - P(q)) \det(t^2 I + P(k)) \pmod p.$$

Here, and in the sequel, we write I for $I(n)$ whenever this notation is unambiguous; also we denote the zero matrix of any size by O.

We now work over the field $\mathbf{F}_p$. Unless otherwise stated vectors will be row vectors.

It is convenient to define a category $\mathcal{E} = \mathcal{E}_{\mathbf{F}_p}$ as follows. Its objects will be pairs (V, α) where V is a finite-dimensional vector space over $\mathbf{F}_p$ and α is a vector space endomorphism of V. A morphism $\phi : (V, \alpha) \to (W, \beta)$ in $\mathcal{E}$ will be a linear map $\phi : V \to W$ with $\phi \circ \alpha = \beta \circ \phi$. (In fact $\mathcal{E}$ is equivalent to the category of finitely generated torsion modules over the polynomial ring $\mathbf{F}_p[X]$.) If (V, α) is an object of $\mathcal{E}$ we define $\chi(V, \alpha, t)$ as the characteristic polynomial of α acting on V, that is, $\chi(V, \alpha, t) = \det(tI - A)$ where A is a matrix representing α with respect to some basis of V. An r by r matrix A defines an object $((\mathbf{F}_p)^r, \alpha)$, denoted by $((\mathbf{F}_p)^r, A)$, where α is the endomorphism defined by A.

It is easy to see that $\mathcal{E}$ is an abelian category, and that if

$$0 \to (V, \alpha) \to (X, \gamma) \to (W, \beta) \to 0$$

is a short exact sequence, then $\chi(X, \gamma, t) = \chi(V, \alpha, t)\chi(W, \beta, t)$. This is because there is a basis for X with respect to which the matrix of γ (acting on row vectors from the right) is

$$\begin{pmatrix} A & O \\ C & B \end{pmatrix}$$

where A and B are matrices representing α and β respectively.

Set $k' = q - k$. We can partition the Pascal matrices $P(k')$ and $P(q)$ as follows:

$$P(k') = \begin{pmatrix} A & B \\ B^t & C \end{pmatrix} \qquad \text{and} \qquad P(q) = \begin{pmatrix} A & B & D \\ B^t & C & O \\ D^t & O & O \end{pmatrix}$$

where $A = P(k)$.

Let $\overline{A}$ denote the matrix obtained by rotating A through 180° (more formally, $\overline{A} = JAJ$ where J is the matrix with entries 1 on the reverse diagonal and 0 elsewhere). Then $P(q)^2 = \overline{P(q)}$ and $P(q)^3 = I$. Hence

$$P(q)^2 = \begin{pmatrix} O & O & \overline{D^t} \\ O & \overline{C} & \overline{B^t} \\ \overline{D} & \overline{B} & \overline{A} \end{pmatrix}.$$

Thus

$$A^2 + BB^t + DD^t = O$$

and so

$$P(k')^2 = \begin{pmatrix} -DD^t & O \\ O & \overline{C} \end{pmatrix}.$$

From $P(q)^2 = \overline{P(q)}$ it follows that $AD = \overline{D^t}$ and from $\overline{P(q)}P(q) = I$ it follows that $\overline{D^t}D^t = I$. Hence $ADD^t = I$ and so

$$P(k')^2 = \begin{pmatrix} -A^{-1} & O \\ O & \overline{C} \end{pmatrix}.$$

Let

$$Q_1 = \begin{pmatrix} O & I(k) & O \\ O & O & I(k) \\ I(k) & O & O \end{pmatrix}.$$

Let $\phi : (\mathbf{F}_p)^{3k} \to (\mathbf{F}_p)^q$ be the map defined by the matrix

$$\begin{pmatrix} I & O & O \\ A & B & D \\ O & O & \overline{D^t} \end{pmatrix}.$$

Then

$$Q_1 \begin{pmatrix} I & O & O \\ A & B & D \\ O & O & \overline{D^t} \end{pmatrix} = \begin{pmatrix} A & B & D \\ O & O & \overline{D^t} \\ I & O & O \end{pmatrix}$$

and

$$\begin{pmatrix} I & O & O \\ A & B & D \\ O & O & \overline{D^t} \end{pmatrix} P(q) = \begin{pmatrix} I & O & O \\ A & B & D \\ O & O & \overline{D^t} \end{pmatrix} \begin{pmatrix} A & B & D \\ B^t & C & O \\ D^t & O & O \end{pmatrix} = \begin{pmatrix} A & B & D \\ O & O & \overline{D^t} \\ I & O & O \end{pmatrix}$$

where we have used the formulas $P(q)^2 = \overline{P(q)}$ and $\overline{P(q)}P(q) = I$. Hence ϕ is a morphism from $((\mathbf{F}_p)^{3k}, Q_1)$ to $((\mathbf{F}_p)^q, P(q))$ in $\mathcal{E}$.

Let

$$Q_2 = \begin{pmatrix} O & I(k) \\ -A^{-1} & O \end{pmatrix}.$$

Let $\psi : (\mathbf{F}_p)^{2k} \to (\mathbf{F}_p)^{k'}$ be the map defined by the matrix

$$\begin{pmatrix} I & O \\ A & B \end{pmatrix}.$$

Then

$$Q_2 \begin{pmatrix} I & O \\ A & B \end{pmatrix} = \begin{pmatrix} A & B \\ -A^{-1} & O \end{pmatrix}$$

and

$$\begin{pmatrix} I & O \\ A & B \end{pmatrix} P(k') = \begin{pmatrix} I & O \\ A & B \end{pmatrix} \begin{pmatrix} A & B \\ B^t & C \end{pmatrix} = \begin{pmatrix} A & B \\ -A^{-1} & O \end{pmatrix}$$

where we have used the formula

$$P(k')^2 = \begin{pmatrix} -A^{-1} & O \\ O & \overline{C} \end{pmatrix}.$$

Hence ψ is a morphism from $((\mathbf{F}_p)^{2k}, Q_2)$ to $((\mathbf{F}_p)^{k'}, P(k'))$ in $\mathcal{E}$.

We need to divide into the cases $k \le q/3$ and $k \ge q/3$. In the former cases ϕ and ψ are injective and in the latter case they are surjective. In the former case we consider their cokernels, in the latter case their kernels.

The matrix B has size k by $q - 2k$. If B has rank k (which is only possible if $k \le q/3$) then ϕ and ψ are injective. If B has rank $q - 2k$ (which is only possible if $k \ge q/3$) then ϕ and ψ are surjective.

The matrix B contains a submatrix

$$\left(\binom{i+j+k}{i}\right)_{i,j=0}^{r-1}$$

where $r = \min(k, q-2k)$. This submatrix has determinant 1 (consider it as a matrix over $\mathbf{Z}$ and reduce it to a Vandermonde matrix or see for instance [2]). Thus B has rank r and indeed ϕ and ψ are injective for $k \le q/3$ and surjective for $k \ge q/3$.

Consider first the case where $k \le q/3$. Let (X_1, θ_1) and (X_2, θ_2) denote the cokernels of $\phi : ((\mathbf{F}_p)^{3k}, Q_1) \to ((\mathbf{F}_p)^q, P(q))$ and $\psi : ((\mathbf{F}_p)^{2k}, Q_2) \to ((\mathbf{F}_p)^{k'}, P(k'))$ in $\mathcal{E}$. Then

$$\chi((\mathbf{F}_p)^q, P(q), t) = \chi((\mathbf{F}_p)^{3k}, Q_1, t)\chi(X_1, \theta_1, t)$$

and

$$\chi((\mathbf{F}_p)^{k'}, P(k'), t) = \chi((\mathbf{F}_p)^{2k}, Q_2, t)\chi(X_2, \theta_2, t).$$

It is apparent that

$$\chi((\mathbf{F}_p)^{3k}, Q_1, t) = (t^3-1)^k$$

and

$$\chi((\mathbf{F}_p)^{2k}, Q_2, t) = \det(t^2 I + A^{-1}) = \det(t^2 I + A)$$

as A and A^{-1} are similar. Hence

$$\det(tI - P(q)) = (t^3-1)^k \chi(X_1, \theta_1, t)$$

and

$$\det(tI - P(k')) = \det(t^2 I + A)\chi(X_2, \theta_2, t).$$

It suffices to prove that (X_1, θ_1) and (X_2, θ_2) are isomorphic in $\mathcal{E}$.

As $\overline{D^t}$ is non-singular, it is apparent that X_1 is isomorphic to $(\mathbf{F}_p)^{q-2k}/Y$ where Y is the row space of B and that the action of θ_1 is induced by that of the matrix C on $(\mathbf{F}_p)^{q-2k}$. It is even more apparent that X_2 is isomorphic to $(\mathbf{F}_p)^{q-2k}/Y$ and that the action of θ_2 is induced by C. Hence (X_1, θ_1) and (X_2, θ_2) are isomorphic in $\mathcal{E}$. This completes the argument in the case $k \le q/3$.

Now suppose that $k \ge q/3$. Let (K_1, θ_1) and (K_2, θ_2) denote the kernels of ϕ : $((\mathbf{F}_p)^{3k}, Q_1) \to ((\mathbf{F}_p)^q, P(q))$ and $\psi : ((\mathbf{F}_p)^{2k}, Q_2) \to ((\mathbf{F}_p)^{k'}, P(k'))$ in $\mathcal{E}$. Then

$$\chi((\mathbf{F}_p)^q, P(q), t)\chi(K_1, \theta_1, t) = \chi((\mathbf{F}_p)^{3k}, Q_1, t)$$

and

$$\chi((\mathbf{F}_p)^{k'}, P(k'), t)\chi(K_2, \theta_2, t) = \chi((\mathbf{F}_p)^{2k}, Q_2, t).$$

Hence

$$\frac{(t^3-1)^k}{\det(tI - P(q))} = \chi(K_1, \theta_1, t)$$

and

$$\frac{\det(t^2 I + A)}{\det(tI - P(k'))} = \chi(K_2, \theta_2, t).$$

It suffices to prove that (K_1, θ_1) and (K_2, θ_2) are isomorphic in $\mathcal{E}$.

As $\overline{D^t}$ is non-singular and has inverse D^t, it is apparent that

$$K_1 = \{(-uA, u, -uDD^t) = (-uA, u, -uA^{-1}) : u \in (\mathbf{F}_p)^k, uB = 0\}$$

and we have

$$(-uA, u, -uA^{-1})Q_1 = (-uA^{-1}, -uA, u).$$

Also

$$K_2 = \{(-uA, u) : u \in (\mathbf{F}_p)^k, uB = 0\}$$

and

$$(-uA, u)Q_2 = (-uA^{-1}, -uA).$$

Hence the linear map

$$(-uA, u, -uA^{-1}) \longmapsto (-uA, u)$$

induces an isomorphism between (K_1, θ_1) and (K_2, θ_2). □

4. Proofs for the prime $p = 2$

Proof of Theorem 1.4. Set $n = 2^l - k$ and $q = 2^l$ where $1 \le k \le 2^{l-1}$.

Theorem 1.3 yields then over $\mathbf{F}_2$

$$\chi_n(t) = \chi_{q-k}(t) = (t^2 + t + 1)^{(q-\epsilon(q))/3-k}(t + 1)^{(q+2\epsilon(q))/3-k} \det(tI + P(k))^2$$

since $x \longmapsto x^2$ is the Frobenius automorphism in characteristic 2.

By induction on l, the only possible irreducible factors of $\det(tI(n) - P(n)) \pmod 2$ are $(1 + t)$ and $(1 + t + t^2)$. The multiplicity $\gamma(n) = \gamma(2^l - k)$ of the factor $(1 + t)$ in this polynomial is recursively defined by

$$\gamma(n) = \frac{2^l + 2(-1)^l}{3} - k + 2\gamma(k)$$

and coincides with the sequence γ of Theorem 1.4. The remaining factor of $\det(tI(n) - P(n)) \pmod 2$ is given by $(1+t+t^2)^{\gamma_2(n)}$ where $\gamma_2(n) = (1/2)(n-\gamma(n))$ and this proves the result. □

Proof of Theorem 1.5. We have for $0 \le k \le 2^{l-1}$

$$\begin{aligned}
\gamma(2^l + k) &= \gamma(2^{l+1} - (2^l - k)) \\
&= \frac{2^{l+1} - 2(-1)^l}{3} - 2^l + k + 2\gamma(2^l - k) \\
&= \frac{2^{l+1} - 2(-1)^l}{3} - 2^l + k + 2\frac{2^l + 2(-1)^l}{3} - 2k + 4\gamma(k)
\end{aligned}$$

which is assertion (i).

We have for all $2^{l-2} \leq k \leq 2^{l-1}$

$$\begin{aligned}\gamma(2^l - k) &= \frac{2^l + 2(-1)^l}{3} - k + \gamma(k) + \gamma(2^{l-1} - (2^{l-1} - k)) \\ &= \frac{2^l + 2(-1)^l}{3} - k + \gamma(k) + \frac{2^{l-1} - 2(-1)^l}{3} - 2^{l-1} \\ &\quad + k + 2\gamma(2^{l-1} - k) \\ &= \gamma(k) + 2\gamma(2^{l-1} - k)\end{aligned}$$

which proves assertion (ii).

Similarly, we have for $1 \leq k \leq 2^l$

$$\begin{aligned}\gamma(2^l + k) - \gamma(2^l + k - 1) &= \gamma(2^{l+1} - (2^l - k)) - \gamma(2^{l+1} - (2^l - k + 1)) \\ &= 1 + 2\gamma(2^l - k) - 2\gamma(2^l - k + 1)\end{aligned}$$

which proves assertion (iii).

Writing $2n = 2^l - 2k$ with $1 \leq k \leq 2^{l-2}$ we have, using induction on n,

$$\begin{aligned}\gamma(2^l - 2k) &= \frac{2^l + 2(-1)^l}{3} - 2k + 2\gamma(2k) \\ &= \frac{2^l + 2(-1)^l}{3} - 2k + 2(k - \gamma(k)) \\ &= (2^{l-1} - k) - \left(\frac{2^{l-1} + 2(-1)^{l-1}}{3} - k + 2\gamma(k)\right) \\ &= (2^{l-1} - k) - \gamma(2^{l-1} - k)\end{aligned}$$

which proves the first equality of assertion (iv) (this equality follows also from the fact that $P(2n)$ is the Kronecker product $P(n) \otimes P(2)$ of $P(n)$ with $P(2)$ over $\mathbf{F}_2$).

We prove the last two identities of assertion (iv) by simultaneous induction as follows: denote the second formula by A_n and the last formula by B_n. We prove first that the truth of B_m for all $m < n$ implies the truth of A_n. In a second step we establish the truth of B_n provided that the identities A_m hold for all $m < n$.

First step: The second identity (referred to by A_n) of assertion (iv) amounts to the equality

$$\gamma(2n - 1) - \gamma(2n) = \frac{4^{b(2n-1)} - 1}{3}.$$

Writing $2n = 2^l - 2k$ with $0 \leq k < 2^{l-2}$ and applying the recursive definition of $\gamma(2n)$ and $\gamma(2n - 1)$ together with identity B_k (which holds by induction) we get

$$\begin{aligned}\gamma(2n - 1) - \gamma(2n) &= \frac{2^l + 2(-1)^l}{3} - (2k + 1) + 2\gamma(2k + 1) \\ &\quad - \frac{2^l + 2(-1)^l}{3} + 2k - 2\gamma(2k)\end{aligned}$$

$$= -1 + 2(\gamma(2k+1) - \gamma(2k))$$
$$= -1 + 2\frac{2^{1+2b(k)}+1}{3} = \frac{4^{1+b(k)}-1}{3}.$$

Since $(2^l - (2k+1)) + 2k = 2^l - 1$ and since $2^l - (2k+1)$ is odd and greater than $2k$ the number of blocks of consecutive 1s in the binary expansion of $2^l - (2k+1)$ exceeds by 1 the number of blocks of consecutive 1s in the binary expansion of $2k$, and hence

$$b(2n-1) = b(2^l - (2k+1)) = b(2k) + 1 = b(k) + 1$$

which establishes the truth of A_n.

Second step: Identity B_n, the last identity of assertion (iv), is equivalent to

$$\gamma(2n+1) - \gamma(2n) = \frac{2^{1+2b(n)}+1}{3}.$$

Writing $2n+1 = 2^l + k$ with $1 \leq k < 2^l$ and applying assertion (iii) and identity $A_{(2^l-k+1)/2}$ (which holds by induction) we have

$$\gamma(2n+1) - \gamma(2n) = 1 + 2\gamma(2^l - k) - 2\gamma(2^l + 1 - k)$$
$$= 1 + 2\frac{4^{b(2^l-k)}-1}{3}$$
$$= \frac{2^{1+2b(2^l-k)}+1}{3}.$$

Since $(2^l + k - 1) + (2^l - k) = 2^{l+1} - 1$ and since $2^l + k - 1$ is even and greater than $2^l - k$, they have the same number of blocks of consecutive 1s in their binary expansions. This shows $b(2^l - k) = b(2n) = b(n)$ and establishes the truth of B_n. □

Acknowledgements

The first author wishes to thank J.-P. Allouche, F. Sigrist, U. Vishne and A. Wassermann for interesting comments and remarks and support from the Swiss National Science Foundation is gratefully acknowledged.

References

[1] J.-P. Allouche, J. Shallit, The ubiquitous Prouhet-Thue–Morse sequence, in: C. Ding, T. Helleseth, H. Niederreiter (Eds.), Proceedings of SETA 98, Springer, 1999.

[2] R. Bacher, Determinants of matrices related to the Pascal triangle, J. Théor. des Nombres Bordeaux 14 (2002) 19–41.

[3] C. Krattenthaler, Advanced determinant calculus, Sém. Lothar. Combin. 42 B42q (1999) 67.

[4] W.F. Lunnon, The Pascal matrix, Fibonacci Quart. 15 (1977) 201–204.