Symmetric Pascal matrices modulo p

Roland Bacher*and Robin Chapman

December 11, 2002

fichier pascalmod.tex dans recherche/binmod2

1 Introduction

This paper deals with symmetric matrices associated to Pascal's triangle. More precisely, we consider the matrix $P(n)$ with coefficients

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

We call $P(n)$ the *symmetric Pascal matrix* of order n. An easy computation yields $P(\infty) = T\,T^t$ 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 $n \in \mathbf{N}$. It implies furthermore that the characteristic polynomial $\det(tI(n) - P(n)) = \sum_{k=0} \alpha_k t^k$ (where $I(n)$ denotes the identity matrix of order n) of $P(n)$ has only positive real roots. The inverse $P(n)^{-1}$ of $P(n)$ is given by

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

where $T(n)^{-1}$ has coefficients $(-1)^{i+j}\binom{i}{j},\ 0 \leq i,j < n$ and is conjugate to $T(n)$. The matrices $P(n)$ and $P(n)^{-1}$ are hence conjugate and have the same characteristic polynomial. The coefficients α_k of $\det(tI(n) - P(n))$ satisfy therefore $\alpha_{n-k} = (-1)^n \alpha_k$ and 1 is hence always an eigenvalue of $P(2n+1)$, cf. [3].

*Support from the Swiss National Science Foundation is gratefully acknowledged.

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

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

The Thue-Morse sequence $s_n = \sum \nu_i \pmod 2$ counts the parity of all non-zero digits of a binary integer $n = \sum \nu_i 2^i$. 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]).

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

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

A similar result holds for the reduction $\pmod 3$ of $P(n)$ with values in $\{-1,0,1\}$.

Proposition 1.1 *Given a power* $q = p^l$ *of a prime* p*, the matrix* $P(q)$ *is of order* 3 *over* $\mathbf{Z}/p\mathbf{Z}$*. Its characteristic polynomial* $\det(tI(q) - P(q))$ *over the finite field* $\mathbf{F}_p$ *is given by*

$$\det(tI(q) - P(q)) = (t^2 + t + 1)^{\frac{q-\epsilon(q)}{3}} (t-1)^{\frac{q+2\epsilon(q)}{3}} \pmod p$$

where $\epsilon(q) \in \{-1,0,1\}$ *satisfies* $\epsilon(q) \equiv q \pmod 3$*. In particular,* $P(q)$ *can be diagonalised over* $\mathbf{F}_{p^2}$ *except for* $p = 3$ *where* $P(3)$ *for instance has a unique Jordan block.*

This proposition (except for the diagonalisation part) admits the following generalisation:

Theorem 1.2 *We have for any power* $q = p^l$ *of a prime* p *and any natural number* $0 \le k \le q/2$ *the equality*

$$\det(tI(q-k) - P(q-k)) =$$

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

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

For $p = 2$ the formulas of Theorem 1.2 define the reduction modulo 2 of the characteristic polynomial of $P(n)$ for all n as follows: Define a sequence $\gamma(0) = 0, \gamma(1), \ldots$ recursively by

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

Theorem 1.3 *We have for all* $n \in \mathbf{N}$

$$\det(P(n) - xI(n)) \equiv (1+x)^{\gamma(n)}(1+x+x^2)^{\gamma_2(n)} \pmod 2$$

where $\gamma_2(n) = \frac{n-\gamma(n)}{2}$.

It follows immediately that the matrix $P(n)^3 - I(n)$ is nilpotent over $\mathbf{Z}/2\mathbf{Z}$ for all $n \in \mathbf{N}$.

The first terms $\gamma(1), \ldots, \gamma(48)$ and $\gamma_2(1), \ldots, \gamma_2(48)$ 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 adjacent ones in the binary representation 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 1.4 *(i) We have* $0 \leq \gamma(n) \leq n$.

(ii) We have

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

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

(iii) We have for all $n \in \mathbf{N}$ *and* $2^{l-2} \leq k \leq 2^{l-1}$

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

(iv) We have

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

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

(v) We have

$$\begin{aligned} \gamma(2n) &= n - \gamma(n) \ , \\ \gamma(2n-1) &= \gamma(2n) + \tfrac{4^{b(2n-1)}-1}{3} = n - \gamma(n) + \tfrac{4^{b(2n-1)}-1}{3} \ , \\ \gamma(2n+1) &= \gamma(2n) + \tfrac{2^{1+2b(n)}+1}{3} = n - \gamma(n) + \tfrac{2^{1+2b(n)}+1}{3} \ . \end{aligned}$$

Let us also remark that matrices with coefficients $\binom{i+j}{i}-1,\ 1\le i,j\le n$ and matrices with coefficients $\binom{i+j+s+t}{i+s},\ 0\le i,j,\ t\in\{0,1\},\ s\in\mathbf{N}$ seem also to behave in interesting ways over $\mathbf{F}_2$.

Theorem 1.2 seems to have many conjectural generalisations, the first of which is given by the following:

Conjecture 1.1 *For $0\le k\le q/2$ (with $q=p^l$ a prime power) there exist integral monic polynomials $c_k(t)=\sum_{j=0}^{4k}\gamma_{j,k}t^j$ of degree $4k$ with palindromic coefficients ($\gamma_{j,k}=\gamma_{4k-j,k}$) such that*

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

over $\mathbf{F}_p$ with $\epsilon(q)\in\{-1,0,1\}$ satisfying $\epsilon(q)\equiv q \pmod 3$.

The first five polynomials $c_k(t)$ seem to be given by

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

These polynomials seem to satisfy many intriguing identities, especially at roots of unity of order $1,2,3$ or 6 (cf. also Theorems 32 and 35 in [2]).

For $p=2$, it follows from Theorem 1.3 and assertion (ii) in Theorem 1.4 that we have

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

(assuming existence of the polynomials $c_k(t)$).

Computations suggest:

Conjecture 1.2 *We have for $0\le k<\frac{3^l}{2}$*

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

This conjecture, together with Theorem 1.1 yields conjectural recursive formulas for $p_n(t)=\det(tI(n)-P(n)) \pmod 3$ as follows: Set $p_0(t)=1 \pmod 3$, $p_0(t)=1-t \pmod 3$. For $n=3^l\pm k>1$ with $0\le k<\frac{3^l}{2}$ the characteristic polynomial $\det(t(n)-P(n)) \pmod 3$ is then conjecturally given by

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

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

Formulas similar (but more involved) to those appearing in Theorem 1.2 and Conjecture 1.1 seem also to exist for $n = ap^l \pm k$, with a and k small.

Also, for $q = p^l$ an odd prime power, only factors of the form $(t \pm 1)$, (t^2+1) and (t^2-t+1) show up in $\det(tI((q\pm 1)/2) - P((q\pm 1)/2))$ with multiplicities depending in a very simple way of $q \pmod{12}$ (these two characteristic polynomials are of course related by Theorem 1.2).

We conclude finally by mentionning a last conjectural observation:

Conjecture 1.3 *Given a prime-power $q = p^l \equiv 2 \pmod 3$, we have*

$$\det(tI(\frac{q+1}{3}) - P(\frac{q+1}{3})) = (t+1)^{(q+1)/3} \pmod p$$

and

$$\det(tI(\frac{2q-1}{3}) - P(\frac{2q-1}{3})) = (t+1)^{(q+1)/3}\ (t-1)^{(q-2)/3}$$

Remark 1.1 *(i) The matrix $C = P(\frac{q+1}{3}) + I(\frac{q+1}{3})$ for $q = p^l \equiv 2 \pmod 3$ a prime-power, seems to have a unique Jordan block of maximal length. For p odd, the rows of $C^{(q+1)/6}$ generate hence a self-dual code over $\mathbf{F}_p$.*

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

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

satisfies then conjecturally also $\tilde{\chi}(t) \equiv (1+t)^n \pmod p$.

The sequel of this paper is organized as follows:

Section 2 is devoted to auto-similar matrices. Such matrices generalise the matrix $\overline{P}(\infty)_2$ and their study implies easily Theorem 1.1.

Section 3 contains a proof of Proposition 1.1 and Theorem 1.2.

Section 4 contains a proof of Theorem 1.3 and 1.4.

2 Autosimilar matrices

Let $b \ge 1$ be a natural integer. An infinite matrix M with coefficients $m_{i,j},\ 0 \le i,j \in \mathbf{N}$ 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, i.e. $\sigma_i, \tau_i \in \{0,\ldots,b-1\}$ for all $i = 0,1,2,\ldots$.

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 $n = 2, \ldots, b$.

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 2.1 *Given a non-degenerate $b-$autosimilar matrix M one has*

$$\det(M(n)) = \prod_{i=0}^{n-1} d_{\nu_i}$$

for all $n = \sum \nu_i b^i$ with $d_0 = 1$ and

$$d_k = \det(M(k+1))/\det(M(k))$$

for $k = 1, \ldots, b-1$.

Remark 2.1 *(i) The set of all unipotent lower-triangular (or upper-triangular) matrices over a given commutative ring (with unit) is a group.*

One can in general compute determinants of arbitrary $b-$autosimilar matrices by applying Corollary 2.1 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 suitable matrix) and by working over the ring of fractions in t.

Proof of Theorem 2.1. Genericity of M implies that we have

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

with $L(b), U(b)$ suitable unipotent upper and lower triangular matrices and with $D(b)$ diagonal having entries $d_{0,0} = 1$ and $d_{k,k} = \det(M(k+1))/\det(M(k))$

for $k = 1, \ldots, b-1$. Extending $L(b), D(b)$ and $U(b)$ in the unique possible way to infinite $b-$autosimilar matrices L, D and U we have

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

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

The identity

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

implies of course immediately Corollary 2.1.

2.1 Binomial coefficients modulo a prime p

Let p be a prime number. We have then

$$(1+x)^n = \prod (1+x)^{\nu_i p^i} \equiv (1+x^{p^i})^{\nu_i} \pmod p$$

(using properties of the Frobenius automorphism in characteristic p). This implies immediately the equality

$$\binom{n}{k} = \prod_i \binom{\nu_i}{\kappa_i}$$

allowing (for small primes) an efficient computation of binomial coefficients (mod p).

This equality shows that the reductions modulo 2 or 3 of the symmetric Pascal triangle P with coefficients

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

respectively

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

are $2-$ (respectively $3-$) autosimilar matrices.

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 2.1 implies now Theorem 1.1.

Remark 2.2 *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.

3 Proof of Proposition 1.1 and Theorem 1.2

Proof of Proposition 1.1 Let R be a commutative ring

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

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

Let us now compute the multiplicities of the three eigenvalues of $P = P(p) \pmod p$ over $\mathbf{F}_p$ (the formula for $P(p^l)$ is then a straightforward consequence of the fact the $P(p^l)$ is the $l-$fold Kronecker product of $P(p)$ with itself).

The easy identity $\binom{2k}{k} = \binom{(p-1)/2}{k}(-4)^k \pmod p$ for p an odd prime and $0 \leq k \leq (p-1)/2$ 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 $\mathrm{tr}(P) \equiv \epsilon(p) \pmod p$ where $\epsilon(p) \in \{-1, 0, 1\}$ satisfies $\epsilon(p) \equiv p \pmod 3$.

Since the characteristic polynomial for P has antisymmetric coefficients ($\alpha_k = -\alpha_{p-k}$) the two eigenvalues $\neq 1$ of P have equal multiplicity α. Lifting into positive integers $\leq \frac{p-1}{2}$ a solution of the linear system $-\alpha + (p - 2\alpha) = \mathrm{tr}(P)$ yields now the result.

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

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*

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

and $X^{(n)}$ *for* $X \in GL_2(\mathbf{F}_p)$ *acts in the obvious way by linear substitutions on homogeneous polynomials of degree* $n-1$ *in* $\mathbf{F}_p[x, y]$.

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 $0 \leq i, j < n$.

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.*

The group G_p *generated by* P *and* L *depends on the prime* p *(but not on the power* l *of* $n = p^l$*). It is isomorphic to a subgroup of* $PGL_2(\mathbf{F}_p)$. *For all but finitely many primes* p, G_p *is isomorphic to* $PSL_2(\mathbf{F}_p)$ *or* $PGL_2(\mathbf{F}_p)$ *according to whether* -1 *is or is not a square in* $\mathbf{F}_p$. *The exceptional primes are* 5, 7 *and* 29 *where* G_p *has of order* 24, 42 *and* 120 *respectively.*

Proof of Theorem 1.2 Using Proposition 1.1, 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 $\phi \circ \alpha = \beta \circ \phi$. 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 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 up 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°. 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 $V = (\mathbf{F}_p)^q$ and $X = (\mathbf{F}_p)^{3k}$. Let

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

Let $\phi : X \to V$ 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 $W = (\mathbf{F}_p)^{k'}$ and $Y = (\mathbf{F}_p)^{2k}$. Let

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

Let $\psi : Y \to W$ 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 $k \leq q/3$ and $k \geq q/3$. 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 $k \leq q/3$) then ϕ and ψ are injective. If B has rank $q-2k$ (which is only possible if $k \geq q/3$) 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). Thus B has rank r and indeed ϕ and ψ are injective for $k \leq q/3$ and surjective for $k \geq q/3$.

Consider first the case where $k \leq q/3$. Let (X_1, θ_1) and (X_2, θ_2) denote the cokernels of $\phi : ((\mathbf{F}_p)^{3k}, Q_1) \to ((\mathbf{F}_p)^q, P(k'))$ 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 nonsingular, 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 $k \leq q/3$.

Now suppose that $k \geq q/3$. Let (K_1, θ_1) and (K_2, θ_2) denote the kernels 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

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

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 nonsingular and has inverse D^t, it is apparent that

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

Also

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

Now

$$(-uA, u, -uA^{-1})P(q) = (x, -uAB + uC, y)$$

for some vectors x and y. But from $P(q)^2 = \overline{P(q)}$ we get $AB + BC = 0$ and so

$$-uAB + uC = uBC + uC = uC$$

as $uB = 0$. Hence $(-uA, u, -uA^{-1})P(q) = (x, uC, y)$. Also

$$(-uA, u)P(k') = (z, -uAB + uC) = (z, uBC + uC) = (z, uC)$$

for some vector z. Thus (K_1, θ_1) and (K_2, θ_2) are both isomorphic to (Z, ω) where $Z = \{u \in (\mathbf{F}_p)^k : uB = 0\}$ and ω is induced by the matrix C. This completes the argument in the case $k \leq q/3$. □

4 Proofs for the prime $p = 2$

Proof of Theorem 1.3. Set $n = 2^l - k$ and $q = 2^l$ where $1 \leq k \leq 2^{l-1}$.

Theorem 1.2 yields then over $\mathbf{F}_2$

$$\det(tI(n) - P(n)) = \det(tI(q-k) - P(q-k)) =$$

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

since $x \longmapsto x^2$ is an 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 $\mu(n) = \mu(2^l - k)$ of the factor $(1+t)$ in this polynomial is hence recursively defined by

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

and coincides hence with the sequence γ of Theorem 1.3. The remaining factor of $\det(tI(n) - P(n)) \pmod 2$ is hence given by $(1+t+t^2)^{\gamma_2(n)}$ where $\gamma_2(n) = \frac{n-\gamma(n)}{2}$ and this proves the result. □

Proof of Theorem 1.4. Assertion (i) is of course obvious since $\gamma(n)$ counts the multiplicity of a root in a polynomial of degree n.

We have for $0 \leq k \leq 2^{l-1}$

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

which is assertion (ii).

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

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

which proves assertion (iii).

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 (iv).

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

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

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

The second identity of assertion (v) amounts to the equality

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

We prove first by induction on n that this identity is equivalent to the last one.

The last identity and induction yield

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

We now divide into cases according to the parity of n.

Suppose first that $n = 2m$ is even. Then inductively

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

Hence

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

But

$$2^{2b(n-1)} = 4^{b(n-1)} = 4^{b(2n-1)}$$

as the binary representation of $n-1$ ends in 1 and that of $2n-1$ is obtained by appending 1.

Now suppose that $n = 2m+1$ is odd. Then

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

Hence

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

But

$$2^{2+2b(n-1)} = 4^{1+b(n-1)} = 4^{b(2n-1)}$$

as the binary representation of $n-1$ ends in 0 and that of $2n-1$ is obtained by appending 1.

This completes the proof of equivalence of the two last identities in assertion (v).

We prove now the last identity by induction on n.

The last identity of assertion (v) is equivalent to

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

Writing $2n+1 = 2^l+k$ with $1 \le k < 2^l$ and applying assertion (iv) and the second identity of assertion (v) (which holds by induction) we have

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

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 $1\ldots1$ in their binary expansion. This shows $b(2^l-k) = b(2n) = b(n)$ and establishes the last identity of assertion (v). □

The first author wishes to thank J-P. Allouche, F. Sigrist, U. Vishne and A. Wassermann for interesting comments and remarks.

References

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

[2] C. Krattenthaler, *Advanced Determinant Calculus*, Sémin. Lothar. Comb. 42, B42q, 67 pages.

[3] W. F. Lunnon, *The Pascal matrix*, Fib. Quart. vol. 15 (1977), 201-204.

Roland Bacher, Institut Fourier, UMR 5582, Laboratoire de Mathématiques, BP 74, 38402 St. Martin d'Hères Cedex, France, Roland.Bacher@ujf-grenoble.fr

Robin Chapman, University of Exeter, School of Mathematical Sciences, North Park Road, EX4 4QE Exeter, UK, rjc@maths.ex.ac.uk