SYMMETRIC NILPOTENT MATRICES WITH MAXIMAL RANK
AND A CONJECTURE OF GROTHENDIECK-KOBLITZ

CHING-LI CHAI
APPENDIX BY MICHAEL LARSEN

(Communicated by Maurice Auslander)

Abstract. All pairs \((p, n)\) such that there exists an \(n \times n\) symmetric matrix \(A\) with entries in the ring \(\mathbb{Z}_p\) of \(p\)-adic integers such that \(A^n = p \cdot U\) with \(U\) invertible in \(M_{n \times n}(\mathbb{Z}_p)\) are determined. It is shown that such matrices \(A\) can be used to construct examples of deformations of abelian varieties.

While contemplating the converse of Grothendieck’s specialization theorem for the Newton polygon of \(p\)-divisible groups and abelian varieties (cf. [G]), I chanced upon the following question in linear algebra.

Q. For which integer \(n\) and prime number \(p\) does there exist an \(n \times n\) symmetric matrix \(A\) with entries in the ring \(\mathbb{Z}_p\) of \(p\)-adic integers such that \(A^n = p \cdot U\) with \(U\) invertible in \(M_{n \times n}(\mathbb{Z}_p)\) ?

It turns out that this seemingly innocuous question has an interesting answer, at least when \(p\) is an odd prime, which we would like to share with the reader. The connection with Koblitz’s conjecture will also be discussed. When \(p = 2\), M. Larsen proved that the answer is always affirmative. It is a pleasure to thank him for writing up his solution as an appendix.

First note that when \(p \neq 2\), the question above has an equivalent formulation:

Q’. For which integer \(n\) and prime number \(p\) does there exist an \(n \times n\) symmetric matrix \(A\) with entries in the prime field \(\mathbb{F}_p\) such that \(A\) is nilpotent and has rank \(n - 1\) ?

The equivalence follows from Hensel’s lemma and an easy derivative calculation:

\[
d(\det(x_{ij})_{1 \leq i, j \leq n}) = \sum_{1 \leq i, j \leq n} A_{ij} \frac{d}{dx_{ij}}
\]

(where \(A_{ij}\) is the \((i, j)\)th cofactor)

\[
= \sum_{1 \leq i \leq n} A_{ii} \frac{d}{dx_{ii}} + 2 \sum_{1 \leq i < j \leq n} A_{ij} \frac{d}{dx_{ij}}
\]

Received by the editors July 31, 1990 and, in revised form, February 5, 1992.

1991 Mathematics Subject Classification. Primary 14K10, 14D10.

The author is partially supported by a grant from NSF.
if we impose the symmetry condition that \( x_{ij} = x_{ji} \) \( \forall 1 \leq i, j \leq n \).

We shall first work out the geometry of symmetric nilpotent matrices with maximal rank. Since the prime 2 causes problems at several places, a familiar phenomenon, we shall restrict ourselves to fields of characteristic \( \neq 2 \). Thus we fix a field \( k \) with \( \text{char}(k) \neq 2 \), a positive integer \( n \), and let \( V = V_n \) be the variety over \( k \) such that \( V(F) = \) the set of all symmetric \( n \times n \) matrices of rank \( n - 1 \) with entries in \( F \), for any field \( F \) over \( k \). The above calculation says that \( V \) is smooth over \( k \). \( V \) has lots of symmetries: the orthogonal group \( O_n \) (for the standard form) operates on \( V \) by \( g: A \mapsto gAg^{-1} = gA^t g \), \( \forall g \in O_n \), \( \forall A \in V \).

**Examples.** (i) When \( n = 2 \),

\[
V_2 = \left\{ \begin{bmatrix} a & b \\ b & -a \end{bmatrix} : a^2 + b^2 = 0, a \neq 0, b \neq 0 \right\};
\]
hence, \( V(\mathbb{F}_p) \neq \emptyset \) iff \( p \equiv 1 \pmod{4} \).

(ii) When \( n = 3 \), the rational point

\[
\begin{bmatrix}
1 & \sqrt{-1} & 1 \\
\sqrt{-1} & -1 & \sqrt{-1} \\
1 & \sqrt{-1} & 0
\end{bmatrix}
\]
in \( V_3(\mathbb{Q}(\sqrt{-1})) \) shows that \( V_3(\mathbb{F}_p) \neq \emptyset \) if \( p \equiv 1 \pmod{4} \).

(iii) When \( n = 3 \) and \( p = 3 \), \( V_3(\mathbb{F}_3) \neq \emptyset \) since

\[
\begin{bmatrix}
0 & 1 & -1 \\
1 & -1 & 0 \\
-1 & 0 & 1
\end{bmatrix}
\]
is a rational point in \( V_3(\mathbb{F}_3) \).

The following lemma is very useful.

**Lemma.** For any field \( F \) over \( k \) and any \( A \) in \( V(F) \), the commutator of \( A \) inside \( M_{n \times n}(F) \) is just \( F[A] = F + FA + FA^2 + \cdots + FA^{n-1} \), which as an \( F \)-algebra is isomorphic to \( F[x]/(x^n) \).

**Proof.** We shall prove this statement for any nilpotent matrix \( B \) of maximal rank. Hence we can assume that \( B \) is already in the canonical form with 1’s below the diagonal. The proof is finished by a direct computation.

Psychologically the first thing we want to know about \( V \) is that it is not empty. Thus let \( N \) be the nilpotent \( n \times n \) matrix with 1’s below the diagonal; we want to find some \( g \in \text{GL}(k) \) such that \( gNg^{-1} \) is symmetric. Clearly \( gNg^{-1} = g^{-1}Ngg \leftrightarrow gNg = gN^t gg \). We know that (by Witt’s theorem) \( g \mapsto gNg^{-1} \) establishes an isomorphism \( O_n \setminus \text{GL}_n \approx Z_n \) since \( \text{char}(k) \neq 2 \), where \( Z_n \) is the variety of all invertible symmetric \( n \times n \) matrices. Hence we are reduced to finding a symmetric invertible matrix \( X \) such that \( XN = XN^t \).

By explicit computation, the necessary and sufficient condition for a symmetric
matrix $Y$ to satisfy $YN = 'NY$ is that $Y$ has the form

$$
\begin{bmatrix}
    a_n & a_{n-1} & \cdots & a_2 & a_1 \\
    a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 & 0 \\
    a_{n-2} & \cdots & a_2 & a_1 & 0 & 0 \\
    \ddots & \cdots & \cdots & \cdots & \cdots & \cdots \\
    a_2 & a_1 & 0 & \cdots & \cdots & \cdots \\
    a_1 & 0 & 0 & \cdots & \cdots & \cdots 
\end{bmatrix}
$$

and the condition for such a $Y$ to be invertible is that the antidiagonal entries (all equal to $a_1$) are invertible. In particular, such $Y$'s surely exist. Note that the above analysis also gives an explicit way to construct points in $V$: one just has to extract a "square root" for an invertible $Y$ as above.

Next we show that $O_n$ operates transitively on $V$. Thus let $A_1$, $A_2$ be elements of $V(\overline{k})$; there exists (by the theory of canonical forms) an element $g \in \text{GL}_n(\overline{k})$ such that $gA_1g^{-1} = A_2$, and we want to show that there exists a $g_1 \in O_n(\overline{k})$ such that $g_1A_1g_1^{-1} = A_2$. We have $gA_1g^{-1} = A_2 \Rightarrow gA_1 = A_2g$, $A_1^tg = t^tgA_2 \Rightarrow t^tgA_1 = t^tgA_2g = A_1^tgg$; hence by the lemma we know that $t^tg \in \overline{k}[A_1]^\times$. Since char($k$) $\neq 2$ and $A_1$ is nilpotent, there exists an $h \in \overline{k}[A_1]^\times$ such that $t^tg = h^2$. (A trivial case of Hensel's lemma, since $\overline{k}[A_1] \approx \overline{k}[x]/(x^n)$.) Let $g_1 = gh^{-1}$. We have $t^tg_1 = h^{-1}t^tggh^{-1} = h^{-1}h^2h^{-1} = 1$ since $h$ is symmetric (as in $A_1$); hence, $g_1 \in O_n(\overline{k})$, and clearly $g_1A_1g_1^{-1} = gA_1g^{-1} = A_2$.

Finally let us pick and fix $A_0 \in V(\overline{k})$. We want to find its stabilizer in $O_n$. Suppose $gA_0g^{-1} = A_0$. By the lemma we know that $g \in \overline{k}[A_0]^\times$; hence, $1 = t^tg = g^2$. Since char($k$) $\neq 2$, we conclude that $g = \pm 1$ again because $\overline{k}[A_0] \approx \overline{k}[x]/(x^n)$. So we have proved:

**Proposition 1.** $V_n$ is a principal homogeneous space for $PO_n = O_n/\{\pm 1\}$ over $k$. Therefore $V_n$ is a principal homogeneous space for $SO_n$ if $n$ is odd, while $V_n$ has two geometric components if $n$ is even.

Now we take $k = \mathbb{F}_p$ ($p \neq 2$). If $n$ is odd, we conclude that $V$ has an $\mathbb{F}_p$-rational point by Lang's theorem. (Every principal homogeneous space for a connected algebraic group over a finite field is trivial, see [La].) If $n = 2m$ is even, again by Lang's theorem we see that $V(\mathbb{F}_p) \neq \emptyset$ iff both geometric components of $V$ are defined over $\mathbb{F}_p$; hence, we must compute the Galois action on the geometric components of $V$. This can be done by constructing rational points over a quadratic extension of $k$, as explained in the first part of the proof of Proposition 1. If we take the $Y$ there to be

$$
Y_0 = \begin{bmatrix}
0 & 0 & \cdots & 0 & 0 & 2 \\
0 & 0 & \cdots & 0 & 2 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
2 & 0 & \cdots & 0 & 0 & 0
\end{bmatrix}
$$

we have to find a $g_0 \in \text{GL}_n$ such that $t^tg_0g_0^{-1} = Y_0$. Any such $g_0$ produces a point $g_0N^g_0^{-1} \in V(\overline{k})$ by the first paragraph in the proof of Proposition 1.

Taking $k$ to be $\mathbb{Q}$, we have

$$
\begin{bmatrix}
1 & -\sqrt{-1} \\
1 & \sqrt{-1}
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
-\sqrt{-1} & \sqrt{-1}
\end{bmatrix} = 
\begin{bmatrix}
0 & 2 \\
2 & 0
\end{bmatrix}.
$$
So we can take \( g_0 \) to be

\[
\begin{bmatrix}
I_m & J_m \\
-\sqrt{-1}J_m & \sqrt{-1}I_m
\end{bmatrix},
\]

where \( J_m \) denotes the \( m \times m \) matrix with 1's on the antidiagonal and 0's elsewhere and \( g_0N_{g_0}^{-1} \in V(\mathbb{Q}(\sqrt{-1})) \). If \( \text{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) = \{\text{id}, \tau\} \), then

\[
g_0^\tau = \begin{bmatrix}
I_m & 0 \\
0 & -I_m
\end{bmatrix} \cdot g_0.
\]

Since

\[
\det\left(\begin{bmatrix}
I_m & 0 \\
0 & -I_m
\end{bmatrix}\right) = (-1)^m,
\]

we see that \( \tau \) operates on the two geometric components of \( V/\mathbb{Q} \) by \((-1)^m\), i.e., \( \tau \) stabilizes both geometric components if \( n \equiv 0 \pmod{4} \), and \( \tau \) interchanges them if \( n \equiv 2 \pmod{4} \). From the splitting behavior of primes in \( \mathbb{Q}(\sqrt{-1})/\mathbb{Q} \), we conclude:

**Proposition 2.** Suppose \( n \) is even and \( p \) is an odd prime number. Then

(i) if \( n \equiv 0 \pmod{4} \) or \( p \equiv 1 \pmod{4} \), then each geometric component of \( V_n/\mathbb{F}_p \) is defined over \( \mathbb{F}_p \) and is a principal homogeneous space under \( \text{PSO}_n = \text{SO}_n/\{\pm 1\} \);

(ii) if \( n \equiv 2 \pmod{4} \) and \( p \equiv 3 \pmod{4} \), then the Frobenius interchanges the two geometric components of \( V_n/\mathbb{F}_p \).

We summarize our results as

**Theorem.** Let \( p \) be an odd prime number and \( n \) a positive integer. Then

\( V_n(\mathbb{F}_p) = \emptyset \) iff \( p \equiv 3 \pmod{4} \) and \( n \equiv 2 \pmod{4} \). Therefore there exists a symmetric \( n \times n \) matrix with entries in \( \mathbb{Z}_p \) whose \( n \)th power is equal to \( p \) times a unit in \( \mathbb{M}_{n \times n}(\mathbb{Z}_p) \) iff \( p \equiv 1 \pmod{4} \) or \( n \equiv 0, 1, \text{ or } 3 \pmod{4} \).

**Remark.** Let \( W = W_n \) be the variety of all symmetric \( n \times n \) matrices. \( \text{O}_n \) operates on \( W \) and \( V \) is contained in the null cone. As the referee pointed out, the ring of invariants of \( \text{O}_n \) operating on \( W \) is a polynomial ring with the coefficients of the characteristic polynomials as generators, at least in characteristic 0. This implies that the null cone has a beautiful structure.

We now turn to discuss the connection with a conjecture of Grothendieck-Koblitz (cf. [Ko]), which states that if \( NP_1, \ldots, NP_m \) is a sequence of Newton polygons with the same end points such that \( NP_{i+1} \) lies above \( NP_i \) for each \( i \), then this sequence can be realized by successive specialization of principally polarized varieties in characteristic \( p > 0 \). To the best of my knowledge, this conjecture is still open and so is the case for Barsotti-Tate groups.\(^1\) Here we shall give some examples such that all slopes of \( NP_m \) are \( \frac{1}{2} \) (this is not a restriction because this \( NP_m \) is the highest possible Newton polygon), by deforming a product of supersingular elliptic curves. We shall not try to state our result in the ultimate generality; rather we only present our calculation as a way to construct some example of deformations.

Let \( k \) be an algebraically closed field of characteristic \( p > 0 \), and let \( M_0 \) be the Dieudonné module of a product of \( r \) copies of supersingular elliptic curves.

\(^1\)Shortly after this paper was submitted, this conjecture was proved by F. Oort. A preliminary note of his important result is available and titled *Moduli of abelian varieties and Newton polygons*.
In other words, $M_0$ has a free $W(k)$ basis $x_1, \ldots, x_r, y_1, \ldots, y_r$, and the Frobenius and Verschubung send $x_i$ to $y_j$: $Fx_i = y_i = Vx_i$, $1 \leq i \leq r$. The product polarization corresponds to the symplectic pairing having $x_1, \ldots, x_r, y_1, \ldots, y_r$ as a symplectic basis: $\langle x_i, y_j \rangle = \delta_{ij}$. Using the Cartier-Dieudonné theory, a general deformation of $M_0$ over a complete local ring $R$ over $k$ can be given as follows:

$$Fx_i = \sum T_{ij}x_j + y_i, \quad Vx_i = y_i, \quad 1 \leq i \leq r,$$

where $T_{ij} = [t_{ij}] = (t_{ij}, 0, 0, \ldots)$ is the Teichmüller representative of $t_{ij}$ in the ring of infinite Witt vectors $W(R)$, $t_{ij} \in R$, $1 \leq i, j \leq r$. If we write $F$ in block form, its entries are $T, pI_r, I_r, 0$, where $T = (T_{ij})$. If we take polarization into account and want the product polarization to extend to the deformation, we must require that $t_{ij} = t_{ji}$, $1 \leq i, j \leq r$. In practice, we shall choose $R$ to be a formal power series ring (possibly with several variables), and we want to estimate the slope of the deformation over the fraction field of $R$. One way to do this is to use the result in [Ka], which requires some information about iteration of Frobenius.

We shall write the $n$th iteration $F^n$ of $F$ in block form with entries $A^{(n)}$, $B^{(n)}$, $C^{(n)}$, $D^{(n)}$. Let us first see some examples:

$n = 2$: $A^{(2)} = TT^\sigma + p$, $B^{(2)} = pT$, $C^{(2)} = T^\sigma$, $D^{(2)} = p$, where $\sigma$ denotes the Frobenius automorphism on $W(R)$.

$n = 3$: $A^{(3)} = TT^\sigma T^\sigma + pT^2 + pT$, $B^{(3)} = pTT^\sigma + p^2$,

$$C^{(3)} = T^\sigma T^2 + p, \quad D^{(3)} = pT^\sigma.$$

$n = 4$: $A^{(4)} = TT^\sigma T^\sigma T^\sigma + pT^2 T^\sigma + pT T^3 + pTT^\sigma + p^2$,

$$B^{(4)} = pTT^\sigma T^3 + p^2 T^2 T^\sigma + p^2 T,$$

$$C^{(4)} = T^\sigma T^2 T^3 + pT^\sigma + pT^3, \quad D^{(4)} = pTT^\sigma T^3 + p^2.$$

$n = 5$: $A^{(5)} = TT^\sigma T^\sigma T^\sigma T^4 + pT^2 T^\sigma T^3 T^4 + pTT^\sigma T^4 + pTT^\sigma T^4$

$$+ pT^2 T^3 T^4 + p^2 T^4 + p^2 T^3 + p^2 T,$$

$$B^{(5)} = pTT^\sigma T^2 T^3 + p^2 T^2 T^3 + p^2 TT^\sigma + p^2 + p^3,$$

$$C^{(5)} = T^\sigma T^2 T^3 T^4 + pT^\sigma T^4 + pT^\sigma T^4 + pTT^\sigma T^4 + p^2 T^4 + p^2 T^3 + p^2 + p^3,$$

$$D^{(5)} = pT^\sigma T^2 T^3 + p^2 T^3 + p^2 T^2.$$

$n = 6$: $A^{(6)} = TT^\sigma T^\sigma T^\sigma T^5 + pT^2 T^\sigma T^3 T^4 T^4 + pTT^\sigma T^4 T^4$

$$+ pTT^\sigma T^4 T^5 + pTT^\sigma T^5 T^3 + pTT^\sigma T^3 T^3 + p^2 T^4 T^3 + p^2 T^3 T^4$

$$+ p^2 T^2 T^4 + p^2 TT^\sigma + p^2 T^2 T^3 + p^2 TT^\sigma + p^2 + p^3,$$

$$B^{(6)} = pTT^\sigma T^2 T^3 T^4 + p^2 T^2 T^3 T^4 + p^2 TT^\sigma T^4 + p^2 TT^\sigma T^4$

$$+ p^2 TT^\sigma T^2 + p^3 T^4 + p^3 T^2 + p^3 T,$$

$$C^{(6)} = T^\sigma T^2 T^3 T^4 T^5 + pT^\sigma T^4 T^4 + pT T^3 T^3 + pTT^\sigma T^4 + pTT^\sigma T^4$

$$+ pT^2 T^3 T^4 + p^2 T^2 T^3 + p^2 T^2 T^3 + pT^2 T^3,$$

$$D^{(6)} = pT^\sigma T^2 T^3 T^4 + p^2 T^3 T^4 + p^2 T^2 T^3 + p^2 T^2 T^3 + p^2 T^2 + p^3.$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
In general we have

\[ A^{(n)} = T T^a T^{σ^2} \cdots T^{σ^{n-1}} + p \cdot \sum \prod (\text{drop a pair of consecutive terms}) \]

\[ + p^2 \cdot \sum \prod (\text{drop two pairs of consecutive terms}) \]

\[ B^{(n)} = p T T^a T^{σ^2} \cdots T^{σ^{n-2}} + p^2 \cdot \sum \prod (\text{drop a pair of consecutive terms}) \]

\[ + p^3 \cdot \sum \prod (\text{drop two pairs of consecutive terms}) \]

\[ C^{(n)} = T^a T^{σ^2} \cdots T^{σ^{n-1}} + p \cdot \sum \prod (\text{drop a pair of consecutive terms}) \]

\[ + p^2 \cdot \sum \prod (\text{drop two pairs of consecutive terms}) \]

\[ D^{(n)} = p T T^a T^{σ^2} \cdots T^{σ^{n-2}} + p^2 \cdot \sum \prod (\text{drop a pair of consecutive terms}) \]

\[ + p^3 \cdot \sum \prod (\text{drop two pairs of consecutive terms}) \]

If we take \( R = k[t] \), \( T = [t] \cdot A \) where \( A \in M_{r \times r}(Z_p) \) and \( A' = p^2 \cdot (\text{unit}) \), \( 2s < r \), then any product of \( m \) terms of the form \( T^{σ^i} \) is always of the form \( p^{m/r^s} \cdot \) (a matrix not congruent to 0 mod \( p \)). Note that such \( A \) exists: start with a cyclic permutation matrix, replace the first \( s \) 1’s by \( p \). Moreover since \([t]^{σ^i} = [r^s] \), there is no cancellation. Therefore \( F^n = p^{(m/r^s)} \cdot \) (a matrix whose determinant is not congruent to 0 mod \( p \)). Thus by Katz’s “basic slope estimate” [Ka, 1.4.3, p. 125], we see that the first \( s \) slopes are all equal to \( s/r \) \( \); therefore, the last \( r \) slopes are all equal to \( (r-s)/r \). This argument also works for higher-dimensional base rings \( R \): take \( s < r/2 \), \( U \in M_{r \times r}(Z_p) \), \( U' = p \cdot (\text{unit}) \), and \( T = [t_0] \cdot I + [t_1] \cdot U + [t_2] \cdot U^2 + \cdots + [t_s] \cdot U^s \). This produces a sequence of Newton polygons \( N P_0, N P_1, \ldots, N P_s, N P_{s+1} \) such that \( N P_i \) has slopes \( i/r \) and \( (t-s)/r \) with multiplicity \( r \) if \( 0 \leq i \leq s \) and \( N P_{s+1} \) has slope \( 1/2 \) and multiplicity \( 2r \). With polarization, we need a symmetric \( U \in M_{r \times r}(Z_p) \) such that \( U' = p \cdot (\text{unit}) \). This is possible if \( p \equiv 1 \) (mod 4), or \( r \equiv 0, 1, 3 \) (mod 4) and \( p > 2 \). Thus we have shown

**Proposition 3.** Let \( r, s \) be positive integers such that \( 2s < r \). Let \( N P_0, N P_1, \ldots, N P_s, N P_{s+1} \) be the Newton polygons connecting \((0, 0)\) to \((2r, r)\) such that \( N P_i \) has slopes \( i/r \) and \( (t-s)/r \) with multiplicity \( r \) for \( 0 \leq i \leq s \) and \( N P_{s+1} \) has slope \( 1/2 \) and multiplicity \( 2r \).

(a) \( N P_0, N P_1, \ldots, N P_s, N P_{s+1} \) can always be realized by a Barsotti-Tate group over \( k[[t_0, t_1, \ldots, t_s]] \).

(b) Assume either \( p \equiv 1 \) (mod 4), or \( r \equiv 0, 1, 3 \) (mod 4) and \( p > 2 \). Then \( N P_0, N P_1, \ldots, N P_s, N P_{s+1} \) can be realized by a principally polarized abelian scheme over \( k[[t_0, t_1, \ldots, t_s]] \).

**Appendix: A 2-adic lifting problem by Michael Larsen**

This appendix gives, for all \( n \in N \), an affirmative answer to the question of whether there exists a symmetric matrix \( A \) in \( M_{n \times n}(Z_2) \) with \( A^n \) equal to \( 2U \), \( U \) invertible.

\(^2\)Michael Larsen was supported by NSF Grant No. DMS-8807203. He is affiliated with the University of Pennsylvania, Philadelphia, Pennsylvania 19104.
We begin by constructing, for each \( n \), an \( n \times n \) symmetric matrix with entries in \( \mathbb{F}_2 \), nilpotent of rank \( n - 1 \). For \( n \) fixed, define \( e_{i,j} \) for \( 1 \leq i, j \leq n \) to be the matrix with \((i, j)\)th entry 1 and all other entries 0. For \( i \) or \( j \) out of range, let \( e_{i,j} = 0 \). Let \( N = \sum_{i=1}^{n} e_{i,i+1} \) denote the standard nilpotent matrix of rank \( n - 1 \). Over \( \mathbb{F}_2 \),

\[
(I + N)^{-1} = I + N + N^2 + \cdots + N^{n-1}.
\]

Define the permutation \( \sigma: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \) as follows:

\[
\sigma(k) = \begin{cases} 
2k & \text{if } k \leq n/2, \\
2(n - k) + 1 & \text{otherwise.}
\end{cases}
\]

Let \( P_\sigma \) denote the corresponding permutation matrix and

\[
M = (I + N)^{-1} P_\sigma^{-1} N P_\sigma (I + N) = \sum_{1 \leq i, j \leq n} e_{i,j} \sum_{i=1}^{n-1} e_{\sigma(i), \sigma(i+1)} \sum_{i=1}^{n} (e_{i,i} + e_{i,i+1}).
\]

Evidently \( M \) is nilpotent of rank \( n - 1 \); we claim that it is symmetric. The cases \( n \) even and \( n \) odd must be considered separately.

Suppose \( n = 2m \). Then

\[
\sum_{i=1}^{n-1} e_{\sigma(i), \sigma(i+1)} = \sum_{i=1}^{m-1} e_{2i, 2i+2} + \sum_{i=1}^{m-1} e_{2i+1, 2i-1} + e_{2m, 2m-1}.
\]

As \( e_{i,j} e_{k,l} = \delta_{j,k} e_{i,l} \),

\[
M = \sum_{j=1}^{m-1} \sum_{i=1}^{2j} e_{i, 2j+2} + \sum_{j=1}^{m-2} \sum_{i=1}^{2j} e_{i, 2j+3} + \sum_{j=1}^{m-1} \sum_{i=1}^{2j+1} e_{i, 2j-1} + \sum_{j=1}^{m-2} \sum_{i=1}^{2j} e_{i, 2j+1} + \sum_{j=1}^{2m} e_{i, 2j}.
\]

Combining the third and fifth terms and likewise the fourth and sixth terms, we get

\[
\sum_{j=1}^{m-1} \sum_{i=1}^{2j} e_{i, 2j+2} + \sum_{j=1}^{m-2} \sum_{i=1}^{2j} e_{i, 2j+3} + \sum_{j=1}^{m} \sum_{i=1}^{2j} e_{i, 2j-1} + \sum_{j=1}^{2m} e_{i, 2j}.
\]

(harmlessly) extending the ranges of summation,

\[
\sum_{j=0}^{m} \sum_{i=1}^{2j} e_{i, 2j+2} + \sum_{j=0}^{m} \sum_{i=1}^{2j} e_{i, 2j+3} + \sum_{j=1}^{m+1} \sum_{i=1}^{2j} e_{i, 2j-1} + \sum_{j=1}^{m+1} \sum_{i=1}^{2j} e_{i, 2j}
\]

\[
= \sum_{k=0}^{m} \left( \sum_{i=1}^{k} e_{i,k} + \sum_{i=1}^{k+1} e_{i,k} \right) + \sum_{k=0}^{m} \left( \sum_{i=1}^{k} e_{i,k} + \sum_{i=1}^{k+2} e_{i,k} \right)
\]

\[
= \sum_{k\text{ even}} \sum_{i=k}^{k+1} e_{i,k} + \sum_{k\text{ odd}} \sum_{i=k}^{k+2} e_{i,k}.
\]
The right-hand side is evidently symmetric; the matrix looks like

\[ M_{2m} = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\
\end{pmatrix}. \]

If \( n = 2m + 1 \),

\[
M = \sum_{j=1}^{m} \sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=1}^{m} \sum_{i=1}^{2j} e_{i,2j+3} + \sum_{j=1}^{m} \sum_{i=1}^{2j-1} e_{i,2j-1} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j+1} + \sum_{i=1}^{2m} e_{i,2m+1}. 
\]

Combining the third and fifth terms, we get

\[
M = \sum_{j=1}^{m} \sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=1}^{m} \sum_{i=1}^{2j} e_{i,2j+3} + m \sum_{j=1}^{m} \sum_{i=1}^{2j-1} e_{i,2j-1} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j+1} - e_{m+1,m+1} 
\]

\[
= e_{m+1,m+1} + \sum_{k \text{ even}} \left( \sum_{i=1}^{k-2} e_{i,k} + \sum_{i=1}^{k+1} e_{i,k} \right) + \sum_{k \text{ odd}} \left( \sum_{i=1}^{k-3} e_{i,k} + \sum_{i=1}^{k+2} e_{i,k} \right) 
\]

\[
= e_{m+1,m+1} + \sum_{k \text{ even}} \sum_{i=k-1}^{k+1} e_{i,k} + \sum_{k \text{ odd}} \sum_{i=k-2}^{k+2} e_{i,k} . 
\]

The right-hand side is again symmetric; it looks like

\[ M_{2m+1} = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 \\
\end{pmatrix}. 
\]
2m – 1. In each case, the row operations leave the first row untouched and replace \( M_n \) by the block diagonal matrix

\[
\begin{pmatrix}
M_{n-1} & 0 \\
0 & (-1)^n
\end{pmatrix}.
\]

In fact, not only does this show that the lower left \( n \times n \) submatrix of \( M_n \) is invertible over \( \mathbb{Z}/2\mathbb{Z} \), it even proves invertibility over \( \mathbb{Z} \). As the first two rows of \( M_n \) are the same, the matrix \( X = 2e_{1,1} + M_n \) is a symmetric \( n \times n \) matrix such that \( X^n/2 \in \text{GL}_n(\mathbb{Z}) \).

References

[CN] C.-L. Chai and P. Norman, Bad reduction of Siegel moduli schemes with \( \Gamma_0(p) \)-level structure, Amer. J. Math. 112 (1990), 1003–1071.

[G] A. Grothendieck, Groupes de Barsotti-Tate et cristaux de Dieudonné, Séminaire de Mathématiques Supérieures, Presses de l'Université de Montréal, Montréal, 1974.


[Ko] N. Koblitz, \( p \)-adic variation of the zeta-function over families of varieties defined over the finite fields, Compositio Math. 31 (1975), 119–218.

