PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 1, September 1993

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:

$$d(\det(x_{ij})_{1\le i,j\le n}) = \sum_{1\le i,j\le n} A_{ij}\, dx_{ij}$$

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

$$= \sum_{1\le i\le n} A_{ii}\, dx_{ii} + 2 \sum_{1\le i<j\le n} A_{ij}\, dx_{ij}$$

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 $\mathrm{char}(k) \neq 2$, 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 $g\colon A \mapsto gAg^{-1} = gA^t g$, $\forall g \in \mathrm{O}_n$, $\forall A \in V$.

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, $V(\mathbb{F}_p) \neq \varnothing$ 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 $V_3(\mathbb{F}_p) \neq \varnothing$ if $p \equiv 1 \pmod 4$.

(iii) When $n = 3$ and $p = 3$, $V_3(\mathbb{F}_3) \neq \varnothing$ 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 $g \in \mathrm{GL}(\bar{k})$ such that gNg^{-1} is symmetric. Clearly $gNg^{-1} = {}^t g^{-1} {}^t N {}^t g \Leftrightarrow {}^t g g N = {}^t N {}^t g g$. We know that (by Witt's theorem) $g \mapsto {}^t g g$ establishes an isomorphism $\mathrm{O}_n \backslash \mathrm{GL}_n \approx Z_n$ since $\mathrm{char}(k) \neq 2$, 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 $XN = {}^t N X$. By explicit computation, the necessary and sufficient condition for a symmetric

matrix Y to satisfy $YN = {}^tNY$ is that Y has the form

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

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 $g \in \mathrm{GL}_n(\overline{k})$ such that $gA_1g^{-1} = A_2$, and we want to show that there exists a $g_1 \in \mathrm{O}_n(\overline{k})$ such that $g_1A_1g_1^{-1} = A_2$. We have $gA_1g^{-1} = A_2 \Rightarrow gA_1 = A_2g$, $A_1{}^tg = {}^tgA_2 \Rightarrow {}^tggA_1 = {}^tgA_2g = A_1{}^tgg$; hence by the lemma we know that ${}^tgg \in \overline{k}[A_1]^\times$. Since $\mathrm{char}(k) \neq 2$ and A_1 is nilpotent, there exists an $h \in \overline{k}[A_1]^\times$ such that ${}^tgg = h^2$. (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 ${}^tg_1g_1 = h^{-1}{}^tggh^{-1} = h^{-1}h^2h^{-1} = 1$ since h is symmetric (as in A_1); hence, $g_1 \in \mathrm{O}_n(\overline{k})$, 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, $1 = {}^tgg = g^2$. Since $\mathrm{char}(k) \neq 2$, 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 $\mathrm{PO}_n = \mathrm{O}_n/\{\pm 1\}$ 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 $V(\mathbb{F}_p) \neq \varnothing$ 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

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

we have to find a $g_0 \in \mathrm{GL}_n$ such that ${}^tg_0g_0 = Y_0$. Any such g_0 produces a point $g_0Ng_0^{-1} \in V(\overline{K})$ 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 $g_0 N g_0^{-1} \in V(\mathbb{Q}(\sqrt{-1}))$. If $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) = \{\mathrm{id}, \tau\}$, 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 τ operates on the two geometric components of $V/\mathbb{Q}$ by $(-1)^m$, i.e., τ stabilizes both geometric components if $n \equiv 0 \pmod 4$, and τ 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 $\mathrm{PSO}_n = \mathrm{SO}_n/\{\pm 1\}$;*

(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 $V_n(\mathbb{F}_p) = \varnothing$ 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 nth power is equal to p times a unit in $M_{n\times n}(\mathbb{Z}_p)$ iff $p \equiv 1 \pmod 4$ or $n \equiv 0, 1$, or $3 \pmod 4$.*

Remark. Let $W = W_n$ be the variety of all symmetric $n \times n$ mattices. O_n operates on W and V is contained in the null cone. As the referee pointed out, the ring of invariants of 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 $x_1, \dots, x_r, y_1, \dots, y_r$, and the Frobenius and Verschibung send x_i to y_i: $Fx_i = y_i = Vx_i$, $1 \le i \le r$. The product polarization corresponds to the symplectic pairing having $x_1, \dots, x_r, y_1, \dots, y_r$ 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:

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

where $T_{ij} = [t_{ij}] = (t_{ij}, 0, 0, \dots)$ is the Teichmüller representative of t_{ij} in the ring of infinite Witt vectors $W(R)$, $t_{ij} \in R$, $1 \le i, j \le r$. 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 $t_{ij} = t_{ji}$, $1 \le i, j \le r$. 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 nth 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 σ denotes the Frobenius automorphism on $W(R)$.

$$\begin{aligned}
n = 3\colon\ & A^{(3)} = TT^\sigma T^{\sigma^2} + pT^{\sigma^2} + pT, \ B^{(3)} = pTT^\sigma + p^2, \\
& C^{(3)} = T^\sigma T^{\sigma^2} + p, \ D^{(3)} = pT^\sigma \\
n = 4\colon\ & A^{(4)} = TT^\sigma T^{\sigma^2} T^{\sigma^3} + pT^{\sigma^2} T^{\sigma^3} + pTT^{\sigma^3} + pTT^\sigma + p^2, \\
& B^{(4)} = pTT^\sigma T^{\sigma^2} + p^2 T^{\sigma^2} + p^2 T, \\
& C^{(4)} = T^\sigma T^{\sigma^2} T^{\sigma^3} + pT^{\sigma^3} + pT^{\sigma^3}, \ D^{(4)} = pT^\sigma T^{\sigma^2} + p^2. \\
n = 5\colon\ & A^{(5)} = TT^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + pT^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + pTT^{\sigma^3} T^{\sigma^4} + pTT^\sigma T^{\sigma^4} \\
& \qquad + pT^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + p^2 T^{\sigma^4} + p^2 T^{\sigma^2} + p^2 T, \\
& B^{(5)} = pTT^\sigma T^{\sigma^2} T^{\sigma^3} + p^2 T^{\sigma^2} T^{\sigma^3} + p^2 TT^{\sigma^3} + p^2 TT^\sigma + p^3, \\
& C^{(5)} = T^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + pT^{\sigma^3} T^{\sigma^4} + pT^\sigma T^{\sigma^4} + pT^\sigma T^{\sigma^2} + p^2, \\
& D^{(5)} = pT^\sigma T^{\sigma^2} T^{\sigma^3} + p^2 T^{\sigma^3} + p^2 T^\sigma. \\
n = 6\colon\ & A^{(6)} = TT^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^5} + pT^{\sigma^2} T^{\sigma^3} T^{\sigma^4} T^{\sigma^5} + pTT^{\sigma^3} T^{\sigma^4} T^{\sigma^5} \\
& \qquad + pTT^\sigma T^{\sigma^4} T^{\sigma^5} + pTT^\sigma T^{\sigma^2} T^{\sigma^5} + pTT^\sigma T^{\sigma^2} T^{\sigma^3} + p^2 T^{\sigma^4} T^{\sigma^5} \\
& \qquad + p^2 T^{\sigma^2} T^{\sigma^5} + p^2 TT^{\sigma^5} + p^2 T^{\sigma^2} T^{\sigma^3} + p^2 TT^\sigma + p^3, \\
& B^{(6)} = pTT^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + p^2 T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + p^2 TT^{\sigma^3} T^{\sigma^4} + p^2 TT^\sigma T^{\sigma^4} \\
& \qquad + p^2 TT^\sigma T^{\sigma^2} + p^3 T^{\sigma^4} + p^3 T^{\sigma^2} + p^3 T, \\
& C^{(6)} = T^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} T^{\sigma^5} + pT^{\sigma^3} T^{\sigma^4} T^{\sigma^5} + pT^\sigma T^{\sigma^4} T^{\sigma^5} + pT^\sigma T^{\sigma^2} T^{\sigma^5} \\
& \qquad + pT^\sigma T^{\sigma^2} T^{\sigma^3} + p^2 T^{\sigma^5} + p^2 T^{\sigma^3} + p^2 T^\sigma, \\
& D^{(6)} = pT^\sigma T^{\sigma^2} T^{\sigma^3} T^{\sigma^4} + p^2 T^{\sigma^3} T^{\sigma^4} + p^2 T^\sigma T^{\sigma^4} + p^2 T^\sigma T^{\sigma^2} + p^3.
\end{aligned}$$

In general we have

$$A^{(n)} = TT^{\sigma}T^{\sigma^2}\cdots T\sigma^{n-1} + p\cdot\sum\prod \text{ (drop a pair of consecutive terms)}$$
$$+ p^2\cdot\sum\prod \text{ (drop two pairs of consecutive terms) } + \cdots,$$
$$B^{(n)} = pTT^{\sigma}T^{\sigma^2}\cdots T^{\sigma^{n-2}} + p^2\cdot\sum\prod \text{ (drop a pair of consecutive terms)}$$
$$+ p^3\cdot\sum\prod \text{ (drop two pairs of consecutive terms) } + \cdots,$$

$$C^{(n)} = T^{\sigma}T^{\sigma^2}\cdots T^{\sigma^{n-1}} + p\cdot\sum\prod \text{ (drop a pair of consecutive terms)}$$
$$+ p^2\cdot\sum\prod \text{ (drop two pairs of consecutive terms) } + \cdots,$$
$$D^{(n)} = pT^{\sigma}T^{\sigma^2}\cdots T^{\sigma^{n-2}} + p^2\cdot\sum\prod \text{ (drop a pair of consecutive terms)}$$
$$+ p^3\cdot\sum\prod \text{ (drop two pairs of consecutive terms) } + \cdots.$$

If we take $R = k[t]$, $T = [t]\cdot A$ where $A \in M_{r\times r}(\mathbb{Z}_p)$ and $A^r = p^s\cdot(\text{unit})$, $2s < r$, 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 $0 \bmod p$). Note that such A exists: start with a cyclic permutation matrix, replace the first s 1's by p. Moreover since $[t]^{\sigma^i} = [t^{p^i}]$, there is no cancellation. Therefore $F^n = p^{[n/r]s}\cdot$ (a matrix whose determinant is not congruent to $0 \bmod p$). Thus by Katz's "basic slope estimate" [Ka, 1.4.3, p. 125], we see that the first r 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 $s < r/2$, $U \in M_{r\times r}(\mathbb{Z}_p)$, $U^r = p\cdot(\text{unit})$, and $T = [t_0]\cdot I_r + [t_1]\cdot U + [t_2]\cdot U^2 + \cdots + [t_s]\cdot U^s$. This produces a sequence of Newton polygons $NP_0, NP_1, \ldots, NP_s, NP_{s+1}$ such that NP_i has slopes i/r and $(t-s)/r$ with multiplicity r if $0 \le i \le s$ and NP_{s+1} has slope $1/2$ and multiplicity $2r$. With polarization, we need a symmetric $U \in M_{r\times r}(\mathbb{Z}_p)$ such that $U^r = p\cdot(\text{unit})$. This is possible if $p \equiv 1 \pmod 4$, or $r \equiv 0, 1, 3 \pmod 4$ and $p > 2$. Thus we have shown

Proposition 3. *Let r, s be positive integers such that $2s < r$. Let NP_0, $NP_1, \ldots, NP_s$, NP_{s+1} be the Newton polygons connecting $(0,0)$ to $(2r, r)$ such that NP_i has slopes i/r and $(t-s)/r$ with multiplicity r for $0 \le i \le s$ and NP_{s+1} has slope $1/2$ and multiplicity $2r$.*

(a) *NP_0, $NP_1, \ldots, NP_s$, NP_{s+1} can always be realized by a Barsotti-Tate group over $k[[t_0, t_1, \ldots, t_s]]$.*

(b) *Assume either $p \equiv 1 \pmod 4$, or $r \equiv 0, 1, 3 \pmod 4$ and $p > 2$. Then $NP_0, NP_1, \ldots, NP_s, NP_{s+1}$ 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[2]

This appendix gives, for all $n \in N$, an affirmative answer to the question of whether there exists a symmetric matrix A in $M_{n\times n}(\mathbf{Z}_2)$ 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 $\mathbf{F}_2$, nilpotent of rank $n-1$. For n fixed, define $e_{i,j}$ for $1 \le i, j \le n$ 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 $\mathbf{F}_2$,

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

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

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

Let P_σ denote the corresponding permutation matrix and

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

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 $e_{i,j} e_{k,l} = \delta_{j,k} e_{i,l}$,

$$\begin{aligned} M = {} & \sum_{j=1}^{m-1} \sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=1}^{m-2} \sum_{i=1}^{2j} e_{i,2j+3} + \sum_{j=1}^{m-1} \sum_{i=1}^{2j+1} e_{i,2j-1} \\ & + \sum_{j=1}^{m-1} \sum_{i=1}^{2j+1} e_{i,2j} + \sum_{i=1}^{2m} e_{i,2m-1} + \sum_{i=1}^{2m} e_{i,2m}. \end{aligned}$$

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

$$\sum_{j=1}^{m-1} \sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=1}^{m-2} \sum_{i=1}^{2j} e_{i,2j+3} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j-1} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j};$$

(harmlessly) extending the ranges of summation,

$$\begin{aligned} & \sum_{j=0}^{m} \sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=0}^{m} \sum_{i=1}^{2j} e_{i,2j+3} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j-1} + \sum_{j=1}^{m} \sum_{i=1}^{2j+1} e_{i,2j} \\ & = \sum_{k \text{ even}} \left(\sum_{i=1}^{k-2} e_{i,k} + \sum_{i=1}^{k+1} e_{i,k} \right) + \sum_{k \text{ odd}} \left(\sum_{i=1}^{k-3} e_{i,k} + \sum_{i=1}^{k+2} e_{i,k} \right) \\ & = \sum_{k \text{ even}} \sum_{i=k-1}^{k+1} e_{i,k} + \sum_{k \text{ odd}} \sum_{i=k-2}^{k+2} e_{i,k}. \end{aligned}$$

The right-hand side is evidently symmetric; the matrix looks like

$$M_{2m} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{pmatrix}.$$

If $n = 2m + 1$,

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

Combining the third and fifth terms, we get

$$\begin{aligned} M &= \sum_{j=1}^{m}\sum_{i=1}^{2j} e_{i,2j+2} + \sum_{j=1}^{m}\sum_{i=1}^{2j} e_{i,2j+3} + \sum_{j=1}^{m+1}\sum_{i=1}^{2j+1} e_{i,2j-1} \\ &\quad + \sum_{j=1}^{m}\sum_{i=1}^{2j+1} e_{i,2j} - e_{m+1,m+1} \\ &= e_{m+1,m+1} + \sum_{k \text{ even}} \left(\sum_{i=1}^{k-2} e_{i,k} + \sum_{i=1}^{k+1} e_{i,k} \right) + \sum_{k \text{ odd}} \left(\sum_{i=1}^{k-3} e_{i,k} + \sum_{i=1}^{k+2} e_{i,k} \right) \\ &= e_{m+1,m+1} + \sum_{k \text{ even}} \sum_{i=k-1}^{k+1} e_{i,k} + \sum_{k \text{ odd}} \sum_{i=k-2}^{k+2} e_{i,k}. \end{aligned}$$

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

$$M_{2m+1} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 0 \end{pmatrix}.$$

To finish the proof, it remains only to show that the matrices constructed in this way can be lifted to $\mathbf{Z}_2$ in such a way that the determinant is in $2\mathbf{Z}_2^*$. The Hensel's lemma argument described above works as long as at least one of the diagonal cofactors $A_{i,i}$ is nonzero. It is easy to prove by induction on n that the cofactor $A_{1,1} \neq 0$. All entries of M_2, and hence all cofactors, are 1. If $n = 2m > 2$, subtract row $2m$ from row $2m - 1$, then row $2m - 2$ from row $2m$, and then add row $2m - 1$ to row $2m$. If $n = 2m + 1$, subtract row $2m$ from row $2m + 1$, add row $2m + 1$ to row $2m$, then add row $2m + 1$ to row

$2m-1$. 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 $\mathbf{Z}/2\mathbf{Z}$, it even proves invertibility over $\mathbf{Z}$. 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 $X^n/2 \in \mathrm{GL}_n(\mathbf{Z})$.

References

[CN] C.-L. Chai and P. Norman, *Bad reduction of Seigel 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.

[Ka] N. Katz, *Slope filtration of F-crystals*, Asterisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 113–164.

[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.

[La] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[No] P. Norman, *An algorithm for computing local moduli of abelian varieties*, Ann. of Math. (2) **101** (1975), 499–509.

[NO] P. Norman and F. Oort, *Moduli of abelian varieties*, Ann. of Math. (2) **112** (1980), 413–439.

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104

E-mail address, C.-L.Chai: chai@math.upenn.edu

E-mail address, M. Larsen: larsen@math.upenn.edu