

Counting Matrices That are Squares

Victor S. Miller

April 2016

Dedicated to Neil Sloane on his 75th Birthday

Abstract

On the math-fun mailing list (7 May 2013), Neil Sloane asked to calculate the number of $n \times n$ matrices with entries in $\{0, 1\}$ which are squares of other such matrices. In this paper we analyze the case that the arithmetic is in \mathbb{F}_2 . We follow the dictum of Wilf (“What is an answer?”) to derive a “effective” algorithm to count such matrices in much less time than it takes to enumerate them. The algorithm which we use involves the analysis of conjugacy classes of matrices. The restricted integer partitions which arise are counted by the coefficients of one of Ramanujan’s mock Theta functions, which we found thanks to Sloane’s OEIS (Online Encyclopedia of Integer Sequences).

Let a_n be the number elements of $\text{Mat}_n(\mathbb{F}_2)$ which are squares, and b_n be the number of elements of $\text{GL}(n, \mathbb{F}_2)$ which are squares. The numerical results strongly suggest that there are constants $\alpha, \beta > 0$ such that $a_n \sim \alpha 2^{n^2}$, $b_n \sim \beta 2^{n^2}$.

1 Introduction

On the math-fun mailing list (7 May 2013), Neil Sloane asked “What is $a(n)$ = the number of $n \times n$ matrices in R that have a square root in R ”, where R is the set of $n \times n$ matrices with entries that are 0 or 1, for various matrix rings.

In this paper we give an answer to his question when $R = \text{Mat}_n(\mathbb{F}_2)$, the $n \times n$ matrices with coefficients in \mathbb{F}_2 , in the sense of an algorithm to calculate $a(n)$, whose values we give for $n \leq 60$. We also calculate the closely related sequence $b(n)$ of matrices which are squares in $\text{GL}_n(\mathbb{F}_2)$. The calculation is based on the observation that whether or not a matrix A is a square is a class-function—i.e., it only depends on the conjugacy class of A . We then use the known characterization of conjugacy classes in $\text{Mat}_n(\mathbb{F}_2)$ along with formulas for the cardinality of their centralizers to derive a method for calculating $a(n)$. Along the way we also found a number of other interesting sequences which were not already in the OEIS.

We should expect that $a(n)$ and $b(n)$ both grow approximately like 2^{n^2} because of a general result about word maps [16]: Let W be a word in the free group on d generators, x_1, \dots, x_d , and G be a group. We define a map from the set $G^d = G \times \dots \times G$ (d times) to G , also denoted by W , by sending (g_1, \dots, g_d) to the element of G obtained by substituting g_i for x_i in W . If W is not the trivial element, then the image $W(G^d)$ is large: If G_n is a sequence of non-abelian simple groups such that $|G_n| \rightarrow \infty$, then

$$\lim_{n \rightarrow \infty} \log(|W(G_n^d)|) / \log(|G_n|) = 1.$$

To apply this to our case, we take $G_n = \text{GL}_n(\mathbb{F}_2)$ (which is simple), $d = 1$, and $W = x_1^2$. This shows that $\lim_{n \rightarrow \infty} \log(b(n)) / \log(|\text{GL}_n(\mathbb{F}_2)|) > 0$. However (see Corollary 1) we have $|\text{GL}_n(\mathbb{F}_2)| \sim \gamma_2 2^{n^2}$ for an explicit $\gamma_2 > 0$. Since $2^{n^2} \geq a(n) \geq b(n)$ we get the above assertion.

Counting squares in simple groups arises in the context of proving that every element in a simple group can be written as the product of two squares [13].

2 Generating and Counting

When faced with a problem such as this one, the first thing to try is to generate all squares and count them. One can do this in a straightforward way: enumerate all matrices of a given size, square them, and keep track of their counts via a data structure such as a hash table. However, one can be much more efficient than that. Since the matrices that we're interested in have all entries in $\{0, 1\}$ it makes sense to use a Gray code to generate all such matrices. There are many different variants of Gray code, but all of them have the property that adjacent matrices in the sequence differ in precisely one position. Suppose that position is (i, j) . Let E denote the matrix which is all 0s except for 1 in the (i, j) position. We'll keep track of A —the current matrix—and $B = A^2$. When we change A to $A + E$, we change B to $(A + E)^2 = A^2 + EA + AE + E^2$. Note, first, that $E^2 = 0$ unless $i = j$, in which case $E^2 = E$. Note also that EA is all 0s except for its i -th row, which is the j -th row of A . Similarly, AE is all 0s except for its j -th column which is the i -th column of A . Thus, if we represent A as n^2 bits in a computer word, we can update B by a few shifts and masking operations, as well as at most 3 exclusive ORs. See Listing 1 on page 16 for a C program implementing this. One can calculate the exact number of 5×5 matrices which are squares in about 0.302 seconds on a fairly standard PC workstation. However, this approach can't be pushed much further in practice, since it needs about 2^{n^2-3} bytes of storage for a table of n^2 bits and has running time proportional to 2^{n^2} . In fact the calculation of $a(6)$ takes 2077.957 seconds on the same workstation.

3 Matrices and Their Conjugacy Classes

We begin by collecting the results about conjugacy classes of matrices over finite fields that we need to derive the algorithm. The main tool is *rational canonical form*, which is a generalization of the well-known Jordan canonical form. Although this is well known (for example, see [15, Chapter XIV]) few sources¹ give the formula for the order of the centralizer of an element. For matrices over finite fields this is originally due to Dickson [6]. An exposition in more modern notation may be found in MacDonalld [20, p. 87].

Definition 1. *Two matrices $A, B \in \text{Mat}_n(K)$, where K is a field, are similar (written $A \sim B$) if there is an invertible $U \in \text{Mat}_n(K)$ with $A = U^{-1}BU$. A K -conjugacy class is a set of all matrices $U^{-1}AU$ for a fixed A and all invertible U . The centralizer of A is $C_K(A) := \{U \in \text{GL}_n(K) : U^{-1}AU = A\}$.*

A matrix A is semisimple if A is similar to a diagonal matrix (over the algebraic closure of the coefficient field). It is semisimple regular if the elements on the diagonal are distinct.

Note (e.g., see [15, Chapter XIV]) that A and B are similar as members of $\text{Mat}_n(K)$ if and only if they are similar as members of $\text{Mat}_n(L)$ where L/K is any field extension.

Every semisimple matrix A over \mathbb{F}_{2^n} is similar to a diagonal matrix. Raising such a matrix to the 2^n power permutes the elements on the diagonal, since A is defined over \mathbb{F}_{2^n} . We have $A \sim A^{2^n}$ which is obviously a square. Thus, the set of squares of matrices over \mathbb{F}_{2^n} contains all semisimple matrices.

If A, B are square matrices, we denote the direct sum by

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

If r is a nonnegative integer denote by $[r]A$ the direct sum of r copies of A .

The key observation (from standard group theory) is that the number of elements in the conjugacy class of A is $|\text{GL}_n(K)|/|C_K(A)|$.

Conjugacy classes have a fixed standard representative given by combinations of integer partitions and K -irreducible polynomials.

Definition 2. *A partition is a non-increasing sequence of nonnegative integers λ , with all but finitely many $\lambda_i = 0$. Each of the λ_i is referred to as a part. The weight $|\lambda| = \sum_i \lambda_i$. The conjugate of a partition λ , written λ' , is defined by $\lambda'_j := \#\{i \mid \lambda_i \geq j\}$. The multiplicities of a partition λ are $m_i(\lambda) = \#\{\lambda_j = i\}$. We have $m_i(\lambda) = \lambda'_i - \lambda'_{i+1}$. Note that $|\lambda| = |\lambda'|$ and that conjugation is an involution.*

It is convenient to also consider the empty partition, denoted by \emptyset , with $|\emptyset| = 0$ and $\emptyset' = \emptyset$.

Let \mathcal{P} denote the set of partitions. We also write partitions in the form $1^{m_1}2^{m_2}\dots$, indicating that i occurs with multiplicity m_i , where we omit those factors with $m_i = 0$.

¹For example: Kung [14] rederived this result independently and Green [12] refers to an unpublished manuscript of Philip Hall, which antedates Dickson's paper.

For a prime power q let $\mathcal{I}(q)$ denote the set of \mathbb{F}_q -irreducible monic polynomials with coefficients in \mathbb{F}_q , and $\mathcal{I}(q)_d$ those elements of $\mathcal{I}(q)$ of degree d . We also denote by $\mathcal{I}'(q)_d = \mathcal{I}(q)_d$ if $d > 1$ and $\mathcal{I}'(q)_1 = \{X - \alpha : \alpha \in \mathbb{F}_q^*\}$, i.e., all of $\mathcal{I}(q)_1$ except for the polynomial X .

Definition 3. Let ϕ be a monic polynomial over a field K , $\phi(X) = \sum_{i=0}^{\deg(\phi)} a_i X^i$. Define the companion matrix

$$M(\phi) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{\deg(\phi)-1} \end{pmatrix}.$$

Note that this is the matrix of multiplication by X on polynomials (mod $\phi(X)$) with respect to the ordered basis $1, X, \dots, X^{\deg(\phi)-1}$.

For convenience, we denote by $M(1)$ the 0×0 matrix.

Proposition 1. Every conjugacy class of an element of $\text{Mat}_n(\mathbb{F}_q)$ is uniquely specified by a function $\Lambda : \mathcal{I}(q) \rightarrow \mathcal{P}$, where for all but finitely many $\phi \in \mathcal{I}$, we have $\Lambda(\phi) = \emptyset$, and for some ϕ , $\Lambda(\phi) \neq \emptyset$. The dimension of such a Λ is $\dim(\Lambda) := \sum_{\phi \in \mathcal{I}} |\Lambda(\phi)| \deg(\phi)$. The standard representative of this conjugacy class is

$$\bigoplus_{\phi \in \mathcal{I}(q)} \bigoplus_i M(\phi^{\Lambda(\phi)_i}).$$

Definition 4. The standard representative for a matrix given by Proposition 1 is called the rational canonical form of the matrix.

Note that the characteristic polynomial of the conjugacy class represented by Λ is $\prod_{\phi \in \mathcal{I}(q)} \phi^{|\Lambda(\phi)|}$ and the minimal polynomial is $\prod_{\phi \in \mathcal{I}(q)} \phi^{\max_i \Lambda(\phi)_i}$.

Definition 5. Let $M \in \text{Mat}_n(K)$, $\phi_M(X)$ denote its characteristic polynomial, and $\psi_M(X)$ denote its minimal polynomial. We say that M is separable if $\phi_M(X)$ has distinct roots in the algebraic closure of K , M is semisimple if $\psi_M(X)$ has distinct roots in the algebraic closure, and cyclic if $\phi_M = \psi_M$.

We note that this definition of semisimple is equivalent to the previous definition.

Definition 6. The q -Pochhammer symbol $(a; q)_n := \prod_{k=0}^{n-1} (1 - aq^k)$ when n is a positive integer. We also set $(a; q)_0 = 1$ and $(a; q)_{-n} = 1/(aq^{-n}; q)_n$.

Proposition 2 (Dickson [6]). Let $\lambda \in \mathcal{P}$ be a partition, and q a prime power. Define $C(\lambda, q) = q^{\sum_i (\lambda'_i)^2} \prod_{i \geq 1} (q^{-m_i(\lambda)}; q)_{m_i(\lambda)}$. The order of the centralizer of an element associated to the data $\Lambda : \mathcal{I}(q) \rightarrow \mathcal{P}$ is $\prod_{\phi \in \mathcal{I}(q)} C(\Lambda(\phi), q^{\deg(\phi)})$.

Given a matrix $A \sim \oplus_i M(\phi(X)^{\lambda_i})$, the vector space of matrices U such that $UA = AU$ has dimension $\sum_i (\lambda_i')^2$. The quantity $\prod_i (q^{-m_i(\lambda)}; q)_{m_i(\lambda)}$ can be seen as a correction factor to specify that U is invertible.

The identity element corresponds to the data $\Lambda(X-1) = 1^n$, and $\Lambda(\phi) = \emptyset$ for $\phi \neq X-1$. Thus we have

Corollary 1. *Let q be a prime power. Then $|\mathrm{GL}_n(q)| = \prod_{k=0}^{n-1} (q^n - q^k) = q^{n^2} (q^{-n}; q)_n$.*

Note that $|\mathrm{GL}_n(q)|/q^{n^2} = \prod_{k=1}^n (1 - q^{-k})$, and the infinite product $\prod_{k=1}^{\infty} (1 - q^{-k})$ converges to some $\gamma_q > 0$. This shows that $|\mathrm{GL}_n(q)| \sim \gamma_q q^{n^2}$. The approximate value of $\gamma_2 \approx 0.28878809508660242$.

4 Powers

We now analyze $M(\phi^r)$, where ϕ is an irreducible monic polynomial, and obtain a characterization of squares of matrices. We start off with a few lemmas which allow us to compute the effect of raising to the r -th power for r a positive integer.

If $\phi(X)$ is a monic polynomial of degree d then $M(X)$ is the matrix of multiplication by X with respect to the ordered basis $1, X, \dots, X^{d-1}$ where multiplication of polynomials is taken (mod $\phi(X)$). If we write down the matrix of multiplication by X with respect to another basis, then it is similar to $M(X)$.

In the following, if $\phi(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ is a polynomial with roots $\alpha_1, \dots, \alpha_n$ in the algebraic closure, and $r > 0$ an integer, denote by $\phi^{(r)}(X) = (X - \alpha_1^r) \cdots (X - \alpha_n^r)$ roots are the r -th powers $\alpha_1^r, \dots, \alpha_n^r$ of the roots of ϕ . If ϕ is defined over \mathbb{F}_q then so is $\phi^{(r)}$. When ϕ is a polynomial over \mathbb{F}_2 , we have $\phi^{(2)}(X) = \phi(X)$.

Lemma 1 (The Chinese Remainder Theorem). *Let $\phi(X)$ and $\psi(X)$ denote relatively prime monic polynomials. Then*

$$M(\phi(X)\psi(X)) \sim M(\phi(X)) \oplus M(\psi(X)).$$

Proof. Since $\phi(X), \psi(X)$ are relatively prime, there are polynomials $u(X), v(X)$ such that

$$u(x)\phi(X) + v(X)\psi(X) = 1.$$

Let $d = \deg(\phi), e = \deg(\psi)$, and $B_1 := ((X^i v(X) \bmod \phi(X))\psi(X) : i = 0, \dots, d-1)$ and $B_2 := ((X^i u(X) \bmod \psi(X))\phi(X) : i = 0, \dots, e-1)$. Let V_1 be the span of B_1 and V_2 the span of B_2 . Then the space spanned by $1, \dots, X^{d+e-1}$ is $V_1 \oplus V_2$, and multiplication by X leaves V_1 and V_2 invariant. Furthermore, the matrix of X with respect to B_1 is $M(\phi)$ and with respect to B_2 is $M(\psi)$. \square

Corollary 2. *Let $\phi(X)$ be a monic polynomial whose factorization in the algebraic closure is $\phi(X) = \prod_i (X - \alpha_i)^{r_i}$, for distinct α_i , and $r_i > 0$. Then*

$$M(\phi(X)) \sim \bigoplus_i (\alpha_i I_{r_i} + M(X^{r_i})),$$

where I_{r_i} is an $r_i \times r_i$ identity matrix and similarity is over the algebraic closure.

Proof. By Lemma 1 it suffices to prove the statement when $\phi(X) = (X - \alpha)^r$ for some $\alpha \in \overline{\mathbb{F}_2}$ and positive integer r . However, we have $X = \alpha + (X - \alpha)$, so multiplication by X is given by the matrix αI_r plus the matrix of multiplication by $(X - \alpha)$. The latter is obviously similar to the matrix of multiplication by $X \bmod X^r$. \square

Lemma 2. *Let n, r be positive integers. Then*

$$M(X^n)^r \sim [n \bmod r]M\left(X^{\lceil n/r \rceil}\right) \oplus [r - (n \bmod r)]M\left(X^{\lfloor n/r \rfloor}\right).$$

Proof. The matrix $M(X^n)$ is the matrix of multiplication by X modulo X^n with respect to the basis $1, X, \dots, X^{n-1}$. Thus $M(X^n)^r$ is the matrix of multiplication by X^r with respect to the same basis. This maps $X^i \mapsto X^{i+r} \mapsto \dots \mapsto X^{i+sr} \mapsto 0$, where $s = \lfloor (n-1-i)/r \rfloor$. When $i < n \bmod r$ we have $s+1 = \lfloor (n+r-1)/r \rfloor = \lceil n/r \rceil$, and $\lfloor n/r \rfloor$ otherwise. \square

Corollary 3. *Let q be a power of 2, r a positive integer, and $\phi \in \mathcal{I}(q)$. Then $M(\phi(X)^r)^2 \sim M(\phi^{(2)}(X)^{\lceil r/2 \rceil}) \oplus M(\phi^{(2)}(X)^{\lfloor r/2 \rfloor})$.*

Proof. Let $\alpha_1, \dots, \alpha_d$ be the roots of $\phi(X)$. By Corollary 2 we have

$$\begin{aligned} M(\phi(X)^r)^2 &\sim \bigoplus_{i=1}^d (\alpha_i I + M(X^r))^2 = \bigoplus_{i=1}^d (\alpha_i^2 I + M(X^r)^2) \\ &= \bigoplus_{i=1}^d (\alpha_i^2 I + M(X^{\lceil r/2 \rceil})) \oplus \bigoplus_{i=1}^d (\alpha_i^2 I + M(X^{\lfloor r/2 \rfloor})) \\ &\sim M\left(\phi^{(2)}(X)^{\lceil r/2 \rceil}\right) \oplus M\left(\phi^{(2)}(X)^{\lfloor r/2 \rfloor}\right). \end{aligned}$$

The first equality follows because the characteristic is 2. The second equality follows from Lemma 2, and the last line from Corollary 2. \square

Corollary 4. *If a matrix $A \in \text{Mat}_n(\mathbb{F}_q)$, where q is a power of 2, is in the conjugacy class with standard representative specified by $\Lambda : \mathcal{I}(q) \rightarrow \mathcal{P}$, then the conjugacy class containing A^2 has its standard representative specified by $\mathcal{M} : \mathcal{I}(q) \rightarrow \mathcal{P}$, where $m_i(\mathcal{M}(\phi)) = 2m_{2i}(\Lambda(\phi^{(2)})) + m_{2i-1}(\Lambda(\phi^{(2)})) + m_{2i+1}(\Lambda(\phi^{(2)}))$ for all ϕ and $i \geq 1$.*

Proof. If

$$A \sim \bigoplus_{\phi \in \mathcal{I}(q)} \bigoplus_j M\left(\phi(X)^{\Lambda(\phi)_j}\right),$$

then

$$A^2 \sim \bigoplus_{\phi \in \mathcal{I}(q)} \bigoplus_j M\left(\phi^{(2)}(X)^{\Lambda(\phi)_j}\right)^2.$$

It thus suffices to show that for all $\phi \in \mathcal{I}(q)$, and $\lambda \in \mathcal{P}$

$$\bigoplus_j M(\phi(X)^{\lambda_j})^2 \sim \bigoplus_j M(\phi^{(2)}(X)^{\mu_j}),$$

where $\mu \in \mathcal{P}$ satisfies $m_i(\mu) = 2m_{2i}(\lambda) + m_{2i-1}(\lambda) + m_{2i+1}(\lambda)$. By Corollary 3 we have

$$M(\phi(X)^{\lambda_j})^2 \sim M(\phi^{(2)}(X)^{\lceil \lambda_j/2 \rceil}) \oplus M(\phi^{(2)}(X)^{\lfloor \lambda_j/2 \rfloor}).$$

If $\lambda_j = 2i$ then it contributes 2 to the multiplicity $m_i(\mu)$. Otherwise it contributes 1, thus giving the assertion. \square

By enumerating all partitions of n one can produce the set of partitions of the form $\mathcal{M}(\phi)$ as in the above corollary. Counting these partitions produces the sequence 1, 1, 2, 3, 4, 5, 7, 10, 13, 16, 21, 28, 35, 43, 55, 70, \dots which is sequence A006950 in the OEIS. There are many comments there about classes of partitions. They include: ‘‘Also the number of partitions of n in which all odd parts occur with multiplicity 1.’’ None of the above partitions fell into any of the classes referred to, but the conjugates did. This yielded Proposition 3 below. The sequence above is also the sequence of coefficients of one of Ramanujan’s mock ϑ functions whose generating function is

$$\vartheta(z) := \prod_{k>0} \frac{1 + z^{2k-1}}{1 - z^{2k}}.$$

Proposition 3. *Let $\Delta : \mathcal{P} \rightarrow \mathcal{P}$, be defined by $m_i(\Delta(\lambda)) = 2m_{2i}(\lambda) + m_{2i-1}(\lambda) + m_{2i+1}(\lambda)$, for all i . Then μ is in the image of Δ if and only if $m_{2i-1}(\mu') \leq 1$ for $i \geq 1$.*

Proof. Let $\mu = \Delta(\lambda)$. We have $\mu'_i = \sum_{j \geq i} m_j(\mu)$. Substituting in the value of $m_j(\mu)$ we obtain

$$\mu'_i = \sum_{j \geq i} (2m_{2j}(\lambda) + m_{2j-1}(\lambda) + m_{2j+1}(\lambda)) \equiv m_{2i-1}(\lambda) \pmod{2}.$$

If $m_j(\mu') \geq 2$ then there is an i such that $j = \mu'_{i+1} = \mu'_i$. We have $m_i(\mu) = \mu'_i - \mu'_{i+1} = 0$ and thus $m_{2i-1}(\lambda) = 0$. The above congruence shows that $j = \mu'_i$ is even. In other words $m_j(\mu') \leq 1$ if j is odd.

For the converse, suppose that we have a partition μ so that $m_{2i-1}(\mu') \leq 1$ for all i . Define the sequence b_i as follows: for all $i \geq 1$ set $b_{2i-1} \in \{0, 1\}$, such that $b_{2i-1} \equiv \mu'_i \pmod{2}$. For all $i \geq 1$ set $b_{2i} = (m_i(\mu) - b_{2i-1} - b_{2i+1})/2$. First, we show that $b_{2i} \in \mathbb{Z}$. We have $m_i(\mu) = \mu'_i - \mu'_{i+1}$. Thus $m_i(\mu) - b_{2i-1} - b_{2i+1} \equiv (\mu'_{i+1} + b_{2i+1}) + (\mu'_i + b_{2i-1}) \equiv 0 \pmod{2}$. Second, we show that $b_{2i} \geq 0$. This is trivially true if $m_i(\mu) \geq 2$, since $b_{2i-1}, b_{2i+1} \in \{0, 1\}$. If $m_i(\mu) = 1$, since $m_i(\mu) \equiv b_{2i-1} + b_{2i+1} \pmod{2}$, not both of the b can be 1. If $m_i(\mu) = 0$, then $\mu'_{i+1} = \mu'_i$, which, by the condition on μ implies that μ'_i and μ'_{i+1} are even. By

the construction above this implies that $b_{2i-1} = b_{2i+1} = 0$, and thus $b_{2i} = 0$. We then construct a partition λ such that $m_i(\lambda) = b_i$. This exists since the only necessary condition on b_i for the existence of such a partition is that $b_i \geq 0$ and $b_j = 0$ for j sufficiently large. \square

The key result in allowing an efficient calculation of our sequences is that the conjugacy classes involved are exactly those with a restriction on the possible partitions, but any irreducible polynomial is allowed.

Definition 7. For each $\phi \in \mathcal{I}(q)$ let $\mathcal{S}_\phi \subseteq \mathcal{P}$ be a subset of partitions containing the empty partition.

We call a sequence $\mathcal{C}_n \subseteq \text{Mat}_n(\mathbb{F}_q)$ of a union of conjugacy classes partition restricted with respect to the family $\{\mathcal{S}_\phi\}$ if the functions $\Lambda : \mathcal{I}(q) \rightarrow \mathcal{P}$ which describe the elements of \mathcal{C}_n are exactly the functions such that $\dim \Lambda = n$ and, for all $\phi \in \mathcal{I}(q)$, we have $\Lambda(\phi) \in \mathcal{S}_\phi$. If all \mathcal{S}_ϕ are the same (in which case we drop the subscript) we call the sequence \mathcal{C}_n partition uniform with respect to \mathcal{S} .

Using these results yields

Theorem 1. Let $\mathcal{C}_n \subseteq \text{Mat}_n(\mathbb{F}_2)$ denote the set of squares of elements of $\text{Mat}_n(\mathbb{F}_2)$. Then \mathcal{C}_n is a union of conjugacy classes and it is partition uniform with respect to $\mathcal{S} = \{\lambda \in \mathcal{P} : m_{2i-1}(\lambda) \leq 1, i \geq 1\} \cup \{\emptyset\}$.

Proof. If a conjugacy class is specified by $\lambda : \mathcal{I}(2) \rightarrow \mathcal{P}$ its standard representative is

$$\bigoplus_{\phi \in \mathcal{I}(2)} \bigoplus_i M\left(\phi^{\lambda(\phi)_i}\right).$$

and thus its square is conjugate to

$$\bigoplus_{\phi \in \mathcal{I}(2)} \bigoplus_i M\left(\phi^{\lambda(\phi)_i}\right)^2.$$

Thus it suffices to consider $M(\phi(X)^r)^2$, where ϕ is irreducible. The proof is finished using Corollary 4 and Proposition 3. \square

Armed with the above characterization of conjugacy classes of squares, one could proceed by enumerating all such classes, and then summing the sizes of the conjugacy classes, to get the desired counts. This, indeed, would adhere to Wilf's dictum² [25] of a "good answer", since the number of such classes appears to be of the order of 2^n . In fact, as we shall see in Theorem 2, they are precisely of this order. The first 60 terms of the sequence of the number of such classes appears in Table 1. However we can do much better, as we shall see in the next section.

²More precisely, if \mathcal{A}_n denotes a class of combinatorial object of "size" n , a good answer would be an algorithm to calculate $|\mathcal{A}_n|$ with running time $o(|\mathcal{A}_n|)$.

Table 1: Conjugacy classes of squares

n	$GL_n(\mathbb{F}_2)$	$Mat_n(\mathbb{F}_2)$
1	1	2
2	2	4
3	5	10
4	10	22
5	20	46
6	41	96
7	82	198
8	166	406
9	334	826
10	667	1668
11	1336	3362
12	2682	6770
13	5360	13590
14	10724	27248
15	21467	54614
16	42936	109378
17	85876	218946
18	171786	438180
19	343574	876738
20	687184	1753998
21	1374427	3508726
22	2748852	7018368
23	5497766	14038006
24	10995706	28077846
25	21991402	56157954
26	43982908	112318900
27	87966150	224642090
28	175932383	449289666
29	351864964	898586438
30	703730584	1797182704
31	1407461288	3594378014
32	2814923196	7188772666
33	5629847656	14377567834
34	11259695532	28755164100
35	22519392276	57510365698
36	45038787489	115020782350
37	90077575358	230041628622
38	180155153036	460083340304
39	360310311906	920166792942
40	720620625522	1840333728182
41	1441241255486	3680667639522
42	2882482522524	7361335523444
43	5764965048250	14722671356642
44	11529930107318	29445343113738
45	23059860237589	58890686756910
46	46119720481194	117781374180336
47	92239440983766	235562749221166
48	184478882017076	471125499580570
49	368957764045976	942251000588770
50	737915528134398	1884502003008980
51	1475831056367066	3769004008432714
52	2951662112765356	7538008019902670
53	5903324225614736	15076016043685054
54	11806648451425570	30152032092453552
55	23613296902912949	60304064191298614
56	47226593806008646	120608128390767918
57	94453187612408280	241216256792193274
58	188906375224938380	482432513597744820
59	377812750450241204	964865027212545410
60	755625500901295794	1929730054447325946

5 Generating Functions

Let $\mathcal{C}_n \subseteq \text{Mat}_n(\mathbb{F}_2)$ be a union of conjugacy classes for each $n \geq 1$. We associate two generating functions with \mathcal{C} . The first has coefficients which give the numbers of elements in the conjugacy class \mathcal{C}_n (scaled by the total number of invertible elements):

$$F_{\mathcal{C}}(x) := 1 + \sum_{n=1}^{\infty} \frac{|\mathcal{C}_n|}{|\text{GL}_n(\mathbb{F}_2)|} x^n.$$

The second has coefficients which give the number of conjugacy classes in \mathcal{C}_n :

$$G_{\mathcal{C}}(x) := 1 + \sum_{n=1}^{\infty} |\#\{\Lambda \in \mathcal{C}_n\}| x^n,$$

where, by abuse of notation, we say that $\Lambda \in \mathcal{C}_n$ if $\Lambda: \mathcal{I}(q) \rightarrow \mathcal{P}$ specifies a conjugacy class in \mathcal{C}_n .

We use the coefficient $|\mathcal{C}_n|/|\mathrm{GL}_n(\mathbb{F}_2)|$ because it is

$$\sum_{\Lambda} \frac{1}{C(\Lambda, q)} \tag{1}$$

where the outer sum is taken over all $\Lambda: \mathcal{I}(q) \rightarrow \mathcal{P}$, specifying the conjugacy classes in \mathcal{C}_n , and because $C(\Lambda, q)$ has a multiplicative decomposition as in Proposition 1.

The reason for the definitions of partition restricted and partition uniform is the following:

Proposition 4. *Let $\mathcal{C}_n \subseteq \mathrm{Mat}_n(\mathbb{F}_q)$ be a union of conjugacy classes, and $F_{\mathcal{C}}(X)$ the associated generating function (resp., $G_{\mathcal{C}}(X)$ is the associated generating function for the number of conjugacy classes). If \mathcal{C}_n is partition restricted with respect to \mathcal{S}_{ϕ} then*

$$F_{\mathcal{C}}(X) = \prod_{\phi \in \mathcal{I}(q)} \sum_{\lambda \in \mathcal{S}_{\phi}} \frac{1}{C(\lambda, q^{\deg(\phi)})} X^{|\lambda| \deg(\phi)}, \tag{2}$$

and

$$G_{\mathcal{C}}(X) = \prod_{\phi \in \mathcal{I}(q)} \sum_{\lambda \in \mathcal{S}_{\phi}} X^{|\lambda| \deg(\phi)}. \tag{3}$$

If \mathcal{C}_n is partition uniform with respect to \mathcal{S} then

$$F_{\mathcal{C}}(X) = \prod_{d=1}^{\infty} \left(\sum_{\lambda \in \mathcal{S}} \frac{1}{C(\lambda, q^d)} X^{|\lambda|d} \right)^{|\mathcal{I}(q)_d|}, \tag{4}$$

and

$$G_{\mathcal{C}}(X) = \prod_{d=1}^{\infty} \left(\sum_{\lambda \in \mathcal{S}} X^{|\lambda|d} \right)^{|\mathcal{I}(q)_d|}. \tag{5}$$

Proof. We use the multiplicative decomposition from Proposition 2 to see that

$$F_{\mathcal{C}}(X) = \sum_{\Lambda} \prod_{\phi \in \mathcal{I}(q)} \frac{1}{C(\Lambda(\phi), q^{\deg(\phi)})} X^{|\Lambda(\phi)| \deg(\phi)},$$

where the sum is over all possible Λ describing the conjugacy classes in \mathcal{C}_n . By the definition of partition restricted, we may interchange the summation and product obtaining Equation (2). By definition of partition uniform we then have Equation (4). A similar argument applies to $G_{\mathcal{C}}$. \square

If we are interested only in classes in $\text{GL}_n(\mathbb{F}_2)$ instead of $\text{Mat}_n(\mathbb{F}_2)$ we modify Equations (4) and (5) by using the exponent $q-1$ instead of $|\mathcal{I}(q)_1| = q$, which corresponds to omitting the irreducible polynomial $\phi(X) = X$.

We now show that the number of conjugacy classes of squares (both for all matrices and for invertible matrices) grows exactly as 2^n .

Lemma 3. *Let q be a prime power. As formal power series we have*

$$1 - qX = \prod_{n=1}^{\infty} (1 - X^n)^{|\mathcal{I}(q)_n|}. \quad (6)$$

Proof. Since both the left- and right-hand sides of Equation (6) have constant term 1, it suffices to show that the logarithmic derivatives of both sides are equal. The logarithmic derivative of the right-hand side is

$$\begin{aligned} - \sum_{n=1}^{\infty} \frac{n|\mathcal{I}(q)_n|X^{n-1}}{1 - X^n} &= - \sum_{n=1}^{\infty} \sum_{j=0}^{\infty} n|\mathcal{I}(q)_n|X^{(j+1)n-1} \\ &= - \sum_{m=1}^{\infty} X^{m-1} \sum_{d|m} d|\mathcal{I}(q)_d| \\ &= - \frac{1}{X} \sum_{m=1}^{\infty} (qX)^m = - \frac{q}{1 - qX}, \end{aligned}$$

which is the logarithmic derivative of the left-hand side. In the above we have used the fact that $\sum_{d|m} d|\mathcal{I}(q)_d| = q^m$. This holds because every element of \mathbb{F}_{q^m} is the root of some irreducible polynomial over \mathbb{F}_q of degree $d \mid m$ (and conversely), and each of those polynomials has exactly d roots. \square

Theorem 2. *Let $a'(n)$ denote the number of conjugacy classes of squares for $\text{Mat}_n(\mathbb{F}_2)$ and $b'(n)$ the number of conjugacy classes of squares for $\text{GL}_n(\mathbb{F}_2)$. We have*

$$1 + \sum_{n=1}^{\infty} a'(n)z^n = \prod_{n=1}^{\infty} \frac{1 - 2z^{2n}}{(1 - 2z^n)(1 - 2z^{4n})}$$

and

$$1 + \sum_{n=1}^{\infty} b'(n)z^n = \prod_{n=1}^{\infty} \frac{(1 - z^{2n})(1 - 2z^{2n})}{(1 + z^{2n-1})(1 - 2z^n)(1 - 2z^{4n})}.$$

From this it follows that there are real $\alpha', \beta' > 0$ such that $a'(n) \sim \alpha'2^n$ and $b'(n) \sim \beta'2^n$.

Proof. When \mathcal{C} is the set of conjugacy classes of squares of all matrices then $G_{\mathcal{C}}(z) = \prod_{d=1}^{\infty} \vartheta(z^d)^{|\mathcal{I}(q)_d|}$. When we are dealing with invertible matrices the

only factor that differs is the one for $d = 1$. Since $|\mathcal{I}(q)'_1| = |\mathcal{I}(q)_1| - 1$, we must divide the above by $\vartheta(z)$. However we have

$$\begin{aligned}\vartheta(z) &= \prod_{n=1}^{\infty} \frac{1 + z^{2n-1}}{1 - z^{2n}} \\ &= \prod_{n=1}^{\infty} \frac{(1 - z^{2n})}{(1 - z^n)(1 - z^{4n})}.\end{aligned}$$

We now apply Lemma 3 to each of the factors and find that

$$G_{\mathcal{C}}(z) = \prod_{n=1}^{\infty} \frac{1 - 2z^{2n}}{(1 - 2z^n)(1 - 2z^{4n})}.$$

This product clearly converges when $|z| < 1/2$, has a simple pole at $z = 1/2$, and has no other singularities when $|z| = 1/2$. We have

$$\alpha' := \lim_{z \rightarrow 1/2} (1 - 2z)G_{\mathcal{C}}(z) = \prod_{n=1}^{\infty} \frac{1 - 2(1/2)^{2n}}{(1 - (1/2)^n)(1 - 2(1/2)^{4n})}.$$

Thus, $a'(n) \sim \alpha' 2^n$. For the case that \mathcal{C} specifies invertible squares we must divide the above by $\vartheta(1/2)$. \square

We may calculate $F_{\mathcal{C}}(X)$ by using any of the standard fast algorithms for manipulating power series [5] but we may exploit its special form for a more efficient calculation as follows.

A large part of the calculation involves calculating a product

$$F(X) = \prod_{d=1}^n f_d(X)^{n_d}$$

for power series $f_d(X)$ whose constant term is 1, and positive integer exponents n_d . We may speed up this calculation substantially as follows: taking the logarithmic derivative, we have

$$\frac{F'(X)}{F(X)} = \sum_{d=1}^n n_d \frac{f'_d(X)}{f_d(X)},$$

of which we're interested in the first $n + 1$ terms. Treating the coefficients of $F(X)$ after the constant term (which is 1) as unknowns, we get a linear system by multiplying both sides by $F(X)$ and equating coefficients. In fact, the linear system is lower triangular, and so may be solved quickly. For large n we may do this more quickly by using the algorithm described in [4]. Making this change sped up the calculation for $n = 14$ from 318 seconds to 1 second. This speed-up improves substantially for larger n .

As an alternative to directly manipulating the coefficients as large rational numbers, we may use the Chinese Remainder Theorem. Choose distinct odd

primes p_1, \dots, p_r so that $\prod_i p_i > 2^{n^2}$, and p_i does not divide $2^k - 1$ for $k \leq n$. Note that by the prime number theorem (or weaker estimates) we may do this with $p_i \approx \log(2^{n^2}) = n^2 \log(2)$, and $r \approx n^2 / \log(n)$. We then have $C(\lambda, q^d) \not\equiv 0 \pmod{p_i}$, so that we may calculate the truncated power series of each of the above summands modulo p_i , and then the truncated version of F_C modulo each of the p_i . We then multiply the coefficients of x^k by the $|\mathrm{GL}_k(\mathbb{F}_2)| \pmod{p_i}$, and finally use the Chinese Remainder Theorem to recover $|S_k|$ since we know that it is a positive integer $\leq 2^{n^2}$.

Note that the proof of Proposition 3 yields an algorithm to decide whether or not a matrix in $\mathrm{Mat}_n(\mathbb{F}_2)$ is a square, and, if so, calculate a square root. Namely, using algorithms for rational canonical form [21] we obtain a change-of-basis matrix and a standard representative. We use the construction in the proof of Proposition 3 to find a partition associated with the class of a square root. Finally, we use the change-of-basis matrix to transform the rational canonical form of the square root.

6 Results

We programmed the algorithm described above in the SAGE system for symbolic calculation [23] and used it to calculate the first 60 terms of the following sequences:

Table 2: Calculation Times

Classes	Partition Count	Time
Squares in $\mathrm{Mat}_n(\mathbb{F}_2)$	641800	429.69 sec
Squares in $\mathrm{GL}_n(\mathbb{F}_2)$	157671	99.30 sec
Separable elements in $\mathrm{Mat}_n(\mathbb{F}_2)$	1	1.11 sec
Separable elements in $\mathrm{GL}_n(\mathbb{F}_2)$	1	1.10 sec
Semisimple elements in $\mathrm{Mat}_n(\mathbb{F}_2)$	60	1.08 sec
Semisimple elements in $\mathrm{GL}_n(\mathbb{F}_2)$	60	1.35 sec

In Table 3 (pages 19–27) we give the first 60 terms of the sequence $a(n)$, the number of $n \times n$ matrices with coefficients in \mathbb{F}_2 which are squares of other such matrices. The related sequence $b(n)$ in which the matrices are invertible is given in Table 4 (pages 27–35). We generated these tables in about 200 seconds each on a workstation.

In order to show that there is an $\alpha > 0$ such that $a(n) \sim \alpha 2^{n^2}$ (and similarly for $b(n)$ and β) it would suffice to show that $F_C(z)$ is holomorphic in the disk $\{z \in \mathbb{C} : |z| \leq 1 + \epsilon\}$ apart from having a simple pole at $z = 1$ with residue $-\alpha/\gamma_2$, where $\gamma_2 := \prod_{n=1}^{\infty} (1 - 2^{-n}) \approx 0.28878809508660242$ (since $|\mathrm{GL}_n(\mathbb{F}_2)| \sim \gamma_2 2^{n^2}$). We conjecture that this is, indeed, the case. Note that Wall [24] has proved similar statements when C specifies the classes of semisimple, regular,

and regular semisimple matrices over a finite field.

As a sanity check on the conjecture we have calculated the coefficients of the first 71 coefficients c_0, \dots, c_{70} of $F_{\mathcal{C}}(z)$, where \mathcal{C} is the classes of squares of invertible matrices, within an accuracy of 2^{-3600} , and set $\widehat{\beta} = c_{70}$ to be the coefficient of z^{70} . We plot below $|c_j - \widehat{\beta}|^{-1/j}$ for $j = 1, \dots, 69$. We have $\widehat{\beta} \approx 0.5844546428649343516383$.

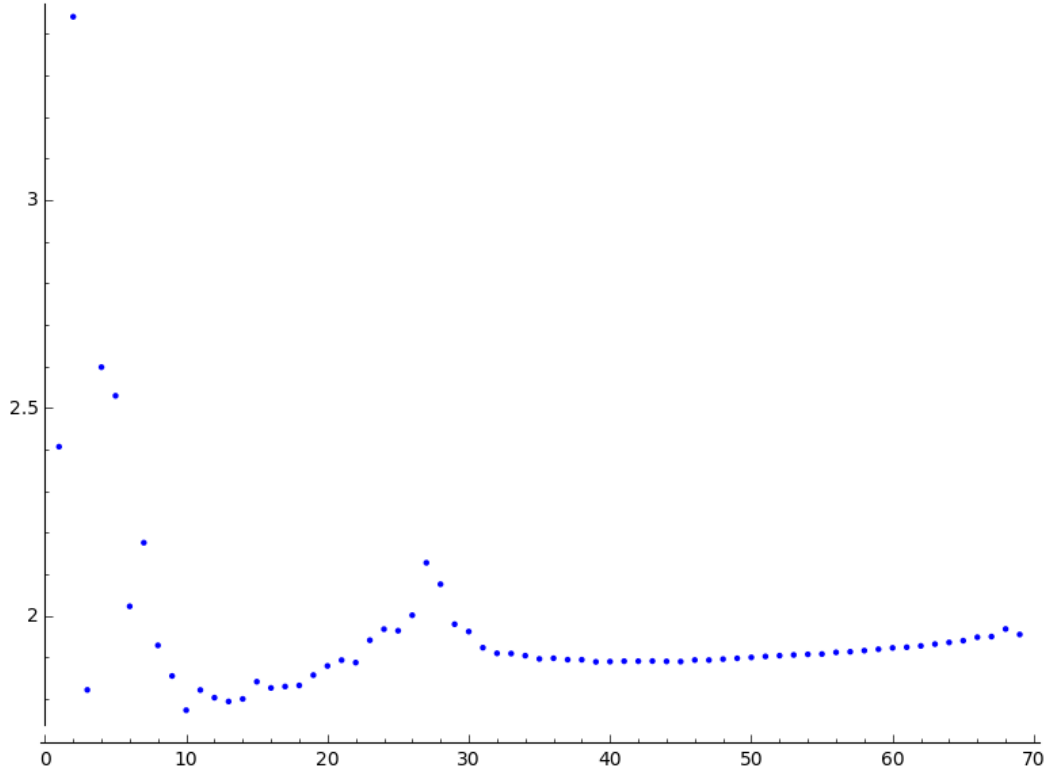


Figure 1: $|c_j - \widehat{\beta}|^{-1/j}$

From Figure 1, it appears that, except for a pole at $z = 1$, $F_{\mathcal{C}}(z)$ is holomorphic in an open disk of radius $1.954579780196859562\dots$ centered at 0. We give a similar plot in Figure 2, where \mathcal{C} is the class of squares of all matrices, and the coefficients of $F_{\mathcal{C}}(z)$ are d_0, d_1, \dots .

From these figures, it appears that $\widehat{\alpha} \approx 1.358036747413654505$, and that, apart from the pole at $z = 1$ that $F_{\mathcal{C}}(z)$ is holomorphic in an open disk of radius $1.931991705356004184580743154\dots$.

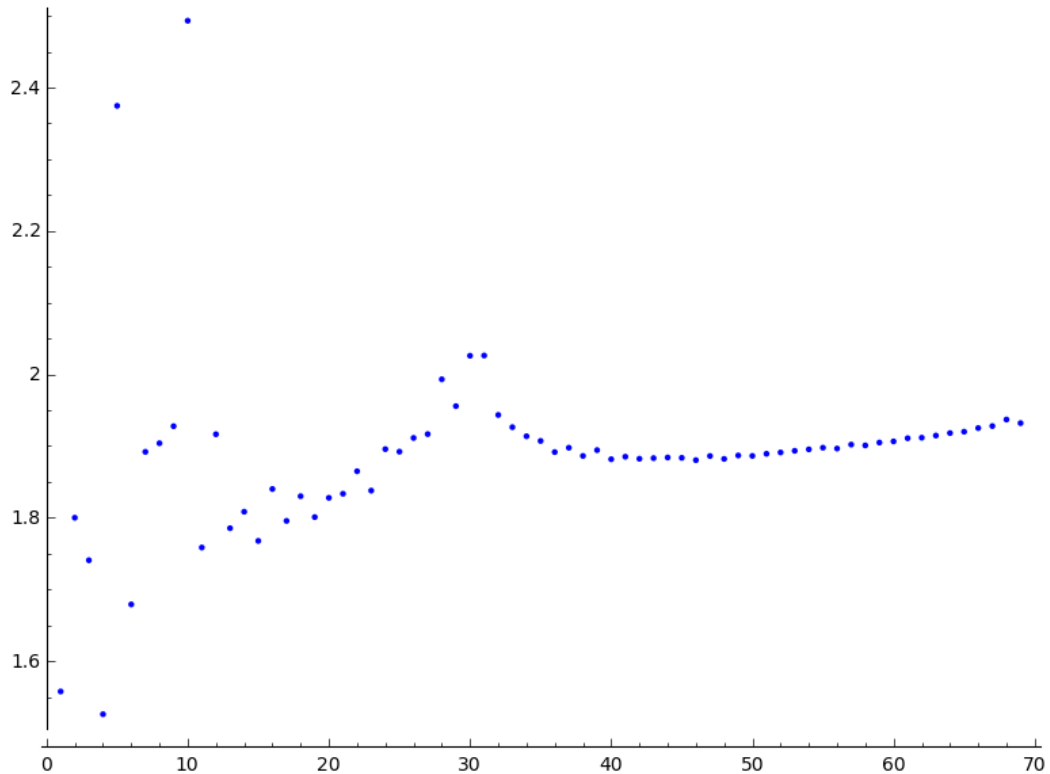


Figure 2: $|d_j - \hat{\alpha}|^{-1/j}$

7 Remarks and Open Problems

The decomposition given in Equation (2) is closely related to the product formula for the cycle index as described in [9, 14, 22]. Following [22], we define a generating function

$$Z_d(q; x) := \frac{1}{[q]_d} \sum_{\alpha \in \text{Mat}_d(\mathbb{F}_q)} \prod_{\phi, \lambda} x_{\phi, \lambda}^{a_{\phi, \lambda}(\alpha)},$$

where $\phi \in \mathcal{I}(q)$, $\lambda \in \mathcal{P}$, $a_{\phi, \lambda} = 1$ if (ϕ, λ) occurs in the description of the conjugacy class of α and 0 if it does not, and $[q]_d = |\text{GL}_d(\mathbb{F}_q)|$. Define $Z_0(q; x) = 1$. We then define a generating function

$$\Phi(u; x) := 1 + \sum_{d \geq 1} Z_d(q; x) u^d.$$

Kung [14] and Stong [22] prove the factorization

$$\Phi(u; x) = \prod_{\phi \in \mathcal{I}(q)} \left(1 + \sum_{\lambda \in \mathcal{P}} \frac{x_{\phi, \lambda}}{C(\lambda, \phi)} u^{|\lambda|d} \right).$$

If our sets \mathcal{C}_n are partition restricted, and we set $x_{\phi, \lambda} = 1$ if $\lambda \in \mathcal{S}_\phi$ and 0 otherwise, then we recover Equation (2).

Fulman [9] and Lehrer [18] have given closed-form expression for the ratios corresponding to α and β in the three cases treated by Wall—the semisimple, regular, and regular semisimple matrices. We leave it as an open problem to prove the conjecture in Section 6 and find a closed-form expression for α and β .

As a generalization of Proposition 3 it would be interesting to find a closed-form expression for the number of partitions λ with the property $m_i(\mu) = 2m_{2i}(\lambda) + m_{2i-1}(\lambda) + m_{2i+1}(\lambda)$ for all i when $m_{2i+1}(\mu') \leq 1$. This amounts to counting the number of integer points in the polytope given by the above equalities and $m_i(\lambda) \geq 0$.

The methods used here should, in principle, be able to be used to answer analogous questions, such as the number of $n \times n$ matrices over \mathbb{F}_3 which are cubes.

8 Acknowledgments

First, and foremost, I'd like to thank Neil Sloane for posing the problem, and for his magnificent creation of the OEIS. It has proven invaluable to me and to countless other mathematicians. I'd also like to thank Bob Guralnick for referring me to his work and others' on related problems, and Jason Fulman for useful correspondence. Last, I'd like to thank the late Herb Wilf whose wonderful works have been an inspiration to me.

A Algorithms

Listings

- 1 C program for exhaustively calculating $a(n)$ 16
- 2 SAGE programs for improved algorithm 18

Listing 1: C program for exhaustively calculating $a(n)$

```
#include <stdlib.h>
#define BITS_PER_BYTE 8
inline void SetBit(unsigned long int *t, const unsigned long int i) {
    const int bits = BITS_PER_BYTE * sizeof(unsigned long int);
    t[i/bits] |= 1L << (i%bits);
}
unsigned long int CountUp(unsigned long int *tab, const long int n) {
    unsigned long int count = 0UL;
    long int i;
    for(i=0; i < n; i++) {
        count += __builtin_popcountl(tab[i]);
    }
    return count;
}
```



```

unsigned long int SloaneExhaust(const int n) {
    const long int n2 = 1L<<(n*n);
    unsigned long int *table;
    const long int lchunk = sizeof(unsigned long int);
    const long int chunk = BITS_PER_BYTE*lchunk;
    const int t_size = (n2 + chunk - 1)/chunk;
    int t;
    unsigned long int A,A2;
    unsigned long int rmask,cmask;
    unsigned long int bigcount;
    table = (unsigned long int *)calloc(t_size,sizeof(unsigned long int));
    A = 0L; B = 0L;

    /* B represents the current value of A2 */
    SetBit(table,B);
    rows_mask = (1L<<n) - 1L;
    col_mask = 0L;
    for(t=0; t < n*n; t += n) {
        col_mask |= 1L<<t;
    }
    for(t=1; t < n2; t++) {
        /* get bit index to be flipped in Gray code */
        const long int k = __builtin_ctz1(t);
        const long int i = k/n;
        const long int j = k%n;
        const unsigned long int Eij = 1L<<k;
        /* Eij represents Ei,j */
        /* B ← B + AE + EA */
        B ^= (((A>>(n*j))&rows_mask)<<(n*i)) ^ (((A>>i)&col_mask)<<j);
        if (i == j)
            B ^= Eij; /* B ← B + Ei,j */
        A ^= Eij; /* A ← A + Ei,j */
        SetBit(table,B);
    }
    bigcount = CountUp(table,t_size);
    free(table);
    return bigcount;
}

```

Listing 2: SAGE programs for improved algorithm

```

def Count(n, all=True):
    return CountGeneral(n, myparts, all=all)

def CountGeneral(n, s, all=True):
    R.<x> = PowerSeriesRing(QQ, default_prec = n+1)
    pp = [R(1) for _ in range(n+1)]
    for w in range(1, n+1):
        for lam in s(w):
            for d in range(1, n//w+1):
                pp[d] += centralizer(lam, QQ(2)^d)^-1*x^(w*d)
    res = BigProduct(pp[1:], [Irr(2, d, all=all) for d in range(1, n+1)], n)
    return [GLorder(-+1, 2)*res[_] for _ in range(n)]

# auxilliary routines
def multiplicity(p):
    # p is a partition
    l = p.conjugate().to_list()
    return [1[-1] - 1[_] for _ in range(1, len(l))] + [1[-1]]

def qPoch(a, q, n):
    return prod([1-a*q^k for k in range(n)])

def centralizer(lam, q):
    if lam.size() == 0:
        return 1
    return q^sum([x^2 for x in lam.conjugate()]) * prod([qPoch(q^(-x), q, x)
        for x in multiplicity(lam)])

def GLorder(n, q):
    return centralizer(Partition(n*[1]), q)

def Irr(q, d, all=True):
    if d == 1 and (not all):
        return q-1
    return sum([moebius(d//n)*(q^n) for n in divisors(d)])/d

def LDeriv(f):
    return f.derivative()/f

# routine for calculating  $\prod_d f_d(X)^{n_d}$ 
def BigProduct(l, p, prec):
    # l are power series, and p are exponents
    n = len(l)
    xx = sum([p[_]*LDeriv(l[_]) for _ in range(n)])
    R = xx.parent().base_ring()
    res = vector(R, xx.padded_list()[ : prec])
    mat = matrix(R, prec, prec)
    for k in range(prec):
        for r in range(1, k+1):
            mat[k, r-1] = -res[k-r]
            mat[k, k] = R(k+1)
    return mat.solve_right(res)

# routines for enumerating the restricted partitions
def OPart(n, k):
    # Partitions of n whose odd parts have multiplicity <=1 and whose largest part
    # is k
    if n < k:
        return
    elif k == 1:
        if n == 1:
            yield [1]
    elif k == 0:
        if n == 0:
            yield []
    elif k == 2: # optimization
        yield (n//2)*[k] + (n%2)*[1]
    else:
        for m in range(1, 1 + (1 if (k%2 == 1) else n//k)):
            for j in range(k):
                for x in OPart(n-m*k, j):
                    yield m*[k] + x

def PPart(n):
    for j in range(1, n+1):
        for x in OPart(n, j):
            yield x

def myparts(n):
    for x in PPart(n):
        if len(x) > 0:
            yield Partition(x).conjugate()

```

B Table of Values

Table 3: Number of matrices which are squares

n	$a(n)$
1	2
2	10
3	260
4	31096
5	13711952
6	28275659056
7	224402782202048
8	7293836994286696576
9	952002419516769475035392
10	497678654312172407869125822976
11	1044660329769242614113093804053562368
12	8745525723307044762290950664928498588583936
13	293618744028817341095271816309320065715829741719552
14	39383702222786673926973162381076522518507786667469626679296
15	21150238597201101682069653858523961291120582792608950528438094020608
16	45410660127461275237941140143536776375549893844693861704643098807104866123776
17	390101945316359714580421140557532387368578828048878080130759759836237802714330925432832
18	13403092871085920406314564188970796007326922629801352652434803959823674593311775472092120554274816
19	1842148103501576330259341331069776540862527169944272971274211116785218870704083461129503157001537715368624128
20	1012715929581700585613681655233620159191511778259156891597878118890449964327025849578125695019384596395869369232406347776
21	2226999137933663296854759620887600536728599120665505974525522236126730830375963094754875023816493012915661680538919480601183075172352
22	19588828198703278571024299401416264358500264411413067748069407899768932799351688152780693582858732032044214430634232341070338629544654409476079616
23	689221525035496756361351647448935634808724062439985671680131113946151648996214949824918971349538588152397714074023306002684810590009478259087817615158466838528
24	96999225638457470690443086827404740787337011595114688517737482297228451981545090738063161699981220240205993932587704016447273787657646768245731249979622904089292863529025536
25	54605721382889187766204689925383026326864129975821837520838168357476058859290345594033710189777492653780301555646503875182087202771205827378610916433830771962609525703076373497856699400192

Number of matrices that are squares

n	$a(n)$
26	122961136232456738518169343544464711179763399804248815337332259234723587578 234533956270697359875932841189737178783464560689962308213955384527271383078 443664719573242249793005840341908430393269940016644096
27	110753550506917102020555183021410730069099534351116000195107290954837639196 390278127919317357842567006118709054368527898948974375930501268646808350747 6543406391845897251131993217903131135469731619281854145750034020302848
28	399031709433631703017658114533204944208797016380910447413480753263631286630 187680402706943884528707729788870214085538958275675636370073207929245103463 594439815677681854732635334887430527595248585202852348447128951774709441461 75165464576
29	575065300710281098354799698636945515036215069783224831546016945423927998809 876244559507156482247776723498896018955558062357068918701833713278521764820 903271902075161790471056722809410709759428576064878482718537457543104342794 0796170433584505195407081472
30	331502574845609405779264315726949818030917035236749565194689899904892663932 545732883591656780469456216125928914976449306118407033196912462871989397626 926142439475238840940875440382615982664011047796215605508428138162078636680 8071004299571412795511487391973836053341536256
31	764392894207102265257847017195653186434340079719358880911937748897711867925 416419210901968210336909174497328805637866069966328810976005745898352790494 856376340734539199780801259837144779245892297256844944872605468280749254207 8364196269325117130912358731372786165189583186680364295077756928
32	705028004537651936561227357524616893268475233792910225603476665277944579128 694085604918278333954394770889008633631164238500480020046020306526854157509 230246825672574690336255481489493698602967432285727673450592479663976145313 40553808760544312522487263263255180927995042599111932972147053600199195988 70593536
33	260109423071121966463724821675986145953519802483044705898190424429473853664 158240234692617302613014113067746581469566728955716940276542618752486267859 808760651625476065965989962871158140160419160074037224472076199266144155431 111702800195208767924524915876535449665055652806680208155642418124114679576 9991650918148429463769055232
34	383853756849133406035126012964222679523109384756186232446969061656662416333 746090106367277766077520069122220327365338683554002238584040425034535766058 498705506287874123465441854064485469856527634848182945126829511496523722269 779637136069219161702159987906566214620332362815342608895051724556916617080 012240962674735484818364564906623227448122146816
35	226587264382730858489316712173373054002678727087621112894003074233503122055 829635948241503692286465079808134076751791603584010397816032404187018196653 062566651656788521804473106057708761800543535820205521366317550434923277438 853015249423935080615203717727686291246225324354023524508494338334882998849 196401143525640636208935675582308109583667399669039793585189927518208

Number of matrices that are squares

n	$a(n)$
36	535014051478432593602051098886578713251030363974540143992863857809242293016 336760826369290130840850122970128519846567854263620861027310881120901559106 635100101088418004669403093862103736867846635347567672375454193839523843952 995439661925917424120416656246129061231071469262317351383424214889757995786 735900653404118755034418763142638937819148805184788333407340981078743807991 349143243063296
37	505306484850377090952054136528643177636145631809804879963431909409843885190 399646700922522967436099738466752167665460907067513188281805798062407117187 475165827196129595609539254771248795731472535793697118508899028698531282710 224010340783312291319721141228852846331711478381162039395076150509688111976 603064822892287330988465161998543687433412159331040156997636198742985441830 0710295787925786216016777093717164032
38	190899392621909091672297758449671251497793885503495393070780138498332588199 126739213837946780217316157905100531492306260274221726331111433933104928123 086843575507590622078703458523258400368699822151814061364275937873164357390 198323995611953841333384478991765336133759828969128213867240123666195206285 503102844123107528834127344812410220963746539359108932168253210565955867203 678801299123371399131147414143200028709501911027019065327616
39	288479005850833281386470553755160883499909549399321054508339127949425564896 761242307125443989929684387509865228134847794879470033216048379333842615146 934578559069911149793211568677127980066109034672604500749803595977824083697 713369687254070316238199375627501945147137469089228455026939932726819510798 582842665928872445148312659072701490938403105731292619540808561328513737884 850498624037311694320958796272825240665017684319650311061031122439995927660 93918208
40	174374859298037759177607806868771460338608773262713895837537449153069787363 214877069554836212544208363517221453120686773097090080577474557721382518774 849558815714937838194335236548814512510108241950897974378685476100502347132 408232252195566033868427569140660913542593267863100295860080588736578126288 140121169247251863455538404717876859081291661795462997998581792242287459087 414394219208339773097205152582841390621966537044644554950564732421076498075 79196449066739750283725112344576
41	421612539389103250260438302247104872090884635208279616406622615286960702381 865930510810601409160339410182499439896382448686373245690812514392820174361 236731312543334307073846693378798108148247041572726111345978989322847487736 537679040602041092908754031724306888405046032788453386147712587153597096811 387349369940379592385837923530309548496200558681720318654660010909493304250 149643395951373270255421392339492181739934608308387697876850483155172119657 22270914156812509301346877131058448280068182815751012352

Number of matrices that are squares

n	$a(n)$
42	407758627794943242240965533703863301082597512086931102955782372508551248319 590087938861007679498995143609851940026435717680263469909997014255150371815 549721202806119860754791061702894852372005871224703749705155869362451747211 718703342659993298452712789057643563495162196971290166274554217615578184213 693473988510636325937874311621036296315650847768483420451731370385903589690 620532535074439285010050507327763335485265537442839091417871824854070797238 745375243514828833896887807027388614282871072341267379121357347891421825221 001216
43	157743978659289374084854278032239446114235541346168087768670281390859367023 749942756517201994317887937687017164331521850609267129898401065413835015595 551681384319701435416929805488718756600383230843372350535370242847303022845 630957097539277495088461524590067922586202161721844745034151122603170374016 606470134726233381918842389798422812362365433568724716132697477695282818144 658663007138875818928700886038787772834644959481651186112152517316939443101 231529539643995853076746588078854323269072544035698763109921880779118004414 76540003296822995963813904252928
44	244096983923540501900643971053468046639609667750034217448120758748536098347 002531113545296507346808398595306978677264035024138778086877632868650682004 671857373127814999395701547147470067340642370583963962243160702139714531592 304214381111676889573726709159119550376012009003126640750422220498845669933 991438232701633471033368199867289712479095970831568791647970557474777659373 226178868395863959454706033967750952741432676285767662132657932957279291191 672075212809983258916687009158625180594882078289709503724811693609971816992 1614175895942917832977936899835093598930185966899488096256
45	151088714933736455410052215679520475685238042939208887469359264986029985334 509095141614003060184407616269654987020003243852061036419568684218940902276 470506546056534302905617326907437845305671325519119450153196102323349388204 431709531498800381776056975385652898602305501611959528952947657472475305668 582724713658500880387295320917910895974404087461661345855439539837131884660 816547128547839593410829409262023118711862131939641215424291008037013558052 848686450205665445925285130785490103476601012189806417739975353149433827000 555401233558109386334061996542722546965026347867390495749009921740428392382 7703939072
46	374077539401472545320799023414419090337576823870556001179566869514382244448 128402001941256590646816099117558207234654880423574023512638797948782972278 297218072924916483836407896348154128788608474300919248088566197591101253272 660155811898804797932005482738395023746196669960089477855353857821600454764 961043735671614775327902254558529683206581139842809886527653402183164437947 365774551866371853913505528962935153730913498736667194978996824047126427213 608576977556414445267467172214744002707955586417109972673007052242698228040 351510070959071357860387837867290388199873596973851473884177204393997354586 9051314852753806951628317942869917696

Number of matrices that are squares

n	$a(n)$
47	370468451057850509011706652948115252447100346200961679679215922112547503074 979293966000042614260565373508995645034649903160254913219389090845604482738 559486373092184507017120330526209394305999257257888185908583850701777153717 527475443445739953077528619812487985605995228207071850662015275176060644296 602222778064561088565781294524611589086919681510727280155192111931234796439 461678039734090796292350217208392930897875900752773594129507486567031458532 705739472169733728130500855379899256248414700204351565040040459599971556977 732159940582785679844090300700761433051784331557617537265673374388833384633 14104804644297177772933467901167903444081130150262624746647584768
48	146757673234114470833937267564852239404343565699366325302576855920096489254 753568286569919757416923797209793264858983183551295918028002214610326420415 553960792308931813488895439541061591975343614040615921604235061305195870597 016081359818087772647737526862111061347106350741543208365418490488172090251 931007997614540188217913862509744316209463091074288276914432136709033791357 29934213235241691124546824318222768930208646501683545522431386983901561979 377331803526023952994960888369191930924742167686688970937366387153855062753 884673949411801189260599146645905776961757211940616040986808906459449715783 726415647810879087425397134895153371786104535540908985424236734416980517403 1553430471894368256
49	232546815704137528957174175375483393986525052809740000211609572190575285537 491096256433917205938962036775606621435690744506687523171793688630715483836 343808927991726680567770503142501212928321976610897501452105580525717552116 594750301490391899638902160110860858868166756345069754005073865971227226755 211684976697446335862433202754057498288140636391450342889704144878211433852 564215250809804221209136413218959530026727826829675671360753259769240571444 594653713264278926236562336218952135475455036333922333388557314232745309370 029021753853809945723602707019448455549445931090278056634362019156100343449 523367976227917475046410140697301883380516246157851083634038712564881043798 375475225345278192227624504685159507133886103552
50	147394055254261703863827388064384189719948811737364846049836836917042697568 905804757848241081182853130727088505891453691956417911692163741395898196837 016865151660821306184590343819210292951343194120736974043603847487896063106 570953854014444507290730867525648674393299842914302525216961995342343732174 403168184464287146479674998671062451015658018128890387231323137544059956722 085215635634465593931797128114209037710026872019872053331134414402191153164 553002774072654152667587549870478232497156075766277684236029785358027291963 774248499247459725019972122054743458863315082922703068961372560006779115134 372803124981771081872889247993069503537634300730881822578782262938566189195 082359209936654436684761488568290353609948898748859794730072019772042029039 616

Number of matrices that are squares

n	$a(n)$
51	373688325226268352716562437618167137906737304064386332910162981575279314874 384471000476659146040084114356726862560236251896306773176624041355066758236 803243331138067292174784148282610104331475297032132283680471552644693381234 879692585786406192386155523824590314031924770050484294865705387644070974321 348663653677693211174004561439986693086982961893904942724002529650671352666 016090902285434640040285505323035927234882161862433943553286961333539384175 586311957312694790432863323104640663755643521626028472967351854376142223967 736003727619548010329399241651952953706586903958310149982334608436174808926 849136685358755068520322055928596589638576431391032335627235953276200959202 332148874165444606646268899690685042032180955051807820871608682512495416165 299029309973823940900604470099968
52	378964983817092021526649549578630783428128605845159206060916165189863232967 168012507274966682008956392752813413667126831605849064833340745844461354806 489723868452744067142707260839510255606013243828797611556773487323988775094 565092641703526312417467860023250325624249955364551495754714439189897697163 383302658719482909510351825551173069130586348474494550707310986793000831005 554706139227103843018545271227559288442419349150759908365813081975509817952 100912532546881039522015775007613471296426184023280700148415604179721189992 290421796811212794967069289966450142567069671734478793698003566818348606023 147028216822149020808870619279195564423070077657338583063741258167570825220 304742638458567156572684369106662591441994877781632407611964214603606137888 9948645461727538576949211888240642764936160565360271919432073216
53	153726460544389033042646744104104391528080278222948328239902387922129286874 587888377121950380984005983003705078710496693445572870298606918167526538612 369628789221172406072071562896299784660497541105663838719689431752721990102 513157668071494616813192239120132803581411728954935573126302722827028582000 732355295917229444792504331006342348039122507217825052201688093885814034140 373922612895375030647554177583682998437748849684828653892277922792763733911 663401241077678496536185540892640990955521591606870721558147998733512697988 754663386891642707058044701622329108903741819274169947526124755097960869558 299110378304225034476326790146055222387626241304270914653868740257968609700 863137762698697318687527089231071623887432126663106754528903923739298088651 202635391432528562964826974717992043410045600471138148007786278015607074159 270190691942884442112

Number of matrices that are squares

n	$a(n)$
54	249435443174472200892782482022767790242411186581947375868109627072942390170 374777489454995044661564028847795765966412884536559735875756374024113033330 761081802881753245342130283831217995372929120982618714345216929180896149517 537060326996302188599174141839087073683925572613550522890075379372578873276 855572032166298944342901945723882026732216214725450009799953779668390342430 872057182832406725672397220248530184087622966141107981295858489599269416204 621416783023395779741327379966980809246036443382479111181261712361484488451 628875201456099855694312665891585467188758041874094247525633450295459656561 377760373604990265867966337226299537431679087850196659181088838212401689491 172841921484326937963329702614325510259299808207648736378565379972626426615 140298662980187312703556247360569407398186447300715492327567524115258029652 94926205197688079746334543569659273614886484528070656
55	161892858500256630897467233731952268572621837909584318279738908859088381145 458482259535871257635764892759916256307481942046874156251339787122669947510 035040600579804324023716988604328408941371196022121442201342132613321852377 143537236251847944868732585709518506458575864080024530682503460862398602603 905363831868205798878705356716463306055365573179382656142482859086879176493 491802576101618279732336166618356126370460343997710650614707599819268657098 906394669756982940887076730959989249451663596992644923815595659105443356418 601675955766663205696109881890921940580466314580199066814291099298191048328 595981293989894610718113688846969115569417342899689632064409863616872105696 446092107469544217634453317747062186452504079096877590926307714301615378797 928930083943509992656250898880271215376544727310395992752916592376533815357 211301335639834461017111436566196109335588805469646216168220950853256885617 94849701888
56	420297890305053167631750296859230531407748708369342934735227725081950075848 421356155304687430049292154157025532376734366830675693227746265421199920402 916865769206488438774434632061206999452621515614940812678402051730765789550 397132103444888090947611668004554030219199490094203655130938726598450077159 573683034749737150176751465831536316983943983469524249114861784986583605890 630529200626601382210962151607662098442925319676179985716825927642587747106 260913808916530424297565334984741415633028300439273241224289554799395497591 72977676808794131237158454367783642393704981811864947834955784693434462499 163153740144716450311830766853065499013780422218223603144343775856459545148 634425709679186260605395174570060614253899018930473856114797918063026945341 024450008059733375472728505049264797547454514494552782231704748498415143267 273993637168106231674607017725533416094576503082829424234269642298630043544 25880455234760201086650241871983982564868096

Number of matrices that are squares

n	$a(n)$
57	436462283095948500176011841246064105839225915864271487079600727116415152810 166444372907526518856758610250351210804297748777883013212047614203118152393 075961887476119067883650653467759566398876949418746479750653672792471869537 549578562972943886272523074990969221632069740170983043108550030526991130865 271590347397198621572443512714909419893603012628031384915611114851701053261 753959299708683746291616419118262988026491782033458251707110329241141022766 152336225747014369555013732793750806880695647083446738682388946587506496701 906856825178482657532281267548276272585472719783981782048072697670031008728 665167696054217225722071637086584887903391664976637202427758775473181455486 988103827227606355120798246422259363210622181394313702911491173280225973275 401451656322289941941485310845435917440020587006831873119359767729047817522 304069238639533846691087315772488506119583287803057577708136539500580017430 492198707500824398384318743508763844417315346021665184467576058199231925583 872
58	181299339311042584221469812223423177240519915913743505514633362963753729377 630826847210154141504856391123681280636623479524089273472296368819637750337 025894241061336299285416984853019243731707038106342175072681913605989557379 217857468554262188638569615007331855173521572715546011526699872556327504574 702132280804441163762325675598794532267723429391083456890305139694748044893 374387602278386263629373013150074311198215433842719797328474291540998791952 213238735198010421220588864991563853838601667046776805054276988050091127421 127172600381343981762736522296799292037638498753791839677173581881079070825 303113513614794477478195082794446146032015712895025235312086828057544018204 512040297064375693875538089646854887072346420579873689886971652957703740375 593032244434167847466281262071455302616479156074981681288303363183982979239 499914349636535052955621479703857592989868841076429727116050951367597874286 379879581012775246477195601167181232102818876630703045076566795386091065893 17525279128313571041632604869892243456
59	301235196786933158945240170233020049888910108243507538284133261540670874786 149800874924763393626289355018562649822141914577933556675885880361654161063 235647309480617178813843461388783301553191304496863737596783437181462299852 436539037170912768561154519840398838162873236745182545429761385404492997710 949584870352502126600241429313380984889717045078410944204860176616989042308 757215675369933680681474596686140994694662886609875072609672844063001983401 653524916088389349479181050195313751154176306493703179891595750173761852826 596976871664446778975927221194805615827818220816290587603675573219850598148 148802484468656292462157107382143767800158632606326539307055064532765316388 881671658846366295433596246733606837781164732213742008411478598597977965198 771840474329649500652538063845642212925409891463887575405705753911462835427 297086888841959224709201409782846745945927978794012471910680059431223129418 613846616762757404615510413433717611700533844107047890597828853866963156730 2420567946006631053316493856390601486162843007873050369676644734728142848

Number of matrices that are squares

n	$a(n)$
60	200205128442484952865821861589610280434391182879829964364052361782269232026 216518181588032003575818590439802275239401294318847150545021667516108537377 559027647238654919172320966834628735375696435293950292161422497315027590485 711463921739754057549077436202940017283075548511663570215666392944378516479 419910396691391357049793461335024225767725507170779605809754827013050316627 380595192969296745763885436461290663405515953025973329459196109261157938320 035322566632495005919563935940805046746765212486652946675725010562614709800 898863571496292001520718020084883634823664861236385038299510089639420338840 346126474208898831801051609326131649090163671073214206856061133486167853989 770773786459212062285873627771283690118714967713392631994153979509585943115 821118054783429173921829268890933454321758084628996857905274423191590322596 980512291993968879221137868243488255480967735468968029637657852639592276833 092866752968790451276852754454237441162121324428367496859877658644620754145 336587657758840199756993552085260357497917127290366030841122160845052151894 6359744770894275848107123619659776

Table 4: Number of invertible matrices which are squares

n	$b(n)$
1	1
2	3
3	126
4	11340
5	5940840
6	12076523928
7	95052257647200
8	3153668941285723200
9	406198470650573931200640
10	215366179177149634500004545792
11	447870507819487666185959047316144640
12	3770394197251690930118967532374966498493440
13	126205342254129164806148123600990735262978861434880
14	16960349752279776751561660450391351891796348875427924676608
15	9099421507577175992020382974051470776190067413539210813509193441280
16	195462885363922835503057403278659591954184242840750977725005618603043334553 60
17	167871260191849432216054590959402266093249254079643516915890152453940198413 194412195840
18	576851608746499396841042400369336874605167754140358727342936826407419056397 4746362542357433352192
19	792781572802352106128482806073479977368548690876342435188785038534849215731 409861941064155848716971103354880

Number of invertible matrices that are squares

n	$b(n)$
20	435844179621394952828028331877590491487847621526388907113290752808405719839 273234051108126200323648090580227063866982400
21	958423089110835503368949658545632437523672746908389057851428046801715870107 112064975179622555650825480533056258670356671991237836800
22	843041087068560164583076447581422268662760965351122050186001940240148731476 1421101925596833458619797098750233098905179944934872097613317042864128
23	296618121504238292017897322298205902091454056814532758872354010248782922658 978885249484672956696996347814561697550110794566945904440941226126633036404 542668800
24	417453102515766854891444290745393254069436433156725767277193920427367561293 149007484808721560581834269955126363155012242252185354518297468654765261855 32025312537189411717120
25	235005143080226799543623679039035485040152991324086076414127436709928036340 233051077562447304582430558039094685936475295763893397523724612592583256296 82822882877248453550684375328269271040
26	529184585582926944232484682421169867118583133187146513460506959556701573251 264719390287173297033391179216404190651457912522637143779808126933100112013 34134110228054691703048469617143834039649837789478912
27	476647086070927956161690357506063555231069521445642420423483022973363552261 684579646548585490282179007171388987303105187034337398262355064303218819137 992655931419391480613728565503408095285972375374755261178263204003840
28	171730209695147285772868802788799240141110352453373243353197648065649200140 776493647937111553599969428912977790491638153047068098331282599203132270971 419325925807910377015733721044990591602340340294499225227008643237661650762 99271372800
29	247489315850033999628810722676770906943347204665493846853218384340163868692 193183561418482979787198441373862636495564049486904714416396351023233641817 863480282386594557103733387299687350052232449741820141699928925138917844918 9887719672310402844154920960
30	142667876047149911940224973672325014878568230341334758423412716064550009954 440753540508543046638985629138487235741751816319018109007003735590234966290 531067553872537859060054808513372049017137130777079371292135769849477185829 2984876209754057007391814879322793193188098048
31	328969726295586929849944718598997614021238140538047955521584905516230543323 201663014975296934585625109058316293186912716636793880369852951229319021150 527066996012764659167824862320878491839430662690457532805085165406844929795 5725628593448426166601875632258606293678253413122922069801041920
32	303421016025226358823214123537112871779315457687682891245761108012403230492 123130304784065455076200434449896835911666599432204081182375433803724360296 110485118810913825764702916018406919855845878424440777662251564524196347536 140667203494513713306416511114552733759804252251371034773766111851844378504 77690880

Number of invertible matrices that are squares

n	$b(n)$
33	111942596872136010527044603322149717331843459862695853737609645243529739301 097840982139685685257831412101744346400088967181786211056158901437659822916 873624085015354331394264291705969328525956499063276402928620643028451724856 717533471814389353713225406017488668821846709953241369367173522485010189659 3082186315783855071391907840
34	165198114584091476964867063755297988418471235075809859820028832490180700915 849050283482255603516462520957134255085960335575175395939119973794417878240 198576940552414887616090824225876829256904102181523550647594655541507367764 981117815513089171118868767256907954747720767148517718081583540979919908303 737778487650956931269569175756596523172083269632
35	975157549989964172309554890234293892242055721980534648315984164564748814404 155242638465852905546974238691385905641541493707107520832197526853496936634 095124178451274392151907787209098750516056597457205688457671726254371335805 447460514983640141682016588961406739910986760049463373427544642070291876172 29321149786590603361374647562098500183890276083760008682250572922880
36	230252566363379653712664551264612992951416752847809407327418370856895817775 022597946062118766097828844192488202895139792899585763080550972634720805363 114226629714482723735979605003019907531663646604601133568190984036155956546 433197845323482275186650454984006259917137035563833917626985589483101877569 914326616735947527558123232269644594970106664338395253135163876964531358774 442536520908800
37	217467400452645529474785262972462359653476652964077947108868718467572129920 575251460361228218263193762495461988580126880169420949920215598325059312452 391329779091726138458893042106204907833201852468640007563303248552644879405 674428236631046662440945653271073034163330253626420674590023788997110554495 440409166380026193466239319530265007043527509232143585638755665229319854023 8497777007966161121016580698716241920
38	821568610291042904426119719139922140368293388276154395893131552961593655046 541819852527650439364814237471445486287176796454553796855394868951483191634 168961118897023165570466760988034359890583680872815286765181036583293241029 270297055322014903045795689388979598771371731961222983080027293166537928958 196763231600128925111276802354235443770758935158170590843899831157257144485 76757103028538609075023736788880032094376735796186818019328
39	124151938205244040463418007969842716998816442498206628548070169965522262319 702250347366603922305633651360398185239314759616628382483086191052047025152 488775580538544149076506455363721403647425385761462148522909120399733579574 333741091435508470945202607150415715942053862103623591712949568504259280442 304920295583462054465045822062407732188445479824791702782916503973971061343 736158990781177105611580067141872650332902532004213002364690195108287437905 22531840

Number of invertible matrices that are squares

n	$b(n)$
40	750452418223752232144030546492961175468866022221496771137490019280222421816 085959696174121332697442112402651952384654907157928000957292452015143784992 686929799551186028921067643075428947632221646454456211944478942612192710347 322777916454192835973898145824997077517724564987933100290318623800555542167 479629238299904151958007853611586142069629791743071837218326158878906057627 805582523897525116392320588301469214380891233377632247435294179465442435798 0879870646253820147176728166400
41	181448260960678753579385225847333780289192227224087041149769827249837089774 161923390486537207639641319536883524510125302556258705890548184603255198783 941418595193894581396414177682279588129421749709313402509342152167264746915 137977847508948712085556085116725647632022192616633681261783403527641302246 106438471188698666676151804193576209042405397162700421287054142426756097049 641514807570952459709008099835792755453390103938879124077021025081803019042 39904505787079406615270314830263718447928566093552025600
42	175485990077482730131483505350297565490671167522773778193916741875869872528 679875358728315138891625169005297325207428034896620896749262082862000275803 847972287757192240918853186806362329687830149228541345649748135109379949782 773790167085712709976381507246067036943402566329590251968281862199094010939 913314483748580226256365862337645512661892164496453462738642571335448328419 983592418929372415320128306592049153917121208593855377908422245099202266210 869401587873354859934378837367351126093076581969882047233236438251810727418 396672
43	678878542037204056966305990850742230150513155549150137241375269768768474444 487919602789895096991282103260369203782238021086979563635029968493029593629 735159220282874454314456601385845321314835643582848699624584263989832788967 004005836568777423606855009434548276771346948711612059633331980117109862585 625552498014399938303401002895312570896727587498799407756760576706810720360 986363274735867485812710296953767048685575152672111468295161937756124043772 452091504999707617024890392636594794002335482892668423931580995148772954581 0066923200601819006035086540800
44	105051366124583389231007739033986896207151209297773978280100632373682487096 889357639861399773769166774208373971795510477166815717704361720038896616105 780067766580426541535876462986918549310392362787861689424302983504882975901 948298242070998684493823481445925466393865465290009723088036613841579718994 696203510912229766022191963755505476608322366905434490752975797284688323937 802291186242985371394789888686958159408699421762690067851036455864535400339 923222251967315559173393867225720669115475222842949946950549598224267314811 5020582724765145929809733884804220776689219729262714552320

Number of invertible matrices that are squares

n	$b(n)$
45	650236461537403257893377432735119076301687830045048227211457323800049167125 828303006739106154428432370867706420942098022581271553514991890439806263233 739458015329785200007572137588697308565964431243345336749636653458291171428 659567691983388195134361481393987761829171079425044003113831816761586692319 687278484762405412261267637673352949781996021110361672229156441035765590180 492979168385803149762388850485634343030136936884920822639762078001868434993 759512755856968733377027382385404166746937715163704108597400331449159483275 214540006429136679666639982960163945696727004476904468946510180896787072550 541721600
46	160990750147927283046386315908708902357210760446324945094609601957602943095 922891379997776581719480785499316568992316332221676714470608712926380064493 257824280372989849721195800021709008309331519923164931746864794494226006842 257107084002704446281262281504654204752363865742912074129867553352372492213 931051082667158768978177583690434612320687610827929332541202601574690154168 738048304789132871186363612339371277562922936477549962873596928751862942121 281797843858549527637875162174510613928844369195344915667017321896009183134 809992537931178380155254407958194638886265086209007373211460610393546534162 0276511822854352799930130008991858688
47	159437516450239438577433986720591421185653033792243941089759371386036890814 946335472497283293731676748231842015638151198085622158383325378724797002122 689189347647530595307472676279264828503002280663441683551169765173242529103 660687045920142799848205495907786236492339941163827081351885550040984930498 101962528852038050065114346153685389528777687280843810702116429038026484073 653043827535843782594443685787407005051268848782684777117480740078179934184 800155694054343627506958145248153966175259932926864505913783164332220438100 459982150796833285379287917781977357839641727515077106286717281061694861503 03975794855156715290023655746679689670046753761884413863982530560
48	631597073209358240035693186128883637263965875199326358295054817018331133545 823683295105917019300936956248492306646801236714291292404849086000791888080 019999793684510776088850979486587413694669511525675921013972308583248453053 678128459536681398031756166225200354463728544564408532153573850022862367299 886086461616441539965941024606897222842632212552797973868928659589673332714 978478456720173049729328897224379147065784200359789054521117018817069634843 553452834219526633742433141557684709675805831082605612365567886158231715395 584650340222804981170317237935942608399744100323044593530946528464773173776 357918624820062149300384385622795605339782631770132086699470151542088945652 508021842572738560

Number of invertible matrices that are squares

n	$b(n)$
49	100080551119541392152750478694439231497590787214713995607121239646503566708 659726483702626834705925254223003956152961469908196991685601625006810494347 228265428961897577723954980557826473035476515646534132058337312215957499105 005894146362260611235094276999769072635130562042373558960106129704265884988 878144788601588487654488534785769709116116578293626682143537214460180018338 196841259153757000181398778931470705711648061973679502461017556102660107970 314355386448976898615192762418780082107268572943320692155401403991517441171 654981868175033197950326321483274978320849412662293177510195400207081977156 928753944645045655166244708104950770787867764426270877818995065578001290158 831812051184911011557633708894011211321127731200
50	634335853489254338109758021047608873639575111894138659051841122164387051608 292667090242163914577145537940191369681097969895615751541586987951180029975 482255647134700305142397837284898327084130101131192908813932161289435363286 203093506701047212562974473716625806429720914616836699685789644481226045921 170729574334986526594291603609562377900303956131645587502232267404696273870 435258381918746702316812998801459327921665512727913170491558965366516545736 372484043223497656230159504104516636146892160640175016624989922208944963593 827366412356535353472126433060401620628894573737606118917536239857690643661 465520889720795032440996740045391916709755482148358288270519145838821938045 333135725430415522047818519382081185273155020830569576181715344615358249041 92
51	160823245084392638298530396839550109928713007572716717255441919289545765909 681177885249188542012328842053692422771595849708471102214005141255268980057 611509365536844979853940158280100351095977429955128518010357146653885660507 609203423125268426303967488122701639972568056903225314895396631028094056638 075950580957484854127962638694770831151209424898964736084706900864305393805 664245274500573127450625164884621441740546146789153017085679742687502531665 598864609251325862476466235137587202133796562194524754500241190108868177322 437663226825004669403618169300477219204695654998608224553441815800126286697 314326310147767337872188641235320114009334819592909787022807150559584892674 329958906420786563033008701571901834952174770794909418679813679696915855504 861238880562070929380393091072000
52	163094146529503116896842867402179161876743843521802511965690188028599026917 923891544345776593062829330364547182949078676427630606672354695402077481219 884966097949088948432824906875075012851536270104115970107848117213821701637 089264927081000612869582121835617519236919026819592755294646909791330944370 725676118877368972767536383303834591799715390748938193541033463993981636254 300806903796814232592348021531993381801965138050604010891224612093991813591 691694749005587272982364205574226715311923866021219409540100204048531471929 431730315677609861394764932854461506302767439854516270401732841948025442619 456486354084027474282327160728845681050219793745687247520271738340963359416 712487237918830261468792769118673502619109547921096145629358346095781847644 5031212396216129442728145308814074774364242407920119758307983360

Number of invertible matrices that are squares

n	$b(n)$
53	661588456773878198105410313565828419900073260636748620247655088946581422112 721466155871886383307213984609129246157720533030081545224299119209925974260 279656270523848810027470768579550017647241921714794779419686805207628386202 445075488380561592613611475800414963957738913836754501223339705889378881521 015543527018282545197762281045319773068293847753974934702858617834002309979 946436904262453002406893016739556024263227569520028277378510277845524646704 998631453600225771128617754774523844862088927230043705784565635413010168443 472688947906421003552836934704271595029102636446821417110683465293036813566 368635056829542704919117278868462982485345334688433451122590897712393857080 806698704701039583221814369365686094507226145275994977039411455963810122903 633775615943709692581888799564497303940703775537205689774537528892537242642 98833092180914995200
54	107348864554684354938619231945591520627448231587530477233028851197341799934 218587246562108768894228574521444882832145725671404386008242840712901939711 875861776852103169608269086607249778154401854734907992570914001594069578412 451293180724286970682860117108842160305769018878865361338653394696810107143 515830332267666317863132245768261026399401456733626332864730909404174694637 414001380577197478128348686278466216740940813515748548950902753734565634022 041201046548086148163719867437347023629062736590229956922754867353186853196 165278338906830983820454182521677708773156408835152960682872521811714322275 746921287375748888239161680237309212166728684494750612443311460325431829327 765341604991651379185410872315761771165278009568165633630273303632309875943 940221094889812036128254410813015446233590963695588175887194558867137162527 54776108304725740696178236584135813707763397299273728
55	696733965243211653604562144925088747514383512426423467302005173167196264006 132063212800912618735748055285586519078177341952709955718207069329686028566 834645948907264494973591827006460658855079394298478350336164038054688081471 555126785533374851986527541216709333994668622641559404560006538949920673820 983790620482292387128208144315670017445420255418458254259795583190182407305 429879908416392862801410673761893164495764785183654010865591053958741208137 165344132434126352681547206378603883804560102864074367204297667241824623804 38412269308891570220227552660706192812660375261419029436119579703309811030 876713077641713905725863075816133108890199243465770275723923782191291561217 69664355585631839714386919466131036226055497522702270750084487191971519718 241928115771322383456789123524310171888847800862545165994659421298960617118 889002466261759285732761557676239484652854297425656531971193291882716582927 0108897280

Number of invertible matrices that are squares

n	$b(n)$
56	180882478948341909822071861408456390963573352111917620621963087812658702581 682932362607221718280008970608872746321349921403256479739776593312022422236 654196439980264927157459377797180940748837475045445426714102978067812316452 443930428483459054460494692792028840694002726229342165639330050042908789560 900604187866840414885132091859462072042590285009072282362636420513691905477 526392140085205443717553465179983125941891130973642675315450429744015923523 752840301082754112729290428120213359251186304695982535452295026110914278922 137423614964504350105420701087141144337033314155158901137369399439960284935 070311067953932753165973641818394360392881915426358100915799573727301887733 820883977589331336507033378311501501877921324556053288788852612476479582338 78413426753740662698808439175212549656121936087062901316129363339316478447 718066076904803980785189828118860634133167997726071474493332541073749817055 24678384424224945172843967663330735203287040
57	187839105441493640923829332832677259630474455743166202332952362073081009378 301201032001332403906484177693517442855040884689135852443916847824737917161 272950622213660556686274573913689898555824922589428200176315513873885583783 899710712792984881063478938794816743924923667008322082549343527953349772567 542873662192481342354853094021074569857177536130883037547075473586219270009 761804079239782603087512542944126778614374726636447013931939642626946695262 386100772283756742813813332488201858320469847879003139534910990904825183000 522412965373795306448457515240420525079525195418913886012690809564213601312 042089121723210243930261941423692949583803640334966792558881949067718949500 731650546495525360849641409796904059849851497516595214307601005820730079114 120483704010849003525378297433674818250603558801227575871753077221173792322 009500754299611581272118927187069935061509629419392858042900909711091082016 440894186584598014125800096455536445001873059874212663781268569798038226206 720
58	780253117675087566440708693324251964948699982285766360736596123356600918546 720913172025929890414063357321546251792288525571974956376039993732212380216 878716856127685561386345087849198922951086215011652848780268546291946027709 902482955890668233970112412832482489555485431166096466900288723386560522768 161761358309225385021056484450349492480530766335112747866811415834851697778 682591243685934809731248120065768446761080881021286422197183695460352481595 192161844347530029039323390676411784671299686450888492547521064949814866646 744663027037955850767842437716583422179692500918584942318940682167149052104 900302838135837399198552320466603203532954524138205989950273197336069249746 236529399366079025804741372133664094646391013008979172494322178725179232506 071212388357437533792695012865447510359805358041154627389758550483167350132 743996852755848590317775316371216049912230006390399764467138249669325416632 369320110862631083316687646153520448868284168906491049016400784031029048326 4099677477483770726135660147168509952

Number of invertible matrices that are squares

n	$b(n)$
59	129641785976523609065004947714372073302653683931919550724372830815804259268 134274521340085594377943025122783736708765158305664030190922092442296765705 898124208264580325449393691990177561974666761693953081213393458314052957004 405438551393967969851999878311079360282817476450908824307670263547055787564 720382808550820719499674596101627492172978199886723376471283803552224373143 427098096022506314831275227070280274556440802647147613098194080147470208243 673730721580080804577596161002006527642980737642657085730266093796689089449 828806303608328054076513267839245218928249708073763736278582171459943322550 789323557495397293543098079040214156180244262621303403289420292970307370737 840150778499879960964844625445640327778297291531148246104342051421752156487 778080108465898378485623441933238054329391819289808421700241556253791055070 263856879497825181554153566192387741534808524890075667203369684258703728154 452537445439800389579005705207975298507684032565820736205245152975970936234 9946632913920935480626905259892165470109537035111461765795673633015726080
60	861617456717757403991694542775678554851826986567179811299786155286974049782 503756451848164437967386651819444173954156478612715533773751725732040293815 480301513797105642348651413962558449799674570245185304284055511345740823006 448610298351001805654119398612550996758344937294451368620144568542497833540 639834578035074326598675462065870313911151096615761516503950524064473134542 712935711368808892154109606995841921790171765489300596730139596865695540344 249024216617981192485365840925201762598639063773803267410841208890975598469 560272675600442219651596753194919444329858601956832355668323043271718482856 938415308981787209780110675524926198467663658829202776756054197468792349073 758405845036141819149655493802049962619136471298137357922914337125968537832 221676757316789469102544961918899665277861902312300283842359510665174220836 052157261946625197843660937475412656449058231847842149471818577938083621088 734168275646049556354903363801764983005878386367425262818718696410222005256 460242806211868610934676397909273611681445706842617379544353781188146242432 614618218707323073176507357593600

References

- [1] OEIS Foundation Inc. (2015). Online Encyclopedia of Integer Sequences. published electronically at <http://www.oeis.org>.
- [2] George E. Andrews. On the theorems of Watson and Dragonette for Ramanujan’s mock theta functions. *American J. Math.*, 88:454–490, 1966.
- [3] Daniel J. Bernstein and Jonathan P. Sorenson. Modular exponentiation via the explicit Chinese remainder theorem. *Math. Comp.*, 76(257):443–454, 2007.
- [4] Alin Bostan and Éric Schost. A simple and fast algorithm for computing exponentials of power series. *Information Processing Letters*, 109:754–756, 2009.

- [5] Richard P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *J. ACM*, 25(4):581–595, 1978.
- [6] Leonard Eugene Dickson. Canonical form of a linear homogeneous substitution in a Galois field. *Amer. J. Math.*, 22(2):121–137, 1900. also in [7, vol. 1, page 71].
- [7] Leonard Eugene Dickson. *The collected mathematical papers of Leonard Eugene Dickson*, volume I. AMS Chelsea, New York, 1975. Editor. A. Adrian, Albert.
- [8] Phillipe Flajolet and Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, Cambridge, 2009.
- [9] Jason Fulman. Cycle indices for the finite classical groups. *J. Group Thy.*, 2(3):251–289, 1999.
- [10] Jason Fulman and Robert Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. AMS*, 2012.
- [11] Jason Fulman and Robert Guralnick. The number of regular semisimple conjugacy classes in the finite classical groups. *Linear Algebra and its Applications*, 439:488–503, 2013.
- [12] J. A. Green. The characters of the finite general linear group. *Trans. AMS*, 80(2):402–447, 1955.
- [13] Robert Guralnick and Gunter Malle. Products of conjugacy classes and fixed point spaces. *J. AMS*, 25(1):77–121, 2012.
- [14] Joseph P. S. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra and its Applications*, 36:141–155, 1981.
- [15] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, Berlin, 2002.
- [16] Michael Larsen. Word maps have large image. *Israel J. Math.*, 139:149–156, 2004.
- [17] Michael Larsen and Aner Shalev. Fibers of word maps and some applications. *J. Algebra*, 354:36–48, 2012.
- [18] G. I. Lehrer. A toral configuration space and regular semisimple conjugacy classes. *Math. Proc. Cambridge Philosophical Soc.*, 118(1):105–113, 1995.
- [19] Martin W. Liebeck, E. A. O’Brien, Aner Shalev, and Pham Huu Tiep. Products of squares in finite simple groups. *Proc. Amer. Math. Soc.*, 140(1):21–33, 2012.

- [20] Ian G. MacDonal. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. Clarendon Press, Oxford, 1979.
- [21] Allan Steel. A new algorithm for the computation of canonical forms of matrices over fields. *J. Symbolic Computation*, 24:409–432, 1997.
- [22] Richard Stong. Some asymptotic results on finite vector spaces. *Advances in Applied Math.*, 9:167–199, 1988.
- [23] The Sage Developers. *Sage Mathematics Software (Version 6.8)*. The Sage Development Team, 2015. <http://www.sagemath.org>.
- [24] G. E. Wall. Counting cyclic and separable matrices over a finite field. *Bull. Austral. Math. Soc.*, 60:253–284, 1999.
- [25] Herbert S. Wilf. What is an answer? *American Math. Monthly*, 89:289–292, 1982.

Keywords: matrix, square, sequence, conjugacy class