THE AMERICAN MATHEMATICAL MONTHLY

Volume 109, Number 2 February 2002

AN OFFICIAL PUBLICATION OF THE MATHEMATICAL ASSOCIATION OF AMERICA

Taylor & Francis
Taylor & Francis Group

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: http://www.tandfonline.com/loi/uamm20

Finite Groups of Matrices Whose Entries Are Integers

James Kuzmanovich & Andrey Pavlichenkov

To cite this article: James Kuzmanovich & Andrey Pavlichenkov (2002) Finite Groups of Matrices Whose Entries Are Integers, The American Mathematical Monthly, 109:2, 173-186, DOI: 10.1080/00029890.2002.11919850

To link to this article: https://doi.org/10.1080/00029890.2002.11919850

Finite Groups of Matrices Whose Entries Are Integers

James Kuzmanovich and Andrey Pavlichenkov

Finite groups of matrices appear early as examples in a first course in abstract algebra, and most of the time these examples are given with integral entries. While these groups provide a setting in which to illustrate new concepts and to pose problems, they also have surprising and beautiful properties. For example, Minkowski proved the unexpected result that $GL(n, \mathbb{Z})$, the group of $n \times n$ matrices having inverses whose entries are also integers, has only finitely many isomorphism classes of finite subgroups. As a consequence, there are only finitely many possible orders for elements of $GL(n, \mathbb{Z})$; fortunately, the possible orders can be determined using linear algebra. In general, the number of possible orders increases as n increases, but even here we have the surprising result that no new possible orders are obtained when going from $GL(2k, \mathbb{Z})$ to $GL(2k + 1, \mathbb{Z})$. This paper is an exposition of these and other related results and questions.

Although finite groups of integral matrices have a long history, most of the beautiful theorems concerning them do not appear in texts and are not known to many algebraists (for example, the first named author). While still an area of active research (see [**7**], [**12**], [**23**], and [**24**]), major parts are accessible to students; indeed, this paper has its origin in a term paper written by the second author for a beginning modern algebra course that used [**9**] as a text. One of our goals for this paper is to be a source of problems, readings, and projects for other students; the topic seems ideal since it synthesizes results from number theory, algebra, and linear algebra, gives a natural and somewhat gentle introduction to deeper subjects not yet encountered by a beginning algebra student, has historical features, and could be a subject of continuing student research. With this goal in mind, the authors have included exercises and have tried to organize the paper so that parts can be read independently, or given to students in outline form. Our second goal is to give the reader examples of current research in the area.

1. FINITE SUBGROUPS OF $GL(n, \mathbb{Z})$ AND $GL(n, \mathbb{Q})$. For a fixed positive integer n, what are the finite subgroups of $GL(n, \mathbb{Z})$? What are the possible orders of elements of $GL(n, \mathbb{Z})$ (again for a fixed n)? The purpose of this section is to put these two questions in perspective. First, we observe that every finite group is isomorphic to a subgroup of $GL(n, \mathbb{Z})$ for all sufficiently large n; hence the questions should be asked for a fixed n. Next, we give an argument due to Minkowski that shows that $GL(n, \mathbb{Z})$ contains only finitely many isomorphism classes of finite groups, a result that is unexpected and not at all obvious. Finally, we show that any finite subgroup of $GL(n, \mathbb{Q})$ is conjugate to (and hence is isomorphic to) a subgroup of $GL(n, \mathbb{Z})$; this allows application of the tools of linear algebra.

Cayley's Theorem, that every group G is isomorphic to a subgroup of the group of all permutations of G, is a standard result in elementary abstract algebra courses. The following exercise, with appropriate hints, is often assigned shortly after covering Cayley's Theorem.

Exercise 1.1. If G is a group of order n, show that G can be embedded in $GL(n, \mathbb{Z})$.

Outline: By Cayley's Theorem, it is sufficient to show that S_n can be embedded in $GL(n,\mathbb{Z})$. For $\sigma \in S_n$ let $T_\sigma : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$ be the linear transformation defined by $T_\sigma(e_i) = e_{\sigma(i)}$ where $\mathcal{E} = \{e_1, e_2, \ldots, e_n\}$ is a basis for $\mathbb{Q}^n$; define a map $\Phi : S_n \longrightarrow GL(n,\mathbb{Z})$ by letting Φ take σ to A_σ where A_σ is the matrix of T_σ with respect to the basis $\mathcal{E}$. Hence the exercise reduces to showing that Φ is an isomorphism. Note that $P_n = \Phi(S_n)$ is the set of all $0-1$ matrices (each entry is either 0 or 1) with exactly one nonzero entry in each row and column. The elements of P_n are called *permutation matrices*.

Exercise 1.2. Let C_n be the subgroup of $GL(n,\mathbb{Z})$ consisting of all diagonal matrices with ± 1 diagonal entries; then $C_n \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n}$. Let $B_n = C_n P_n$. Show that B_n is a subgroup with $|B_n| = 2^n n!$.

Let $\nu_p : M_n(\mathbb{Z}) \longrightarrow M_n(\mathbb{Z}_p)$ be reduction mod p for a prime p (we omit the subscript p if there is no confusion about p); for example, if $p = 3$, then

$$\nu\left(\begin{bmatrix} 5 & 8 \\ 3 & 5 \end{bmatrix}\right) = \begin{bmatrix} \bar{2} & \bar{2} \\ \bar{0} & \bar{2} \end{bmatrix}.$$

It is easy to verify that ν is a ring homomorphism, and hence when restricted to $GL(n,\mathbb{Z})$ that $\nu : GL(n,\mathbb{Z}) \longrightarrow GL(n,\mathbb{Z}_p)$ is a group homomorphism.

The next few beautiful results are due to Minkowski; they show that up to isomorphism $GL(n,\mathbb{Z})$ contains only finitely many finite subgroups. Additional results may be found in [**18**].

Proposition 1.3. *Let q be a prime and suppose that $g^q = I$ for $g \in GL(n,\mathbb{Z})$. If $p \neq 2$ is a prime, and if $\nu(g) = I$, then $g = I$.*

Proof. The proof is by contradiction. Suppose g is a nonidentity element with $\nu(g) = I$. We can write $g = I + pH_1$ for some nonzero matrix H_1. Let d be the greatest common divisor of the entries of H_1; then $g = I + pH_1 = I + pdH$, where the greatest common divisor of the entries of H is 1. Applying the binomial theorem, we have

$$I = g^q = (I + pdH)^q = I + qpdH + \frac{q(q-1)}{2}p^2d^2H^2 + \cdots$$

It follows that $0 = qH + \frac{1}{2}q(q-1)pdH^2 + p^2(\cdots)$. Thus p divides qH_{ij} for all i, j; this in turn implies that $p = q$, since the greatest common divisor of the entries of H is 1. Recall that $p \neq 2$; thus $p - 1$ is even. Consequently, $0 = H + \frac{1}{2}p(p-1)dH^2 + p(\cdots)$, and therefore p divides H_{ij} for all i, j. This contradicts the fact that 1 is the greatest common divisor of the entries of H. Hence $H = H_1 = 0$ and $g = I$. ∎

Theorem 1.4 (Minkowski). *If G is a finite subgroup of $GL(n,\mathbb{Z})$, then G is isomorphic to a subgroup of $GL(n,\mathbb{Z}_p)$ for all primes $p \neq 2$. In particular, $GL(n,\mathbb{Z})$ contains, up to isomorphism, only finitely many finite subgroups.*

Proof. Let $p \neq 2$ be a prime and let G be a finite nonidentity subgroup of $GL(n,\mathbb{Z})$; we show that $\nu|_G$ is an isomorphism between G and a subgroup of $GL(n,\mathbb{Z}_p)$. Suppose that $G \cap \ker\nu \neq \{I\}$. Then there is a prime q and a nonidentity element g of G such that $g^q = I$ and $\nu(g) = I$. By Proposition 1.3 it must be the case that $g = I$; this is a contradiction, and the theorem follows. ∎

Exercise 1.5. Show that $GL(n, \mathbb{Z})$ has infinitely many distinct elements of order 2; hence the 'up to isomorphism' condition in Theorem 1.4 is necessary.

If A is a group, let $A^{(n)} = \underbrace{A \times A \times \cdots \times A}_{n}$. A finitely generated Abelian group G is called *free of rank n* if $G \cong \mathbb{Z}^{(n)}$. We represent the elements of $\mathbb{Z}^{(n)}$ as column vectors of integers; note that $\mathbb{Z}^{(n)}$ is a subgroup of the vector space of rational column vectors, $\mathbb{Q}^{(n)}$. Let $\{e_i : 1 \le i \le n\}$ be the standard basis of $\mathbb{Q}^{(n)}$. Part of the conclusion of the Fundamental Theorem of Finitely Generated Abelian Groups is that a finitely generated Abelian group with no elements of finite order (called torsionfree) is free; see [**4**, p. 160]. A related result is the fact that a subgroup of a free Abelian group of rank n is free with rank less than or equal to n; see [**4**, p. 371].

The following theorem shows that every finite subgroup of $GL(n, \mathbb{Q})$ is isomorphic to a subgroup of $GL(n, \mathbb{Z})$; therefore, when considering our questions, we may work with either $GL(n, \mathbb{Z})$ or $GL(n, \mathbb{Q})$. A generalization appears in [**25**, App. 1].

Theorem 1.6. *If G is a finite subgroup of $GL(n, \mathbb{Q})$, then G is conjugate to a subgroup of $GL(n, \mathbb{Z})$.*

Proof. View $M_n(\mathbb{Q})$ as the ring of $\mathbb{Q}$-linear transformations of $\mathbb{Q}^{(n)}$ acting by left multiplication on column vectors. If $A \in M_n(\mathbb{Q})$, then $A \in M_n(\mathbb{Z})$ if and only if $A\vec{b} \in \mathbb{Z}^{(n)}$ for all $\vec{b} \in \mathbb{Z}^{(n)}$.

Let $F = \sum_{g \in G} g(\mathbb{Z}^{(n)})$. Note that $g(F) \subseteq F$ for all $g \in G$. Since $\{g(e_i) : 1 \le i \le n, g \in G\}$ is a finite generating set for F, the Fundamental Theorem of Abelian Groups ensures that F is free. Let d be a common denominator for all of the coordinates of all the $g(e_i)'$s; then $dF \subseteq \mathbb{Z}^{(n)}$. Hence F is isomorphic to a subgroup of $\mathbb{Z}^{(n)}$; since $\mathbb{Z}^{(n)} \subseteq F$, it follows that F has rank n. Therefore F is isomorphic to $\mathbb{Z}^{(n)}$; let $\gamma : \mathbb{Z}^{(n)} \longrightarrow F$ be such an isomorphism. Define a linear transformation $\Gamma : \mathbb{Q}^{(n)} \longrightarrow \mathbb{Q}^{(n)}$ by $\Gamma(e_i) = \gamma(e_i)$ for $i = 1, 2, \ldots, n$, and let C be the matrix of Γ with respect to the standard basis. Then Γ is given by left multiplication by C, and when restricted to $\mathbb{Z}^{(n)}$, Γ is equal to γ. Since $g(F) \subseteq F$, it follows that $C^{-1}gC(\mathbb{Z}^{(n)}) \subseteq \mathbb{Z}^{(n)}$ for all $g \in G$. Hence $C^{-1}GC \subset M_n(\mathbb{Z}) \cap GL(n, \mathbb{Q}) = GL(n, \mathbb{Z})$. ■

The following (non-obvious) Corollary, is obtained by using Theorem 1.6 to transfer the content of Corollary 1.4 about $GL(n, \mathbb{Z})$ to $GL(n, \mathbb{Q})$.

Corollary 1.7. *Up to isomorphism $GL(n, \mathbb{Q})$ contains only finitely many finite subgroups.*

2. ORDERS OF ELEMENTS OF $GL(n, \mathbb{Z})$.

In Section 1 we showed that there are only finitely many possibilities for orders (finite) of elements of $GL(n, \mathbb{Z})$ (and $GL(n, \mathbb{Q})$). The purpose of this section is to determine what orders are possible.

Example 2.1. *The matrix*

$$A = \begin{bmatrix} 2 & -16 & 3 & -1 \\ 1 & -2 & 0 & 0 \\ 4 & 5 & -3 & 1 \\ 0 & 35 & -8 & 3 \end{bmatrix}$$

has order 12. *Verifying that A has order* 12 *without the aid of a computer algebra system would require considerable calculation, but by the end of the section the reader* *will see how this matrix was obtained and why it has order* 12. *The reader will also be able to show that* $GL(4, \mathbb{Z})$ *has no elements with finite orders larger than* 12.

We must first discuss the mth roots of unity and cyclotomic polynomials; roots of unity are essentially the elements of finite order in 1×1 complex matrices, so it is not surprising that they are important in our arguments. For a more complete discussion of roots of unity and cyclotomic polynomials see [**4**].

2.2. The roots of $x^m - 1$ are called mth *roots of unity*. They are

$$\{e^{2k\pi i/m} = \cos(2k\pi/m) + i\sin(2k\pi/m) : k = 1, 2, \dots, m\}.$$

In the complex plane, the roots of unity are evenly placed on the unit circle starting at 1. Under multiplication of complex numbers the set of mth roots of unity is a cyclic group, and the generators of this group are called *primitive* mth roots of unity. There are $\phi(m)$ primitive mth roots of unity, where $\phi(m)$ is Euler's ϕ-function; $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

2.3. The mth cyclotomic polynomial $\Phi_m(x)$ is defined by $\Phi_m(x) = \prod_\gamma (x - \gamma)$ where γ ranges over all primitive mth roots of unity. We need the following properties of the cyclotomic polynomials.

1. All coefficients of $\Phi_m(x)$ are integers.
2. The degree of $\Phi_m(x)$ is $\phi(m)$.
3. Each $\Phi_m(x)$ is irreducible over $\mathbb{Q}$.
4. The irreducible factorization of $x^m - 1$ is given by $x^m - 1 = \prod_{d|m} \Phi_d(x)$.

2.4. Given a positive integer m, it is not difficult to construct a matrix of order m in $\phi(m) \times \phi(m)$ matrices. Let A be the companion matrix of $\Phi_m(x)$. If $p(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$, then the *companion matrix* C of $p(x)$ is

$$C = \begin{bmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{k-1} \end{bmatrix}.$$

Then $p(x)$ is the characteristic polynomial of its companion matrix C and $p(C) = 0$. Since the coefficients of $\Phi_m(x)$ are integers, A is an integer matrix. Also, since $\Phi_m(x)$ is an irreducible factor of $x^m - 1$, $A^m = I$ and this is true for no lower power of A; that is, A has order m. We make explicit use of this construction when $m = p^e$ for a prime p; note that $\phi(p^e) = (p-1)p^{e-1}$.

Example 2.5. *We construct a matrix of order* 12 *in* 4×4 *matrices* $(4 = \phi(12))$. *If we factor* $x^{12} - 1$, *then we see that* $\Phi_{12}(x) = x^4 - x^2 + 1$. *Our desired matrix is the corresponding companion matrix*

$$C = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

By performing row operations on the identity, each consisting of adding an integer multiple of one to another, we obtain a matrix

$$B = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix}$$

whose inverse also has integral entries. The matrix $A = BCB^{-1}$ is then a matrix of order 12 *with integral entries. This is the matrix of Example* 2.1.

Remark 2.6. Examining $\Phi_n(x)$ for small values of n would lead to the conjecture that the coefficients of $\Phi_n(x)$ are all ± 1. This is not the case, however; the first counterexample is $\Phi_{105}(x)$, which has two coefficients of -2. In fact, every integer appears as the coefficient of a cyclotomic polynomial; see [**29**].

Theorem 2.7. *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ with $p_1 < p_2 < \cdots < p_t$. Then $GL(n, \mathbb{Q})$, and hence $GL(n, \mathbb{Z})$, has an element of order m if and only if*

1. $\sum_{i=1}^{t} (p_i - 1)p_i^{e_i - 1} - 1 \le n$ *for* $p_1^{e_1} = 2$, *or*
2. $\sum_{i=1}^{t} (p_i - 1)p_i^{e_i - 1} \le n$ *otherwise.*

Proof. Let $W : \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined for $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ by $W(m) = \sum_{i=1}^{t} (p_i - 1)p_i^{e_i - 1} - 1$ when $p_1^{e_1} = 2$ and $W(m) = \sum_{i=1}^{t} (p_i - 1)p_i^{e_i - 1}$ otherwise. Theorem 2.7 can be restated as: $GL(n, \mathbb{Q})$ has an element of order m if and only if $W(m) \le n$.

Suppose that m is a positive integer with $W(m) \le n$; we produce an element of $GL(n, \mathbb{Q})$ of order m. First suppose $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ with $p_1^{e_1} \ne 2$. As shown in (2.4), we can construct an $(p_i - 1)p_i^{e_i - 1} \times (p_i - 1)p_i^{e_i - 1}$ matrix A_i of order $p_i^{e_i}$. Then

$$B = A_1 \oplus A_2 \oplus \cdots \oplus A_t = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_t \end{bmatrix}$$

has order m. If $W(m) = n$, then $A = B$ is the desired matrix. If $W(m) < n$, then $A = B \oplus I_s$ is the desired matrix, where $s = n - W(m)$. Now suppose $p_1^{e_1} = 2$. Then $W(m/2) = \sum_{i=2}^{t} (p_i - 1)p_i^{e_i - 1} \le n$, and by the previous discussion, $GL(n, \mathbb{Q})$ has an element A of order $m/2$. Since $m/2$ is odd, $-A$ has order m.

Conversely, suppose that $A \in GL(n, \mathbb{Q})$ has order m for $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Let $m_A(x)$ be the minimal polynomial of A and let the irreducible factorization of $m_A(x)$ be $m_A(x) = m_1(x)^{f_1} m_2(x)^{f_2} \cdots m_s(x)^{f_s}$. Since the roots of $x^m - 1$ are distinct, and since $m_A(x)$ divides $x^m - 1$, we must have $f_1 = f_2 = \cdots = f_s = 1$. By property (4) of (2.3), for each $i = 1, 2, \ldots, s$, it must be that $m_i(x) = \Phi_{d_i}(x)$ for some divisor d_i of m. Since the order of A is m, we have $\operatorname{lcm}(d_1, d_2, \ldots, d_s) = m$. By primary decomposition, A is similar over $\mathbb{Q}$ to a matrix of the form

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_s \end{bmatrix},$$

where the minimal polynomial of A_i is $\Phi_{d_i}(x)$ for $i = 1, 2, \ldots, s$. For each i, let ℓ_i be the size of the square matrix A_i. Then $\ell_i \geq \text{degree}(m_i(x)) = \phi(d_i)$; consequently, $\sum_{i=1}^{s} \phi(d_i) \leq \sum_{i=1}^{s} \ell_i = n$. The theorem now follows if we can show that $W(m) \leq \sum_{i=1}^{s} \phi(d_i)$; this is precisely the content of the following lemma. ■

Lemma 2.8. *If $m \in \mathbb{N}$ and if $\{d_1, d_2, \ldots, d_s\}$ is a set of distinct divisors of m such that $\operatorname{lcm}(d_1, d_2, \ldots, d_s) = m$, then $W(m) \leq \sum_{i=1}^{s} \phi(d_i)$.*

Proof. Let the prime factorization of m be $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Since $m = \operatorname{lcm}(d_1, d_2, \ldots, d_s)$, there exists a set of integers $\{c_1, c_2, \ldots, c_s\}$ such that for each i, c_i is a divisor of d_i, $c_1 c_2 \cdots c_s = m$, and $\gcd(c_i, c_j) = 1$ for all $i \neq j$. Since c_i divides d_i, $\phi(c_i) \leq \phi(d_i)$, and hence $\sum_{i=1}^{s} \phi(c_i) \leq \sum_{i=1}^{s} \phi(d_i)$. For each i, let $S_i = \{p_j^{e_j} : p_j^{e_j} | c_i\}$. Since $c_1, \ldots, c_s$ are pairwise relatively prime, and since $m = c_1 c_2 \cdots c_s$, for each i, $c_i = \prod_{p_j^{e_j} \in \mathcal{S}_i} p_j^{e_j}$, and $S_1, \ldots, S_s$ partition $\{p_1^{e_1}, p_2^{e_2}, \ldots, p_t^{e_t}\}$, the set of maximal prime power factors of m. Furthermore, given $p_j^{e_j}$ there exists a unique $i(j)$ such that $p_j^{e_j}$ divides $c_{i(j)}$; assume, renumbering if necessary, that $p_1^{e_1}$ divides c_1. Since $\phi(ab) \geq \phi(a) + \phi(b)$ for all $a, b > 2$, $\phi(c_i) \geq \sum_{p_j^{e_j} \in \mathcal{S}_i} \phi(p_j^{e_j})$ for all $i > 1$. Suppose $p_1^{e_1} \neq 2$. Then by the same reason we have $\phi(c_1) \geq \sum_{p_j^{e_j} \in \mathcal{S}_1} \phi(p_j^{e_j})$, and hence $\sum_{i=1}^{s} \phi(c_i) \geq \sum_{j=1}^{t} \phi(p_j^{e_j}) = W(m)$. On the other hand, if $p_1^{e_1} = 2$, then $\phi(c_1) \geq \sum_{p_j^{e_j} \in \mathcal{S}_1, j \neq 1} \phi(p_j^{e_j}) = (\sum_{p_j^{e_j} \in \mathcal{S}_1} \phi(p_j^{e_j})) - 1$, and again $\sum_{i=1}^{s} \phi(c_i) \geq W(m)$. ■

The sums in (1) and (2) of Theorem 2.7 are always *even*. This gives the following very surprising and amusing Corollary.

Corollary 2.9. *$GL(2k, \mathbb{Q})$ has an element of order m if and only if $GL(2k+1, \mathbb{Q})$ does.*

Example 2.10. *For small values of n, Theorem* 2.7 *allows us to calculate easily the possible orders of elements of $GL(n, \mathbb{Z})$. For example, $GL(2, \mathbb{Z})$ has elements of order* 2, 3, 4, *and* 6. *By Corollary* 2.9, *$GL(3, \mathbb{Z})$ has elements of the same orders. Similarly, $GL(4, \mathbb{Z})$ and $GL(5, \mathbb{Z})$ have elements of order* 2, 3, 4, 5, 6, 8, 10, *and* 12.

Exercise 2.11. What are the possible orders of elements in $GL(2, \mathbb{R})$?

Exercise 2.12. Consider $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt{2}$. Show that $GL(2, \mathbb{Q}(\sqrt{2}))$ contains an element of order 8. Recall from Example 2.10 that this is not the case for $GL(2, \mathbb{Q})$.

Determining the possible orders of integer or rational matrices is a natural question, and many variants of Theorem 2.7 have appeared in the literature; few seem to have been aimed at a general audience, but the reader may find several of the following references to be of interest. The earliest proof is due to Vaidyanathaswamy [**33**]. See our Paragraph 3.2 for how the authors discovered the proof in [**15**]. Other proofs are given in [**28**] and [**13**]; a very recent proof is in [**7**]. In a slightly different direction, Hanson has studied the problem of finding the minimal n for which $GL(n, \mathbb{Q})$ has an element of order m [**10**]. Volvacev discusses how to find the possible orders of matrices over an arbitrary field [**34**]. Taussky and Todd also have studied orders of matrices; see [**30**], [**31**], and [**32**].

3. ASYMPTOTIC RESULTS. Let $\mathcal{H}(n)$ denote the maximal order of an element of finite order of $GL(n, \mathbb{Z})$. In this section we study the asymptotic growth rate of the sequence $\{\mathcal{H}(n)\}$.

3.1. The first few terms of of the sequence $\mathcal{H}(n)$ are given in Table 1.

TABLE 1.

n	$\mathcal{H}(n)$	n	$\mathcal{H}(n)$
2	6	4	12
6	30	8	60
10	120	12	210
14	420	16	840
18	1260	20	2520
22	2520	24	5040

3.2. N. J. Sloane and S. Plouffe have compiled and published an extensive list of integer sequences [**26**], and, in addition, Sloane has made available a computer program that identifies integer sequences. The program can be accessed at http://www.research.att.com/~njas/sequences/. While [**26**] did not contain $\{\mathcal{H}(n)\}$, the program returned the reference [**15**]. Amusingly, this was the way the authors found their first reference on the orders of elements of $GL(n, \mathbb{Z})$.

Let $\mathcal{G}(n)$ denote the maximal order of an element of the symmetric group S_n. Finding the first few terms of the sequence $\{\mathcal{G}(n)\}$ is commonly given as an exercise in a beginning abstract algebra class. At a more advanced level the statistical properties of the orders of elements of the symmetric groups have received considerable attention; see [**5**]. The asymptotic growth of $\{\mathcal{G}(n)\}$ was determined early in the last century by Landau. We determine the growth rate of $\{\mathcal{H}(n)\}$ by relating it to that of $\{\mathcal{G}(n)\}$; we make considerable use of Miller's excellent exposition (which is very suitable for student use) of Landau's Theorem [**17**].

Theorem 3.3 (Landau). *If $\mathcal{G}(n)$ is the maximal order of an element of S_n, then*

$$\lim_{n\to\infty} \frac{\ln \mathcal{G}(n)}{\sqrt{n \ln n}} = 1.$$

Before relating the sequences $\{\mathcal{H}(n)\}$ and $\{\mathcal{G}(n)\}$, we need to develop some properties of the prime decomposition of $\mathcal{H}(n)$. These are analogous to those of $\mathcal{G}(n)$ given in [**17**].

3.4. Let p denote a generic prime and let $P(n)$ be the smallest prime such that $\sum_{p<P(n)} p \leq n$ and $\sum_{p\leq P(n)} p > n$. Let $Q(n)$ be the smallest prime such that $\sum_{p<Q(n)}(p-1) \leq n$ and $\sum_{p\leq Q(n)}(p-1) > n$. Observe that since $\pi(P(n)) < P(n)$, either $Q(n) = P(n)$, or $Q(n)$ is the successor prime to $P(n)$. It follows from Chebyshev's Theorem that there is a prime between $P(n)$ and $2P(n)$ so that in either case we have $Q(n) < 2P(n)$. In a discussion relating to a fixed n, we do not explicitly indicate the functional dependence and write P and not $P(n)$.

3.5. Let the function T be defined by $T(\prod p_i^{e_i}) = \sum(p_i - 1)p_i^{e_i-1}$. Recall from Corollary 2.9 that $\mathcal{H}(2\ell) = \mathcal{H}(2\ell+1)$; hence if n is odd, then it follows from Theorem 2.7 that $GL(n, \mathbb{Z})$ has an element of order m if and only if $T(m) \leq n$. Consequently, $\mathcal{H}(n)$ is the largest positive integer with $T(\mathcal{H}(n)) \leq n$. Later we show that this is true for all $n > 2$. Let the function S be defined by $S(\prod p_i^{e_i}) = \sum p_i^{e_i}$. Then as shown in Miller [**16**, Corollary 1], S_n has an element of order m if and only if $S(m) \leq n$.

Proposition 3.6. *$\mathcal{H}(n)$ is a multiple of* 4 *for $n \geq 4$. Consequently, for $n > 2$, $\mathcal{H}(n)$ is the largest integer with $T(\mathcal{H}(n)) \leq n$.*

Proof. There is no loss of generality in taking n to be odd and assuming that $T(\mathcal{H}(n)) \leq n$.

Suppose that $4 = 2^2$ does not divide $\mathcal{H}(n)$. If a matrix A has odd order k, then $-A$ has order $2k$; hence $\mathcal{H}(n) = 2p_2^{e_2} \cdots p_t^{e_t}$.

Suppose there is a prime $q_{\ell+1}$ such that $q_{\ell+1}$ divides $\mathcal{H}(n)$, while the previous prime q_ℓ does not. Let $m = (2q_\ell/q_{\ell+1})\mathcal{H}(n)$. Then by Chebyshev's Theorem, $m > \mathcal{H}(n)$, but $T(m) \leq T(\mathcal{H}(n))$. Hence we may assume that there are no gaps in the factorization of $\mathcal{H}(n)$.

Now suppose that there is a prime p such that p^e divides $\mathcal{H}(n)$ with $e \geq 2$. Let k be such that $p - 1 < 2^k < 2(p-1)$, and let $m = (2^k/p)\mathcal{H}(n)$. Note that $m > \mathcal{H}(n)$. Calculation yields

$$\begin{aligned} T(m) &= T(\mathcal{H}(n)) + 2^k + (p-1)p^{e-2} - (p-1)p^{e-1} \\ &\leq T(\mathcal{H}(n)) + 2(p-1) + (p-1)p^{e-2} - (p-1)p^{e-1} \\ &= T(\mathcal{H}(n)) + (p-1)[2 + p^{e-2}(1-p)] \\ &< T(\mathcal{H}(n)) \leq n. \end{aligned}$$

This contradicts the maximality of $T(\mathcal{H}(n))$, so we may assume that $\mathcal{H}(n)$ is square free. If $\mathcal{H}(n) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdots p_t$ is a product of primes with no gaps, then let $m = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdots p_t$; calculation shows that $m > \mathcal{H}(n)$, but $T(m) \leq T(\mathcal{H}(n))$. This gives the result for $n \geq 25$; the final result follows from Table 1 of values of $\mathcal{H}(n)$. The last statement now follows from Theorem 2.7. ■

The following lemma gives the remaining factorization properties of $\mathcal{H}(n)$ that we need.

Lemma 3.7. *Let $Q = Q(n)$ and $P = P(n)$ be defined as in* 3.4.

1. *The number of distinct prime factors of $\mathcal{H}(n)$ is at most $\pi(Q)$.*
2. *Let p_1 be a prime that does not divide $\mathcal{H}(n)$ and let p_2 be a prime greater than p_1. If $p_2^{e_2}$ is the highest power of p_2 that divides $\mathcal{H}(n)$, then $e_2 \leq 1$.*
3. *Let q be a prime with $q > 3$. If q^e with $e \geq 2$ is the highest power of q that divides $\mathcal{H}(n)$, then $q^e \leq 2Q < 4P$ and $q \leq \sqrt{2Q} < 2\sqrt{P}$.*
4. *If 2^e is the highest power of* 2 *that divides $\mathcal{H}(n)$, then $2^e \leq 4Q < 8P$. If 3^e is the greatest power of* 3 *that divides $\mathcal{H}(n)$, then $3^e \leq 3Q < 6P$.*

Proof. Let $\mathcal{H}(n) = (\prod_{i=1}^{r} q_i^{e_i})(\prod_{j=1}^{s} p_j)$ where $e_i > 1$ for all $i = 1, \dots, r$.

(1) Since $T(\mathcal{H}(n)) \leq n$, we must have $\sum_{i=1}^{r}(q_i - 1)q_i^{e_i - 1} + \sum_{j=1}^{s}(p_i - 1) \leq n$; consequently, $\sum_{i=1}^{r}(q_i - 1) + \sum_{j=1}^{s}(p_i - 1) \leq n$. Since Q is the smallest prime such that $\sum_{p<Q} p - 1 \leq n$, it follows that $r + s \leq \pi(Q)$.

(2) Suppose not; that is, suppose that $e_2 > 1$. Let k be such that $p_2 - 1 < p_1^k \leq p_1(p_2 - 1)$, and let $m = (p_1^k/p_2)\mathcal{H}(n)$. We have $m \geq \mathcal{H}(n)$, since $p_1^k \geq p_2$; the inequality is in fact strict since p_1 and p_2 are primes. We have

$$T(m) = T(\mathcal{H}(n))) + \underbrace{(p_1 - 1)p_1^{k-1} + (p_2 - 1)p_2^{e_2 - 2} - (p_2 - 1)p_2^{e_2 - 1}}_{B}$$

Then

$$\begin{aligned} B &= (p_1 - 1)p_1^{k-1} - (p_2 - 1)^2 p_2^{e_2 - 2} \\ &\leq (p_1 - 1)(p_2 - 1) - (p_2 - 1)^2 \\ &= (p_2 - 1)((p_1 - 1) - (p_2 - 1)) < 0. \end{aligned}$$

Thus $T(m) < T(\mathcal{H}(n))$, which is a contradiction since $m > \mathcal{H}(n)$.

(3) Let P^* be the smallest prime not dividing $\mathcal{H}(n)$. Note that $P^* \leq Q$. Let q be a prime greater than 3 such that q^e divides $\mathcal{H}(n)$ with $e > 1$. By (2) if $q > P^*$, then $e \leq 1$; hence we may assume that $q < P^*$. Suppose that $q^e > 2P^*$. We have $q < P^* < qP^*$. Let $m = (P^*/q)\mathcal{H}(n)$. Then $m > \mathcal{H}(n)$ and $T(m) = T(\mathcal{H}(n)) + \underbrace{[(P^* - 1) + (q - 1)q^{e-2} - (q - 1)q^{e-1}]}_{B}$. It is sufficient to show that the quantity B in the square brackets is negative. This is indeed the case since

$$\begin{aligned} B &= P^* - 1 + 2q^{e-1} - q^{e-2} - q^e \\ &< P^* - 1 + \frac{1}{2}q^e - q^{e-2} - q^e \\ &< P^* - 1 - q^{e-2} - P^* < 0. \end{aligned}$$

Thus $T(m) < T(\mathcal{H}(n))$ with $m > \mathcal{H}(n)$, which is a contradiction; hence $q^e \leq 2P^* \leq 2Q$. Since $e \geq 2$, we have $q \leq \sqrt{2Q} < 2\sqrt{P}$.

(4) This proof is similar to that of (3) and is left as an exercise. ■

Exercise 3.8. Prove the following properties of the prime factorization of $\mathcal{H}(n)$.

1. How does the proof of Proposition 3.6 depend on the hypothesis that 4 does not divide $\mathcal{H}(n)$?
2. Prove (4) of Lemma 3.7.
3. Let p_1 and p_2 be primes with $p_1 < p_2$. If $p_1^{e_1}$ (respectively, $p_2^{e_2}$) is the highest power of p_1 (respectively, p_2) that divides $\mathcal{H}(n)$, then $e_2 \leq e_1 + 1$. This is a generalization of (2) of Lemma 3.7.
4. Let p_1 and p_2 be primes neither of which divides $\mathcal{H}(n)$. If q is a prime greater than $p_1 + p_2$, then q does not divide $\mathcal{H}(n)$.
5. If q is a prime greater than $2Q$, then q does not divide $\mathcal{H}(n)$.

Exercise 3.9. See [**19**] for many other interesting properties of the sequence $\{\mathcal{G}(n)\}$. The reader can try to prove analogs for $\{\mathcal{H}(n)\}$.

We can now prove that $\ln \mathcal{G}(n)$ and $\ln \mathcal{H}(n)$ grow at the same asymptotic rate. The proof of the following theorem is taken from [**22**]; another proof is in [**14**]. See [**7**, Theorem 3.3] for an upper bound on $\ln \mathcal{H}(n)$.

Theorem 3.10. *If $\mathcal{H}(n)$ is the maximal finite order of an element of $GL(n, \mathbb{Z})$, then*

$$\lim_{n\to\infty} \frac{\ln \mathcal{H}(n)}{\sqrt{n \ln n}} = 1.$$

Proof. Since S_n can be embedded in $GL(n, \mathbb{Z})$ (see Exercise 1.1), $\mathcal{G}(n) \le \mathcal{H}(n)$. The strategy of the proof is to show that $\mathcal{H}(n) \le \mathcal{G}(n + n^\gamma)$ for $0 < \gamma < 1$ and then apply Landau's Theorem (Theorem 3.3) that $\lim_{n\to\infty} \mathcal{G}(n)/\sqrt{n \ln n} = 1$. The fact that $\gamma < 1$ ensures that $\ln \mathcal{G}(n + n^\gamma) \sim \ln \mathcal{G}(n)$.

Let $\mathcal{H}(n) = (\prod_{i=1}^r q_i^{e_i})(\prod_{j=1}^s p_j)$ where $e_i > 1$ for all $i = 1, \dots, r$. Then

$$\begin{aligned} T(\mathcal{H}(n)) &= T\left(\left(\prod_{i=1}^r q_i^{e_i}\right)\left(\prod_{j=1}^s p_j\right)\right) \\ &= \sum_{i=1}^r (q_i - 1) q_i^{e_i - 1} + \sum_{j=1}^s (p_j - 1) \le n. \end{aligned}$$

Hence $\sum_{i=1}^r q_i^{e_i} + \sum_{j=1}^s p_j \le n + \sum_{j=1}^r q_i^{e_i-1} + s$. By Lemma 3.7 (2), (3), and (4) each $q_i^{e_i-1} < 8P/2 = 4P$ and there are at most $\pi(2\sqrt{P})$ terms. Consequently, $\sum_{j=1}^r q_i^{e_i-1} < 4P\pi(2\sqrt{P})$. From Lemma 3.7 (1) we have $s < \pi(Q) < \pi(2P)$. Combining yields $S(\mathcal{H}(n)) < n + 4P\pi(2\sqrt{P}) + \pi(2P)$; that is, $S(\mathcal{H}(n)) < N$ for $N = n + 4P\pi(2\sqrt{P}) + \pi(2P)$. As noted in 3.5, this implies that S_N has an element of order $\mathcal{H}(n)$. Hence $\mathcal{H}(n) \le \mathcal{G}(N) = \mathcal{G}(n + 4P\pi(2\sqrt{P}) + \pi(2P))$. It was shown in [**16**, p. 505] that $P \sim \sqrt{n \ln n} \sim \ln \mathcal{G}(n)$; hence for sufficiently large n we have

$$P < \sqrt{n \cdot n^{\frac{2}{10}}} = n^{\frac{6}{10}}.$$

Thus, again for sufficiently large n, we have

$$\begin{aligned} n + 4P\pi(2\sqrt{P}) + \pi(2P) &< n + 4 \cdot n^{\frac{6}{10}} \cdot 2 \cdot n^{\frac{6}{20}} + 2 \cdot n^{\frac{6}{10}} \\ &\le n + 8n^{\frac{18}{20}} + 2n^{\frac{12}{20}} \\ &< n + n^\gamma, \end{aligned}$$

where γ is any real number such that $18/20 < \gamma < 1$. Thus since $\mathcal{H}(n)$ and $\mathcal{G}(n)$ are nondecreasing, we have

$$\limsup_{n\to\infty} \frac{\ln \mathcal{H}(n)}{\sqrt{n \ln n}} < \lim_{n\to\infty} \frac{\ln \mathcal{G}(n + n^\gamma)}{\sqrt{n \ln n}}$$

$$= \lim_{n\to\infty} \frac{\sqrt{(n+n^\gamma)\ln(n+n^\gamma)}}{\sqrt{n\ln n}}$$

$$= \lim_{n\to\infty} \sqrt{\left(\frac{n+n^\gamma}{n}\right)\left(\frac{\ln(n+n^\gamma)}{\ln n}\right)} = 1.$$

Since

$$\liminf_{n\to\infty} \frac{\ln \mathcal{H}(n)}{\sqrt{n\ln n}} \geq \lim_{n\to\infty} \frac{\ln \mathcal{G}(n)}{\sqrt{n\ln n}} = 1,$$

we have

$$\lim_{n\to\infty} \frac{\ln \mathcal{H}(n)}{\sqrt{n\ln n}} = 1. \qquad \blacksquare$$

Exercise 3.11. Theorem 3.10 shows that $\{\ln \mathcal{H}(n)\}$ and $\{\ln \mathcal{G}(n)\}$ grow at the same rate. What about $\{\mathcal{H}(n)\}$ and $\{\mathcal{G}(n)\}$? Since S_n embeds in $GL(n,\mathbb{Z})$, it is obvious that $\mathcal{H}(n) \geq \mathcal{G}(n)$; in fact, it is almost as easy to see that $\mathcal{H}(n)/\mathcal{G}(n) \geq 2$. Show $\mathcal{H}(n)/\mathcal{G}(n) \geq 2$.

What is $\limsup_{n\to\infty} \mathcal{H}(n)/\mathcal{G}(n)$? The authors do not even know if the sequence $\{\mathcal{H}(n)/\mathcal{G}(n)\}$ is unbounded. To investigate this question, the second author wrote a computer program to calculate $\mathcal{H}(n)/\mathcal{G}(n)$ for $n \leq 100{,}000$. The results are summarized in Table 2. The sequence of ratios seems to grow very slowly; the maximum ratio for $n \leq 100{,}000$ occurs first at $n = 22{,}434$.

TABLE 2.

N	$\max\left\{\frac{\mathcal{H}(n)}{\mathcal{G}(n)} : n \leq N\right\}$
76	13.000
160	20.667
730	27.721
2,176	40.746
22,434	50.978
100,000	50.978

4. FINITE SUBGROUPS OF *GL*(2, $\mathbb{Q}$).

What are the finite subgroups of $GL(2,\mathbb{Q})$? A complete solution to this problem is given by Newman in [**17**, p. 180]; he uses consequences of a strengthened version of Minkowski's Theorem 1.4. Recently, Mackiw gave a solution to the problem designed for abstract algebra students [**16**]; it appears that his solution could be given in outline form to undergraduates with the details left as a student project. We propose an approach that uses more linear algebra, and less group theory, than that of Mackiw.

First, recall that the dihedral group of order $2n$, denoted D_n, is given by generators and relations as follows: $D_n = \langle a, b : a^2 = e, b^n = e, a^{-1}ba = b^{n-1}\rangle$. The group D_n is geometrically realized as the group of symmetries of the regular n-gon. Another group that can be given by generators and relations is the quaternion group H of order 8. It is given by $H = \langle a, b : b^4 = e, a^2 = b^2 a^{-1}ba = b^3\rangle$.

Project 4.1. If G is a finite subgroup of $GL(2, \mathbb{Q})$, then G is isomorphic to one of the following groups:

$$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_6, D_3, D_4, D_6.$$

Conversely, all these groups occur as subgroups of $GL(2, \mathbb{Q})$.

The ideas in the following exercise together with its extensive hint can be used to complete Project 4.1.

Exercise 4.2. If G is a 2-subgroup of $GL(2, \mathbb{Q})$ with a cyclic normal subgroup of order 4, show that $G \cong \mathbb{Z}_4$ or $G \cong D_4$. **Extensive hint:** Assume that $|G| > 4$ and let $\langle h \rangle \lhd G$ with $o(h) = 4$. The characteristic polynomial of h is a divisor of $x^4 - 1$, and thus since $o(h) = 4$, the characteristic polynomial must be $x^2 + 1$. Consequently, h is similar to the companion matrix of $x^2 + 1$; see [**4**, p. 456]. Hence there is no loss of generality in assuming that

$$h = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

and

$$\langle h \rangle = \{h, h^2, h^3, I\} = \left\{ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, -I, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, I \right\}.$$

Since G is 2-group, there exists $g \in G - \langle h \rangle$ with $g^2 \in \langle h \rangle$; say

$$g = \begin{bmatrix} x & y \\ z & w \end{bmatrix}.$$

By the normality of $\langle h \rangle$, either (1) $ghg^{-1} = h$ or (2) $ghg^{-1} = h^3$. In each case calculation can be used to complete the argument.

It follows from Exercise 4.2 that no subgroup of $GL(2, \mathbb{Q})$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ or the quaternion group H. Note that both $\mathbb{Z}_4 \times \mathbb{Z}_2$ and the quaternion group H can be embedded in $GL(2, \mathbb{C})$. Also note that while $GL(3, \mathbb{Q})$ has the same possible orders of elements as does $GL(2, \mathbb{Q})$ (Corollary 2.9), it does contain a copy of $\mathbb{Z}_4 \times \mathbb{Z}_2$. See [**18**, p. 180] for a list of all the isomorphism classes of finite subgroups of $GL(3, \mathbb{Q})$.

5. FINITE SUBGROUPS OF $GL(n, \mathbb{C})$.

Since $\mathbb{C}$ contains all mth roots of unity for every positive integer m, $GL(n, \mathbb{C})$ contains elements of all possible orders; consequently, $GL(n, \mathbb{C})$ has infinitely many non-isomorphic finite subgroups and Minkowski's Theorem cannot hold. Thus one might suspect that being a subgroup of $GL(n, \mathbb{C})$ is not a very strong property, but this is not the case. There are many implications for such groups, and we will be interested in one of them: Jordan's Theorem (1878) says there exists a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that if G is a finite subgroup of $GL(n, \mathbb{C})$, then G has a normal Abelian subgroup A with $[G : A] \leq f(n)$. One immediate consequence of Jordan's Theorem is that up to isomorphism $GL(n, \mathbb{C})$ contains only finitely many finite non-Abelian simple groups (a group is *simple* if it has no nontrivial normal subgroups). Over the years many mathematicians have produced functions $f(n)$ giving a bound as specified in Jordan's Theorem, but as late as 1971 (see [**3**, p. 178]), the best $f(n)$ known was $f(n) = n!\,(6^{n-1})^{\pi(n+1)+1}$, produced by Blichfeldt in 1917. In 1984 Weisfeiler announced a major improvement in [**35**]. Unfortunately, Weisfeiler disappeared—literally, while hiking in the Andes—before a proof appeared; recent evidence indicates that he may have been one of the 'desaparecidos' of the military government of General Pinochet in Chile [**11**]. Feit [**6**] and Friedland [**8**] indicate that Weisfeiler's proofs exist in manuscript form [**36**], where he gave the even stronger following theorem.

Theorem 5.1. *If G is a finite subgroup of $GL(n, \mathbb{C})$ and $n > 63$, then G contains a normal Abelian subgroup A with $[G : A] \leq (n + 2)!$.*

Weisfeiler included 'Post-Classification' in the title of [**35**] to indicate that his proof depends upon the classification of finite simple groups. Finding and classifying the finite simple groups was one of the major unsolved problems in algebra during most of this century. The problem finally yielded in 1980 (it is hard to give an exact date, but this is generally accepted) to an attack that was organized by Daniel Gorenstein and involved the work of many algebraists. Since the proof consists of about 15,000 pages published in many papers in many journals, the final result is often called 'The Enormous Theorem'. A brief, but captivating, discussion of the Enormous Theorem and the current efforts (also a 'group project') to simplify its proof are in [**1**]. Another good discussion with more details is in [**27**].

6. FINITE SUBGROUPS OF $GL(n, \mathbb{Q})$ OF MAXIMAL ORDER. What is the maximal possible order of a finite subgroup of $GL(n, \mathbb{Q})$? In [**7**] Friedland conjectured that for large values of n the maximal such order is $2^n n!$ and that all subgroups of that order are isomorphic to the group B_n of Exercise 1.2. Feit [**6**] showed that this is the case except for $n = 2, 4, 6, 7, 8, 9, 10$, and for each of these values of n he found maximal subgroups, which are unique up to conjugacy. Friedland [**8**] gave a simpler proof for sufficiently large n. Both proofs use Weisfeiler's result and hence depend on the classification of finite simple groups; it is ironic that the known proofs of such an easy to state result depend on the 'Enormous Theorem'.

Theorem 6.1. *For $n > 10$ the maximal order of a finite subgroup of $GL(n, \mathbb{Q})$ is $2^n n!$, and any subgroup of this order is conjugate to B_n.*

Project 4.1 shows that a subgroup of maximal possible order of $GL(2, \mathbb{Q})$ must be isomorphic to D_6 and must have order 12; it thus cannot be isomorphic to B_2. Moreover, any copy of D_4 in $GL(2, \mathbb{Q})$ is a maximal finite subgroup that is not of maximal possible order. Finding the maximal finite subgroups of $GL(n, \mathbb{Q})$ is a difficult problem, and it wasn't until 1965 that Dade found the maximal finite subgroups of $GL(4, \mathbb{Q})$ [**2**]. Since that time, theoretical work has been combined with computations on ever-faster computers to provide knowledge of the maximal subgroups of $GL(n, \mathbb{Q})$; they are known for values of n less than or equal to 22; see [**23**].

REFERENCES

1. B. Cipra, Are group theorists simpleminded, in *What's Happening in the Mathematical Sciences, 1995–1996*, American Mathematical Society, Providence, 1996.
2. E. C. Dade, The maximal finite groups of 4 × 4 integral matrices, *Illinois J. Math.* **9** (1965) 99–122.
3. L. Dornhoff, *Group Representation Theory, Part A*, Marcel Dekker, New York, 1971.
4. D. S. Dummit and R. M. Foote, *Abstract Algebra*, 2nd ed., Prentice Hall, Upper Saddle River, 1999.
5. P. Erdös and P. Turán, On some problems of statistical group theory, *Z. Wahrscheinlichkeitstheorie verw. Gebeite* **18** (1965) 151–163.
6. W. Feit, Orders of Finite Linear Groups, preprint.

7. S. Friedland, Discrete groups of unitary isometries and balls in hyperbolic manifolds, *Linear Algebra Appl.* **241–243** (1996) 305–341.
8. S. Friedland, The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$, *Proc. Amer. Math. Soc.* **125** (1997) 3519–3526.
9. J. Gallian, *Contemporary Abstract Algebra*, 2nd ed., D. C. Heath, Lexington, 1990.
10. R. Hanson, Minimum dimension for a square matrix of order n, *College Math. J.* **21** (1990) 28–34.
11. V. Kac and O. Weisfeiler, Letter to the Editor, *Notices Amer. Math. Soc.* **48** (2001) 7–8.
12. Y. R. Katznelson, On the orders of finite subgroups of $GL(n, \mathbb{Z})$, *Expo. Math.* **12** (1994) 453–457.
13. D. Kirby, Integer matrices of finite order, *Rend. Mat. (6)* **2** (1969) 403–408.
14. G. Levitt and J.-L. Nicolas, On the maximum order of torsion elements in $GL(n, Z)$ and $Aut(F_n)$, *J. Algebra* **208** (1998) 630–642.
15. H. Lüneburg, *Galoisfelder, Kriesteilungskörper und Schieberegisterfolgen*, B. I. Wissenschaftsverlag, Mannheim, 1979.
16. G. Mackiw, Finite groups of 2 × 2 integer matrices, *Math. Mag.* **69** (1996) 356–361.
17. W. Miller, The maximum order of an element of a finite symmetric group, *Amer. Math. Monthly* **94** (1987) 497–506.
18. M. Newman, *Integral Matrices*, Academic Press, New York, 1972.
19. J.-L. Nicolas, Ordre maximal d'un élément du group des permutations et highly composite numbers, *Bull. Soc. Math. France* **97** (1969) 129–191.
20. J.-L. Nicolas, Calcul de l'ordre maximum d'un élément du groupe symétrique, *Rev. Francaise Informat. Rescherche Operationelle* **3** (1969) 43–50.
21. A. Pavlichenkov, Orders of Elements in $GL(n, \mathbb{Q})$, Term Paper in Modern Algebra, Wake Forest University, Fall, 1994.
22. A. Pavlichenkov, Independent Study Notes, Summer, 1995.
23. W. Plesken and G. Nebe, *Finite Rational Matrix Groups*, Memoir of the American Mathematical Society, no. 556, Providence, 1995.
24. D. N. Rockmore and K. Tan, A note on the order of finite subgroups of $GL(n, \mathbb{Z})$, *Arch. Math.* **64** (1995) 283–288.
25. J.-P. Serre, *Lie Algebras and Lie Groups*, Springer-Verlag, Berlin, 1992.
26. N. J. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York, 1995.
27. R. Solomon, On finite simple groups and their classification, *Notices Amer. Math. Soc.* **42** (1995) 231–239.
28. D. A. Suprunenko, On the order of an element of a group of integral matrices, *Dokl. Akad. Nauk. BSSR* **7** (1963) 221–223.
29. J. Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987) 279–280.
30. O. Taussky, Matrices of rational integers, *Bull. Amer. Math. Soc.* **66** (1960) 327–345.
31. O. Taussky and J. Todd, Matrices with finite period, *Proc. Edinburgh Math. Soc.* **6** (1939) 128–134.
32. O. Taussky and J. Todd, Matrices of finite period, *Proc. Royal Irish Acad.* **46** (1941) 113–121.
33. R. Vaidyanathaswamy, On the possible periods of integer-matrices, *J. London Math. Soc.* **3** (1928) 268–272.
34. R. T. Volvacev, On the order of an element of a matrix group, *Vesci. Akad. Navuk. BSSR, Ser. Fiz.-Mat. Navuk* no. 2 (1965), 11–16.
35. B. Weisfeiler, Post-classification version of Jordan's Theorem on finite linear groups, *Proc. Nat. Acad. Sci. U.S.A.* **81** (1984) 5278–5279.
36. B. Weisfeiler, On the Size and Structure of Finite Linear Groups, preprint.

JAMES KUZMANOVICH received his undergraduate degree from Rose-Hulman and his Ph.D. in 1970 from the University of Wisconsin. His research interests are in noncommutative algebra. He also enjoys reading and gardening (even in the red clay of North Carolina). He has a collection of mathematical postage stamps; part of his collection can be viewed at http://www.math.wfu.edu/∼kuz/Stamps/stamppage.htm.
Wake Forest University, Winston-Salem, NC 27109
kuz@wfu.edu

ANDREY PAVLICHENKOV received his undergraduate degree in mathematics from Wake Forest University. He is completing an M.Sc. in finance, economics, and econometrics from City University of London. He likes to travel and enjoys mountaineering.
Marshal Birusova St 43-71, Moscow, Russia 12
A.Pavlichenkov@hotmail.com