A Note on the Order of Finite Subgroups of $GL(n, \mathbf{Z})$

Daniel N. Rockmore
Dept. of Math and Computer Science
Dartmouth College
Hanover, NH 03755*

Ki-Seng Tan
Dept. of Mathematics
Columbia University
NY, NY 10027

July 11, 1995

Abstract

A simple upper bound on the size of finite subgroups of $GL(n, \mathbf{Z})$ is given. Only elementary number-theoretic arguments are used, thereby avoiding previous methods depending on estimates of the Jordan number and the classification of finite simple groups.

1 Introduction

In this note we give an upper bound on the size of any finite subgroup of $GL(n, \mathbf{Z})$. The example of signed permutation matrices shows that such subgroups can have size at least $(n!)2^n$. In fact, W. Feit has recently announced [3] that by using some unpublished results of B. Weisfeiler and the classification of finite simple groups (cf. [5]), it can be shown that this *is* the upper bound on the size of such subgroups, except for $n = 2, 4, 6, 7, 8, 9,$ and 10 for which the Weyl groups of some of the exceptional groups provide counterexamples.

Here we show by only elementary number-theoretic considerations,

Theorem 1 *For any $\epsilon > 0$, there exists a constant C depending only on ϵ such that any finite subgroup $G < GL(n, \mathbf{Z})$ has order at most $(n!)^{1+\epsilon} C^n$.*

To simplify statements let $FS(n)$ denote the size of the largest finite subgroup of $GL(n, \mathbf{Z})$. Elementary divisibility conditions yield a naive upper bound of $FS(n) < (2n)!$ [7]. Friedland [4] gives a more precise estimate involving the **Jordan number**, denoted $j(n)$. The Jordan number is defined as the maximal index of a normal abelian subgroup of any finite subgroup $\Gamma < GL(n, \mathbf{R})$. The existence of such a bound is a well-known result of Jordan. Friedland shows ([4], Corollary 3.4) that $FS(n) \leq 2^n j(n)$. Consequently, one method of estimating $FS(n)$ is to estimate $j(n)$. Towards this direction the best known result proved to date is that due to Speiser [10] which states that

$$\log j(n) \leq n \log 12 + \log n! + nZ(n) \log 12$$

*D. Rockmore supported in part by an NSF Math Sciences Postdoctoral Fellowship

where $Z(n)$ is the number of primes in the interval $[1, n]$. Classical results due to Chebyshev show that $.92\frac{n}{\log n} < Z(n) < 1.11\frac{n}{\log n}$ (cf. [1], p. 55) and hence we obtain

$$\log j(n) \leq O(\frac{n^2}{\log n}).$$

Note that in fact, the subsequent derived bound of $FS(n)$ is far from the conjectured bound as asymptotically,

$$\frac{n^2}{\log n} \geq (n \log n)n^{\delta} \geq n^{\delta} \log(n!)$$

for any $0 \leq \delta < 1$. This then gives an asymptotic bound of $FS(n) \leq O(2^n (n!)^{1+n^{\delta}})$.

A better bound for $j(n)$ has been announced by Weisfeiler [13]. He asserts that by using the classification of finite simple groups it can be shown that $\log j(n) \leq O(n \log n)$. Unfortunately this assertion is still unproved. Its proof would give a bound of $FS(n)$ of the now known asymptotic order. We refer the reader to Friedland's interesting paper [4] for a more thorough discussion of these and related issues.

We proceed from a different point of view, instead deriving an asymptotic estimate for $FS(n)$ from a well-known divisibility criteria for orders of finite subgroups of $GL(n, \mathbf{Z})$. We use only elementary number-theoretic arguments.

Remark. In recent work, Y. Katznelson has apparently independently obtained results similar to ours [6]. We thank Professor Shmuel Friedland for bringing the work of Feit and Katznelson to our attention before the final version of this paper was prepared.

2 Main Result

Our starting point is the following classical divisibility result, which is essentially due to Minkowski ([8], see also [11], Section 3.3).

Proposition 1 *For any $n \geq 2$ and prime p define*

$$\nu_n(p) = \left[\frac{n}{p-1}\right] + \left[\frac{n}{(p-1)p}\right] + \cdots + \left[\frac{n}{(p-1)p^n}\right] + \cdots \tag{1}$$

where $\left[\frac{n}{m}\right]$ denotes the integer part of $\frac{n}{m}$.

Then the order of any finite subgroup of $GL(n, \mathbf{Z})$ divides

$$L(n) = \prod_{p \leq n} p^{\nu_n(p)}$$

and thus is also bounded by $L(n)$.

Thus, we seek only to bound $L(n)$ in order to bound $FS(n)$.

Theorem 1 *Given $\epsilon > 0$, there exists $C > 0$, depending only on ϵ such that $L(n) \leq (n!)^{1+\epsilon} \cdot C^n$.*

Proof: The idea is simply to break up the product $L(n)$ into pieces which can be estimated in terms of ϵ. Besides the definition of $\nu_n(p)$ (1) it is also useful to make the definition

$$\mu_n(p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots. \tag{2}$$

Note that (see e.g. [8], p. 200)

$$\prod_p p^{\mu_n(p)} = n!. \tag{3}$$

We have

$$\begin{aligned} \nu_n(p) &\leq \tfrac{n}{p-1} + \tfrac{n}{p(p-1)} + \cdots \\ &\leq \tfrac{n}{p-1} \cdot \tfrac{p}{(p-1)} = \tfrac{np}{(p-1)^2}. \end{aligned} \tag{4}$$

Let $N > 4$ be an integer such that for all $p \geq N$,

$$\frac{p(p+2)}{(p-1)^2} \leq 1 + \epsilon.$$

Let $S_N = \{p \mid p \geq N \text{ and } p^2 + 2p \leq 2n\}$. We now estimate $\nu_n(p)$ in five distinct cases.

Case 1: $p = 2$.

In this case,

$$\begin{aligned} \nu_n(p) &= [n] + \left[\tfrac{n}{2}\right] + \cdots + \left[\tfrac{n}{2^k}\right] + \cdots \\ &= [n] + \mu_n(2) \leq n + \mu_n(2) \end{aligned}$$

Case 2: $p = 3$.

Here,

$$\begin{aligned} \nu_n(p) &= \left[\tfrac{n}{2}\right] + \left[\tfrac{n}{6}\right] + \cdots + \left[\tfrac{n}{2\cdot 3^k}\right] + \cdots \\ &\leq \left[\tfrac{n}{2}\right] + \left[\tfrac{n}{3}\right] + \cdots + \left[\tfrac{n}{3^k}\right] + \cdots \\ &= \left[\tfrac{n}{2}\right] + \mu_n(3) \leq \tfrac{n}{2} + \mu_n(3) \end{aligned}$$

Case 3: $3 < p < N$. In this case, $p^2 - 5p \geq 0$ so that

$$p^3 - 2p^2 - 2p + 1 \geq p^3 - 3p^2 + 3p - 1$$

and

$$(p+1)(p^2 - 3p + 1) \geq (p-1)^3.$$

Hence, since by assumption $p + 1 \leq N$, we have

$$N((p-1)^2 - p) \geq (p-1)^3$$

so that

$$N((p-1)^2 - p) + (p-1)^2 - p(p-1)^2 \geq 0$$

and

$$(N+1)(p-1)^2 - pN - p(p-1)^2 \geq 0,$$

giving

$$\frac{(N+1) - p}{p} \geq \frac{N}{(p-1)^2}.$$

Consequently,

$$\begin{aligned} \nu_n(p) \leq \tfrac{np}{(p-1)^2} \leq \tfrac{nN}{(p-1)^2} &\leq n(\tfrac{N+1-p}{p}) \\ &\leq n \cdot \left[\tfrac{N}{p}\right] \\ &\leq n \cdot \mu_N(p). \end{aligned}$$

Case 4: $p \in S_N$.

If $p \in S_N$ we have

$$\nu_n(p) \leq \frac{np}{(p-1)^2} \leq \frac{n}{p+2}(1+\epsilon)$$

and

$$\begin{aligned} np &\le np + 2n - p^2 - 2p \\ &= (p+2)(n-p). \end{aligned}$$

Hence,

$$\frac{n}{p+2} \le \frac{n-p}{p} \le \left[\frac{n}{p}\right]$$

yielding

$$\nu_n(p) \le \left[\frac{n}{p}\right](1+\epsilon) \le \mu_n(p)(1+\epsilon).$$

Case 5: $p^2 + 2p > 2n$.

We may now assume that $p > 4$. Thus we have that $2(p^2 - p) > p^2 + 2p > 2n$ so that $p^2 - p > n$. Consequently,

$$\begin{aligned} \nu_n(p) &= \left[\tfrac{n}{p-1}\right] + \left[\tfrac{n}{p^2-p}\right] + \cdots \\ &= \left[\tfrac{n}{p-1}\right] \\ &= \left[\tfrac{n}{p}\right] + (\left[\tfrac{n}{p-1}\right] - \left[\tfrac{n}{p}\right]) \\ &= \left[\tfrac{n}{p}\right] + \delta_n(p) = \mu_n(p) + \delta_n(p). \end{aligned}$$

Since $\frac{n}{p-1} - \frac{n}{p} = \frac{n}{(p-1)\cdot p} < 1$ we have $\delta_n(p) = 0$ or 1.

Combining these five cases and using (3) yields

$$\begin{aligned} L(n) &= \prod_{p\le n} p^{\nu_n(p)} \\ &\le 2^{n+\mu_n(2)} \cdot 3^{\frac{n}{2}+\mu_n(3)} \cdot \prod_{p\le n,\ 3<p<N} p^{n\mu_N(p)} \cdot \\ &\quad \prod_{p\le n,\ p\in S_N} p^{\mu_n(p)(1+\epsilon)} \cdot \prod_{p\le n,\ p^2+2p>2n} p^{\mu_n(p)+\delta_n(p)} \\ &\le (2\sqrt{3}N!)^n (n!)^{1+\epsilon} \cdot \prod_{p\le n,\ p^2+2p>2n} p. \end{aligned}$$

Finally, using the estimate (cf. [2])

$$T(n) := \prod_{p\le n} p \le e^{1.2n}$$

yields

$$L(n) \le (e^{1.2} 2\sqrt{3}N!)^n (n!)^{1+\epsilon}.$$

□

Remark: It is well-known that any finite subgroup of $GL(n,\mathbf{Q})$ is conjugate to a finite subgroup of $GL(n,\mathbf{Z})$ (see, eg., [12], p. 124) and similarly, any finite subgroup of $GL(n,\mathbf{Q}(t_1,\ldots,t_r))$ (for indeterminates $t_1,\ldots,t_r$, $r \ge 1$) is conjugate to a finite subgroup of $GL(n,\mathbf{Z})$ [9]. Consequently we have the following simple corollary.

Corollary *Let F denote any of the fields $\mathbf{Q}$ or $\mathbf{Q}(t_1,\ldots,t_r)$ for indeterminates $t_1,\ldots,t_r$, $(r \ge 1)$. Given $\epsilon > 0$, there exists a constant C, depending only on ϵ (as in Theorem 1), such that any finite subgroup $G < GL(n,F)$ has order less than or equal to $n!^{1+\epsilon}C^n$.*

3 Analysis of the Constant

In this section we give a brief analysis of the dependence on ϵ of the constant C of Theorem 1 and its Corollary. Recall that $C = e^{1.2}2\sqrt{3}N!$ where $N > 4$ is any integer such that for all primes p, $p \geq N$, we have

$$\frac{p(p+2)}{(p-1)^2} \leq 1 + \epsilon.$$

Thus, we seek to bound N in terms of ϵ.

We note first that since the rational function $\frac{x(x+2)}{(x-1)^2}$ is decreasing for $x > 4$, it suffices to find N such that

$$\frac{N(N+2)}{(N-1)^2} \leq 1 + \epsilon.$$

To simplify this, it is in turn enough to find N, such that

$$\frac{(N+2)^2}{(N-1)^2} \leq 1 + \epsilon$$

or

$$\frac{N+2}{N-1} \leq \sqrt{1+\epsilon}.$$

Thus, we arrive at

$$\begin{aligned} N &\geq \tfrac{3(1+\sqrt{1+\epsilon})}{\epsilon} + 1 \\ &\geq \tfrac{3(1+1+\frac{\epsilon}{2}-\delta)}{\epsilon} + 1 \end{aligned}$$

where (using Taylor's Theorem) $0 \leq \delta \leq \frac{1}{8}\epsilon^2$. Thus, we may take

$$N = \left[\frac{6}{\epsilon} + \frac{7}{2}\right]$$

giving

$$C = \left[\frac{6}{\epsilon} + \frac{7}{2}\right]! e^{1.2} 2\sqrt{3}.$$

References

[1] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, NY, 1980.

[2] W. and F. Ellison. *Prime Numbers.* John Wiley and Sons, Inc., NY, 1985.

[3] W. Feit. Private correspondence. September 5, 1994.

[4] S. Friedland. Discrete groups of unitary isometries and balls in hyperbolic manifolds. Preprint. 1993.

[5] D. Gorenstein. *The Classification of Finite Simple Groups.* Vol. 1, Plenum Press, NY, 1982.

[6] Y. Katznelson. On the orders of finite subgroups of $GL(n, \mathbf{Z})$. Preprint. 1994.

[7] M. Newman. *Integral Matrices*, Pure and Applied Mathematics, Volume 45, Academic Press, NY, 1972.

[8] H. Minkowski. Zur Theorie der positiven quadratischen Formen, *J. Crelle* **101** (1887), 196-202 (*Gesamm. Abh. I*, 212-218).

[9] D. Rockmore and K.-S. Tan. Deciding finiteness for matrix groups over function fields. Technical Report PCS-TR94-227, Department of Computer Science, Dartmouth College, 1993.

[10] A. Speiser. *Die theorie der gruppen von endlicher ordnung.* 3rd ed., Birkhauser, Basel. 1956

[11] J. P. Serre. Arithmetic groups. in C. T. C. Wall (Ed.), *Homological Group Theory*, LMS no. 36, Cambridge Univ. Press, Cambridge, Eng., 1979, 105-136.

[12] J. P. Serre. *Lie Algebras and Lie Groups (2^{nd} edition)*, LNM 1500, Springer-Verlag, NY, 1992.

[13] B. Weisfeiler. Post-classification of Jordan's theorem on finite linear groups, *Proc. Natl. Acad. Sci. USA* **81** (1984), 5278-5279.