1. Introduction

For an integer $m \geq 2$, write $(\mathbb{Z}/m)\times$ for the units modulo $m$: these are the numbers mod $m$ with multiplicative inverses. We have $a$ mod $m \in (\mathbb{Z}/m)\times$ if and only if $\gcd(a, m) = 1$. When $m$ is a prime power $p^k$ with $k \geq 1$, the units modulo $p^k$ are all residues mod $p^k$ besides the multiples of $p$, since being relatively prime to $p^k$ is the same as not being divisible by $p$. Therefore

$$|(\mathbb{Z}/p^k)\times| = |\{0, 1, 2, \ldots, p^k - 1\} - \{0, p, 2p, 3p, \ldots, (p^k - 1)p\}| = p^k - p^{k-1} = p^{k-1}(p - 1).$$

A fundamental result in number theory, going back to Gauss, is that the group $(\mathbb{Z}/p)^\times$ is cyclic for every prime $p$: there is an element of $(\mathbb{Z}/p)^\times$ with order $p - 1$. When $p$ is an odd prime, there is a similar result for powers of $p$.

**Theorem 1.1.** For an odd prime $p$ and integer $k \geq 2$, the group $(\mathbb{Z}/p^k)^\times$ is cyclic.

This is false for $2^k$ when $k \geq 3$, e.g. $(\mathbb{Z}/8)^\times = \{1, 3, 5, 7 \mod 8\}$ has order 4 and each unit modulo 8 squares to 1, so no unit modulo 8 has order 4.

A proof that all groups $(\mathbb{Z}/p)^\times$ are cyclic is in Appendix A. Building on that, we will show how to prove Theorem 1.1 using $p$-adic numbers. Then, using $p$-adic numbers in another way, we will apply Theorem 1.1 to compute a bound on the order of finite subgroups of $\text{GL}_n(\mathbb{Q})$.

2. The groups $(\mathbb{Z}/(p^k))^\times$ are cyclic

We will prove Theorem 1.1 by using a Teichmüller representative to lift a generator of $(\mathbb{Z}/p)^\times$ multiplicatively into the $p$-adics.

**Proof.** By Theorem A.6, $(\mathbb{Z}/p)^\times$ is cyclic. Let a generator of it be $g \bmod p$ and let $\omega(g) \in \mathbb{Z}_p$ be the Teichmüller representative for $g$, so $\omega(g)^{p-1} = 1$ and $\omega(g) \equiv g \bmod p$.

Integers modulo $p^k$ and $p$-adic integers modulo $p^k$ amount to the same thing. In the language of algebra, $\mathbb{Z}/p^k$ and $\mathbb{Z}_p/p^k$ are isomorphic rings in a natural way.

We are going to show the product $(1 + p)\omega(g)$ is a generator of $(\mathbb{Z}/p^k)^\times$ for all $k$. That is, if $a$ is an integer such that $a \equiv (1 + p)\omega(g) \bmod p^k$ then $a \bmod p^k$ generates $(\mathbb{Z}/p^k)^\times$.

Since $(\mathbb{Z}/p^k)^\times$ has size $p^{k-1}(p - 1)$, it suffices to prove $((1 + p)\omega(g))^m \equiv 1 \bmod p^k$ only if $m$ is divisible by $p^{k-1}(p - 1)$.

Congruences mod $p^k$ remain valid as congruences mod $p$, so

$$((1 + p)\omega(g))^m \equiv 1 \bmod p^k \implies ((1 + p)\omega(g))^m \equiv 1 \bmod p \implies g^m \equiv 1 \bmod p,$$

so $\frac{(p - 1)}{m}$ since $g \bmod p$ is a generator of $(\mathbb{Z}/p)^\times$. Thus

$$((1 + p)\omega(g))^m = (1 + p)^m \omega(g)^m = (1 + p)^m,$$
where the only units are an actual quotient of multiplicative groups. This can’t be done working in the integers $\mathbb{Z}$. What makes $b$ a generator of $\mathbb{Z}/p\mathbb{Z}$ earlier that $u\omega$ being a generator of $(\mathbb{Z}/p^2)^\times$.

**Corollary 2.1.** If $p$ is an odd prime and $a \pmod{p^2}$ is a generator of $(\mathbb{Z}/p^2)^\times$ then $a \pmod{p^k}$ is a generator of $(\mathbb{Z}/p^k)^\times$ for all $k \geq 2$.

**Proof.** In $\mathbb{Z}_p^\times$ set $a = \omega(a)u$, where $\omega(a)$ is the Teichmuller representative of $a$, so $u \in 1 + p\mathbb{Z}_p$ (since $a \equiv \omega(a) \pmod{p}$).

**Claim:** $\omega(a)$ has order $p - 1$ and $|u - 1|_p = 1/p$ (i.e., $u \in 1 + p\mathbb{Z}_p$ and $u \not\in 1 + p^2\mathbb{Z}_p$).

**Proof of claim:** Let $d \geq 1$ be the order of $a \pmod{p}$, so $d \mid (p - 1)$. We want to prove $d = p - 1$. From $a^d \equiv 1 \pmod{p}$, raising both sides to the $p$th power gives us $a^{dp} \equiv 1 \pmod{p^2}$ with the modulus “improved” to $p^2$. Therefore $p(p - 1) \mid dp$, so $(p - 1) \mid d$. We noted earlier that $d \mid (p - 1)$ too, so $d = p - 1$. The order of $a \pmod{p}$ and $\omega(a)$ are the same, so $\omega(a)$ has order $p - 1$.

Since $|u - 1|_p \leq 1/p$, if $|u - 1|_p \neq 1/p$ then $|u - 1|_p \leq 1/p^2$, so $u \equiv 1 \pmod{p^2}$. Then $a = \omega(a)u \equiv \omega(a) \pmod{p^2}$, so $a^{p-1} \equiv \omega(a)^{p-1} \equiv 1 \pmod{p^2}$, which contradicts $a \pmod{p^2}$ being a generator of $(\mathbb{Z}/p^2)^\times$. Thus $|u - 1|_p = 1/p$. This finishes the proof of the claim.

When we proved in Theorem 1.1 that $(1 + p)\omega(g) \pmod{p^k}$ has order $(p - 1)p^{k-1}$, the properties we used about $g$ and $1 + p$ were that $g \pmod{p}$ has order $p - 1$ and $|(1 + p) - 1|_p = 1/p$. Since $\omega(a)$ has order $p - 1$ and $|u - 1|_p = 1/p$, the arguments used for $(1 + p)\omega(g)$ can be applied word for word to $u\omega(a) = a$, so $a \pmod{p^k}$ generates $(\mathbb{Z}/p^k)^\times$ for all $k \geq 2$. 

**Remark 2.2.** Here is a more conceptual description of what is going on in terms of $p$-adic quotient groups. We can view $(\mathbb{Z}_p/p^k)^\times$ as an isomorphic group built from $p$-adic units:

$$(\mathbb{Z}/p^k)^\times \cong (\mathbb{Z}_p/p^k)^\times \cong \mathbb{Z}_p^\times/(1 + p^k\mathbb{Z}_p).$$

The second isomorphism arises because elements of $(\mathbb{Z}_p/p^k)^\times$ are represented by $p$-adic units, and when $u$ and $v$ are $p$-adic units we have

$$u = v \text{ in } \mathbb{Z}_p/p^k \iff u \equiv v \pmod{p^k} \iff \frac{u}{v} \equiv 1 \pmod{1 + p^k\mathbb{Z}_p} \iff u = v \text{ in } \mathbb{Z}_p^\times/(1 + p^k\mathbb{Z}_p).$$

What makes $\mathbb{Z}_p^\times/(1 + p^k\mathbb{Z}_p)$ a nice model for the multiplicative group $(\mathbb{Z}/p^k)^\times$ is that it is an actual quotient of multiplicative groups. This can’t be done working in the integers alone, where the only units are $\pm1$.

Writing $a = \omega(a)u$ provides a direct product decomposition $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, where $\mu_{p-1}$ is the (cyclic) group of $(p - 1)$th roots of unity in the $p$-adic integers. Thus

$$\mathbb{Z}_p^\times/(1 + p^k\mathbb{Z}_p) \cong (\mu_{p-1} \times (1 + p\mathbb{Z}_p))/(1 + p^k\mathbb{Z}_p) \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)/(1 + p^k\mathbb{Z}_p).$$

---

1 In general for $x$ and $y$ in $\mathbb{Z}_p$, if $x \equiv y \pmod{p}$ then $x^p \equiv y^p \pmod{p^2}$. More generally, if $x \equiv y \pmod{p^k}$ then $x^p \equiv y^p \pmod{p^{k+1}}$. 

---
Therefore so the direct product is also cyclic.

2. Proof.

For Theorem 2.3.

This is a direct product of cyclic groups of orders $p$ and $k$.

We can figure out what the multiplicative quotient group $(1 + p\mathbb{Z}_p)/(1 + p^k\mathbb{Z}_p)$ looks like concretely by using the $p$-adic logarithm to turn it into an additive quotient group. Since $p \neq 2$, the function $\log: 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$ is an isomorphism, and since the $p$-adic logarithm is an isometry we get $\log(1 + p^k\mathbb{Z}_p) = p^k\mathbb{Z}_p$. Thus

$$(1 + p\mathbb{Z}_p)/(1 + p^k\mathbb{Z}_p) \cong p\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}_p/p^k-1 \cong \mathbb{Z}/p^k-1 = \text{cyclic group of order } p^k-1.$$ 

Therefore

$$(\mathbb{Z}/p^k)^\times \cong \mathbb{Z}^\times_p/(1 + p^k\mathbb{Z}_p) \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)/(1 + p^k\mathbb{Z}_p) \cong \mathbb{Z}/(p - 1) \times \mathbb{Z}/p^k-1.$$ 

This is a direct product of cyclic groups of orders $p - 1$ and $p^k - 1$, which are relatively prime, so the direct product is also cyclic.

The structure of the group $(\mathbb{Z}/2^k)^\times$ can be studied similarly to the case of odd $p$, but for $k \geq 3$ these groups will turn out not to be cyclic. They are almost cyclic: there is a cyclic subgroup of order equal to half the size of the group.

Theorem 2.3. For $k \geq 3$, $(\mathbb{Z}/2^k)^\times = (-1, 5 \mod 2^k) = \{\pm 5^j \mod 2^k : j \geq 0\}$.

Proof. The group $(\mathbb{Z}/2^k)^\times$ has order $2^k - 1 = 2^k - 1$. We will show $5 \mod 2^k$ has order $2^k - 2$. For $m \in \mathbb{Z}^+$ and $b \in 1 + 4\mathbb{Z}_2$ we have $|b^m - 1|_2 = |m|_2|b - 1|_2$: see Appendix B. Therefore

$$5^m \equiv 1 \mod 2^k \iff |5^m - 1|_2 \leq \frac{1}{2^k} \iff |m|_2|5 - 1|_2 \leq \frac{1}{2^k} \iff |m|_2 \leq \frac{1}{2^k - 2} \iff 2^k - 2 \mid m,$$

so $5 \mod 2^k$ has order $2^k - 2$. No power of $5 \mod 2^k$ is ever $-1 \mod 2^k$ since $5 \equiv 1 \mod 4$. Therefore $-1 \mod 2^k \notin \langle 5 \mod 2^k \rangle$, and since $-1 \mod 2^k$ has order 2 the subgroup $\{\pm 5^j \mod 2^k : j \geq 0\}$ of $(\mathbb{Z}/2^k)^\times$ has order $2 \cdot 2^k - 2 = 2^k - 1 = |(\mathbb{Z}/2^k)^\times|$, which makes this subgroup equal to the whole group.

Remark 2.4. We can explain the group structure of $(\mathbb{Z}/2^k)^\times$ by writing it as a quotient group of $\mathbb{Z}_2^\times$. Since $\mathbb{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$, for $k \geq 2$ we have

$$(\mathbb{Z}/2^k)^\times \cong (\mathbb{Z}_2^\times/2^k)^\times \cong \mathbb{Z}_2^\times/(1 + 2^k\mathbb{Z}_2) \cong \langle \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 2^k\mathbb{Z}_2) \rangle = \langle \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 2^k\mathbb{Z}_2) \rangle.$$ 

Using the 2-adic logarithm isomorphism $1 + 4\mathbb{Z}_2 \cong 4\mathbb{Z}_2$, which is also an isometry, we get

$$(1 + 4\mathbb{Z}_2)/(1 + 2^k\mathbb{Z}_2) \cong 4\mathbb{Z}_2/2^k\mathbb{Z}_2 \cong \mathbb{Z}_2/2^k-2 \cong \mathbb{Z}/2^k-2,$$

so $(\mathbb{Z}/2^k)^\times \cong \{\pm 1\} \times \mathbb{Z}/2^k-2$.

3. Bounding finite subgroups of $\text{GL}_n(\mathbb{Q})$

How large can a finite group of matrices be? If we allow matrix entries from the complex numbers, or even the real numbers, then there is no upper bound in general. For example, if $d$ is a positive integer then a counterclockwise rotation by $2\pi/d$ radians in the plane $\mathbb{R}^2$ is represented by the matrix

$$
\begin{pmatrix}
\cos(2\pi/d) & -\sin(2\pi/d) \\
\sin(2\pi/d) & \cos(2\pi/d)
\end{pmatrix}
$$
in \( \text{GL}_2(\mathbb{R}) \) that has order \( d \), so \( \text{GL}_2(\mathbb{R}) \) contains finite subgroups of arbitrarily large order.

If we restrict the numbers in the matrices to be rational, however, then there is an upper bound on how large a finite matrix group can be in terms of the size of the matrices. This result is due to Minkowski [4]. Our argument is adapted from [2, Chap. 4, Sect. 2].

**Theorem 3.1** (Minkowski, 1887). For each \( n \geq 1 \) every finite subgroup of \( \text{GL}_n(\mathbb{Q}) \) has order dividing a number \( M(n) \) that depends only on \( n \).

For example, it turns out that \( M(2) = 24 \), so every finite subgroup of \( \text{GL}_2(\mathbb{Q}) \) has order dividing \( 24 = 2^3 \cdot 3 \). We are not claiming that there actually is a subgroup of \( \text{GL}_2(\mathbb{Q}) \) with order 24. In fact the largest size is 12, but there are subgroups of order not dividing 12 and those orders all divide 24 (see below for a subgroup of order 8).

**Example 3.2.** The matrix \( \left( \begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right) \) has order 6.

**Example 3.3.** Let \( r = \left( \begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right) \) and \( s = \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) \). Then \( r \) has order 4, \( s \) has order 2, and \( sr = r^{-1}s \), so the group \( \langle r, s \rangle \) generated by \( r \) and \( s \) in \( \text{GL}_2(\mathbb{Q}) \) has order 8.

The proof of Theorem 3.1 will use the finite groups \( \text{GL}_n(\mathbb{Z}/p) \). Just as the symmetric group \( S_n \) has order \( n! \) that is a product of \( n \) integers, the order of \( \text{GL}_n(\mathbb{Z}/p) \) has an explicit formula that is a product of \( n \) terms.

**Lemma 3.4.** For each prime \( p \), \( | \text{GL}_n(\mathbb{Z}/p) | = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \).

**Proof.** See Appendix C. The proof is based on linear algebra over the field \( \mathbb{Z}/p \).

Now we prove Theorem 3.1.

**Proof.** Let \( G \) be a finite subgroup of \( \text{GL}_n(\mathbb{Q}) \). Since \( G \) contains only finitely many matrices, and each rational number is in \( \mathbb{Z}/p \) for all large primes \( p \), the matrices in \( G \) have entries in \( \mathbb{Z}/p \) for all large \( p \), so there is a prime \( p_0 \) such that \( G \subseteq M_n(\mathbb{Z}_{p_0}) \) for all \( p > p_0 \). We write \( \text{GL}_n(\mathbb{Z}_{p_0}) \) for the group of \( n \times n \) matrices with \( \mathbb{Z}_{p_0} \)-entries that have inverses also with \( \mathbb{Z}_{p_0} \)-entries; the condition for a matrix \( A \in M_n(\mathbb{Z}_{p_0}) \) to belong to \( \text{GL}_n(\mathbb{Z}_{p_0}) \) is that \( \det A \in \mathbb{Z}_{p_0}^\times \). If \( A \in \text{GL}_n(\mathbb{Q}) \) has finite order then \( \det A \in \mathbb{Q}^\times \) has finite order, so \( \det A = \pm 1 \). Therefore by Cramer’s rule for inverting matrices, \( G \subseteq \text{GL}_n(\mathbb{Z}_{p_0}) \) for all \( p > p_0 \).

**Claim:** For every prime \( p > p_0 \), the order of \( G \) divides \( | \text{GL}_n(\mathbb{Z}/p) | \).

**Proof of claim:** We can view \( G \) inside \( \text{GL}_n(\mathbb{Z}_{p_0}) \). Reducing matrix entries modulo \( p \) sends each matrix \( A \) in \( \text{GL}_n(\mathbb{Z}_{p_0}) \) to a matrix \( \overline{A} \) in \( \text{GL}_n(\mathbb{Z}/p) \), which can be regarded as \( \text{GL}_n(\mathbb{Z}/p) \) by the natural identification of \( \mathbb{Z}_{p_0}/p \) with \( \mathbb{Z}/p \). (We have \( \overline{A} \in \text{GL}_n(\mathbb{Z}/p) \) since \( \det A \equiv \pm 1 \implies \det A \equiv 0 \mod p \implies \det \overline{A} \equiv 0 \in \mathbb{Z}/p \).) Reduction \( \text{GL}_n(\mathbb{Z}_{p_0}) \to \text{GL}_n(\mathbb{Z}/p) \) is a group homomorphism.

The key point is that when \( p > p_0 \), two matrices \( A \) and \( B \) in the finite group \( G \) can’t reduce \( \mod p \) to the same matrix in \( \text{GL}_n(\mathbb{Z}/p) \). Indeed, suppose \( A \equiv B \mod p \). Then \( AB^{-1} \) belongs to \( G \), so it has finite order, and \( AB^{-1} \equiv I_n \mod p \). We will show \( AB^{-1} = I_n \), so \( A = B \), by using a norm on \( p \)-adic matrices.

For each \( n \times n \) matrix \( X = (x_{ij}) \) in \( M_n(\mathbb{Q}_p) \), define its \( p \)-adic matrix norm to be the maximum \( p \)-adic absolute value of the entries:

\[ ||X||_p := \max_{i,j} |x_{ij}|_p. \]

Thus \( M_n(\mathbb{Z}_p) = \{ X \in M_n(\mathbb{Q}_p) : ||X||_p \leq 1 \} \). Check that (i) \( ||X+Y||_p \leq \max(||X||_p, ||Y||_p) \), (ii) \( ||XY||_p \leq ||X||_p ||Y||_p \), and (iii) \( ||aX||_p = ||a||_p ||X||_p \) for \( a \) in \( \mathbb{Q}_p \) and \( p \)-adic matrices \( X \).
From the equivalence of the first and third relations in (3.2) we can start counting. For prime \( p \) that makes \( p > p_0 \) (so \( p > 2 \)), we have

\[
AB^{-1} \equiv I_n \mod p \implies AB^{-1} \in I_n + pM_n(Z_p) \implies ||(AB^{-1})^m - I_n||_p = |m|_p||AB^{-1} - I_n||_p
\]

for all \( m \geq 1 \). In the last equation, let \( m \) be the (finite!) order of \( AB^{-1} \) in \( G \) to see that \( 0 = |m|_p||AB^{-1} - I_n||_p \). Thus \( ||AB^{-1} - I_n||_p = 0 \), so \( AB^{-1} - I_n = O \), from which we get \( A = B \).

We have shown the reduction mod \( p \) homomorphism \( G \to GL_n(Z_p/p) \) is injective for \( p > p_0 \), so \( |G| \) divides the order of \( GL_n(Z_p/p) \cong GL_n(Z/p) \). This completes the proof of the claim.

The order of \( GL_n(Z/p) \) in Lemma 3.4 can be rewritten by factoring out the largest power of \( p \):

\[
(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = (p^n - 1)p(p^{n-1} - 1) \cdots p^{n-1}(p - 1) \]
\[
= p^{1+\cdots+n-1}(p - 1)(p^{n-1} - 1) \cdots (p - 1) \]
\[
= p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1). \tag{3.1}
\]

To bound \( |G| \), pick a prime \( q \). We will get an upper bound \( e_n(q) \) for \( \text{ord}_q(|G|) \) and find \( e_n(q) = 0 \) if \( q > n + 1 \), so \( |G| \) divides \( \prod_{q \leq n+1} q^{e_n(q)} \), where the product runs over primes less than or equal to \( n + 1 \). (Recall the examples of finite subgroups of \( GL_2(Q) \) earlier had order divisible only 2 and 3, which are less than or equal to \( n + 1 = 3 \) in this case.)

For prime \( p > p_0 \), \( \text{ord}_q(|G|) \leq \text{ord}_q(|GL_n(Z/p)|) \). If \( p \neq q \) then by (3.1)

\[
\text{ord}_q(|GL_n(Z/p)|) \leq \text{ord}_q((p^n - 1)(p^{n-1} - 1) \cdots (p - 1)) = \sum_{i=1}^{n-1} \text{ord}_q(p^i - 1).
\]

We will choose for \( p \) a large prime different from \( q \) that makes \( \text{ord}_q(p^i - 1) \) easy to calculate.

If \( q \neq 2 \) then \((Z/q^k)^{\times}\) is cyclic for all \( k \geq 1 \). An integer that is a generator of \((Z/q^2)^{\times}\) is also a generator of \((Z/q^k)^{\times}\) for all \( k \geq 1 \) by Corollary 2.1. Let \( b \) mod \( q^2 \) generate \((Z/q^2)^{\times}\), so \( (b, q^2) = 1 \). We will now use a famous theorem of Dirichlet about primes in arithmetic progression: if \( a \) and \( m \) are relatively prime integers then there are infinitely many primes \( p \equiv a \mod m \).

By Dirichlet’s theorem, there are infinitely many primes \( p \equiv b \mod q^2 \). Choose such a prime \( p \) with \( p > p_0 \). Necessarily \( p \neq q \) since \((p, q^2) = (b, q^2) = 1 \). The number \( \text{ord}_q(p^i - 1) \) is the largest integer \( k \) that makes \( q^k \mid (p^i - 1) \), or equivalently that makes \( p^i \equiv 1 \mod q^k \). Since \( p \) mod \( q^k \) generates \((Z/q^k)^{\times}\),

\[
q^k \mid (p^i - 1) \iff p^i \equiv 1 \mod q^k \iff q^{k-1}(q - 1) \mid i. \tag{3.2}
\]

From the equivalence of the first and third relations in (3.2) we can start counting.

- The number of \( p^i - 1 \) with \( 1 \leq i \leq n \) that are divisible by \( q \) is the number of multiples of \( q - 1 \) up to \( n \), and that number is \( n/(q - 1) \).
• The number of $p^i - 1$ with $1 \leq i \leq n$ that are divisible by $q^2$ is the number of multiples of $q(q-1)$ up to $n$, and that number is $\lfloor n/(q(q-1)) \rfloor$.

• The number of $p^i - 1$ with $1 \leq i \leq n$ that are divisible by $q^3$ is the number of multiples of $q^2(q-1)$ up to $n$, and that number is $\lfloor n/(q^2(q-1)) \rfloor$.

• For each $k \geq 1$, the number of $p^i - 1$ with $1 \leq i \leq n$ that are divisible by $q^k$ is the number of multiples of $q^{k-1}(q-1)$ up to $n$, and that number is $\lfloor n/(q^{k-1}(q-1)) \rfloor$.

Putting this all together, the multiplicity of the prime $q$ in $|GL_n(\mathbb{Z}/p)|$, if $p \mod q^2$ generates $(\mathbb{Z}/q^2)^\times$, is

$$e_n(q) := \left\lfloor \frac{n}{q-1} \right\rfloor + \left\lfloor \frac{n}{q(q-1)} \right\rfloor + \left\lfloor \frac{n}{q^2(q-1)} \right\rfloor + \cdots + \sum_{j \geq 0} \left\lfloor \frac{n}{q^j(q-1)} \right\rfloor.$$  \hfill (3.3)

This formally infinite series is really finite because the $j$-th term is 0 once $q^j(q-1) > n$. In particular, if $q > n+1$ then $q - 1 > n$ and all terms in the sum vanish. Thus $q$ does not divide $|G|$ if $q > n + 1$, so the only possible odd prime factors of $|G|$ are primes up to $n+1$, and the highest power of $q$ dividing $|G|$ is at most $q^{e_n(q)}$.

When $q = 2$ a similar analysis can be made with Dirichlet’s theorem for modulus 8 (not for modulus 4 = 2, as the case of odd $q$ might suggest), although it is a bit more complicated because the groups $(\mathbb{Z}/2^k)^\times$ for $k \geq 3$ are not cyclic but only “half-cyclic”: there’s a cyclic subgroup filling up half the group. The result, whose details we omit (see [5, Sect. 1.3.4]), is that ord$_2(|G|)$ is bounded above by the same formula as (3.3) when $q = 2$, that is, by the sum

$$e_n(2) := \sum_{j \geq 0} \left\lfloor \frac{n}{2^j} \right\rfloor,

Putting everything together, each finite subgroup of $GL_n(\mathbb{Q})$ divides the integer

$$M(n) = \prod_q q^{e_n(q)} = \prod_{q \leq n+1} q^{e_n(q)}$$

where $e_n(q)$ is given by (3.3) for all primes $q$. The table below gives some sample values.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$M(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
</tr>
<tr>
<td>4</td>
<td>5760</td>
</tr>
<tr>
<td>5</td>
<td>11520</td>
</tr>
<tr>
<td>6</td>
<td>2903040</td>
</tr>
<tr>
<td>7</td>
<td>5806080</td>
</tr>
</tbody>
</table>

For each prime $q$ the exponent $e_n(q)$ in $M(n)$ is optimal in the sense that there does exist a subgroup of $GL_n(\mathbb{Q})$ of order $q^{e_n(q)}$ [1, pp. 392-394], [5, Sect. 1.4].

**Remark 3.5.** The largest possible order of a finite subgroup of $GL_n(\mathbb{Q})$ is $2^n n!$ except when $n = 2, 4, 6, 7, 8, 9,$ and 10, and for every $n$ (no exceptions) the subgroups of $GL_n(\mathbb{Q})$ with maximal order are conjugate. See [3].

**Appendix A. Cyclicity of $(\mathbb{Z}/p)^\times$**

To prove $(\mathbb{Z}/p)^\times$ is cyclic for each prime $p$, we can suppose $p > 2$. We are going to use the prime factorization of $p - 1$. Say

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m},$$

where the $q_i$ are distinct primes and $e_i \geq 1$. We will show $(\mathbb{Z}/p)^\times$ has elements of order $q_i^{e_i}$ for each $i$ and their product furnishes a generator of $(\mathbb{Z}/p)^\times$.
As a warm-up, let’s show for each prime \( q \) dividing \( p - 1 \) that there is an element of order \( q \) in \( (\mathbb{Z}/p)\times \). While this a consequence of Cauchy’s theorem for all finite groups, abelian or nonabelian, we want to give a proof that uses a special feature of \( (\mathbb{Z}/p)\times \): it is the nonzero elements of the field \( \mathbb{Z}/p \).

**Lemma A.1.** If \( q \) is a prime dividing \( p - 1 \) then there is an element of \( (\mathbb{Z}/p)\times \) with order \( q \). Specifically, there is an \( a \in (\mathbb{Z}/p)\times \) such that \( a^{(p-1)/q} \neq 1 \), and necessarily \( a^{(p-1)/q} \) has order \( q \) in \( (\mathbb{Z}/p)\times \).

**Proof.** The polynomial equation \( a^{(p-1)/q} = 1 \) in \( \mathbb{Z}/p \) has at most \( (p-1)/q \) solutions in \( \mathbb{Z}/p \) since \( \mathbb{Z}/p \) is a field, and \( (p-1)/q \) is less than \( p-1 = |(\mathbb{Z}/p)\times| \). Therefore \( (\mathbb{Z}/p)\times \) has an element \( a \) such that \( a^{(p-1)/q} \neq 1 \).

Set \( b = a^{(p-1)/q} \) in \( \mathbb{Z}/p \). Then \( b \neq 1 \) and \( b^q = (a^{(p-1)/q})^q = a^{p-1} = 1 \) in \( (\mathbb{Z}/p)\times \) by Fermat’s little theorem, so the order of \( b \) mod \( p \) divides \( q \) and is not 1. Since \( q \) is prime, the only choice for the order of \( b \) mod \( p \) is \( q \).

That proof is not saying that if \( a^{(p-1)/q} \neq 1 \) in \( \mathbb{Z}/p \) then \( a \) mod \( p \) has order \( q \). It is saying that a power of the form \( a^{(p-1)/q} \) mod \( p \) has order \( q \) if the power is not 1 (or 0).

**Example A.2.** Take \( p = 19 \). By Fermat’s little theorem, all \( a \) in \( \mathbb{Z}/19\times \) satisfy \( a^{18} = 1 \). Since 18 is divisible by 3, the lemma is telling us that whenever \( a^{18k}/3 \neq 1 \), \( a^{18k}/3 \) has order 3. From the second row of the table below, which runs over the nonzero numbers mod 19, we find 2 different values of \( a^6 \) mod 19 other than 1: 7 and 11. They both have order 3.

<table>
<thead>
<tr>
<th>( a ) mod 19</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a^6 ) mod 19</td>
<td>1</td>
<td>7</td>
<td>7</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

If a prime \( q \) divides \( p - 1 \) more than once, then the same reasoning as in Lemma A.1 leads to elements of higher \( q \)-power order in \( (\mathbb{Z}/p)\times \).

**Lemma A.3.** If \( q \) is a prime and \( q^e \mid (p-1) \) for a positive integer \( e \), then there is an element of \( (\mathbb{Z}/p)\times \) with order \( q^e \). Specifically, there is an \( a \in (\mathbb{Z}/p)\times \) such that \( a^{(p-1)/q^e} \neq 1 \) in \( (\mathbb{Z}/p)\times \), and necessarily \( a^{(p-1)/q^e} \) has order \( q^e \) in \( (\mathbb{Z}/p)\times \).

**Proof.** As in the proof of Lemma A.1, there are fewer than \( p-1 \) solutions to \( a^{(p-1)/q^e} = 1 \) in \( \mathbb{Z}/p \) since \( \mathbb{Z}/p \) is a field, so there is an \( a \) in \( (\mathbb{Z}/p)\times \) where \( a^{(p-1)/q^e} \neq 1 \) in \( \mathbb{Z}/p \).

Set \( b = a^{(p-1)/q^e} \) in \( \mathbb{Z}/p \), which makes sense since \( q^e \) is a factor of \( p-1 \) (we are not using fractional exponents). Then \( b^q^e = (a^{(p-1)/q^e})^q^e = a^{p-1} = 1 \) in \( (\mathbb{Z}/p)\times \) by Fermat’s little theorem, so the order of \( b \) mod \( p \) divides \( q^e \). Since \( q \) is prime, the (positive) factors of \( q^e \) other than \( q^e \) are factors of \( q^{e-1} \). Since \( b^{q^{e-1}} = (a^{(p-1)/q^e})^{q^{e-1}} = a^{(p-1)/q^e} \neq 1 \) in \( (\mathbb{Z}/p)\times \), by the choice of \( a \), the order of \( b \) mod \( p \) does not divide \( q^{e-1} \). Thus the order of \( b \) in \( (\mathbb{Z}/p)\times \) must be \( q^e \).

**Example A.4.** Returning to \( p = 19 \), the number \( p-1 = 18 \) is divisible by the prime power 9. In the table below we list the \( a \) for which \( a^{(p-1)/3} = a^6 \neq 1 \) and below that list the corresponding values of \( a^{18/9} = a^2 \): these are 4, 5, 6, 9, 16, and 17, and all have order 9.

<table>
<thead>
<tr>
<th>( a ) mod 19</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a^6 ) mod 19</td>
<td>7</td>
<td>7</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>( a^2 ) mod 19</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>6</td>
<td>17</td>
<td>5</td>
<td>17</td>
<td>6</td>
<td>16</td>
<td>9</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**Remark A.5.** Lemma A.3 can be proved in another way using unique factorization of polynomials with coefficients in \( \mathbb{Z}/p \). Because all nonzero numbers mod \( p \) are roots of
Proof. We will present the case $q = p$ of the $q^i$ are such

Proof. We may take $a$ since a nonzero polynomial over a field has no more roots than its degree. Therefore there is an $a$ in $\mathbb{Z}/p$ fitting $a^{q^e} = 1$ and $a^{q^e - 1} \neq 1$. All such $a$ have order $q^e$.

**Theorem A.6.** For each prime $p$, the group $(\mathbb{Z}/p)^\times$ is cyclic.

*Proof.* We may take $p > 2$, so $p - 1 > 1$. Write $p - 1$ as a product of primes:

$$p - 1 = q_1^{e_1}q_2^{e_2} \cdots q_m^{e_m}.$$ 

By Lemma A.3, for each $i$ from 1 to $m$ there is $b_i \in (\mathbb{Z}/p)^\times$ with order $q_i^{e_i}$. These orders are relatively prime, and $(\mathbb{Z}/p)^\times$ is abelian, so the product of the $b_i$’s has order equal to the product of the $q_i^{e_i}$’s, which is $p - 1$. Thus, $b_1b_2 \cdots b_m$ generates $(\mathbb{Z}/p)^\times$. \hfill $\Box$

**Appendix B. Computing $|b^m - 1|_p$ and $||B^m - I_n||_p$**

The two theorems we prove here were used in the proofs of Theorems 1.1, 2.3, and 3.1.

**Theorem B.1.** Let $p$ be prime. When $p > 2$ and $b \in 1 + p\mathbb{Z}_p$,

$$|b^m - 1|_p = |m|_p |b - 1|_p$$

for $m \geq 1$. When $p = 2$ and $b \in 1 + 4\mathbb{Z}_2$, $|b^m - 1|_2 = |m|_2 |b - 1|_2$ for $m \geq 1$.

*Proof.* We will present the case $p > 2$ and leave the case $p = 2$ to the reader.

Check the identity for general $m \geq 1$ follows from the cases $(p, m) = 1$ and $m = p$:

$$(p, m) = 1 \implies |b^m - 1|_p = |b - 1|_p, \quad \text{and} \quad |b^p - 1|_p = \frac{1}{p} |b - 1|_p.$$ 

**Case 1:** $(p, m) = 1$.

To prove $|b^m - 1|_p = |b - 1|_p$, we can assume $b \neq 1$ and $m \geq 2$ since it is obvious when $b = 1$ or $m = 1$. Set $c = b - 1$, so

$$b^m - 1 = (1 + c)^m - 1 = mc + \sum_{k=2}^{m} \binom{m}{k} c^k.$$ 

We have $|mc|_p = |c|_p = |b - 1|_p$. Since $0 < |c|_p \leq 1/p$, $| \sum_{k=2}^{m} \binom{m}{k} c^k |_p \leq \max_{2 \leq k \leq m} |c|_p^k = |c|_p^2 < |c|_p = |b - 1|_p$ (the last inequality would not be correct if $c = 0$). Thus

$$|b^m - 1|_p = |b - 1|_p.$$ 

**Case 2:** $m = p$.

To prove $|b^p - 1|_p = (1/p) |b - 1|_p$, as in Case 1 we can assume $b \neq 1$. Set $c = b - 1$, so

$$b^p - 1 = (1 + c)^p - 1 = pc + \sum_{k=2}^{p} \binom{p}{k} c^k.$$ 

We have $|pc|_p = (1/p) |c|_p = (1/p) |b - 1|_p$. Since $0 < |c|_p \leq 1/p$, if $2 \leq k \leq p - 1$ (there are such $k$ since $p > 2$), then $p \mid \binom{p}{k}$, so $|\binom{p}{k} c^k|_p \leq (1/p) |c|_p^k \leq (1/p) c^2 \leq (1/p) |c|_p = (1/p) |b - 1|_p$. Also $|\binom{p}{k} c^p|_p = |c|_p^p \leq |c|_p^3 \leq (1/p) |c|^2_2 < (1/p) |c|_p = (1/p) |b - 1|_p$, so

$$|b^p - 1|_p = \frac{1}{p} |b - 1|_p.$$ 

$\Box$
Theorem B.2. Let \( p \) be prime. When \( p > 2 \) and \( B \in 1 + p M_n(\mathbb{Z}_p) \)

\[ ||B^m - I_n||_p = |m|_p ||B - I_n||_p \]

for \( m \geq 1 \). When \( p = 2 \) and \( B \in 1 + 4 M_n(\mathbb{Z}_2) \), \( ||B^m - I_n||_2 = |m|_2 ||B - I_n||_2 \) for \( m \geq 1 \).

When this was used in the proof of Theorem 3.1, we did not need the case \( p = 2 \).

Proof. It is left to the reader to check the proof of Theorem B.1 still works in the matrix setting, using \( ||XY||_p \leq ||X||_p ||Y||_p \) with \( p \)-adic matrices instead of \( |xy|_p = |x|_p |y|_p \) with \( p \)-adic numbers and using \( ||aX||_p = |a|_p ||X|| \) for \( p \)-adic scalars \( a \) and matrices \( X \). Even though matrix multiplication is not usually commutative, we can use the binomial theorem to expand \( (I_n + B)^m \) just as with \((1 + b)^n\) since \( I_n \) and \( B \) commute. \( \square \)

Appendix C. The Order of \( \text{GL}_n(\mathbb{Z}/p) \)

To compute \( |\text{GL}_n(\mathbb{Z}/p)| \) in Lemma 3.4, view the columns of a matrix in \( M_n(\mathbb{Z}/p) \) as an ordered list of \( n \) elements of \((\mathbb{Z}/p)^n\). The matrix is invertible if and only if the columns are a basis of \((\mathbb{Z}/p)^n\). In an \( n \)-dimensional vector space, \( n \) vectors are a basis if and only if they are linearly independent, so count how many ordered lists of \( n \) vectors in \((\mathbb{Z}/p)^n\) are linearly independent. Every set of linearly independent vectors in \((\mathbb{Z}/p)^n\) can be extended to a basis, so we can build up elements of \( \text{GL}_n(\mathbb{Z}/p) \) column by column.

1. The first column can be anything in \((\mathbb{Z}/p)^n\) but the zero vector, since every nonzero vector can be extended to a basis. Therefore the first column has \( p^n - 1 \) choices.

2. Having picked the first column, the second column can be an arbitrary vector in \((\mathbb{Z}/p)^n\) that is linearly independent of the first column: such a choice makes the first two columns linearly independent and every pair of linearly independent vectors in \((\mathbb{Z}/p)^n\) can be extended to a basis (if \( n \geq 2 \)). Since the first column has \( p \) scalar multiples, the second column has \( p^n - p \) choices.

3. The third column (if \( n \geq 3 \)) has to be chosen linearly independently of the first two, which span a 2-dimensional subspace of \((\mathbb{Z}/p)^n\), so the third column has \( p^n - p^2 \) choices and every such choice is allowed since a set of 3 linearly independent vectors in \((\mathbb{Z}/p)^n\) can be extended to a basis (if \( n \geq 3 \)).

The process continues, with the \( j \)th column being anything outside the span of the first \( j - 1 \) columns, so the \( j \)th column has \( p^n - p^{j-1} \) choices. We are done when \( j = n \), so

\[ |\text{GL}_n(\mathbb{Z}/p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}). \]

References


