PRIME POWERS UNITS AND FINITE SUBGROUPS OF $\mathrm{GL}_n(\mathbf{Q})$

KEITH CONRAD

1. Introduction

For an integer $m \geq 2$, write $(\mathbf{Z}/m)^\times$ for the units modulo m: these are the numbers mod m with multiplicative inverses. We have $a \bmod m \in (\mathbf{Z}/m)^\times$ 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

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

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

Theorem 1. *For an odd prime p and integer $k \geq 2$, the group $(\mathbf{Z}/p^k)^\times$ is cyclic.*

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

We will not discuss here a proof that the groups $(\mathbf{Z}/p)^\times$ are cyclic, but building on that we will show how to prove Theorem 1 using p-adic numbers. Then, using p-adic numbers in another way, we will apply Theorem 1 to compute a bound on the order of finite subgroups of $\mathrm{GL}_n(\mathbf{Q})$.

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

We will prove Theorem 1 using a Teichmüller representative to lift a generator of $\mathbf{Z}/p$ into the p-adics.

Proof. We are taking for granted that $(\mathbf{Z}/p)^\times$ is cyclic, so it has a generator $g \bmod p$. Let $\omega(g) \in \mathbf{Z}_p^\times$ be the Teichmuller representative for g, so $\omega(g)^{p-1} = 1$ and $\boxed{\omega(g) \equiv g \bmod p}$.

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

We are going to show the product $(1 + p)\omega(g)$ is a generator of $(\mathbf{Z}/p^k)^\times$ 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 $(\mathbf{Z}/p^k)^\times$.

Since $(\mathbf{Z}/p^k)^\times$ 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

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

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

$$((1 + p)\omega(g))^m = (1 + p)^m \omega(g)^m = (1 + p)^m,$$

so

$$((1+p)\omega(g))^m \equiv 1 \bmod p^k \Longrightarrow (1+p)^m \equiv 1 \bmod p^k \Longrightarrow |(1+p)^m - 1|_p \leq \frac{1}{p^k}.$$

For every positive integer m and $b \in 1 + p\mathbf{Z}_p$, we have $|b^m - 1|_p = |m|_p|b-1|_p$ (this needs $p \neq 2$). Taking $b = 1+p$,

$$|(1+p)^m - 1|_p = |m|_p|(1+p)-1|_p = \frac{|m|_p}{p}.$$

Therefore $|(1+p)^m - 1|_p \leq 1/p^k \Longrightarrow |m|_p/p \leq 1/p^k \Longrightarrow |m|_p \leq 1/p^{k-1} \Longrightarrow \boxed{p^{k-1} \mid m}$.

From $(p-1) \mid m$ and $p^{k-1} \mid m$ we get $p^{k-1}(p-1) \mid m$ since $p-1$ and p^{k-1} are relatively prime. That completes the proof. □

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

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

Claim: $\omega(a)$ has order $p-1$ and $|u-1|_p = 1/p$ (*i.e.*, $u \in 1+p\mathbf{Z}_p$ and $u \notin 1+p^2\mathbf{Z}_p$).

Proof of claim: Let $d \geq 1$ be the order of $a \bmod p$, so $d \mid (p-1)$. We want to prove $d = p-1$. From $a^d \equiv 1 \bmod p$, raising both sides to the pth power gives us $a^{dp} \equiv 1 \bmod p^2$ with the modulus "improved" to p^2.[1] 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 $a \bmod p$ 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 $u \equiv 1 \bmod p^2$. Then $a = \omega(a)u \equiv \omega(a) \bmod p^2$, so $a^{p-1} \equiv \omega(a)^{p-1} \equiv 1 \bmod p^2$, which contradicts $a \bmod p^2$ being a generator of $(\mathbf{Z}/p^2)^\times$. Thus $|u-1|_p = 1/p$. This finishes the proof of the claim.

When we proved in Theorem 1 that $(1+p)\omega(g) \bmod p^k$ has order $(p-1)p^{k-1}$, the properties we used about g and $1+p$ were that $g \bmod p$ 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 $a \bmod p^k$ generates $(\mathbf{Z}/p^k)^\times$ for all $k \geq 2$. □

Remark 3. Here is a more conceptual description of what is going on in terms of p-adic quotient groups. We can view $(\mathbf{Z}_p/p^k)^\times$ as an isomorphic group built from p-adic units:

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

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

$$u = v \text{ in } \mathbf{Z}_p/p^k \Longleftrightarrow u \in v + p^k\mathbf{Z}_p \Longleftrightarrow \frac{u}{v} \in 1 + p^k\mathbf{Z}_p \Longleftrightarrow u = v \text{ in } \mathbf{Z}_p^\times/(1+p^k\mathbf{Z}_p).$$

What makes $\mathbf{Z}_p^\times/(1+p^k\mathbf{Z}_p)$ a nice model for the multiplicative group $(\mathbf{Z}/p^k)^\times$ 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 ± 1.

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

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

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

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

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

Therefore

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

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 $(\mathbf{Z}/2^k)^\times$ 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 4. *For $k \geq 3$, $(\mathbf{Z}/2^k)^\times = \langle -1, 5 \bmod 2^k\rangle = \{\pm 5^j \bmod 2^k : j \geq 0\}$.*

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

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

so $5 \bmod 2^k$ has order 2^{k-2}. No power of $5 \bmod 2^k$ is ever $-1 \bmod 2^k$ since $5 \equiv 1 \bmod 4$ while $-1 \equiv 3 \bmod 4$. Therefore $-1 \bmod 2^k \notin \langle 5 \bmod 2^k\rangle$, and since $-1 \bmod 2^k$ has order 2 the subgroup $\{\pm 5^j \bmod 2^k : j \geq 0\}$ of $(\mathbf{Z}/2^k)^\times$ has order $2 \cdot 2^{k-2} = 2^{k-1} = |(\mathbf{Z}/2^k)^\times|$, which makes this subgroup equal to the whole group. □

Remark 5. We can explain the group structure of $(\mathbf{Z}/2^k)^\times$ by writing it as a quotient group of $\mathbf{Z}_2^\times$. Since $\mathbf{Z}_2^\times = \{\pm 1\} \times (1+4\mathbf{Z}_2)$, for $k \geq 2$ we have

$$\begin{aligned}(\mathbf{Z}/2^k)^\times &\cong (\mathbf{Z}_2/2^k)^\times \\ &\cong \mathbf{Z}_2^\times/(1+2^k\mathbf{Z}_2) \\ &\cong (\{\pm 1\} \times (1+4\mathbf{Z}_2))/(1+2^k\mathbf{Z}_2) \\ &\cong \{\pm 1\} \times (1+4\mathbf{Z}_2)/(1+2^k\mathbf{Z}_2).\end{aligned}$$

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

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

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

3. Bounding finite subgroups of $\mathrm{GL}_n(\mathbf{Q})$

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 if any positive integer then a counterclockwise rotation by $2\pi/d$ radians in the plane $\mathbf{R}^2$ 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 $\mathrm{GL}_2(\mathbf{R})$ that has order d, so $\mathrm{GL}_2(\mathbf{R})$ 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 [3].

Theorem 6 (Minkowski, 1887)**.** *For each $n \geq 1$ every finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$ 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 $\mathrm{GL}_2(\mathbf{Q})$ has order dividing $24 = 2^3 \cdot 3$. We are not claiming that there actually is a subgroup of $\mathrm{GL}_2(\mathbf{Q})$ with order 24. In fact the largest size is 12, but there are subgroups of order not dividing 12 (see below for an example of order 8).

Example 7. The matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ has order 6.

Example 8. 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 $\mathrm{GL}_2(\mathbf{Q})$ has order 8.

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

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

Proof of claim: We can view G inside $\mathrm{GL}_n(\mathbf{Z}_p)$. Reducing matrix entries modulo p sends each matrix A in $\mathrm{GL}_n(\mathbf{Z}_p)$ to a matrix $\overline{A}$ in $\mathrm{GL}_n(\mathbf{Z}_p/p)$, which can be regarded as $\mathrm{GL}_n(\mathbf{Z}/p)$ by the natural identification of $\mathbf{Z}_p/p$ with $\mathbf{Z}/p$. (We have $\overline{A} \in \mathrm{GL}_n(\mathbf{Z}_p/p)$ since $\det A = \pm 1 \Longrightarrow \det A \not\equiv 0 \bmod p \Longrightarrow \det \overline{A} \neq 0$ in $\mathbf{Z}/p$.) Reduction $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{Z}_p/p)$ also preserves multiplication.

The key point is that two matrices A and B in G can't reduce mod p to the same matrix in $\mathrm{GL}_n(\mathbf{Z}_p/p)$. Indeed, suppose $A \equiv B \bmod p$. Then AB^{-1} belongs to G, so it has finite order, and $AB^{-1} \equiv I_n \bmod p$. To deduce that $AB^{-1} = I_n$, so $A = B$, we will use a norm on p-adic matrices.

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

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

For example, $\mathrm{M}_n(\mathbf{Z}_p) = \{X \in \mathrm{M}_n(\mathbf{Q}_p) : ||X||_p \leq 1\}$. It is left to the reader to check $||X + Y||_p \leq \max(||X||_p, ||Y||_p)$ and $||XY||_p \leq ||X||_p||Y||_p$. (It is not generally true that $||XY||_p = ||X||_p||Y||_p$, but the inequality $||XY||_p \leq ||X||_p||Y||_p$ is sufficient to see matrix multiplication, like matrix addition, is continuous on $\mathrm{M}_n(\mathbf{Q}_p)$ relative to the matrix norm $||\cdot||_p$.)

For $p > 2$ and a p-adic integer x such that $x \equiv 1 \bmod p$, we have $|x^m - 1|_p = |m|_p|x-1|_p$ for every positive integer m. It turns out the same equation holds for matrices: if $X \equiv I_n \bmod p$ (that is, $||X - I_n||_p \leq 1/p$) then $||X^m - I_n||_p = |m|_p||X - I_n||_p$ for all positive integers m. Returning to the matrices A and B in G satisfying $A \equiv B \bmod p$, where $p > p_0$ (so $p > 2$),

we have

$$AB^{-1} \equiv I_n \bmod p \Longrightarrow ||AB^{-1} - I_n||_p \leq \frac{1}{p} \Longrightarrow ||(AB^{-1})^m - I_n||_p = |m|_p||AB^{-1} - I_n||_p$$

for all positive integers m. 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 that reduction mod p is an injective mapping $G \to \mathrm{GL}_n(\mathbf{Z}_p/p)$ for $p > p_0$, so $|G|$ divides the order of $\mathrm{GL}_n(\mathbf{Z}_p/p) \cong \mathrm{GL}_n(\mathbf{Z}/p)$. This completes the proof of the claim.

Like the symmetric group S_n, whose order $n!$ is a product of n integers, the order of the group $\mathrm{GL}_n(\mathbf{Z}/p)$ has an explicit formula that is a product of n terms.

Fact: The finite group $\mathrm{GL}_n(\mathbf{Z}/p)$ has order

$$\begin{aligned} (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) &= (p^n-1)p(p^{n-1}-1)\cdots p^{n-1}(p-1) \\ &= p^{1+\cdots+n-1}(p^n-1)(p^{n-1}-1)\cdots)p-1) \\ &= p^{n(n-1)/2}(p^n-1)(p^{n-1}-1)\cdots(p-1). \end{aligned} \tag{3.1}$$

We will not discuss the proof of this, which relies on linear algebra.

To bound $|G|$ pick a prime q. We will get an upper bound $e_n(q)$ for $\mathrm{ord}_q(|G|)$ 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 $\mathrm{GL}_2(\mathbf{Q})$ earlier had order divisible only 2 and 3, which are less than or equal to $n+1 = 3$ in this case.)

For prime $p > p_0$, $\mathrm{ord}_q(|G|) \leq \mathrm{ord}_q(|\,\mathrm{GL}_n(\mathbf{Z}/p)|)$. If $p \neq q$ then by (3.1)

$$\mathrm{ord}_q(|\,\mathrm{GL}_n(\mathbf{Z}/p)|) \leq \mathrm{ord}_q((p^n-1)(p^{n-1}-1)\cdots(p-1)) = \sum_{i=1}^{n-1} \mathrm{ord}_q(p^i-1).$$

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

If $\boxed{q \neq 2}$ then $(\mathbf{Z}/q^k)^\times$ is cyclic for all $k \geq 1$. An integer that is a generator of $(\mathbf{Z}/q^2)^\times$ is also a generator of $(\mathbf{Z}/q^k)^\times$ for all $k \geq 1$ by Corollary 2. Let $b \bmod q^2$ generate $(\mathbf{Z}/q^2)^\times$, so $(b, q^2) = 1$. We will now bring in a famous theorem of Dirichlet about primes in arithmetic progression.

Theorem 9 (Dirichlet)**.** *If a and m are relatively prime integers then there are infinitely many primes $p \equiv a \bmod m$.*

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

$$q^k \mid (p^i - 1) \Longleftrightarrow p^i \equiv 1 \bmod q^k \Longleftrightarrow q^{k-1}(q-1) \mid i.$$

From the equivalence of the first and third relations 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 $[n/(q(q-1))]$.
- 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 $[n/(q^2(q-1))]$.

- 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 $[n/(q^{k-1}(q-1))]$.

Putting this all together, the multiplicity of the prime q in $|\mathrm{GL}_n(\mathbf{Z}/p)|$, if $p \bmod q^2$ generates $(\mathbf{Z}/q^2)^\times$, is

$$e_n(q) := \left[\frac{n}{q-1}\right] + \left[\frac{n}{q(q-1)}\right] + \left[\frac{n}{q^2(q-1)}\right] + \cdots = \sum_{j \geq 0} \left[\frac{n}{q^j(q-1)}\right]. \tag{3.2}$$

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 $\boxed{q = 2}$ a similar analysis can be made with Dirichlet's theorem for modulus 8 (not for modulus $4 = 2^2$, as the case of odd q might suggest), although it is a bit more complicated because the groups $(\mathbf{Z}/2^k)^\times$ 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 [4, Sect. 1.3.4]), is that $\mathrm{ord}_2(|G|)$ is bounded above by the same formula as (3.2) when $q = 2$, that is, by the sum

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

Putting everything together, each finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$ 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 (3.2) for all primes q. The table below gives some sample values.

n	1	2	3	4	5	6	7
$M(n)$	2	24	48	5760	11520	2903040	5806080

□

For each prime q the exponent $e_n(q)$ in $M(n)$ is optimal in the sense that there does exist a subgroup of $\mathrm{GL}_n(\mathbf{Q})$ of order $q^{e_n(q)}$ [1, pp. 392-394], [4, Sect. 1.4].

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

References

[1] N. Bourbaki, "Lie Groups and Lie Algebras, Chapter 1-3," Springer-Verlag, 1998.

[2] S. Friedland, The maximal orders of finite subgroups of $\mathrm{GL}_n(\mathbf{Q})$, *Proc. Amer. Math. Soc.* **125** (1997), 3519–3526.

[3] H. Minkowski, Zur Theorie der positiven quadratische Formen, *J. reine angew. Math.* **101** (1887), 196–202.

[4] J-P. Serre, Bounds for the orders of the finite subgroups of $G(k)$, in: "Group Representation Theory," EPFL Press (2007), 405–450, online at https://arxiv.org/pdf/1011.0346.pdf.