

# 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

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

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 1.1.** *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.

A proof that all groups  $(\mathbf{Z}/p)^\times$  are cyclic is in Section 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  $\mathrm{GL}_n(\mathbf{Q})$ .

## 2. THE GROUPS $(\mathbf{Z}/(p^k))^\times$ ARE CYCLIC

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

*Proof.* By Theorem A.6,  $(\mathbf{Z}/p)^\times$  is cyclic. Let a generator of it be  $g \bmod p$  and let  $\omega(g) \in \mathbf{Z}_p^\times$  be the Teichmüller 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 rings 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

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

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

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

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

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.  $\square$

**Corollary 2.1.** *If  $p$  is an odd prime and  $a \pmod{p^2}$  is a generator of  $(\mathbf{Z}/p^2)^\times$  then  $a \pmod{p^k}$  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 Teichmüller representative of  $a$ , so  $u \in 1 + p\mathbf{Z}_p$  (since  $a \equiv \omega(a) \pmod{p}$ ).

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

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  $a^{dp} \equiv 1 \pmod{p^2}$  with the modulus “improved” to  $p^2$ .<sup>1</sup> 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  $(\mathbf{Z}/p^2)^\times$ . 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  $(\mathbf{Z}/p^k)^\times$  for all  $k \geq 2$ .  $\square$

**Remark 2.2.** 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

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

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  $\pm 1$ .

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  $\mu_{p-1}$  is the (cyclic) group of  $(p-1)$ th roots of unity in the  $p$ -adic integers. Thus

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

<sup>1</sup>In general for  $x$  and  $y$  in  $\mathbf{Z}_p$ , 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  $x^p \equiv y^p \pmod{p^{k+1}}$ .

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  $\log: 1 + p\mathbf{Z}_p \rightarrow p\mathbf{Z}_p$  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 2.3.** 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.  $\square$

**Remark 2.4.** 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  $d$  is a 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 [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  $\mathrm{GL}_n(\mathbf{Q})$  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 and they divide 24 (see below for a subgroup of order 8).

**Example 3.2.** The matrix  $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$  has order 6.

**Example 3.3.** Let  $r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . 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  $G \subset M_n(\mathbf{Z}_p)$  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  $A \in M_n(\mathbf{Z}_p)$  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  $\bar{A}$  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  $\bar{A} \in \mathrm{GL}_n(\mathbf{Z}_p/p)$  since  $\det A = \pm 1 \implies \det A \not\equiv 0 \pmod{p} \implies \det \bar{A} \not\equiv 0 \pmod{p}$ .) Reduction  $\mathrm{GL}_n(\mathbf{Z}_p) \rightarrow \mathrm{GL}_n(\mathbf{Z}_p/p)$  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  $A \equiv B \pmod{p}$ . Then  $AB^{-1}$  belongs to  $G$ , so it has finite order, and  $AB^{-1} \equiv I_n \pmod{p}$ . 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  $X = (x_{ij}) \in M_n(\mathbf{Q}_p)$ , 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,  $M_n(\mathbf{Z}_p) = \{X \in M_n(\mathbf{Q}_p) : \|X\|_p \leq 1\}$ . 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  $M_n(\mathbf{Q}_p)$  relative to the matrix norm  $\|\cdot\|_p$ .)

For  $p > 2$  and a  $p$ -adic integer  $x$  such that  $x \equiv 1 \pmod{p}$ , 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  $X \equiv I_n \pmod{p}$  (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  $A \equiv B \pmod{p}$ , where  $p > p_0$  (so  $p > 2$ ),

we have

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

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  $G \rightarrow \mathrm{GL}_n(\mathbf{Z}_p/p)$  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.

**Theorem 3.4.** *For each prime  $p$ ,  $|\mathrm{GL}_n(\mathbf{Z}/p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ .*

*Proof.* See Section B. The proof is based on linear algebra over the field  $\mathbf{Z}/p$ .  $\square$

The order of  $\mathrm{GL}_n(\mathbf{Z}/p)$  can be rewritten by factoring out the largest power of  $p$ :

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

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 2.1. Let  $b \pmod{q^2}$  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 3.5** (Dirichlet). *If  $a$  and  $m$  are relatively prime integers then there are infinitely many primes  $p \equiv a \pmod{m}$ .*

By Dirichlet's theorem there are infinitely many primes  $p \equiv b \pmod{q^2}$ . 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  $p^i \equiv 1 \pmod{q^k}$ . Since  $p \pmod{q^k}$  generates  $(\mathbf{Z}/q^k)^\times$ ,

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

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  $\lfloor n/(q - 1) \rfloor$ .

- 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

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

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 [5, 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], [5, Sect. 1.4].

**Remark 3.6.** 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 [3].

#### APPENDIX A. CYCLICITY OF $(\mathbf{Z}/p)^\times$

To prove  $(\mathbf{Z}/p)^\times$  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  $(\mathbf{Z}/p)^\times$  has elements of order  $q_i^{e_i}$  for each  $i$  and their product furnishes a generator of  $(\mathbf{Z}/p)^\times$ .

As a warm-up, let's show for each prime  $q$  dividing  $p-1$  that there is an element of order  $q$  in  $(\mathbf{Z}/p)^\times$ . 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  $(\mathbf{Z}/p)^\times$ : it is the nonzero elements of the field  $\mathbf{Z}/p$ .

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

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

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

That proof is *not* saying that if  $a^{(p-1)/q} \neq 1$  in  $\mathbf{Z}/p$  then  $a \bmod p$  has order  $q$ . It is saying that a power of the form  $a^{(p-1)/q} \bmod p$  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  $(\mathbf{Z}/19)^\times$  satisfy  $a^{18} = 1$ . Since 18 is divisible by 3, the lemma is telling us that whenever  $a^{18/3} \neq 1$ ,  $a^{18/3}$  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  $a^6 \bmod 19$  other than 1: 7 and 11. They both have order 3.

$a \bmod 19$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$a^6 \bmod 19$	1	7	7	11	7	11	1	1	11	11	1	1	11	7	11	7	7	1

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

**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  $(\mathbf{Z}/p)^\times$  with order  $q^e$ . Specifically, there is an  $a \in (\mathbf{Z}/p)^\times$  such that  $a^{(p-1)/q} \neq 1$  in  $(\mathbf{Z}/p)^\times$ , and necessarily  $a^{(p-1)/q^e}$  has order  $q^e$  in  $(\mathbf{Z}/p)^\times$ .*

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

Set  $b = a^{(p-1)/q^e}$  in  $\mathbf{Z}/p$ , 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  $(\mathbf{Z}/p)^\times$  by Fermat's little theorem, so the order of  $b \bmod p$  divides  $q^e$ . Since  $q$  is prime, the (positive) factors of  $q^e$  other than  $q^e$  are factors of  $q^{e-1}$ . Since  $b^{q^{e-1}} = (a^{(p-1)/q^e})^{q^{e-1}} = a^{(p-1)/q} \neq 1$  in  $(\mathbf{Z}/p)^\times$ , by the choice of  $a$ , the order of  $b \bmod p$  does not divide  $q^{e-1}$ . Thus the order of  $b$  in  $(\mathbf{Z}/p)^\times$  must be  $q^e$ .  $\square$

**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.

$a \bmod 19$	2	3	4	5	6	9	10	13	14	15	16	17
$a^6 \bmod 19$	7	7	11	7	11	11	11	11	7	11	7	7
$a^2 \bmod 19$	4	9	16	6	17	5	5	17	6	16	9	4

**Remark A.5.** Lemma A.3 can be proved in another way using unique factorization of polynomials with coefficients in  $\mathbf{Z}/p$ . Because all nonzero numbers mod  $p$  are roots of

$T^{p-1} - 1$ , this polynomial factors mod  $p$  as  $(T - 1)(T - 2) \cdots (T - (p - 1))$ . Being a product of distinct linear factors, every factor of  $T^{p-1} - 1$  is also a product of distinct linear factors, so in particular, every factor of  $T^{p-1} - 1$  has as many roots in  $\mathbf{Z}/p$  as its degree. For a prime power  $q^e$  dividing  $p - 1$ ,  $T^{q^e} - 1$  divides  $T^{p-1} - 1$ , so there are  $q^e$  solutions of  $a^{q^e} = 1$  in  $\mathbf{Z}/p$ . This exceeds the number of solutions of  $a^{q^{e-1}} = 1$  in  $\mathbf{Z}/p$ , which is at most  $q^{e-1}$  since a nonzero polynomial over a field has no more roots than its degree. Therefore there is an  $a$  in  $\mathbf{Z}/p$  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  $(\mathbf{Z}/p)^\times$  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  $b_i \in (\mathbf{Z}/p)^\times$  with order  $q_i^{e_i}$ . These orders are relatively prime, and  $(\mathbf{Z}/p)^\times$  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,  $b_1 b_2 \cdots b_m$  generates  $(\mathbf{Z}/p)^\times$ .  $\square$

## APPENDIX B. THE ORDER OF $\mathrm{GL}_n(\mathbf{Z}/p)$

To compute  $|\mathrm{GL}_n(\mathbf{Z}/p)|$ , view the columns of an  $n \times n$  matrix with entries in  $\mathbf{Z}/p$  as an ordered list of  $n$  elements of  $(\mathbf{Z}/p)^n$ . The matrix is invertible if and only if *the columns are a basis of  $(\mathbf{Z}/p)^n$* . Since a set of  $n$  vectors in an  $n$ -dimensional vector space is a basis if and only if it is linearly independent, we will count how many ordered lists of  $n$  vectors in  $(\mathbf{Z}/p)^n$  are linearly independent. Since every set of linearly independent vectors in  $(\mathbf{Z}/p)^n$  can be extended to a basis, we can build up elements of  $\mathrm{GL}_n(\mathbf{Z}/p)$  column by column.

- (1) The first column can be anything in  $(\mathbf{Z}/p)^n$  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  $(\mathbf{Z}/p)^n$  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  $(\mathbf{Z}/p)^n$  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  $(\mathbf{Z}/p)^n$ , 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  $(\mathbf{Z}/p)^n$  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  $|\mathrm{GL}_n(\mathbf{Z}/p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ .

## REFERENCES

- [1] N. Bourbaki, "Lie Groups and Lie Algebras, Chapter 1-3," Springer-Verlag, 1998.
- [2] J. W. S. Cassels, "Local Fields," Cambridge Univ. Press, Cambridge, 1986.
- [3] S. Friedland, The maximal orders of finite subgroups of  $\mathrm{GL}_n(\mathbf{Q})$ , *Proc. Amer. Math. Soc.* **125** (1997), 3519–3526.
- [4] H. Minkowski, Zur Theorie der positiven quadratische Formen, *J. reine angew. Math.* **101** (1887), 196–202.
- [5] 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>.