ORDERS OF ELEMENTS IN A GROUP

KEITH CONRAD

1. Introduction

Let G be a group and $g \in G$. We say g has *finite order* if $g^n = e$ for some positive integer n. For example, -1 and i have finite order in $\mathbf{C}^\times$, since $(-1)^2 = 1$ and $i^4 = 1$. The powers of g repeat themselves every n turns: for any integers a and k,

$$g^{a+nk} = g^a g^{nk} = g^a (g^n)^k = g^a.$$

Thus the sequence of powers of g looks like $\{e, g, g^2, \ldots, g^{n-1}, e, g, g^2, \ldots\}$.

The least $n \geq 1$ such that $g^n = e$ is called the *order* of g. If there is no such n (that is, $g^n \neq e$ for every $n \geq 1$), we say g has *infinite order*. For example, in the group $\mathbf{C}^\times$, -1 has order 2, i has order 4, and 7 has infinite order. For any positive integer n, the complex number

$$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

is an example of an element of $\mathbf{C}^\times$ with order n.

If G is a finite group, every $g \in G$ has finite order. The proof is as follows. Since the set of powers $\{g^a : a \in \mathbf{Z}\}$ is a subset of G and the exponents a run over all integers, an infinite set, there must be a repetition: $g^a = g^b$ for some $a < b$ in $\mathbf{Z}$. Then $g^{b-a} = e$, so g has finite order. (Taking the contrapositive, if g has infinite order its integral powers have no repetitions: $g^a = g^b \Longrightarrow a = b$.)

There are three questions about elements of finite order that we want to address:

(1) When $g \in G$ has a known finite order, how can we tell when two powers g^k and g^ℓ are the same directly in terms of the exponents k and ℓ?
(2) When g has finite order, how is the order of a power g^k related to the order of g?
(3) When two elements g_1 and g_2 of a group have finite order, how is the order of their product $g_1 g_2$ related to the orders of g_1 and g_2?

We will find essentially complete answers to the first two questions, and only a partial answer to the third question.

In the case of finite abelian groups, we will see that the order of any element divides the size of the group.[1] Then, as application of that divisibility relation, we will derive some classical congruences from number theory that can be used to test efficiently whether or not a large integer is prime without having to factor it. (This is very important in cryptography.)

The most important theorems to understand well are Theorems 3.2, 3.4, and 3.12.

[1]This result is also true in the non-abelian case, but not by the proof we will give here for abelian groups.

2. Examples

We have already seen that -1 and i in $\mathbf{C}^\times$ have orders 2 and 4, respectively. Let's look at the meaning of the order of an element in the groups $(\mathbf{Z}/(m))^\times$ and S_m.

Example 2.1. An integer modulo m lies in $(\mathbf{Z}/(m))^\times$ precisely when it is relatively prime to m, which can be effectively determined using Euclid's algorithm. To say $a \bmod m$ has order n in $(\mathbf{Z}/(m))^\times$ means

$$a^n \equiv 1 \bmod m, \quad a^j \not\equiv 1 \bmod m \text{ for } 1 \leq j < n.$$

There is no simple-minded formula for the order of a random element of $(\mathbf{Z}/(m))^\times$; it just is what it is and you have to make computations to figure it out. For instance, 2 and 2^2 are not 1 mod 7 and $2^3 \equiv 1 \bmod 7$, so 2 has order 3 in $(\mathbf{Z}/(7))^\times$. Since $2^j \not\equiv 1 \bmod 23$ for $1 \leq j < 11$ and $2^{11} \equiv 1 \bmod 23$, 2 has order 11 in $(\mathbf{Z}/(23))^\times$. For any $m \geq 3$, -1 has order 2 in $(\mathbf{Z}/(m))^\times$ since $(-1)^2 \equiv 1 \bmod m$ while $-1 \not\equiv 1 \bmod m$. Watch out for $m = 2$: since $-1 \equiv 1 \bmod 2$, in the group $(\mathbf{Z}/(2))^\times$, which is actually a group with only one element, -1 has order 1, not 2!

Example 2.2. In a symmetric group S_m, let

$$\sigma = (a_1\ a_2\ \cdots\ a_r)$$

be an r-cycle. The n-th power σ^n shifts each a_i by n terms. (A power of a cycle need not be a cycle, *e.g.*, $(1234)^2 = (13)(24)$.) The least $n \geq 1$ such that σ^n is the identity is $n = r$. That is, an r-cycle has order r. For instance, any transposition has order 2.

Armed with this information about orders of cycles, we will compute the order of a general permutation in S_m, using its disjoint cycle decomposition, in Theorem 3.6.

3. Basic Properties of Orders

Let G be a group, written multiplicatively. For $g \in G$, the subgroup *generated* by g is

$$\langle g \rangle = \{g^k : k \in \mathbf{Z}\}.$$

This is easily seen to be a subgroup: it is closed under multiplication and inversion.

Theorem 3.1. *To say g has finite order in G is equivalent to saying $\langle g \rangle$ is a finite group.*

Proof. If g has finite order, suppose $g^n = e$ for some $n > 0$. Consider a general power of g, say g^k with $k \in \mathbf{Z}$. By the division theorem in $\mathbf{Z}$, there are integers q and r such that $k = nq + r$ with $0 \leq r < n$. Then

$$g^k = g^{nq} g^r = g^r,$$

so

$$\langle g \rangle = \{e, g, g^2, \cdots, g^{n-1}\},$$

which shows $\langle g \rangle$ is a finite group.

Conversely, suppose $\langle g \rangle$ is a finite group. Then g certainly has just a finite number of different powers. As k runs through the integers, the powers g^k must repeat: $g^{k_1} = g^{k_2}$ for different integers k_1 and k_2. We may take $k_1 < k_2$ without loss of generality. Then $g^{k_2 - k_1} = e$, with $k_2 - k_1$ a positive integer, so g has finite order. □

When $g^n = e$, n might not be as small as possible, so the repetition in the powers of g may really occur more often than every n turns. For example, $(-1)^4 = 1$, so Theorem 3.1 says the only powers of -1 are $(-1)^k$ for $k \in \{0, 1, 2, 3\}$, but we know that in fact a more economical list is $(-1)^k$ for $k \in \{0, 1\}$. This is connected with the fact that $(-1)^2 = 1$.

This observation leads to a strengthening of Theorem 3.1: the order of g is the size of the group $\langle g \rangle$ when g has finite order.

Theorem 3.2. *Let $g^n = e$ for some $n \geq 1$, with n chosen as small as possible. Then*
(1) $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.
(2) $\#\langle g \rangle = n$. *That is, the powers listed in part* (1) *are different from each other.*

Proof. First we show (1). Given an arbitrary power g^k, write $k = nq + r$ where $0 \leq r \leq n - 1$. Then $g^k = g^r$, just as in the previous proof, so every power of g is some g^r where $0 \leq r \leq n - 1$. This means

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\},$$

which establishes (1). So far we have *not* used the minimality of n.

Now we prove (2). We already have a list of n powers that exhaust $\langle g \rangle$, namely g^r for $0 \leq r \leq n - 1$. To prove $\#\langle g \rangle = n$, we must prove these powers are all distinct. Here is where the minimality of n is going to be used.

If our list of powers contains any repetitions, then

$$g^i = g^j$$

where $1 \leq i < j \leq n - 1$. (Be attentive to the inequalities here.) Then

$$g^{j-i} = e, \tag{3.1}$$

and $0 < j - i < n$. This contradicts the definition of n, since we found a power of g equal to e where the exponent $j - i$ is a positive integer less than n, while n is the minimal positive integer satisfying $g^n = e$. Hence we have a contradiction, so the powers among $\{e, g, g^2, \ldots, g^{n-1}\}$ are distinct from one another. Thus $\#\langle g \rangle = n$. □

Remark 3.3. When G is a finite group, every element must have finite order. However, the converse is false: there are infinite groups where each element has finite order. For example, in the group of all roots of unity in $\mathbf{C}^\times$ each element has finite order.

Theorem 3.2 gives a nice combinatorial interpretation of the order of g, when it is finite: the order of g is the size of the group $\langle g \rangle$. In fact, this even works when g has infinite order (then $\langle g \rangle$ is an infinite group), so the order of g is always the size of $\langle g \rangle$.

The finite order of an element is linked to periodicity in its powers, as follows.

Theorem 3.4. *Let $g \in G$ and g have order n. Then $g^k = e$ if and only if $n|k$.*

This is the most fundamental property of the order of an element in a group. Be sure you really understand the ideas in the proof! Try it out on powers of i in $\mathbf{C}^\times$ (having order $n = 4$).

Proof. If $n|k$, say $k = nm$, then $g^k = g^{nm} = (g^n)^m = e$. For the converse direction, we use the division theorem. Supposing that $g^k = e$, write $k = nq + r$ with integers q and r such that $0 \leq r < n$. Then

$$e = g^k = (g^n)^q g^r = g^r.$$

Since $0 \leq r < n$, the minimality built into n as the order of g forces r to be zero (why?). Thus $k = nq$, so $n|k$. □

Corollary 3.5. *Let $g \in G$ have order n. For $k, \ell \in \mathbf{Z}$, $g^k = g^\ell$ if and only if $k \equiv \ell \bmod n$.*

Proof. Write the condition $g^k = g^\ell$ as $g^{k-\ell} = e$. Now use Theorem 3.4. □

Here is a concrete application of Theorem 3.4: we find a formula for the order of a permutation in a symmetric group. In Example 2.2, we saw that an r-cycle has order r. Now we deal with a general permutation, which is not necessarily a cycle.

Theorem 3.6. *For $\sigma \in S_m$, write it as a product of disjoint cycles:*

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t,$$

where σ_i is a cycle with length r_i, $1 \leq i \leq t$. The order of σ is the least common multiple $[r_1, r_2, \ldots, r_t]$.

Proof. Since disjoint cycles commute,

$$\sigma^a = \sigma_1^a \sigma_2^a \cdots \sigma_t^a.$$

Because the σ_i's permute elements from disjoint sets, σ^a is the identity if and only if each σ_i^a is the identity. (Be sure you understand that.) As σ_i has order r_i, σ_i^a is the identity if and only if $r_i | a$ (by Theorem 3.4). Therefore

$$\begin{aligned} \sigma^a = (1) &\iff \text{each } \sigma_i^a = (1), \\ &\iff r_i | a \text{ for all } i, \\ &\iff [r_1, r_2, \ldots, r_t] | a, \end{aligned}$$

where $[r_1, r_2, \ldots, r_t]$ denotes the least common multiple of the r_i's, which are the lengths of the disjoint cycles σ_i. Therefore the order of σ is $[r_1, r_2, \ldots, r_t]$. □

Example 3.7. Consider

$$\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9\ 10).$$

The cycles appearing here are disjoint. The order of σ is $[4, 6] = 12$.

If σ is not written as a product of disjoint cycles, determine its disjoint cycle decomposition first in order to compute the order of σ.

Example 3.8. Consider

$$\sigma = (123)(241).$$

The 3-cycles here each have order 3, but σ does *not* have order $[3, 3] = 3$. The cycles are not disjoint. The disjoint cycle decomposition of σ is

$$\sigma = (13)(24)$$

so the order of σ is 2.

Corollary 3.9. *A permutation $\sigma \in S_n$ has prime order p if and only if it is a product of disjoint p-cycles.*

Proof. Let the decomposition of σ into disjoint cycles be $\sigma_1 \sigma_2 \cdots \sigma_t$, and we can assume the σ_i's are all nontrivial cycles. (We allow $t = 1$: a single cycle is a product of 1 disjoint cycle.) Letting r_i be the order of σ_i, $r_i > 1$ and computing the order of this product tells us $p = [r_1, \ldots, r_t]$. Therefore each r_i is a factor of p and is greater than 1, so every r_i is p. Conversely, if each r_i is p then of course their least common multiple is p. So σ has order p if and only if it is a disjoint product of p-cycles. □

This theorem is not saying an element of order p is a p-cycle. It's a disjoint product of p-cycles. For example, $(12)(34)(56)$ has order 2 and $(123)(456)$ has order 3.

Remark 3.10. Do not confuse the parity of a permutation being even or odd with the order of a permutation being even or odd: they are separate concepts. For example, (12) is an odd permutation with even order 2, (123) is an even permutation with odd order 3, and $(12)(34)$ is an even permutation with even order 2. There is no odd permutation with odd order: if $\sigma^m = (1)$ and m is odd, then taking the sign of both sides shows $\mathrm{sgn}(\sigma)^m = 1$. An odd power of -1 is -1, so we must have $\mathrm{sgn}(\sigma) = 1$. Thus an odd permutation (such as (12) or $(12)(23)(34) = (1234)$) always has even order.

Returning to general groups G, we compare the orders of g and g^k when g has finite order. Let g have order n. Since $(g^k)^n = (g^n)^k = e$, the order of g^k divides n by Theorem 3.4. Which factor of n is it?

Example 3.11. Suppose g has order 12, so any power of g has order that is a factor of 12. It is plausible that g^2 has order 6: since g takes 12 powers until it first cycles around to the identity, g^2 takes only 6 powers to get there. Thus g^2 has order $6 = 12/2$. On the other hand, it is absurd to say g^8 has order $12/8$, as $12/8$ is not an integer. The successive powers of g^8 are

$$g^8 \neq e, \quad (g^8)^2 = g^{16} = g^4 \neq e, \quad (g^8)^3 = g^{24} = g^{12\cdot 3} = e,$$

so g^8 has order 3, which we can write as $12/4$. What we divide 12 by to get the order of g^8 is not 8, but the largest factor that 8 has in common with 12, namely 4.

Theorem 3.12. *Let g have order n in a group and k be an integer.*

1. *If $k|n$ then g^k has order n/k.*
2. *If $(k, n) = 1$ then g^k has order n. That is, raising g to a power relatively prime to its order doesn't change the order.*
3. *For general $k \in \mathbf{Z}$, g^k has order $n/(k, n)$.*

The third part includes the first two parts as special cases (if $k|n$ then $n/(k, n) = n/k$, and if $(k, n) = 1$ then $n/(k, n) = n$), but we state those special cases separately because they are worth knowing on their own *and* because they can be proved independently of the general case. Understanding the proof of the first two parts of the theorem will help you better understand the proof of the third part. Basic to everything will be Theorem 3.4.

Proof. Let t be the (unknown) order of g^k, so $(g^k)^t = e$ and t is the minimal positive exponent that fits this equation. We want to show $t = n/k$ if $k|n$, $t = n$ if $(k, n) = 1$, and $t = n/(k, n)$ in general.

1) We assume $k|n$. The condition $(g^k)^t = e$ is the same as $g^{kt} = e$, so $n|kt$ by Theorem 3.4. Thus $n \leq kt$, so $n/k \leq t$. We also have the reverse inequality: since $(g^k)^{n/k} = g^{k(n/k)} = g^n = e$, $t \leq n/k$ by the definition of what the order of an element is. From $t \leq n/k$ and $n/k \leq t$, we have $t = n/k$.

2) We assume $(k, n) = 1$ and want to show g^k has order n. The key idea we will need is that if $a|bc$ and $(a, b) = 1$, then $a|c$. It would be good to review how that is proved if you don't recall the argument.

The equation $(g^k)^t = e$ is the same as $g^{kt} = e$, so $n|kt$ by Theorem 3.4. Since n and k are relatively prime, from $n|kt$ we conclude that $n|t$, so $n \leq t$. We have the reverse inequality too: $(g^k)^n = g^{kn} = (g^n)^k = e^k = e$, so $t \leq n$ by the definition of the order of an element. Therefore $t = n$.

3) In the general case, for any k, we want to show $t = n/(k,n)$. The equation $(g^k)^t = e$ is the same as $g^{kt} = e$, so $n|kt$ by Theorem 3.4. Write $kt = nm$ for some $m \in \mathbf{Z}$.

Factor (n,k) out of both n and k: $n = (n,k)n'$ and $k = (n,k)k'$, so $(n',k') = 1$. Notice $n' = n/(n,k)$, so we want to show $t = n'$. In the equation $kt = nm$ we can cancel (n,k) from both sides:

$$kt = nm \Longrightarrow (k,n)k't = (k,n)n'm \Longrightarrow k't = n'm,$$

so $n'|k't$. Since n' and k' are relatively prime, from $n'|k't$ we get $n'|t$, so $n' \leq t$.

We have the reverse inequality too:

$$(g^k)^{n'} = g^{kn'} \stackrel{!}{=} g^{nk'} = (g^n)^{k'} = e^{k'} = e.$$

Let's explain the equality with the exclamation point. The exponents kn' and nk' are equal since they are each the same as $kn/(n,k)$.

From $(g^k)^{n'} = e$ we have $t \leq n'$. Earlier we saw $n' \leq t$, so $t = n' = n/(k,n)$ and we are done. □

Example 3.13. If g has order 12, here is a list of orders of the initial powers of g. The order of g^k is equal to $12/(k,12)$. Compute successive powers of g^k for each k to verify directly that the values in the table are correct.

k	1	2	3	4	5	6	7	8	9	10	11	12
order of g^k	12	6	4	3	12	2	12	3	4	6	12	1

Example 3.14. If g has order n, then g^{-1} has order n, since $(n,-1) = 1$. This result can also be seen directly, since the powers of g^{-1} are the same as the powers of g, but simply appear in reverse order when written out (why?).

Example 3.15. If g has order 12, g^k has order 12 precisely when $(k,12) = 1$. Look at the table above and notice 12 appears under $k = 1, 5, 7, 11$, which are relatively prime to 12.

4. Order of products

How is the order of a product g_1g_2 related to the orders of the individual factors g_1 and g_2? In this generality not much can be said!

Example 4.1. We saw in Example 3.8 that in S_4, (123) and (241) each have order 3 while their product $(123)(241) = (13)(24)$ has order 2.

Example 4.2. Suppose g has order 5. Then g^{-1} has order 5 and g^2 has order 5, but the product $gg^{-1} = e$ has order 1 while the product $gg^2 = g^3$ has order 5.

Example 4.3. Two elements can have finite order while their product has infinite order. Consider, in $\mathrm{GL}_2(\mathbf{R})$, the matrices

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Check yourself that A^2 and B^2 equal the identity matrix, so A and B both have order 2. Meanwhile,

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has infinite order: $(AB)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, which is the identity matrix only for $n = 0$. The product $BA = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = (AB)^{-1}$ also has infinite order.

Example 4.4. There is a finite group containing two elements with order 2 whose product has *any* desired finite order greater than 2. Pick $m \geq 3$ and view the matrices A and B from Example 4.3 as having entries that are integers mod m. Then A and B are now interpreted in the finite group $\mathrm{GL}_2(\mathbf{Z}/(m))$. Since $-1 \not\equiv 1 \bmod m$, both A and B have order 2 in $\mathrm{GL}_2(\mathbf{Z}/(m))$. Their product $AB = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{Z}/(m))$ has order m.

The moral of the last two examples is that in general *nothing* can be said about the order of the product of two elements of finite order: it might be anything at all. However, if the two elements commute with each other, we can say a lot. (In the last three examples, the pair of elements do not commute.) What is special about commuting elements is that the product of commuting elements that each have finite order also has finite order: if $g_1^{n_1} = e$, $g_2^{n_2} = e$, and $g_1g_2 = g_2g_1$, then $(g_1g_2)^{n_1n_2} = g_1^{n_1n_2}g_2^{n_1n_2} = ee = e$. For example, if $g_1^6 = e$ and $g_2^4 = e$ then $(g_1g_2)^{24} = g_1^{24}g_2^{24} = e$. So when g_1 has order dividing 6 and g_2 has order dividing 4 and $g_1g_2 = g_2g_1$, g_1g_2 has order dividing 24.

Actually, we can bound the order of g_1g_2 by something a little bit better in general than the product n_1n_2. The least common multiple $[n_1, n_2]$ is divisible by n_1 and n_2, so $(g_1g_2)^{[n_1,n_2]} = g_1^{[n_1,n_2]}g_2^{[n_1,n_2]} = e$. For example, if $g_1^6 = e$ and $g_2^4 = e$ then $(g_1g_2)^{12} = g_1^{12}g_2^{12} = e$. So when g_1 has order dividing 6 and g_2 has order dividing 4 and $g_1g_2 = g_2g_1$, g_1g_2 has order dividing 12, not just 24.

When the orders of g_1 and g_2 are relatively prime, we can say *exactly* what the order of g_1g_2 is:

Theorem 4.5. *Let g_1 and g_2 commute, where g_1 has order n_1 and g_2 has order n_2, with $(n_1, n_2) = 1$. Then g_1g_2 has order n_1n_2.*

In words, for *commuting* elements with *relatively prime* orders, the order of their product is the product of their orders.

Proof. Since
$$(g_1g_2)^{n_1n_2} = g_1^{n_1n_2}g_2^{n_1n_2} = (g_1^{n_1})^{n_2}(g_2^{n_2})^{n_1} = e,$$
we see g_1g_2 has finite order, which must divide n_1n_2 by Theorem 3.4.

Let n be the order of g_1g_2. In particular, $(g_1g_2)^n = e$. From this we will show $n_1|n$ and $n_2|n$. Since g_1 and g_2 commute,
$$g_1^n g_2^n = e. \tag{4.1}$$
Raising both sides of (4.1) to the power n_2 (to kill off the g_2 factor) gives
$$g_1^{nn_2} = e.$$
Therefore $n_1|nn_2$ by Theorem 3.4. Since $(n_1, n_2) = 1$, we conclude $n_1|n$. Now raising both sides of (4.1) to the power n_1 gives $g_2^{nn_1} = e$, so $n_2|nn_1$ by Theorem 3.4, and thus $n_2|n$.

Since $n_1|n$, $n_2|n$ *and* $(n_1, n_2) = 1$, we conclude that $n_1n_2|n$. Since we already showed $n|n_1n_2$ (in the first paragraph of the proof), we conclude $n = n_1n_2$. □

Example 4.6. In $(\mathbf{Z}/(21))^\times$, -1 has order 2 and 4 has order 3. Therefore $-4 = 17$ has order 6.

Example 4.7. If g_1 has order 5, g_2 has order 8, and g_1 and g_2 commute, then g_1g_2 has order 40.

Example 4.8. For noncommuting elements with relatively prime orders, Theorem 4.5 can fail. In S_5, (123) has order 3 and (15342) has order 5 while $(123)(15342) = (15)(34)$ has order 2, not $3 \cdot 5 = 15$.

The least common multiple is not just an upper bound on the order of a product of commuting elements, but can be realized as the order of *some* product of their powers:

Corollary 4.9. *Let g_1 and g_2 commute, where g_1 has order n_1 and g_2 has order n_2. For some integers a_1 and a_2, $g_1^{a_1}g_2^{a_2}$ has order $[n_1, n_2]$.*

Proof. The basic idea is to write $[n_1, n_2]$ as a product of two relatively prime factors and then find exponents a_1 and a_2 such that $g_1^{a_1}$ and $g_2^{a_2}$ have orders equal to those factors. Then the order of $g_1^{a_1}$ and $g_2^{a_2}$ will be equal to the product of the factors (Theorem 4.5), which is $[n_1, n_2]$ by design.

Here are the details. Factor n_1 and n_2 into primes:

$$n_1 = p_1^{e_1} \cdots p_r^{e_r}, \quad n_2 = p_1^{f_1} \cdots p_r^{f_r}.$$

We use the same list of (distinct) primes in these factorizations, and use an exponent 0 on a prime that is not a factor of one of the integers. The least common multiple is

$$[n_1, n_2] = p_1^{\max(e_1,f_1)} \cdots p_r^{\max(e_r,f_r)}.$$

Break this into a product of two factors, one being a product of the prime powers where $e_i \geq f_i$ and the other using prime powers where $e_i < f_i$. Call these two numbers k_1 and k_2:

$$k_1 = \prod_{e_i \geq f_i} p_i^{e_i}, \quad k_2 = \prod_{e_i < f_i} p_i^{f_i}.$$

Then $[n_1, n_2] = k_1k_2$ and $(k_1, k_2) = 1$ (since k_1 and k_2 have no common prime factors). By construction, $k_1|n_1$ and $k_2|n_2$. Then $g_1^{n_1/k_1}$ has order k_1 and $g_2^{n_2/k_2}$ has order k_2. Since these orders are relatively prime and the two powers of g_1 and g_2 commute with each other, $g_1^{n_1/k_1}g_2^{n_2/k_2}$ has order $k_1k_2 = [n_1, n_2]$. □

Example 4.10. Suppose g_1 has order $n_1 = 60 = 2^2 \cdot 3 \cdot 5$ and g_2 has order $n_2 = 630 = 2 \cdot 3^2 \cdot 5 \cdot 7$. Then $[n_1, n_2] = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. We can write this as $(2^2 \cdot 5) \cdot (3^2 \cdot 7)$, where the first factor appears in n_1, the second in n_2, and the factors are relatively prime. Then g_1^3 has order $2^2 \cdot 5$ and g_2^{10} has order $3^2 \cdot 7$. These orders are relatively prime, so $g_1^3g_2^{10}$ has order $2^2 \cdot 5 \cdot 3^2 \cdot 7 = [n_1, n_2]$.

Since the same power of 5 appears in both n_1 and n_2, there is another factorization of $[n_1, n_2]$ we can use: placing the 5 in the second factor, we have $[n_1, n_2] = (2^2)(3^2 \cdot 5 \cdot 7)$. Then g_1^{15} has order 2^2 and g_2^2 has order $3^2 \cdot 5 \cdot 7$. These orders are relatively prime, so $g_1^{15}g_2^2$ has order $2^2 \cdot 3^2 \cdot 5 \cdot 7 = [n_1, n_2]$.

5. Finite Abelian Groups and Primality Testing

The equivalence in the next theorem will lead us to an interesting way to distinguish prime numbers from composite numbers.

Theorem 5.1. *The following conditions on a finite group G of size N are equivalent:*

(a) *For all $g \in G$, $g^N = e$.*
(b) *For all $g \in G$, the order of g divides N.*

Proof. (a) ⇒ (b): If $g^N = e$ then the order of g divides N by Theorem 3.4.

(b) ⇒ (a): Let g have order n. If $n|N$, say $N = nn'$, then $g^N = (g^n)^{n'} = e^{n'} = e$. □

Theorem 5.1 is *not* saying (a) is true or (b) is true for a group G, but only that one is true for G if and only if the other is true for G. By a trick that depends on commutativity, we will show (a) is true when G is abelian.

Theorem 5.2. *For any finite abelian group G of size N, $g^N = e$ for all $g \in G$.*

Proof. Write out the elements of G, say $G = \{g_1, g_2, \ldots, g_N\}$. Now consider the product of each with g:

$$\{gg_1, gg_2, \ldots, gg_N\}. \tag{5.1}$$

Since $gg_i = gg_j$ if and only if $g_i = g_j$, sending g_i to gg_i is a one-to-one function from G to itself. As G is finite, the function is onto as well. That means (5.1) is just another listing of the elements of G, except perhaps in a different order:

$$G = \{g_1, g_2, \ldots, g_N\} = \{gg_1, gg_2, \ldots, gg_N\}.$$

Since G is abelian, we can multiply the elements in both lists and equate:

$$\begin{aligned} g_1 g_2 \cdots g_N &= (gg_1)(gg_2)\cdots(gg_N) \\ &= g^N(g_1 g_2 \cdots g_N). \end{aligned}$$

Now cancel every g_i from both sides: $g^N = e$. □

Corollary 5.3. *In a finite abelian group with size N, each element has order dividing N.*

Proof. This is immediate from Theorem 5.2 and (a) ⇒ (b) in Theorem 5.1. □

Remark 5.4. For a general finite group, (a) and (b) in Theorem 5.1 are true, but to prove this for non-abelian groups requires a different approach: prove (b) first, and then (a) follows from Theorem 5.1. The proof of (b) uses cosets and we don't discuss it here.

What does Theorem 5.2 say for the groups $(\mathbf{Z}/(p))^\times$, where p is prime? Every non-zero congruence class modulo p is invertible, so $\#(\mathbf{Z}/(p))^\times = p - 1$. Theorem 5.2 in this case is a result going back to Fermat, called *Fermat's little theorem* (which got this whole business started).

Theorem 5.5 (Fermat)**.** *If p is prime and a is any integer with $a \not\equiv 0 \bmod p$, $a^{p-1} \equiv 1 \bmod p$.*

Example 5.6. Let $p = 7$. As the following table shows, the first time an element of $(\mathbf{Z}/(7))^\times$ has a power equal to 1 may vary, but all powers hit 1 at exponent $6 = p - 1$.

k	1	2	3	4	5	6
$1^k \bmod 7$	1	1	1	1	1	1
$2^k \bmod 7$	2	4	1	2	4	1
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1	4	2	1
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1	6	1	6	1

What is the analogue of Fermat's little theorem for $(\mathbf{Z}/(m))^\times$ when m is composite? It is most definitely *not* that $a^{m-1} \equiv 1 \bmod m$ for any a with $(a, m) = 1$. Indeed, the exponent in Theorem 5.2 is the size of the group, and $(\mathbf{Z}/(m))^\times$ does not have size $m - 1$ when m is

composite (non-trivial factors of m are not relatively prime to m). The size of $(\mathbf{Z}/(m))^\times$ is an irregularly growing function of m. It is traditionally denoted $\varphi(m)$:

$$\varphi(m) = \#(\mathbf{Z}/(m))^\times = \#\{1 \leq a \leq m : (a, m) = 1\}.$$

For instance, $\varphi(p) = p - 1$ when p is prime. The following table lists $\varphi(m)$ for $m \leq 15$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Using the group $(\mathbf{Z}/(m))^\times$ in Theorem 5.2, we get a generalization of Fermat's little theorem, which is due to Euler.

Theorem 5.7 (Euler)**.** *For any positive integer m, $a^{\varphi(m)} \equiv 1 \bmod m$ for every a that is relatively prime to m.*

Example 5.8. Taking $m = 15$, Euler's theorem says any a that is relatively prime to 15 satisfies $a^8 \equiv 1 \bmod 15$.

When m is composite, $\varphi(m) < m - 1$, so the exponent in Euler's theorem is not $m - 1$. This suggests (but does not prove) that, for composite m, $a^{m-1} \not\equiv 1 \bmod m$ for *some* a between 1 and $m - 1$. In practice such a are often (but not always!) easy to find. This is a simple but powerful way to *prove* an integer m is composite: find some a in $\{1, 2, \ldots, m-1\}$ such that $a^{m-1} \not\equiv 1 \bmod m$. If there is even one such a, then m violates the conclusion of Fermat's little theorem (which is about *every* a from 1 to $m - 1$ when m is prime), so m must be composite.

Example 5.9. Take $m = 15$. What is $2^{14} \bmod 15$? The powers of 2 mod 15 are 2, 4, 8, 1, 2, 4, 8, 1,..., repeating with period 4, so $2^{14} \equiv 2^2 \equiv 4 \bmod 15$. Therefore 15 is not a prime number.

This might seem like a dumb example: you already know 15 is composite because you know it factors as 3×5. The Fermat way of proving 15 is composite is different, since it tells us 15 is composite without telling us anything about its factorization. This teaches us something surprising: proving compositeness is not the same as finding a non-trivial factor (even though it appears otherwise from the definition of composite numbers).

Example 5.10. Let $m = 116670466859$. Since

$$2^{m-1} \equiv 44351214905 \bmod m,$$

m is composite. The congruence does not tell us an explicit non-trivial factor of m. It only tells us that m does not satisfy the conclusion of Fermat's little theorem, and that suffices to know m is composite.

The computation of $a^{m-1} \bmod m$ can be carried out very quickly on a computer (writing the exponent in base 2, the exponentiation reduces to repeated squaring, which can be done modulo m rapidly, while real exponentiation can explode), so it is feasible in practice to prove the compositeness of large numbers by finding counterexamples to Fermat's little theorem for modulus m. Moreover, if one choice of a doesn't violate Fermat's little theorem, we can pick another a and try again. (Fermat's little theorem is about all a from 1 to $m-1$.)

Example 5.11. Let $m = 341$. Then $2^{340} \equiv 1 \bmod 341$. This does not tell us anything; just because it is consistent with Fermat's little theorem (if m were prime), it does not prove m is prime. We try another base, 3. Since $3^{340} \equiv 56 \bmod 341$, Fermat's little theorem is not true for 341, so 341 is composite.

Definition 5.12. If $a \not\equiv 0 \bmod m$ and $a^{m-1} \not\equiv 1 \bmod m$, we say a is a (Fermat) *witness* to the compositeness of m.

As soon as we find one witness, m is provably composite. Using some further group theory, it can be shown that if there is even one Fermat witness that is *relatively prime* to m, then at least 50% of the numbers from 1 to $m-1$ are Fermat witnesses. With those kinds of percentages, we can expect to get a Fermat witness pretty quickly; probably no more than a handful of tests will be needed before we find a witness.

The 50% lower bound on the proportion of Fermat witnesses was based on the assumption that m has a Fermat witness that is relatively prime to m. Often such witnesses exist, and one of them is found after just a few trials. However, there do exist composite m for which all Fermat witnesses have a factor in common with m. These numbers are called Carmichael numbers, and the Fermat test will run about as slowly as trial division for these numbers. There are infinitely many Carmichael numbers, but in practice one doesn't run across them too often.

In addition to its greater speed over trial division in proving a number is composite, the Fermat test has another advantage over trial division: failures of the test are informative. If we do 10 trial divisions and find no factors of m, we still are uncertain about whether m is prime or composite and we haven't learned anything since we expect most numbers less than m aren't factors of m anyway. But if we do 10 Fermat tests and find no example with $a^{m-1} \not\equiv 1 \bmod m$, we are *morally* convinced m is a prime (the "probability" it is not prime is at most $(1/2)^{10} \approx .00098$), although we get no proof it really is prime by this method (maybe m is a Carmichael number).

The upshot of this discussion is that Fermat's little theorem provides a method of proving an integer is composite that does not search for factors. Instead, it uses algebra in the groups $(\mathbf{Z}/(m))^\times$ to attempt to distinguish between prime m and composite m.

6. Appendix: A Converse to Theorem 4.5

While Theorem 4.5 shows that a product of commuting elements with relatively prime orders has a predictable order, we can ask what can be said if we *start* with $g \in G$ of order n and write $n = n_1 n_2$ where $(n_1, n_2) = 1$. Can we express g as a product of commuting elements with orders n_1 and n_2? If so, are the commuting elements unique? Yes and Yes. That is, Theorem 4.5 admits a strong kind of converse, as follows.

Theorem 6.1. *Let $g \in G$ have order n, where $n = n_1 n_2$ with $(n_1, n_2) = 1$. Then we can write $g = g_1 g_2$ where g_1 has order n_1, g_2 has order n_2, and $g_1 g_2 = g_2 g_1$. Moreover, such g_1 and g_2 are unique in the group G.*

Example 6.2. To concretely illustrate the construction we will give in the proof, we give an example first. Suppose g has order $40 = 5 \cdot 8$. Then $g = g_1 g_2$ where $g_1 = g^{16}$ and $g_2 = g^{-15}$ have respective orders 5 and 8 (using Theorem 3.12). Since g_1 and g_2 are powers of g, they commute!

Remark 6.3. The group in Theorem 6.1 is arbitrary, possibly non-abelian.

Proof. Since $(n_1, n_2) = 1$, $n_1 x + n_2 y = 1$ for some integers x and y. In particular, $n_1 x \equiv 1 \bmod n_2$ and $n_2 y \equiv 1 \bmod n_1$. Then

$$g = g^1 = g^{n_1 x} g^{n_2 y}.$$

By Theorem 3.12, g^{n_1} has order $n/n_1 = n_2$. Since $(x, n_2) = 1$ (why?), $(g^{n_1})^x = g^{n_1 x}$ has order n_2 by Theorem 3.12. Similarly, $g^{n_2 y}$ has order n_1.

Let $g_1 = g^{n_2 y}$ and $g_2 = g^{n_1 x}$. These satisfy the conclusion of the theorem. In particular, g_1 and g_2 commute, since they are powers of g.

Now we treat uniqueness. Suppose

$$g = g_1 g_2 = g_1' g_2',$$

where $g_1, g_2 \in G$ and $g_1', g_2' \in G$ have the relevant properties: g_1 has order n_1, g_2 has order n_2, $g_1 g_2 = g_2 g_1$, and likewise for g_1' and g_2'. We want to show $g_1 = g_1'$ and $g_2 = g_2'$.

Since $g_1 g_2 = g_1' g_2'$, raising to the power n_1 implies $g_2^{n_1} = (g_2')^{n_1}$ (here we need commutativity of g_1 with g_2 and g_1' with g_2'). Raising further to the power x gives $g_2^{n_1 x} = (g_2')^{n_1 x}$. Since g_2 and g_2' both have order n_2 and $n_1 x \equiv 1 \bmod n_2$, we can replace the exponent $n_1 x$ with 1 and find that $g_2 = g_2'$. Then the equation $g_1 g_2 = g_1' g_2'$ implies $g_1 = g_1'$. □

Corollary 6.4. *The unique elements g_1 and g_2 from Theorem 6.1 are powers of g.*

Proof. In the constructive part of the proof of Theorem 6.1, we defined g_1 and g_2 as suitable powers of g. Since the choice of commuting g_1 and g_2 is unique, we're done. □

That g_1 and g_2 commute in Theorem 6.1 is essential in the proof of their uniqueness, and without commutativity we can find additional pairs satisfying the other conditions. For example, in S_9 let

$$g = (124)(35)(6789).$$

The cycles here are disjoint, so g has order $[3, 2, 4] = 12$. We can write 12 as $3 \cdot 4$, and here are two ways of writing g as a product $g_1 g_2$ of an element g_1 of order 3 and an element g_2 of order 4:

$$g_1 = (124), \quad g_2 = (35)(6789)$$

and

$$g_1 = (123), \quad g_2 = (2435)(6789).$$

The first pair commutes while the second pair does not. It is the first pair that is constructed in Theorem 6.1. Notice $(124) = g^4$ and $(35)(6789) = g^{-3}$.