drawn (see FIGURE). This number will of course depend on the particular chord selected but at the end there will be one new region for every chord and one for every intersection. The number of chords is $\binom{n}{2}$ and the number of intersections is $\binom{n}{4}$ as before. Hence the number of regions is $1+\binom{n}{2}+\binom{n}{4}$.

REFERENCES

1. R. K. Guy, The strong law of small numbers, *Amer. Math. Monthly* (1988), 697–712.
2. A. M. Yaglom and I. M. Yaglom, *Challenging Mathematical Problems with Elementary Solutions*, Vol. I, Dover Publications, Mineola, NY, 1987.

On the Order of a Product in a Finite Abelian Group

DIETER JUNGNICKEL
Universität Augsburg
D-86135 Augsburg, F.R. Germany

The following result from elementary group theory is included in virtually every course in abstract algebra:

LEMMA 1. *Let a and b be two elements of a finite abelian group G with orders m and n, respectively. If m and n are co-prime, then the product ab has order mn.*

Lemma 1 can be used to find elements of increasingly larger order in G. This has many interesting applications, both theoretic and algorithmic. One usually applies Lemma 1 to show that G is cyclic if, and only if, its exponent agrees with its order; this result in turn is used to show that a finite subgroup of the multiplicative group of a field is cyclic. (See, e.g., Jacobson [**1**, Theorems 1.4 and 2.18] or van der Waerden [**5**, §§42 and 43].) Lemma 1 is also the basis of the standard algorithm (due to Gauss) for determining primitive elements for finite fields (i.e., generators for the multiplicative groups) and then primitive polynomials, see e.g. Jungnickel [**3**, §2.5]. These are important tasks if one actually wants to perform arithmetic in finite fields, which in turn is fundamental for applications, e.g. in cryptography. See [**3**] (and the references cited there) for more information on this topic.

In some of my algebra classes, students asked the quite natural question: What happens in the situation of Lemma 1 if one drops the hypothesis that m and n are co-prime.* Trivially, $(ab)^{\operatorname{lcm}(m,n)}=1$, so that the order of ab satisfies

$$o(ab)\mid \operatorname{lcm}(m,n). \tag{1}$$

Usually, some student suggests that one should actually have equality in (1). Though this might seem a reasonable conjecture, it is not difficult to find counterexamples. Here is a simple series of such examples.

*I do not know of any textbook treating this question. Weak versions of some of the results below (i.e., Corollary 1, the special case $f=d$ of Lemma 3 and the corresponding construction) were already obtained in [**2**].

Example 1 Let x generate a cyclic group of order $2pq$, where p and q are distinct odd primes, and put $a := x^q$ and $b := x^p$. Then we have $m = 2p$ and $n = 2q$, hence $\operatorname{lcm}(m, n) = 2pq$. But $ab = x^{p+q}$ has order at most (in fact, exactly) pq, since $p + q$ is even.

If one examines Example 1 more closely, one realizes that the groups A and B generated by a and b, respectively, intersect in a subgroup of order 2. Might this be the reason why the order of ab differs from $\operatorname{lcm}(a, b)$ by a factor of 2? As we shall see in the following example, the situation is not quite that simple. (This example can actually be generalized considerably, cf. Theorem 2 below.) Nevertheless, the size of the intersection of A and B indeed plays an important role, as Lemma 2 and Theorem 1 below will indicate.

Example 2 Choose three distinct primes p, q, r and assume $p < q < r$. Let G be a cyclic group of order pqr, generated by the element g, and put $a := g^q$ and $b := g^p$. Then $m = pr$, $n = qr$ and $A \cap B$ has order r; here $ab = g^{p+q}$ has order pqr (since pqr is co-prime with $p + q$). Now select the smallest positive integer x for which $q + xp \equiv 0 \pmod r$ and replace b by $b' := g^{xp}$. Note that

$$q + xp \leq q + (r - 1)p < rq;$$

thus qr cannot divide $q + xp$, and therefore q cannot divide x. Hence b' also has order n, but now ab' has order pq.

LEMMA 2. *Let a and b be two elements of a finite abelian group G with orders m and n, respectively, and put $d :=$ gcd(m, n). Denote the subgroups of G generated by a and b by A and B, respectively, and assume that $A \cap B$ has order s (where s divides d). Then the order of the product ab satisfies the condition*

$$\frac{mn}{ds} \mid o(ab) \mid \frac{mn}{d} = \operatorname{lcm}(m, n). \tag{2}$$

Proof. Write $k := o(ab)$. As noted in (1), k divides $\operatorname{lcm}(m, n)$. Now observe that $(ab)^k = 1$ implies

$$a^k = b^{-k} =: c \in A \cap B. \tag{3}$$

By hypothesis, $A \cap B$ is a cyclic group of order s. Since the unique subgroup of A of order s is generated by $a^{m/s}$, we have $c = a^{xm/s}$ for some positive integer x. In view of (3) this implies

$$k \equiv x\frac{m}{s} \pmod m,$$

and hence m/s divides k. A similar argument (applied to B) shows that n/s also divides k, and therefore $\operatorname{lcm}(m/s, n/s)$ divides k. Using $\gcd(m/s, n/s) = d/s$, one sees that $\operatorname{lcm}(m/s, n/s) = mn/ds$.

COROLLARY 1. *Let a and b be two elements of a finite abelian group G with orders m and n, respectively, and put $d :=$ gcd(m, n). Then the order of the product ab satisfies the condition*

$$\frac{mn}{d^2} \mid o(ab) \mid \frac{mn}{d} = \operatorname{lcm}(m, n). \tag{4}$$

As we will see next, not every integer allowed by the preceding conditions can actually occur as the order of the product ab for a suitable choice of a and b. In the situation of Lemma 2, we have $o(ab) = mn/df$ for some divisor f of s. We now obtain a further condition on f.

LEMMA 3. *Under the assumptions of Lemma* 2, *write* $o(ab) = mn/df$ *for some divisor* f *of* s. *Then* f *satisfies the condition*

$$\gcd(f, m/d) = \gcd(f, n/d) = 1. \tag{5}$$

Proof. We analyze the situation encountered in the proof of Lemma 2 more closely (using the hypothesis $k = mn/df$) and claim that the element c defined in (3) has order f. To see this, write $e' := o(c)$ and note first

$$c^f = a^{kf} = a^{mn/d} = (a^m)^{n/d} = 1,$$

so that e' divides f. On the other hand, c actually belongs to the unique subgroup of order e' of $A \cap B$, and the same argument as in the proof of Lemma 2 (now applied to e' instead of s) shows that $\operatorname{lcm}(m/e', n/e') = mn/de'$ divides $k = mn/df$. Therefore f has to divide e', and we indeed obtain $e' = f$. But the elements of A of order f are precisely the elements of the form $a^{xm/f}$ for some positive integer x that is co-prime with f. Hence we have

$$c = a^k = a^{xm/f} \quad \text{with} \gcd(x, f) = 1,$$

and thus $mn/df \equiv xm/f \pmod m$. This implies $n/d \equiv x \pmod f$, and therefore indeed $\gcd(n/d, f) = 1$. Similarly, we also obtain $\gcd(m/d, f) = 1$.

We can now give the following improved version of Lemma 2.

THEOREM 1. *Let* a *and* b *be two elements of a finite abelian group* G *with orders* m *and* n, *respectively, and put* $d := \gcd(m, n)$. *Denote the subgroups of* G *generated by* a *and* b *by* A *and* B, *respectively, and assume that* $A \cap B$ *has order* s (*where* s *divides* d). *Let* e *be the largest divisor of* s *satisfying condition* (5) *above. Then the order of the product* ab *satisfies*

$$\frac{mn}{de} \mid o(ab) \mid \frac{mn}{d\varepsilon}, \tag{6}$$

where $\varepsilon = 1$ *if* e *is odd and* $\varepsilon = 2$ *otherwise.*

Proof. By Lemma 2, $o(ab) = mn/df$ for some divisor f of s. Since f has to satisfy condition (5), one immediately concludes that $o(ab)$ must be a multiple of mn/de, where e is the largest divisor satisfying condition (5). Regarding the upper bound in (6), we already know that $o(ab)$ divides mn/d. Now assume that e is even; then s and mn/d are likewise even. Since e satisfies condition (5), m/d and n/d are odd. So $a^{mn/2d} = b^{mn/2d}$ is the unique involution in $A \cap B$. This implies $(ab)^{mn/2d} = 1$, proving the assertion.

An algorithm for determining the integer e defined in Theorem 1 can be found in Lüneburg [4, Ch. IV]. We will soon see that Theorem 1 is best possible (for every choice of m, n and s): Both the lower and the upper bound can always be realized. To this purpose we require the following simple auxiliary result that shows that every invertible residue modulo m can be "lifted" to an invertible residue modulo n for an arbitrary multiple n of m.

LEMMA 4. *Let* m *be a positive integer, let* n *be any multiple of* m, *and let* α *be an arbitrary integer that is invertible modulo* m. *Then there exists an integer* β *that is invertible modulo* n *and satisfies* $\alpha \equiv \beta \pmod m$.

Proof. It clearly suffices to consider the case where $n = mp$ for some prime p. By hypothesis, $\gcd(\alpha, m) = 1$; we need to determine an integer β with $\gcd(\beta, mp) = 1$ and $\alpha \equiv \beta \pmod m$. If p divides m or if p does not divide α, we may simply take $\beta := \alpha$. Thus assume that p divides α, but not m. Then we can choose $\beta := \alpha + m$.

THEOREM 2. *Let m, n and s be arbitrary positive integers for which s divides both m and n. Then there exists a finite abelian group G with cyclic subgroups A and B of orders m and n, respectively. $A \cap B$ is a group of sizes and the generators a, a' for A and b, b' for B satisfy*

$$o(ab) = \frac{mn}{de} \quad \textit{and} \quad o(a'b') = \frac{mn}{d\varepsilon}, \tag{7}$$

where d, e and ε are defined as in Theorem 1.

Proof. Let G be the finite abelian group generated by two elements x and y of order m and n, respectively, satisfying the relation $x^{m/s} = y^{n/s} =: c$. (For an explicit construction of this group, see the remark following this proof.) Let A and B be the subgroups of G generated by x and y, respectively. Then the generators of A are precisely the elements of the form $a := x^{\alpha}$, where α is a positive integer satisfying $\gcd(\alpha, m) = 1$; similarly, the generators of B are precisely the elements of the form $b := y^{\beta}$, where β is a positive integer satisfying $\gcd(\beta, n) = 1$. By Theorem 1, mn/de divides $o(ab)$ for every choice of α and β. We first want to select α and β in such a way that equality holds. We compute

$$(ab)^{mn/de} = \left(x^{m/e}\right)^{\alpha n/d} \cdot \left(y^{n/e}\right)^{\beta m/d} = \left(c^{s/e}\right)^{(\alpha n + \beta m)/d}. \tag{8}$$

By hypothesis, $\gcd(e, m/d) = \gcd(e, n/d) = 1$. Thus we can choose positive integers α' and β' with

$$\alpha' \frac{n}{d} \equiv 1 \pmod e \quad \text{and} \quad \beta' \frac{m}{d} \equiv -1 \pmod e.$$

Since e is a common divisor of m and n, Lemma 4 guarantees the existence of positive integers α and β satisfying

$$\alpha \equiv \alpha' \pmod e, \quad \beta \equiv \beta' \pmod e \quad \text{and} \quad \gcd(\alpha, m) = \gcd(\beta, n) = 1.$$

With this choice of α and β, we have

$$(\alpha n + \beta m)/d \equiv (\alpha' n + \beta' m)/d \equiv 0 \pmod e,$$

and thus (8) yields the desired conclusion $(ab)^{mn/de} = 1$, since $c^{s/e}$ has order e. Finally, generators a' and b' satisfying $o(a'b') = mn/d\varepsilon$ can be determined in an analogous way by selecting α' and β' with

$$\alpha' \frac{n}{d} \equiv \beta' \frac{m}{d} \equiv 1 \pmod e.$$

One then obtains

$$(a'b')^{mn/de} = \left(c^{s/e}\right)^{(\alpha n + \beta m)/d} = \left(c^{s/e}\right)^2.$$

This shows $o(a'b') = (mn/de) \cdot o(c^{2s/e})$, which easily gives the assertion.

We remark that the group G used in the proof of Theorem 2 is, of course, uniquely determined by the properties required there. An explicit construction can be given as follows. Let v and w be generators for cyclic groups of orders m and n, respectively, put $H := \langle v \rangle \times \langle w \rangle$, and note that $U := \langle (v^{m/s}, w^{n/s}) \rangle$ is a subgroup of order s of H. Now define

$$G := H/U, \quad x := (v,1)U \quad \text{and} \quad y := (1, w^{-1})U.$$

Then x and y generate groups of orders m and n, respectively, which intersect in a subgroup of order s (generated by $x^{m/s} = y^{n/s} =: c$), since one has

$$x^{m/s}(y^{-1})^{n/s} = (v^{m/s},1)U \cdot (1, w^{n/s})U = (v^{m/s}, w^{n/s})U = U.$$

As a consequence of Theorem 2, we obtain the following result, which gives a complete answer to our original question for all choices of m and n.

THEOREM 3. *Let m and n be arbitrary positive integers, put $d :=$ gcd(m,n), and let k be any positive integer satisfying*

$$\frac{mn}{df} \mid k \mid \frac{mn}{d}, \tag{9}$$

where f is the largest divisor of d for which one has

$$\gcd(f, m/d) = \gcd(f, n/d) = 1. \tag{10}$$

Then there exist a finite abelian group G and elements a and b of G with orders m and n, respectively, such that $o(ab) = k$.

Proof. Note that $k = mn/ds$ for some divisor s of f, and apply Theorem 2 with this choice of s. Because of condition (10), one has $e = s$, and thus the first case of (7) gives the assertion.

REFERENCES

1. N. L. Jacobson, *Basic Algebra I, 2nd edition*, Freeman, San Francisco, 1985.
2. D. Jungnickel, Eine Bemerkung über endliche abelsche Gruppen, *Math. Semesterber.* **34** (1987), 116–120.
3. D. Jungnickel, *Finite fields. Structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993.
4. H. Lüneburg, *On the rational normal form of endomorphisms: A primer to constructive algebra*, Bibliographisches Institut, Mannheim, 1987.
5. B. L. van der Waerden, *Algebra I (8. Auflage)*, Springer, Berlin, 1971.

On Copying a Compact Disk to Cassette Tape: An Integer-Programming Approach

SAUL I. GASS
College of Business and Management
University of Maryland
College Park, MD 20742

1. The musical tape It is always rewarding when a question from a student challenges both the instructor and the class. During a lecture on model formulation using integer variables, a student inquired as to whether there was a model and