Math 345
10-1-2020

Review Problems for Test 2

These problems are provided to help you study. The presence of a problem on this handout does not imply that there *will* be a similar problem on the test. And the absence of a topic does not imply that it *won't* appear on the test.

1. U_n is the set of elements of $\mathbb{Z}_n$ which are relatively prime to n. It is a group under multiplication mod n. Consider, in particular, the group U_{13}.

(a) Find the order of $5 \in U_{13}$.

(b) Find 8^{-1} in U_{13}.

(c) List the elements of the subgroup $\langle 10 \rangle$ of U_{13}.

2. (a) List the elements of the subgroup of $\mathbb{Z}_{24}$ generated by 10.

(b) List the elements of the subgroup $\langle 10 \rangle$ of

$$U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}.$$

3. (a) Find the order of 48 in $\mathbb{Z}_{172}$.

(b) Find the order of 13 in U_{35}.

4. (a) Let G be a group, and let $g \in G$. Prove that if $n > 0$ and $g^n = 1$, then n is a multiple of the order of g.

(b) Suppose that G is a group, $g \in G$, and $g^{12} = 1$. What are the possibilities for the order of g?

5. (a) Find the order of 142 in $\mathbb{Z}_{156}$.

(b) Find an element n in $\mathbb{Z}_{156}$ such that n has order 26 but $n > 78$.

6. (a) Construct a multiplication table for U_{18}, the group of units mod 18.

(b) U_{18} is cyclic. List all the generators of U_{18}.

7. List the elements of all the subgroups of $\mathbb{Z}_{10}$. What elements generate $\mathbb{Z}_{10}$?

8. (a) List the elements of the subgroup of order 12 in $\mathbb{Z}_{24}$.

(b) Find all the generators of the subgroup of order 12 in $\mathbb{Z}_{24}$.

9. Find a generator for the following subgroup of $\mathbb{Z}$:

$$H = \left\{12x + 30y - 33z \;\middle|\; x, y, z \in \mathbb{Z}\right\}.$$

10. Consider the group $\mathbb{Z} \times \mathbb{Z}$ with the operation of componentwise addition. Prove directly that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic by showing that no element of the group is a generator.

11. Consider the integers $\mathbb{Z}$ with the group operation

$$m * n = m + n - 4.$$

Taking for granted that this gives a group structure on $\mathbb{Z}$, prove that $(\mathbb{Z}, *)$ is cyclic by exhibiting a generator. Note: The identity for $(\mathbb{Z}, *)$ is 4, and $n^{-1} = 8 - n$.

12. (a) Give an example of a group G and elements $x, y \in G$, such that x has order 2 and y has order 4, and $\langle x \rangle \cap \langle y \rangle$ has order 2.

Note: Remember that the intersection of two sets consists of the elements commmon to both, and the intersection of subgroups is a subgroup.

(b) Give an example of a group G and elements $x, y \in G$, such that x has order 2 and y has order 4, and $\langle x \rangle \cap \langle y \rangle$ has order 1.

13. Suppose x and y are elements of a group G, x has order 9, and y has order 16. The intersection $\langle x \rangle \cap \langle y \rangle$ is a subgroup of G. What is the order of $\langle x \rangle \cap \langle y \rangle$?

Hint: If A is a subgroup of B, then $|A| \mid |B|$. And $\langle x \rangle \cap \langle y \rangle$ is a subgroup of $\langle x \rangle$ and of $\langle y \rangle$.

14. Reduce $261^{519} \pmod{521}$ to a number in the range $\{0, 1, \ldots, 520\}$. Note: 521 is prime.

15. Reduce $263^{305} \pmod{307}$ to a number in the range $\{0, 1, \ldots 306\}$. Note: 307 is prime.

16. Reduce $448^{217} \pmod{449}$ to a number in the range $\{0, 1, \ldots, 448\}$.

17. Simplify $\dfrac{250!}{63} \pmod{251}$ to a number in the range $\{0, 1, \ldots, 250\}$.

18. Reduce $386! \pmod{389}$ to a number in the range $\{0, 1, \ldots 388\}$. Note: 389 is prime.

19. Prove that $309^{100} + 404^{102} = 1 \pmod{101 \cdot 103}$.

20. List all the elements of A_4 in disjoint cycle notation. For each element, give its order. (Remember that A_4 is the subgroup of S_4 consisting of the **even** permutations.)

21. Write the following permutation as a product of disjoint cycles *and* as a product of transpositions. (Multiply permutations from right to left.)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 6 & 5 & 1 & 3 & 7 & 2 \end{pmatrix}$$

22. (a) What is the order of the permutation $(2\ 6\ 4\ 1)(3\ 5)$?

(b) What is the order of the permutation $(2\ 6\ 1)(1\ 3\ 5\ 4)$?

23. Let X be a set, and let S_X denote the group of permutations of X under function composition.

(a) Suppose $Y \subset X$, and let

$$H = \{\sigma \in S_X \mid \sigma(Y) = Y\}.$$

Thus, H consists of permutations which send Y to itself. Prove that H is a subgroup of S_X.

(b) Suppose $X = \{1, 2, 3, 4\}$ and $Y = \{1, 4\}$. List the permutations in S_4 which send Y to itself.

24. Compute the product of the permutations and write the answer as a product of disjoint cycles. (Multiply the permutations right to left.)

(a) $(1\ 5\ 3\ 4)(4\ 2\ 6)$.

(b) $(1\ 6\ 3)^{-1}(3\ 4\ 2)^2$.

(c) $[(2\ 4)(3\ 4)]^{722}$.

25. Write $(4\ 6\ 7\ 1)$ as a product of transpositions. Is this permutation odd or even?

26. Compute

$$(2\ 4\ 1\ 3)(3\ 5\ 1\ 6)(2\ 4)(2\ 4\ 1\ 3)^{-1}.$$

27. How many elements of S_6 send the set $\{3, 5\}$ into the set $\{3, 5\}$?

28. Let $S_{\mathbb{Z}}$ denote the group of permutations of $\mathbb{Z}$ under function composition. Define

$$H = \left\{\sigma \in S_{\mathbb{Z}} \;\middle|\; \sigma(\mathbb{Z}^+) \subset \mathbb{Z}^+\right\}.$$

Thus, H consists of permutations of the integers which take the positive integers into the positive integers. For example, consider $f : \mathbb{Z} \to \mathbb{Z}$ given by

$$f(x) = x + 3.$$

f is bijective, since its inverse is given by $g(x) = x - 3$. And if $x > 0$, then $f(x) = x + 3 > 0 + 3 = 3$, so $f \in H$.

Check each subgroup axiom as it applies to H. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

29. Find the order of $(44, 36)$ in $\mathbb{Z}_{56} \times \mathbb{Z}_{40}$

30. (a) Find an element of order 12 in $\mathbb{Z}_6 \times \mathbb{Z}_8$.

(b) Prove that there is no element of order 16 in $\mathbb{Z}_6 \times \mathbb{Z}_8$.

31. List the elements of the subgroup $\langle(4, 6)\rangle$ of $\mathbb{Z}_{10} \times \mathbb{Z}_{30}$.

32. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition. Let

$$H = \{(x, y) \mid x, y \in \mathbb{Z} \times \mathbb{Z} \mid 2x = 7y\}.$$

Prove that H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

33. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition. Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by

$$f(x, y) = (2x + 3y, 7x - y).$$

(a) Prove that f is a group map.

(b) Prove that $\ker f = \{(0, 0)\}$.

34. (a) List the elements of the subgroup $\langle(3, 7)\rangle$ in $U_8 \times U_{10}$.

(b) List the elements of the subgroup $\langle 3\rangle \times \langle 7\rangle$ in $U_8 \times U_{10}$.

35. Find a subgroup of order 8 in $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$. Does this group have any elements of order 8?

36. (a) List the elements of order 8 in $\mathbb{Z}_8 \times \mathbb{Z}_6$.

(b) List the elements of order 8 in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

37. Find the primary decomposition and invariant factor decomposition for $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_{75}$.

38. (a) Determine the largest order of an element of $\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{40}$.

(b) Find a specific element of largest order in $\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{40}$.

39. $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ and $\mathbb{Z}_{20}$ are abelian groups of order 20. Explain why they aren't isomorphic.

40. Determine all isomorphism classes of abelian groups of order $2^3 \cdot 3^3$. For each isomorphism class, give the primary decomposition and the corresponding invariant factor decomposition.

41. Suppose G is an abelian group of order 16.

(a) If no element of G has order greater than 2, what are the possible primary decompositions of G?

(b) If G has at least one element of order 8, what are the possible primary decompositions of G?

42. Suppose G is an abelian group of order 1701 and the largest order of an element of G is 63 What are the possible invariant factor decompositions for G?

43. (a) Can $\mathbb{Z}_5$ be isomorphic to the direct product of two of its proper subgroups?

(b) Can $\mathbb{Z}_8$ be isomorphic to the direct product of two of its proper subgroups?

(c) Can S_3 be isomorphic to the direct product of two of its proper subgroups?

44. Suppose A, B, C, and D are groups, all with the operation denoted by multiplication. Suppose that $f : A \to C$ and $g : B \to D$ are group maps. Define $f \times g : A \times B \to C \times D$ by

$$(f \times g)(a, b) = (f(a), g(b)).$$

(a) Prove that $f \times g$ is a group map.

(b) Prove that

$$\ker(f \times g) = \{(a, b) \in A \times B \mid a \in \ker f \quad \text{and} \quad b \in \ker g\}.$$

45. (a) Explain why $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$ are not *identical* as sets.

(b) Show that if G and H are groups, then $G \times H \approx H \times G$.

46. (a) Suppose a group has 48 elements. What are the possiblities for the order of a subgroup of G?

(b) A subgroup of a group contains 7 elements. The subgroup has 3 left cosets. What is the order of the group?

47. List the elements of the cosets of $\langle 11 \rangle$ in U_{30}.

48. List the elements of the cosets of $\langle 8 \rangle$ in $\mathbb{Z}_{12}$.

49. List the elements of the cosets of $\langle (1, (1\ 3)) \rangle$ in $\mathbb{Z}_3 \times S_3$.

50. (a) List the cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

(b) What coset of $4\mathbb{Z}$ contains 771?

Solutions to the Review Problems for Test 2

1. U_n is the set of elements of $\mathbb{Z}_n$ which are relatively prime to n. It is a group under multiplication mod n. Consider, in particular, the group U_{13}.

(a) Find the order of $5 \in U_{13}$.

(b) Find 8^{-1} in U_{13}.

(c) List the elements of the subgroup $\langle 10 \rangle$ of U_{13}.

(a)

$$\begin{aligned} 5^2 &= 12 \pmod{13} \\ 5^3 &= 125 = 8 \pmod{13} \\ 5^4 &= 625 = 1 \pmod{13} \end{aligned}$$

Therefore, the order of 5 is 4.

(b)

13	-	5
8	1	3
5	1	2
3	1	1
2	1	1
1	2	0

$$8 \cdot 5 + 13 \cdot (-3) = 1$$
$$8 \cdot 5 = 1 \pmod{13}$$

Hence, $8^{-1} = 5$ in U_{13}. □

(c)

$$10^2 = 100 = 9 \pmod{13}$$
$$10^3 = 1000 = 12 \pmod{13}$$
$$10^4 = 10000 = 3 \pmod{13}$$
$$10^5 = 100000 = 4 \pmod{13}$$
$$10^6 = 1000000 = 1 \pmod{13}$$

Hence,

$$\langle 10 \rangle = \{1, 10, 9, 12, 3, 4, 1\}. \quad \square$$

---

2. (a) List the elements of the subgroup of $\mathbb{Z}_{24}$ generated by 10.

(b) List the elements of the subgroup $\langle 10 \rangle$ of U_{21}.

(a) I add 10 to itself (mod 24) until I get back to 0:

$$\langle 10 \rangle = \{0, 10, 20, 6, 16, 2, 12, 22, 8, 18, 4, 14\}. \quad \square$$

$$U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}.$$

(b) I multiply 10 by itself (mod 21) until I get back to 1:

$$\langle 10 \rangle = \{1, 10, 16, 13, 4, 19\}. \quad \square$$

---

3. (a) Find the order of 48 in $\mathbb{Z}_{172}$.

(b) Find the order of 13 in U_{35}.

(a) Since $(48, 172) = 4$, the order of 48 is $\dfrac{172}{4} = 43$.

In other words, if you add 48 to itself 43 times, you'll get 0 mod 172, and no smaller multiple of 48 gives 0. □

(b) I don't know that U_{35} is cyclic, so I'll do the computation directly. I raise 13 to successive powers (mod 35) until I get 1, the identity in U_{35}:

$$13^2 = 169 = 29, \quad 13^3 = 2197 = 27, \quad 13^4 = 28561 = 1.$$

Therefore, 13 has order 4 in U_{35}. □

---

4. (a) Let G be a group, and let $g \in G$. Prove that if $n > 0$ and $g^n = 1$, then n is a multiple of the order of g.

(b) Suppose that G is a group, $g \in G$, and $g^{12} = 1$. What are the possibilities for the order of g?

(a) Let m be the order of g, so $a^m = 1$. By the Division Algorithm,

$$n = qm + r, \quad \text{where} \quad 0 \le r < m.$$

Then

$$1 = a^n = a^{qm+r} = (a^m)^q \cdot a^r = 1 \cdot a^r = a^r.$$

Thus, $a^r = 1$. But m is the smallest positive power of a such that $a^m = 1$, and $0 \le r < m$. Therefore, r can't be positive, so $r = 0$. This means that $n = qm$, so n is multiple of the order of g. □

(b) By (a), the order of g must divide 12. Therefore, the order of g could be 1, 2, 3, 4, 6, or 12. □

---

5. (a) Find the order of 142 in $\mathbb{Z}_{156}$.

(b) Find an element n in $\mathbb{Z}_{156}$ such that n has order 26 but $n > 78$.

(a) The order is $\dfrac{156}{(142, 156)} = \dfrac{156}{2} = 78$. □

(b) Since the order of n is $\dfrac{156}{(n, 156)}$, I want

$$\frac{156}{(n, 156)} = 26, \quad \text{or} \quad (n, 156) = \frac{156}{26} = 6.$$

Notice that $156 = 6 \cdot (2 \cdot 13)$. Therefore, I can ensure that $(n, 156) = 6$ by taking a multiple $6k$ of 6 such that k does *not* have 2 or 13 as a factor. I also want $6k > 78$, so $k > 13$. The easiest way to do this is to take k to be a prime number greater than 13; I'll use $k = 17$. Thus, $n = 6k = 6 \cdot 17 = 102$.

Now 102 is greater than 78, and $(102, 156) = 6$, so 102 has order $\dfrac{156}{6} = 26$ in $\mathbb{Z}_{156}$. □

---

6. (a) Construct a multiplication table for U_{18}, the group of units mod 18.

(b) U_{18} is cyclic. List all the generators of U_{18}.

(a)

	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

□

(b) 5 generates U_{18}:

$$\langle 5\rangle = \{1, 5, 7, 17, 13, 11\}.$$

To find the other generator, note that U_{18} is cyclic of order 6. In $\mathbb{Z}_6$, the cyclic group of order 6, the generators are 1 and $-1 = 5$. So the other generator of U_{18} must be $5^{-1} = 11$. $\square$

---

7. List the elements of all the subgroups of $\mathbb{Z}_{10}$. What elements generate $\mathbb{Z}_{10}$?

There is one subgroup of order n for each natural number n dividing 10. Hence, there are subgroups of order 1, 2, 5, and 10. I have

$$\begin{aligned} \langle 1\rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \\ \langle 2\rangle &= \{0, 2, 4, 6, 8\} \\ \langle 5\rangle &= \{0, 5\} \\ \langle 0\rangle &= \{0\} \end{aligned}$$

The generators are 1, 3, 7, and 9: The elements which are relatively prime to 10. $\square$

---

8. (a) List the elements of the subgroup of order 12 in $\mathbb{Z}_{24}$.

(b) Find all the generators of the subgroup of order 12 in $\mathbb{Z}_{24}$.

(a) The subgroup of order 12 in $\mathbb{Z}_{24}$ is

$$\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}. \quad \square$$

(b) Since $\mathbb{Z}_{24}$ is cyclic, the subgroup $\langle 2\rangle$ of order 12 is a cyclic group of order 12.

Now $\mathbb{Z}_{12}$ is cyclic of order 12, and the generators are the elements relatively prime to 12, namely 1, 5, 7, and 11. But $\mathbb{Z}_{12}$ and $\langle 2\rangle$ are isomorphic by the function $f(x) = 2x \pmod{24}$. So the generators of $\langle 2\rangle$ are

$$2 \cdot 1 = 2, \quad 2 \cdot 5 = 10, \quad 2 \cdot 7 = 14, \quad 2 \cdot 11 = 22. \quad \square$$

---

9. Find a generator for the following subgroup of $\mathbb{Z}$:

$$H = \left\{12x + 30y - 33z \;\middle|\; x, y, z \in \mathbb{Z}\right\}.$$

Note that H must be cyclic, since it's a subgroup of $\mathbb{Z}$.

The greatest common divisor of 12, 30, and -33 is 3, so I'll show that 3 generates H:

$$H = \langle 3\rangle.$$

First, if $12x + 30y - 33z \in H$, then

$$12x + 30y - 33z = 3(4x + 10y - 11z) \in \langle 3\rangle.$$

Conversely, note that

$$3 = 12 \cdot 0 + 30 \cdot (-1) - 33 \cdot (-1) \in H.$$

Hence,

$$3n = 12 \cdot 0 + 30 \cdot (-n) - 33 \cdot (-n) \in H.$$

This shows that $\langle 3\rangle \subset H$.

Therefore, $H = \langle 3 \rangle$. $\square$

---

10. Consider the group $\mathbb{Z} \times \mathbb{Z}$ with the operation of componentwise addition. Prove directly that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic by showing that no element of the group is a generator.

No element of the form $(x, 0)$ can generate: If $n \cdot (x, 0) = (1, 1)$, then $(x, 0) = (1, 1)$, and the equality of the second components gives a contradiction. This shows that $(1, 1)$ is not in the subgroup generated by $(x, 0)$, so $\langle (x, 0) \rangle \neq \mathbb{Z} \times \mathbb{Z}$.

A similar argument shows that no element of the form $(0, y)$ can generate.

Assume, then, that (x, y) is a generator, where $x, y \neq 0$. I claim that $(1, 0)$ is not a multiple of (x, y). For if $(1, 0) = n \cdot (x, y)$, then

$$(1, 0) = n \cdot (x, y)$$
$$(1, 0) = (nx, ny)$$

Equating the second components, I get $ny = 0$, so $n = 0$ (since $y \neq 0$). But equating the first components now gives

$$1 = nx = 0 \cdot x = 0.$$

This contradiction shows that $(1, 0)$ is not in the subgroup generated by (x, y), so $\langle (x, y) \rangle \neq \mathbb{Z} \times \mathbb{Z}$.

Therefore, no element of $\mathbb{Z} \times \mathbb{Z}$ generates, so $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. $\square$

---

11. Consider the integers $\mathbb{Z}$ with the group operation

$$m * n = m + n - 4.$$

Taking for granted that this gives a group structure on $\mathbb{Z}$, prove that $(\mathbb{Z}, *)$ is cyclic by exhibiting a generator.

Notice that

$$3 * 3 = 3 + 3 - 4 = 2$$
$$3 * (3 * 3) = 3 * 2 = 3 + 2 - 4 = 1$$
$$3 * (3 * (3 * 3)) = 3 * 1 = 3 + 1 - 4 = 0$$

For $n \geq 1$, write

$$3^n = \overbrace{3 * 3 * \cdots * 3}^{\text{n times}}.$$

The pattern above suggests the formula

$$3^n = 4 - n \quad \text{for} \quad n \geq 1.$$

Since $3^1 = 3$ and $4 - 1 = 3$, the result is true for $n = 1$.

Assume that $3^n = 4 - n$. Then

$$\begin{aligned} 3^{n+1} &= 3 * 3^n \\ &= 3 + 3^n - 4 \\ &= 3 + (4 - n) - 4 \\ &= 3 - n \\ &= 4 - (n + 1) \end{aligned}$$

This proves the result for $n + 1$, so the result is true for all $n \geq 1$ by induction.

As $n = 1, 2, 3, \ldots$, the powers $3^n = 4 - n$ give the numbers $3, 2, 1, 0, -1, \ldots$.

The identity in $(\mathbb{Z}, *)$ is 4, so $3^0 = 4$.

To get the numbers greater than 4, just take inverses. If $n \ge 1$, then

$$3^{-n} = (3^n)^{-1} = (4-n)^{-1} = 8 - (4-n) = 4+n.$$

As $n = 1, 2, 3, \ldots$, the negative powers $3^{-n} = 4+n$ give the numbers $5, 6, 7, \ldots$.
This shows that every element in $\mathbb{Z}$ is a power of 3, so 3 is a generator and $(\mathbb{Z}, *)$ is cyclic. $\square$

---

12. (a) Give an example of a group G and elements $x, y \in G$, such that x has order 2 and y has order 4, and $\langle x \rangle \cap \langle y \rangle$ has order 2.

(b) Give an example of a group G and elements $x, y \in G$, such that x has order 2 and y has order 4, and $\langle x \rangle \cap \langle y \rangle$ has order 1.

(a) In $\mathbb{Z}_4$, the element 1 has order 4 and the element 2 has order 2. I have

$$\langle 1 \rangle = \{0, 1, 2, 3\} \quad \text{and} \quad \langle 2 \rangle = \{0, 2\}.$$

Thus, $\langle 1 \rangle \cap \langle 2 \rangle$ has order 2:

$$\langle 1 \rangle \cap \langle 2 \rangle = \{0, 2\}. \quad \square$$

(b) In $\mathbb{Z}_2 \times \mathbb{Z}_4$, consider the subgroups

$$\langle (1,0) \rangle = \{(0,0), (1,0)\} \quad \text{and} \quad \langle (0,1) \rangle = \{(0,0), (0,1), (0,2), (0,3)\}.$$

Then $(1,0)$ has order 2 and $(0,1)$ has order 4. Moreover,

$$\langle (1,0) \rangle \cap \langle (0,1) \rangle = \{(0,0)\}.$$

So the intersection has order 1.

Here's a more complicated example.

In D_4, the group of symmetries of a square, let r denote rotation through 90° counterclockwise. Then r generates a subgroup of order 4:

$$\langle r \rangle = \{\text{id}, r, r^2, r^3\}.$$

r^2 is rotation through 180°, and r^3 is rotation through 270°.

Let m denote a reflection — say reflection across a line through the center bisecting opposite sides of the square. Then m generates a subgroup of order 2:

$$\langle m \rangle = \{\text{id}, m\}.$$

Now

$$\langle r \rangle \cap \langle m \rangle = \{\text{id}\}.$$

To see that m can't be an element of $\langle r \rangle$, note that m "flips the square over", whereas none of the rotations r, r^2 or r^3 do this. So the two subgroups can't overlap in two elements, because this would mean $m \in \langle r \rangle$.

In this case, the intersection $\langle r \rangle \cap \langle m \rangle$ has order 1. $\square$

---

13. Suppose x and y are elements of a group G, x has order 9, and y has order 16. The intersection $\langle x \rangle \cap \langle y \rangle$ is a subgroup of G. What is the order of $\langle x \rangle \cap \langle y \rangle$?

$\langle x \rangle \cap \langle y \rangle$ is a subgroup of $\langle x \rangle$, which is a cyclic group of order 9. Therefore, the order of $\langle x \rangle \cap \langle y \rangle$ is 1, 3, or 9.

$\langle x\rangle \cap \langle y\rangle$ is a subgroup of $\langle y\rangle$, which is a cyclic group of order 16. Therefore, the order of $\langle x\rangle \cap \langle y\rangle$ is 1, 2, 4, 8, or 16.

The only way of satisfying both of these conditions is if the order of $\langle x\rangle \cap \langle y\rangle$ is 1. □

---

14. Reduce $261^{519} \pmod{521}$ to a number in the range $\{0, 1, \ldots, 520\}$. Note: 521 is prime.

By Fermat's Theorem,

$$261^{520} = 1 \pmod{521}.$$

Let $x = 261^{519} \pmod{521}$. Then

$$\begin{aligned} x &= 261^{519} \pmod{521} \\ 261 \cdot x &= 261 \cdot 261^{519} \pmod{521} \\ 261x &= 261^{520} \pmod{521} \\ 261x &= 1 \pmod{521} \\ 2 \cdot 261x &= 2 \cdot 1 \pmod{521} \\ 522x &= 2 \pmod{521} \\ x &= 2 \pmod{521} \end{aligned}$$

Note: In general, to solve an equation like "$261x = 1 \pmod{521}$", I'd need to find $261^{-1} \pmod{521}$ using the Extended Euclidean algorithm. But I happened to notice that 261 was half of $522 = 1 \pmod{521}$, so I had a shortcut. □

---

15. Reduce $263^{305} \pmod{307}$ to a number in the range $\{0, 1, \ldots 306\}$. Note: 307 is prime.

By Fermat's theorem, $263^{306} = 1 \pmod{307}$. So

$$\begin{aligned} x &= 263^{305} \pmod{307} \\ 263x &= 263^{306} = 1 \pmod{307} \end{aligned}$$

307	-	7
263	1	6
44	5	1
43	1	1
1	43	0

$$\begin{aligned} 6 \cdot 307 + (-7) \cdot 263 &= 1 \\ (-7) \cdot 263 &= 1 \pmod{307} \\ 300 \cdot 263 &= 1 \pmod{307} \end{aligned}$$

Hence, $263^{-1} = 300 \pmod{307}$.
Therefore,

$$\begin{aligned} 300 \cdot 263x &= 300 \cdot 1 \pmod{307} \\ x &= 300 \pmod{307} \end{aligned}$$ □

---

16. Reduce $448^{217} \pmod{449}$ to a number in the range $\{0, 1, \ldots, 448\}$.

Since $448 = -1 \pmod{449}$, I have

$$448^{217} = (-1)^{217} = -1 = 448 \pmod{449}. \quad \square$$

---

17. Simplify $\dfrac{250!}{63} \pmod{251}$ to a number in the range $\{0, 1, \ldots, 250\}$.

By Wilson's theorem, $250! = -1 \pmod{251}$. So

$$x = \frac{250!}{63} \pmod{251}$$
$$63x = 250! = -1 \pmod{251}$$

251	-	4
63	3	1
62	1	1
1	62	0

$$1 = (63, 251) = 4 \cdot 63 + (-1) \cdot 251.$$

It follows that $63^{-1} = 4 \pmod{251}$, so

$$4 \cdot 63x = 4 \cdot (-1) \pmod{251}$$
$$x = -4 = 247 \pmod{251} \quad \square$$

---

18. Reduce $386! \pmod{389}$ to a number in the range $\{0, 1, \ldots 388\}$. Note: 389 is prime.

Let $x = 386! \pmod{389}$. Then

$$x = 386! \pmod{389}$$
$$388 \cdot 387 \cdot x = 388 \cdot 387 \cdot 386! \pmod{389}$$
$$388 \cdot 387 \cdot x = 388! \pmod{389}$$
$$388 \cdot 387 \cdot x = -1 \pmod{389}$$
$$(-1) \cdot (-2) \cdot x = -1 \pmod{389}$$
$$2x = -1 \pmod{389}$$
$$195 \cdot 2x = 195 \cdot -1 \pmod{389}$$
$$390x = -195 \pmod{389}$$
$$x = 194 \pmod{389} \quad \square$$

---

19. Prove that $309^{100} + 404^{102} = 1 \pmod{101 \cdot 103}$.

Since $101 \not| 309$, Fermat's Theorem gives $309^{100} = 1 \pmod{101}$. Since $101 \mid 404$, it follows that

$$309^{100} + 404^{102} = 1 + 0 = 1 \pmod{101}.$$

Similarly, $103 \not| 404$, so Fermat's Theorem gives $404^{102} = 1 \pmod{103}$. Since $103 \mid 309$, it follows that

$$309^{100} + 404^{102} = 0 + 1 = 1 \pmod{103}.$$

Since $309^{100} + 404^{102}$ is congruent to 1 mod 101 and mod 103, and since $(101, 103) = 1$, it follows that

$$309^{100} + 404^{102} = 1 \pmod{101 \cdot 103}. \quad \square$$

---

20. List all the elements of A_4 in disjoint cycle notation. For each element, give its order.

A_4 is the subgroup of even permutations in S_4. This is half of S_4: twelve elements. To list them, note that if a, b, and c are distinct, $(a\ b\ c) = (a\ c)(a\ b)$ is even, and these 3-cycles have order 3. And if the pairs $\{a, b\}$ and $\{c, d\}$ are distinct, then $(a\ b)(c\ d)$ is even, and has order 2. (In particular, such a product of transpositions is different from the 3-cycles mentioned earlier.)

If you simply list all possible 3-cycles and all possible products of disjoint transpositions (and the identity), you wind up with 12 elements — all of A_4.

Element of A_4	Order
id	1
(1 2)(3 4)	2
(1 3)(2 4)	2
(1 4)(2 3)	2
(1 2 3)	3
(1 2 4)	3
(1 3 4)	3
(1 3 2)	3
(1 4 2)	3
(1 4 3)	3
(2 3 4)	3
(2 4 3)	3

$\square$

---

21. Write the following permutation as a product of disjoint cycles *and* as a product of transpositions. (Multiply permutations from right to left.)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 6 & 5 & 1 & 3 & 7 & 2 \end{pmatrix}$$

Right-to-left:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 6 & 5 & 1 & 3 & 7 & 2 \end{pmatrix} = (1\ 4\ 5)(2\ 8)(3\ 6) = (1\ 5)(1\ 4)(2\ 8)(3\ 6). \quad \square$$

---

22. (a) What is the order of the permutation $(2\ 6\ 4\ 1)(3\ 5)$?

(b) What is the order of the permutation (2 6 1)(1 3 5 4)?

(a) (2 6 4 1) has order 4 and (3 5) has order 2. Since the cycles are disjoint, they commute, and the order of the product is the least common multiple of the orders of the factors: $[4, 2] = 4$. □

(b) The cycles are not disjoint, so I have to multiply and write the product in disjoint cycle form first:

	1	2	3	4	5	6
(1 3 5 4)						
	3	2	5	1	4	6
(2 6 1)						
	3	6	5	2	4	1

Thus, (2 6 1)(1 3 5 4) = (1 3 5 4 2 6), and the permutation has order 6. □

---

23. Let X be a set, and let S_X denote the group of permutations of X under function composition.

(a) Suppose $Y \subset X$, and let
$$H = \{\sigma \in S_X \mid \sigma(Y) = Y\}.$$

Thus, H consists of permutations which send Y to itself. Prove that H is a subgroup of S_X.

(b) Suppose $X = \{1, 2, 3, 4\}$ and $Y = \{1, 4\}$. List the permutations in S_4 which send Y to itself.

(a) First, $\text{id}(Y) = Y$, so $\text{id} \in H$.
Suppose $\sigma, \tau \in H$, so $\sigma(Y) = Y$ and $\tau(Y) = Y$. Then

$$(\sigma \cdot \tau)(Y) = \sigma[\tau(Y)] = \sigma(Y) = Y.$$

Hence, $\sigma \cdot \tau \in H$.
Finally, suppose $\sigma \in H$, so $\sigma(Y) = Y$. Then

$$\begin{aligned} \sigma^{-1}[\sigma(Y)] &= \sigma^{-1}(Y) \\ Y &= \sigma^{-1}(Y) \end{aligned}$$

Therefore, $\sigma^{-1} \in H$.
Hence, H is a subgroup of S_X. □

(b) The permutations in S_4 which send Y to itself are id, (1 4), (2 3), and (1 4)(2 3). □

---

24. Compute the product of the permutations and write the answer as a product of disjoint cycles. (Multiply the permutations right to left.)

(a) (1 5 3 4)(4 2 6).

(b) $(1\ 6\ 3)^{-1}(3\ 4\ 2)^2$.

(c) $[(2\ 4)(3\ 4)]^{722}$.

(a)

1	2	3	4	5	6	
						(4 2 6)
1	6	3	2	5	4	
						(1 5 3 4)
5	6	4	2	3	1	

$$(1\ 5\ 3\ 4)(4\ 2\ 6) = (1\ 5\ 3\ 4\ 2\ 6). \quad \square$$

(b)

$$(1\ 6\ 3)^{-1}(3\ 4\ 2)^2 = (3\ 6\ 1)(3\ 2\ 4) = (1\ 3\ 2\ 4\ 6).$$

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & & (3\ 2\ 4) \\ 1 & 4 & 2 & 3 & 5 & 6 \\ & & & & & & (3\ 6\ 1) \\ 3 & 4 & 2 & 6 & 5 & 1 \end{array}$$

(c) First, $(2\ 4)(3\ 4) = (2\ 4\ 3)$.

$$\begin{array}{ccc} 2 & 3 & 4 \\ & & & (3\ 4) \\ 2 & 4 & 3 \\ & & & (2\ 4) \\ 4 & 2 & 3 \end{array}$$

Since $(2\ 4\ 3)$ has order 3,

$$[(2\ 4)(3\ 4)]^{722} = (2\ 4\ 3)^{722} = [(2\ 4\ 3)^3]^{240} \cdot (2\ 4\ 3)^2 = \text{id} \cdot (2\ 4\ 3)^2 = (2\ 3\ 4). \quad \square$$

---

25. Write $(4\ 6\ 7\ 1)$ as a product of transpositions. Is this permutation odd or even?

$$(4\ 6\ 7\ 1) = (4\ 1)(4\ 7)(4\ 6).$$

Since it's a product of 3 transpositions, it is odd. $\square$

---

26. Compute

$$(2\ 4\ 1\ 3)(3\ 5\ 1\ 6)(2\ 4)(2\ 4\ 1\ 3)^{-1}.$$

You can do this directly by multiplying out the permutations.

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ & & & & & & (3\ 1\ 4\ 2) \\ 4 & 3 & 1 & 2 & 5 & 6 \\ & & & & & & (2\ 4) \\ 2 & 3 & 1 & 4 & 5 & 6 \\ & & & & & & (3\ 5\ 1\ 6) \\ 2 & 5 & 6 & 4 & 1 & 3 \\ & & & & & & (2\ 4\ 1\ 3) \\ 4 & 5 & 6 & 1 & 3 & 2 \end{array}$$

Alternatively, you can use the following fact about the conjugate of a cycle by a permutation: If σ and τ are permutations and τ is written as a product of cycles, then $\sigma\tau\sigma^{-1}$ can be found by applying σ to the elements of the cycles in τ.

That is, just apply $(2\ 4\ 1\ 3)$ to each of the numbers in $(3\ 5\ 1\ 6)$, then to each of the numbers in $(2\ 4)$. This gives

$$(2\ 4\ 1\ 3)(3\ 5\ 1\ 6)(2\ 4)(2\ 4\ 1\ 3)^{-1} = (2\ 5\ 3\ 6)(4\ 1). \quad \square$$

---

27. How many elements of S_6 send the set $\{3,5\}$ into the set $\{3,5\}$?

Let $\sigma \in S_6$ be a permutation which sends the set $\{3,5\}$ into the set $\{3,5\}$. Since permutations are injective, different elements must go to different places. Thus, either

$$\sigma(3) = 3 \quad \text{and} \quad \sigma(5) = 5, \quad \text{or} \quad \sigma(3) = 5 \quad \text{and} \quad \sigma(5) = 3.$$

That is, there are two possibilities.
σ also permutes the elements $\{1,2,4,6\}$ among themselves. There are $4! = 24$ such permutations.
Therefore, there are a total of $24 \cdot 2 = 48$ elements of S_6 which send the set $\{3,5\}$ into the set $\{3,5\}$. □

---

28. Let $S_{\mathbb{Z}}$ denote the group of permutations of $\mathbb{Z}$ under function composition. Define

$$H = \left\{\sigma \in S_{\mathbb{Z}} \,\middle|\, \sigma(\mathbb{Z}^+) \subset \mathbb{Z}^+\right\}.$$

(H is the set of permutations of the set of integers that take positive integers to positive integers.)
Check each subgroup axiom as it applies to H. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

Suppose that $\tau, \sigma \in H$, so $\tau(\mathbb{Z}^+) \subset \mathbb{Z}^+$ and $\sigma(\mathbb{Z}^+) \subset \mathbb{Z}^+$. Then

$$(\tau \cdot \sigma)(\mathbb{Z}^+) = \tau(\sigma(\mathbb{Z}^+)) \subset \tau(\mathbb{Z}^+) \subset \mathbb{Z}^+.$$

Therefore, $\tau \cdot \sigma \in H$.
Since $\text{id}(\mathbb{Z}^+) = \mathbb{Z}^+ \subset \mathbb{Z}^+$, it follows that $\text{id} \in H$.
Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by

$$f(n) = n + 1.$$

f is bijective: Its inverse is $f^{-1}(n) = n - 1$. Thus, $f \in S_{\mathbb{Z}}$. Moreover, if $n \in \mathbb{Z}^+$, then $n > 0$, so

$$f(n) = n + 1 > 0 + 1 = 1.$$

Hence, $f(n) \in \mathbb{Z}^+$, and so $f(\mathbb{Z}^+) \subset \mathbb{Z}^+$. Thus, $f \in H$.
However, $f^{-1} \notin H$, since $f^{-1}(1) = 0 \notin \mathbb{Z}^+$.
Thus, H is not a subgroup of $S_{\mathbb{Z}}$. □

---

29. Find the order of $(44, 36)$ in $\mathbb{Z}_{56} \times \mathbb{Z}_{40}$.

The order of 44 in $\mathbb{Z}_{56}$ is

$$\frac{56}{(56,44)} = \frac{56}{4} = 14.$$

The order of 36 in $\mathbb{Z}_{40}$ is

$$\frac{40}{(40,36)} = \frac{40}{4} = 10.$$

Hence, the order of $(44, 36)$ in $\mathbb{Z}_{56} \times \mathbb{Z}_{40}$ is $[14, 10] = 70$. □

---

30. (a) Find an element of order 12 in $\mathbb{Z}_6 \times \mathbb{Z}_8$.

(b) Prove that there is no element of order 16 in $\mathbb{Z}_6 \times \mathbb{Z}_8$.

(a) 2 has order 3 in $\mathbb{Z}_6$ and 2 has order 4 in $\mathbb{Z}_8$, so $(2,2)$ has order $[3,4] = 12$ in $\mathbb{Z}_6 \times \mathbb{Z}_8$. □

(b) Let $(a,b) \in \mathbb{Z}_6 \times \mathbb{Z}_8$. Suppose a has order m in $\mathbb{Z}_6$ and b has order n in $\mathbb{Z}_8$. The order of (a,b) is $[m,n]$.
Assume that $[m,n] = 16$.
The divisors of 6 and 8 are

$$6:\ 1,\ 2,\ 3,\ 6$$

$$8:\ 1,\ 2,\ 4,\ 8$$

Thus, $m \in \{1,2,3,6\}$ and $n \in \{1,2,4,8\}$.
If $m = 3$ or $m = 6$, then $3 \mid m \mid [m,n] = 16$, which is a contradiction. Hence, $m = 1$ or $m = 2$.
If $m = 1$, then

$$16 = [m,n] = [1,n] = n.$$

But 16 is not a divisor of 8, as n is assumed to be. This is a contradiction.
Finally, suppose $m = 2$. Since there are only 4 possibilities for n, I'll just check cases:

$$[2,1] = 2, \quad [2,2] = 2, \quad [2,4] = 4, \quad [2,8] = 8.$$

In no case do I have $[m,n] = 16$.
This final contradiction shows that no element of $\mathbb{Z}_6 \times \mathbb{Z}_8$ has order 16. □

---

31. List the elements of the subgroup $\langle (4,6) \rangle$ of $\mathbb{Z}_{10} \times \mathbb{Z}_{30}$.

$$\langle (4,6) \rangle = \{(0,0),(4,6),(8,12),(2,18),(6,24)\}. \quad □$$

---

32. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition. Let

$$H = \{(x,y) \mid x,y \in \mathbb{Z} \times \mathbb{Z} \mid 2x = 7y\}.$$

Prove that H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

Since $2 \cdot 0 = 0 = 7 \cdot 0$, it follows that $(0,0) \in H$.
Suppose $(x,y) \in H$. Then

$$\begin{aligned} 2x &= 7y \\ -2x &= -7y \\ 2(-x) &= 7(-y) \end{aligned}$$

Hence,

$$-(x,y) = (-x,-y) \in H.$$

Suppose $(a,b),(c,d) \in H$. Then

$$2a = 7b \quad \text{and} \quad 2c = 7d.$$

Hence,

$$\begin{aligned} 2a + 2c &= 7b + 7d \\ 2(a+c) &= 7(b+d) \end{aligned}$$

Therefore,

$$(a,b) + (c,d) = (a+c, b+d) \in H. \quad □$$

---

33. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition. Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by

$$f(x, y) = (2x + 3y, 7x - y).$$

(a) Prove that f is a group map.

(b) Prove that $\ker f = \{(0, 0)\}$.

(a) A direct computation:

$$f[(a, b)+(c, d)] = f(a+c, b+d) = (2(a+c)+3(b+d), 7(a+c)-(b+d) = (2a+2c+3b+3d, 7a+7c-b-d) =$$

$$((2a + 3b) + (2c + 3d), (7a - b) + (7c - d) = (2a + 3b, 7a - b) + (2c + 3d, 7c - d) = f(a, b) + f(c, d).$$

Alternatively, note that f can be represented using matrix multiplication:

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 3 \\ 7 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Write

$$A = \begin{bmatrix} 2 & 3 \\ 7 & -1 \end{bmatrix}, \quad u = \begin{bmatrix} a \\ b \end{bmatrix}, \quad v = \begin{bmatrix} c \\ d \end{bmatrix}.$$

Then by properties of matrix multiplication,

$$f(u + v) = A(u + v) = Au + Av = f(u) + f(v). \quad \square$$

(b) Suppose $(x, y) \in \ker f$. Then

$$f(x, y) = (2x + 3y, 7x - y) = (0, 0).$$

Hence,

$$2x + 3y = 0, \quad 7x - y = 0.$$

Multiply the second equation by 3 and add it to the first equation:

$$\begin{array}{r} 2x + 3y = 0 \\ \underline{21x - 3y = 0} \\ 23x = 0 \\ x = 0 \end{array}$$

Plugging this into $7x - y = 0$ gives $-y = 0$, so $y = 0$. Therefore, $(x, y) = (0, 0)$. Hence, $\ker f = \{(0, 0)\}$.
$\square$

---

34. (a) List the elements of the subgroup $\langle(3, 7)\rangle$ in $U_8 \times U_{10}$.

(b) List the elements of the subgroup $\langle 3\rangle \times \langle 7\rangle$ in $U_8 \times U_{10}$.

Note that the operations are multiplication mod 8 in U_8 and multiplication mod 10 in U_{10}.

(a) $\langle(3, 7)\rangle$ consists of powers of $(3, 7)$.

$$\langle(3, 7)\rangle = \{(1, 1), (3, 7), (1, 9), (3, 3)\}. \quad \square$$

(b) First,

$$\langle 3\rangle = \{1, 3\} \quad \text{in} \quad U_8.$$

$$\langle 7\rangle = \{1, 7, 9, 3\} \quad \text{in} \quad U_{10}.$$

$\langle 3\rangle \times \langle 7\rangle$ consists of pairs where the first component is in $\langle 3\rangle$ and the second component is in $\langle 7\rangle$:

$$\langle 3\rangle \times \langle 7\rangle = \{(1,1), (1,7), (1,9), (1,3), (3,1), (3,7), (3,9), (3,3)\}. \quad \square$$

Note that the answers to (a) and (b) are different!

---

35. Find a subgroup of order 8 in $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$. Does this group have any elements of order 8?

Since $8 \not| 12$ and $8 \not| 14$, neither $\mathbb{Z}_{12}$ nor $\mathbb{Z}_{14}$ has a subgroup of order 8.

But I can get a subgroup of order 8 by taking the product of a subgroup of order 4 in $\mathbb{Z}_{12}$ and a subgroup of order 2 in $\mathbb{Z}_{14}$. Thus, $\langle 3\rangle \times \langle 7\rangle$ is a subgroup of order 8 in $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$.

If $(a, b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{14}$, then the order of (a, b) is $[\text{ord}(a), \text{ord}(b)]$. But $\text{ord}(a) \mid 12$, so $\text{ord}(a) = 1, 2, 3, 4, 6, 12$, and $\text{ord}(b) \mid 14$, so $\text{ord}(b) = 1, 2, 7, 14$. No combination of these numbers will give $[\text{ord}(a), \text{ord}(b)] = 8$. Hence, there are no elements of order 8. $\square$

---

36. (a) List the elements of order 8 in $\mathbb{Z}_8 \times \mathbb{Z}_6$.

(b) List the elements of order 8 in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

(a) Let $\text{ord}(x)$ denote the order of x. If $(a, b) \in \mathbb{Z}_8 \times \mathbb{Z}_6$, then the order of (a, b) is $[\text{ord}(a), \text{ord}(b)]$. Suppose $[\text{ord}(a), \text{ord}(b)] = 8$. By Lagrange's theorem, I also have

$$\text{ord}(a) \mid 8 \quad \text{and} \quad \text{ord}(b) \mid 6.$$

Thus, $\text{ord}(a) = 1, 2, 4, 8$ and $\text{ord}(b) = 1, 2, 3, 6$. Of the 16 possible combinations of values, the ones that give $[\text{ord}(a), \text{ord}(b)] = 8$ are

$$\text{ord}(a) = 8 \quad \text{and} \quad \text{ord}(b) = 1, 2.$$

The elements of order 8 in $\mathbb{Z}_8$ are 1, 3, 5, and 7.

The elements of order 1 or 2 in $\mathbb{Z}_6$ are 0 and 3.

Thus, the elements of order 8 in $\mathbb{Z}_8 \times \mathbb{Z}_6$ are

$$(1,0), \quad (3,0), \quad (5,0), \quad (7,0), \quad (1,3), \quad (3,3), \quad (5,3), \quad (7,3). \quad \square$$

(b) Let $\text{ord}(x)$ denote the order of x. If $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, then the order of (a, b) is $[\text{ord}(a), \text{ord}(b)]$. Suppose $[\text{ord}(a), \text{ord}(b)] = 8$. By Lagrange's theorem, I also have

$$\text{ord}(a) \mid 4 \quad \text{and} \quad \text{ord}(b) \mid 6.$$

Thus, $\text{ord}(a) = 1, 2, 4$ and $\text{ord}(b) = 1, 2, 3, 6$. Of the 12 possible combinations of values, no combination gives $[\text{ord}(a), \text{ord}(b)] = 8$. Hence, $\mathbb{Z}_4 \times \mathbb{Z}_6$ has no elements of order 8. $\square$

---

37. Find the primary decomposition and invariant factor decomposition for $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_{75}$.

The primary decomposition is

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}.$$

$$\begin{array}{cc} 2 & 4 \\ 3 & 3 \\ & 25 \\ \hline 2 & 300 \end{array}$$

The invariant factor decomposition is $\mathbb{Z}_6 \times \mathbb{Z}_{300}$. □

---

38. (a) Determine the largest order of an element of $\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{40}$.

(b) Find a specific element of largest order in $\mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}_{40}$.

(a) The largest possible order of an element is

$$[10, 15, 40] = 120.$$

Alternative method: The primary decomposition is

$$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_5.$$

From this, I find that the invariant factor decomposition is

$$\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{120}.$$

The top factor is $\mathbb{Z}_{120}$, so the largest order of an element is 120. □

(b) $(1, 1, 1)$ is an element of order $[10, 15, 40] = 120$. □

---

39. $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ and $\mathbb{Z}_{20}$ are abelian groups of order 20. Explain why they aren't isomorphic.

$\mathbb{Z}_{20}$ has elements of order 20 — for instance, 1 has order 20.
If $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_{10}$, then

$$10 \cdot (x, y) = (10x, 10y) = (0, 0).$$

Therefore, no element of $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ has order greater than 10.
Therefore, $\mathbb{Z}_2 \times \mathbb{Z}_{10}$ and $\mathbb{Z}_{20}$ aren't isomorphic. □

---

40. Determine all isomorphism classes of abelian groups of order $2^3 \cdot 3^3$. For each isomorphism class, give the primary decomposition and the corresponding invariant factor decomposition.

Factor 2^3 and 3^3 into prime powers:

$$2^3: \quad 2^3, 2 \cdot 2^2, 2 \cdot 2 \cdot 2$$

$$3^3: \quad 3^3, 3 \cdot 3^2, 3 \cdot 3 \cdot 3$$

The primary decompositions and their corresponding invariant factor decompositions are:

Primary decomposition	Invariant factor decomposition
$\mathbb{Z}_8 \times \mathbb{Z}_{27}$	$\mathbb{Z}_{216}$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_9$	$\mathbb{Z}_3 \times \mathbb{Z}_{72}$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{24}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{27}$	$\mathbb{Z}_2 \times \mathbb{Z}_{108}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9$	$\mathbb{Z}_6 \times \mathbb{Z}_{36}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{54}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$	$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{18}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_6$

□

---

41. Suppose G is an abelian group of order 16.

(a) If no element of G has order greater than 2, what are the possible primary decompositions of G?

(b) If G has at least one element of order 8, what are the possible primary decompositions of G?

(a) The primary decompositions for abelian groups of order 16 are

$$\mathbb{Z}_{16}, \quad \mathbb{Z}_2 \times \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

$1 \in \mathbb{Z}_{16}$ has order 16, $(0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_8$ has order 8, $(1,1) \in \mathbb{Z}_4 \times \mathbb{Z}_4$ has order 4, and $(0,0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ has order 4. So if no element of G has order greater than 2, then G cannot be isomorphic to any of the first four groups.

On the other hand, if $(a,b,c,d) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, then

$$2(a,b,c,d) = (0,0,0,0).$$

This proves that every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order at most 2. Therefore, if no element of G has order greater than 2, the primary decomposition of G is

$$G \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2. \quad \square$$

(b) If $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_4$, then $4(a,b) = (0,0)$.

Therefore, elements of $\mathbb{Z}_4 \times \mathbb{Z}_4$ have order at most 4.

If $(a,b,c) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$4(a,b,c) = (0,0,0).$$

Therefore, elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ have order at most 4.

I already showed that elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ have order at most 2.

Therefore, if G has at least one element of order 8, G cannot be isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

On the other hand, $2 \in \mathbb{Z}_{16}$ has order 8, and $(0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_8$ has order 8. These groups *do* have elements of order 8.

Hence, if G has at least one element of order 8, the possible primary decompositions of G are

$$\mathbb{Z}_{16} \quad \text{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_8. \quad \square$$

---

42. Suppose G is an abelian group of order 1701 and the largest order of an element of G is 63 What are the possible invariant factor decompositions for G?

It would be really tedious to list all the possible invariant factor decompositions for groups of order 1701. However, this isn't necessary.

Note that $\dfrac{1701}{63} = 27$. The invariant factor decomposition for G has the form

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n} \times \mathbb{Z}_{63}.$$

Here $d_1 \mid d_2 \mid \cdots \mid d_n \mid 63$ and $d_1 d_2 \cdots d_n = 27$.

The possible factorizations of 27 are $3 \cdot 3 \cdot 3$, $3 \cdot 9$, and 27. Now $27 \not| 63$, so the last one is ruled out. The possible invariant factor decompositions are

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{63} \quad \text{and} \quad \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{63}. \quad \square$$

43. (a) Can $\mathbb{Z}_5$ be isomorphic to the direct product of two of its proper subgroups?

(b) Can $\mathbb{Z}_8$ be isomorphic to the direct product of two of its proper subgroups?

(c) Can S_3 be isomorphic to the direct product of two of its proper subgroups?

(a) $\mathbb{Z}_5$ does not have any proper subgroups, so it can't be isomorphic to the direct product of two of its proper subgroups. $\square$

(b) Suppose $\mathbb{Z}_8$ is isomorphic to $A \times B$, where A and B are proper subgroups of $\mathbb{Z}_8$. Then one of A, B has order 2, while the other has order 4. Suppose without loss of generality that $|A| = 2$ and $|B| = 4$.

Using multiplicative notation, $x^2 = 1$ for all $x \in A$, while $y^4 = 1$ for all $y \in B$. Then if $(x, y) \in A \times B$,

$$(x, y)^4 = (x^4, y^4) = (1, 1).$$

Therefore, elements of $A \times B$ have order no greater than 4.

However, $\mathbb{Z}_8$ has elements of order 8 (such as 1).

This contradiction proves that $\mathbb{Z}_8$ can't be isomorphic to the direct product of two of its proper subgroups. $\square$

(c) Proper subgroups of S_3 have order 2 or 3, so they're isomorphic to $\mathbb{Z}_2$ (order 2) or $\mathbb{Z}_3$ (order 3). Both $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are abelian, and the product of abelian groups is abelian — but S_3 is nonabelian. So S_3 can't be isomorphic to the direct product of two of its proper subgroups. $\square$

---

44. Suppose A, B, C, and D are groups, all with the operation denoted by multiplication. Suppose that $f : A \to C$ and $g : B \to D$ are group maps. Define $f \times g : A \times B \to C \times D$ by

$$(f \times g)(a, b) = (f(a), g(b)).$$

(a) Prove that $f \times g$ is a group map.

(b) Prove that

$$\ker(f \times g) = \{(a, b) \in A \times B \mid a \in \ker f \quad \text{and} \quad b \in \ker g\}.$$

flushpar (a) Let $(a, b), (c, d) \in A \times B$. Then

$$(f \times g)\left[(a, b) \cdot (c, d)\right] = (f \times g)(ac, bd) = (f(ac), g(bd)) = (f(a)f(c), g(b)g(d)) =$$

$$(f(a), g(b)) \cdot (f(c), g(d)) = (f \times g)(a, b) \cdot (f \times g)(c, d).$$

Therefore, $f \times g$ is a group map. $\square$

(b) Let $(a, b) \in \ker(f \times g)$. By definition,

$$(f \times g)(a, b) = (1, 1), \quad \text{so} \quad (f(a), g(b)) = (1, 1), \quad \text{hence} \quad f(a) = 1 \quad \text{and} \quad g(b) = 1.$$

$f(a) = 1$ means $a \in \ker f$ and $g(b) = 1$ means $b \in \ker g$. Therefore,

$$(a, b) \in \{(a, b) \in A \times B \mid a \in \ker f \quad \text{and} \quad b \in \ker g\}.$$

Conversely, suppose

$$(a, b) \in \{(a, b) \in A \times B \mid a \in \ker f \quad \text{and} \quad b \in \ker g\}.$$

$a \in \ker f$ means $f(a) = 1$, and $b \in kerg$ means $g(b) = 1$. Therefore,

$$(f(a), g(b)) = (1, 1), \quad \text{so} \quad (f \times g)(a, b) = (1, 1).$$

Hence, $(a, b) \in \ker(f \times g)$.
Since each of the sets is contained in the other, it follows that

$$\ker(f \times g) = \{(a, b) \in A \times B \mid a \in \ker f \quad \text{and} \quad b \in \ker g\}. \quad \square$$

---

45. (a) Explain why $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_2$ are not *identical* as sets.

(b) Show that if G and H are groups, then $G \times H \approx H \times G$.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_3$ consists of ordered pairs (x, y), where $x \in \mathbb{Z}_2$ and $y \in \mathbb{Z}_3$. $\mathbb{Z}_3 \times \mathbb{Z}_2$ consists of ordered pairs (x, y), where $x \in \mathbb{Z}_3$ and $y \in \mathbb{Z}_2$.

Thus, for example, an element $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ can't be an element of $\mathbb{Z}_3 \times \mathbb{Z}_2$: x is an element of $\mathbb{Z}_2$, but to be in $\mathbb{Z}_3 \times \mathbb{Z}_2$ it should be an element of $\mathbb{Z}_3$. $\square$

(b) Define $f : G \times H \to H \times G$ by

$$f(g, h) = (h, g) \quad \text{for} \quad g \in G, \quad h \in H.$$

f is a group map: If $a, c \in G$ and $b, d \in H$, then

$$f((a, b)(c, d)) = f(ac, bd) = (bd, ac) = (b, a)(d, c) = f(a, b)f(c, d).$$

Define $g : H \times G \to G \times H$ by

$$g(h, g) = (g, h) \quad \text{for} \quad g \in G, \quad h \in H.$$

Then

$$f[g(h, g)] = f(g, h) = (h, g),$$
$$g[f(g, h)] = g(h, g) = (g, h).$$

Therefore, f and g are inverses. Thus, f is bijective, so f is an isomorphism. $\square$

---

46. (a) Suppose a group has 48 elements. What are the possiblities for the order of a subgroup of G?

(b) A subgroup of a group contains 7 elements. The subgroup has 3 left cosets. What is the order of the group?

(a) By Lagrange's theorem, the order of a subgroup must divide the order of the group. Therefore, a subgroup of a group of order 48 can have 1, 2, 3, 4, 6, 8, 12, 16, 24, or 48 elements. $\square$

(b) By Lagrange's theorem, the order of a group equals the order of a subgroup times the index of the subgroup — i.e. the number of left or right cosets. Therefore, the group has order $7 \cdot 3 = 21$ elements. $\square$

---

47. List the elements of the cosets of $\langle 11 \rangle$ in U_{30}.

$$\begin{aligned} \langle 11 \rangle &= \{1, 11\} \\ 7 \cdot \langle 11 \rangle &= \{7, 17\} \\ 13 \cdot \langle 11 \rangle &= \{13, 23\} \\ 19 \cdot \langle 11 \rangle &= \{19, 29\} \end{aligned} \quad \square$$

48. List the elements of the cosets of $\langle 8 \rangle$ in $\mathbb{Z}_{12}$.

$$\begin{aligned} \langle 8 \rangle &= \{0, 8, 4\} \\ 1 + \langle 8 \rangle &= \{1, 9, 5\} \\ 2 + \langle 8 \rangle &= \{2, 10, 6\} \\ 3 + \langle 8 \rangle &= \{3, 11, 7\} \end{aligned} \quad \square$$

49. List the elements of the cosets of $\langle (1, (1\ 3)) \rangle$ in $\mathbb{Z}_3 \times S_3$.

Remember that the operation is addition mod 3 in the first component and permutation multiplication (right to left) in the second. For example,

$$(0, (1\ 2)) \cdot (2, (1\ 3)) = (0 + 2, (1\ 2)(1\ 3)) = (2, (1\ 3\ 2)).$$

The cosets are

$$\begin{aligned} \langle (1, (1\ 3)) \rangle &= \{(0, \text{id}), (1, (1\ 3)), (2, \text{id}), (0, (1\ 3)), (1, \text{id}), (2, (1\ 3))\} \\ (0, (1\ 2) \cdot \langle (1, (1\ 3)) \rangle &= \{(0, (1\ 2)), (1, (1\ 3\ 2)), (2, (1\ 2)), (0, (1\ 3\ 2)), (1, (1\ 2)), (2, (1\ 3\ 2))\} \\ (0, (2\ 3) \cdot \langle (1, (1\ 3)) \rangle &= \{(0, (2\ 3)), (1, (1\ 2\ 3)), (2, (2\ 3)), (0, (1\ 2\ 3)), (1, (2\ 3)), (2, (1\ 2\ 3))\} \end{aligned} \quad \square$$

50. (a) List the cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

(b) What coset of $4\mathbb{Z}$ contains 771?

(a)

$$4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

$$1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$

$$2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$

$$3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}. \quad \square$$

(b) Since $771 = 3 \pmod{4}$, I have $771 \in 3 + 4\mathbb{Z}$. $\square$

We are all special cases. - Albert Camus