Math 345/504
2–4–2018

Review Sheet for Test 1

These problems are provided to help you study. The presence of a problem on this sheet does not imply that there will be a similar problem on the test, and the absence of a topic from this sheet does not imply that the topic will not appear on the test.

1. A binary operation is defined on $\mathbb{Z}$ by

$$a * b = a^2 + b^2.$$

(a) Prove or disprove: $*$ is associative.

(b) Prove or disprove: $*$ is commutative.

(c) Prove or disprove: $*$ has an identity element.

2. Use the associative law (for 3 elements at a time) to show that if G is a group and $a, b, c \in G$, then

$$(a \cdot b) \cdot (c \cdot d) = a \cdot ((b \cdot c) \cdot d).$$

3. Let p be a prime number.

(a) How many elements of $\mathbb{Z}_p$ have multiplicative inverses?

(b) How many elements of $\mathbb{Z}_{p^2}$ have multiplicative inverses?

4. For each set below, check the axioms for a group. If an axiom is violated, give a specific counterexample.

(a) The set $\{1, 3, 7, 9\}$ under multiplication mod 10.

(b) The set of 2×2 matrices with real entries under matrix multiplication.

(c) The set of positive integers under multiplication.

(d) The set of integers under the operation $x * y = xy + 1$.

(e) The set of rational numbers under division.

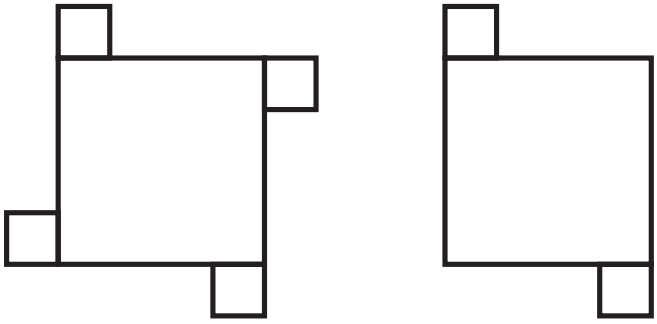
(f) The following set of 2×2 matrices under matrix addition:

$$G = \left\{ \begin{bmatrix} x & x \\ y & y \end{bmatrix} \;\middle|\; x, y \in \mathbb{Z} \right\}.$$

(g) The set of all pairs of real numbers (a, b), where $a, b \neq 0$, under the operation

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

5. Describe the symmetries of each of the following figures.



(a) (b)

6. Let G be a group and let $a, b, c \in G$. Simplify the following expressions as much as possible:

(a) $a^{-1}(ab^3)^2b^{-4}$

(b) $b(a^{-1}b)^{-2}a^{-1}$.

(c) $(ab^2)^{-1}(ba^2)^{-1}$.

(d) $(abc)^2c^{-1}b^{-1}a^{-5}$.

7. Let G be a group and let $a, b, x \in G$. Solve the following equation for x:

$$a^2b^{-1}x(ab)^2 = a^3b^{-3}aba^2b.$$

8. Let a and b be elements of a group G, with $a \neq b$. Suppose that the integers m and n are relatively prime. Prove that either $a^m \neq b^m$ or $a^n \neq b^n$.

9. (a) Give an example of a finite nonabelian group.

(b) Give an example of an infinite group which is not countable.

10. Let G be a group, let $a, b \in G$, and suppose that $ab = ba$. Prove that for all $n \geq 1$,

$$ab^n = b^n a.$$

11. (a) Find the inverse of $\begin{bmatrix} 2 & 6 \\ 1 & 5 \end{bmatrix}$ in the group $GL(2, \mathbb{Z}_7)$.

(b) Explain why $GL(2, \mathbb{Z}_7)$ is *not* a group under addition.

12. In each case, a group and a subset of the group are given. Check each axiom for a subgroup as applied to the subset. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

(a) The subset $H = \{\ldots, -3\sqrt{2}, -2\sqrt{2}, -\sqrt{2}, 0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots\}$ of the group $\mathbb{R}$ of real numbers under addition.

(b) The following subset of $GL(2, \mathbb{R})$:

$$K = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \;\middle|\; ad = 1 \right\}.$$

(c) The subset J of the group $\mathbb{R}^2$ under vector addition consisting of vectors $\langle a, b \rangle$ which satisfy $a = b^2$.

(d) The subset $H = \{x \in G \mid x^2 = 1\}$ in an abelian group G.

(e) The subset $P = \{(x, y, z) \in \mathbb{Z}^3 \mid 3x + 4y = 5z\}$. ($\mathbb{Z}^3$ is a group under component-wise addition [i.e. vector addition].)

(f) The subset $K = \{A \in M(2, \mathbb{R}) \mid ABA = 0\}$, where $B \in M(2, \mathbb{R})$ is a fixed matrix and 0 denotes the 2×2 zero matrix.

13. Suppose that G is a group, H is a subgroup of G, and $g \in G$. Let

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Prove that gHg^{-1} is a subgroup of G.

14. Suppose H and K are subgroups of a group G, and suppose that

$$hk = kh \quad \text{for all} \quad h \in H \quad \text{and} \quad k \in K.$$

Define

$$HK = \{hk \mid h \in H \quad \text{and} \quad k \in K\}.$$

Prove that HK is a subgroup of G.

15. Consider the following function $f : \mathbb{Z}_3 \to \mathbb{Z}_4$:

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 2.$$

Is f a group homomorphism?

16. In each case, determine whether the function is a homomorphism.

(a) $\mathbb{R}[x]$ is the group of polynomials with real coefficients under polynomial addition and $g : \mathbb{R}[x] \to (\mathbb{R}, +)$ is defined by

$$g(\phi(x)) = \phi(1).$$

(So, for example, if $\phi(x) = x^2 - 4x + 7$, then $g(\phi(x)) = 1^2 - 4 \cdot 1 + 7 = 4$.)

(b) $h : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by

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

(c) $\phi : \mathbb{Z} \times \mathbb{Z} \to (\mathbb{Z}, +)$ is defined by

$$\phi(x, y) = 2x + 3y.$$

(Here $\mathbb{Z} \times \mathbb{Z}$ is a group under component-wise addition [i.e. "vector addition"], so $(a, b) + (c, d) = (a + c, b + d)$.)

(d) $\det : GL(n, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$ is the determinant function, $GL(n, \mathbb{R})$ is the group of invertible $n \times n$ real matrices under matrix multiplication, and $\mathbb{R}^*$ is the group of nonzero real numbers under multiplication.

(e) $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$ is defined by

$$f(x) = x^2 - 1.$$

17. The function $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ defined by $f(x) = 3x \pmod{12}$ is a group map.

(a) Find $\ker f$.

(b) Find $\operatorname{im} f$.

(c) Find $f^{-1}(\{6\})$.

Note: Remember that $f^{-1}(\{6\})$ is the set of elements which f takes to 6. What elements produce 6 as an output when they're plugged into f?

18. Define $f : \mathbb{R}^* \to \mathbb{R}^*$ by

$$f(x) = x^2.$$

($\mathbb{R}^*$ is the group of nonzero reals under multiplication.)

(a) Prove that f is a group map.

(b) Find $\ker f$ and $\operatorname{im} f$.

19. Define $f : \mathbb{Z}_3 \to \mathbb{Z}_8$ by $f(x) = 5x \pmod{8}$. Is f a group map?

20. Let G and H be groups, and let $\phi : G \to H$ be a group map. Let $g \in G$. Prove that if g has finite order, then the order of $\phi(g)$ divides the order of g.

21. $\mathbb{R}$ is a group under the operation

$$a * b = a + b - 2.$$

Define $f : (\mathbb{R}, +) \to (\mathbb{R}, *)$ by

$$f(x) = x + 2.$$

Show that f is an isomorphism.

22. Prove that if $f : G \to H$ is an invertible group map, then f^{-1} is a group map. (Thus, if f is an isomorphism, then its inverse is as well.)

23. Suppose n and x are integers, $n > 0$,

$$n \mid 2x + 5 \quad \text{and} \quad n \mid 3x + 4.$$

Prove that $n = 1$ or $n = 7$.

24. Suppose that n and x are integers, n is odd,

$$n \mid 2x + 1 \quad \text{and} \quad n \mid 2x + 3.$$

Prove that $n = 1$.

25. Find the greatest common divisor of 3462 and 118 and write it as a linear combination of 3462 and 118 with integer coefficients.

26. Use the Extended Euclidean Algorithm to find 49^{-1} in $\mathbb{Z}_{61}$.

27. Prove that if m is an integer, then $(6m + 4, 5m + 3) = 1$ or 2. Give specific values of m which show that both cases can occur.

28. Prove that if $a, b \in \mathbb{Z}$, then $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$.

29. If two integers differ by 1000, can they both be divisible by 7?

30. Find the greatest common divisor and the least common multiple of $p^3q^{10}r^2$ and p^5q^7, where p, q, and r are distinct primes.

31. If p, q, and r are distinct prime numbers, how many positive divisors does pqr have?

32. (a) For what integers n is $n^2 - 3n + 2$ prime?

(b) Calvin Butterball says: "Since $n^2 + 2n + 2$ doesn't factor, $n^2 + 2n + 2$ is always prime." Is Calvin correct?

33. Suppose $a, b, c \in \mathbb{Z}$ and $c \mid ab$. Prove that $c \mid (a, c)(b, c)$.

34. Suppose x and n are positive integers. Prove that

$$(x - 1)^2 \mid x^n - nx(x - 1) - 1.$$

35. Prove that if $n \geq 1$, then

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2.$$

36. Prove that there is no integer x such that $78x = 61 \pmod{91}$.

37. Solve the equation $34x + 63 = 191 \pmod{225}$.

38. Compute $\displaystyle\sum_{n=1}^{100} n! \pmod 8$.

39. Recall that

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Suppose p is an odd prime. Compute

$$\binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p-1} + \binom{p}{p} \pmod{p}.$$

40. Prove that if $n \in \mathbb{Z}$, then $n^3 + 3n + 5$ is not divisible by 7.

41. Prove that there are no integers m and n such that $11m^2 - 4n^2 = 33$.

42. Solve the following modular equation and simplify your answer to a number in the range $\{0, 1, \ldots, 60\}$.

$$8x + 55 = 14(2x + 3) \pmod{61}.$$

43. (a) Prove that the following equation has no solutions:

$$6x = 7 \pmod{12}.$$

(b) Bonzo McTavish says that the following equation has no solutions:

$$2x = 6 \pmod{10}.$$

Bonzo says: "In the last problem, 6 and 12 weren't relatively prime, so you couldn't find $6^{-1} \pmod{12}$ and that's why the equation had no solutions. In this problem, 2 and 10 aren't relatively prime, so this equation has no solutions, either."

Show that Bonzo is incorrect.

Solutions to the Review Sheet for Test 1

1. A binary operation is defined on $\mathbb{Z}$ by

$$a * b = a^2 + b^2.$$

(a) Prove or disprove: $*$ is associative.

(b) Prove or disprove: $*$ is commutative.

(c) Prove or disprove: $*$ has an identity element.

(a)

$$(1 * 2) * 3 = (1 + 4) * 3 = 5 * 3 = 25 + 9 = 34,$$

$$1 * (2 * 3) = 1 * (4 + 9) = 1 * 13 = 1 + 169 = 170.$$

Since $(1 * 2) * 3 \neq 1 * (2 * 3)$, it follows that $*$ is not associative. □

(b) Let $a, b \in \mathbb{Z}$. Then

$$a * b = a^2 + b^2 = b^2 + a^2 = b * a.$$

Hence, $*$ is commutative. □

(c) Suppose e is an identity for $*$. Then in particular, $e * (-1) = -1$. But

$$e * (-1) = e^2 + (-1)^2 = e^2 + 1 > 0.$$

Hence, $e * (-1) \neq -1$. This contradiction shows that there is no identity element for $*$. □

---

2. Use the associative law (for 3 elements at a time) to show that if G is a group and $a, b, c \in G$, then

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

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

(The associative law (for 3 elements at a time) can be used to show that "any two groupings" of a product are equal — but usually, this kind of verification is omitted as being obvious and tedious. But you should understand by example how you could get from one such grouping to another by regrouping 3 elements at a time. □

---

3. Let p be a prime number.

(a) How many elements of $\mathbb{Z}_p$ have multiplicative inverses?

(b) How many elements of $\mathbb{Z}_{p^2}$ have multiplicative inverses?

(a) The elements in $\mathbb{Z}_p$ which have multiplicative inverses are the elements which are relatively prime to p. Since p is prime, 1, 2, ..., $p-1$ are all relatively prime to p. Therefore, these $p-1$ elements of $\mathbb{Z}_p$ have multiplicative inverses. □

(b) The elements in $\mathbb{Z}_{p^2}$ which have multiplicative inverses are the elements which are relatively prime to p^2. I'll count the number of elements which are *not* relatively prime to p^2 and subtract this from p^2, the number of elements in $\mathbb{Z}_{p^2}$.

If $n \in \mathbb{Z}_{p^2}$ is *not* relatively prime to p^2, then it must have a common factor with p^2 other than 1. The only factors of p^2 other than 1 are p and p^2, and both of these are divisible by the prime p. Thus, $n \in \mathbb{Z}_{p^2}$ is *not* relatively prime to p^2 if and only if it's divisible by p.

What elements of $\mathbb{Z}_{p^2}$ are divisible by p? Here are the multiples of p:

$$0, \quad p, \quad 2p, \quad 3p, \ldots, (p-1)p.$$

There are p of them; that is, there are p elements of $\mathbb{Z}_{p^2}$ which are *not* relatively prime to p^2. Hence, there are $p^2 - p$ elements which are relatively prime to p^2 — and therefore, $p^2 - p$ elements which have multiplicative inverses.

Here's a specific example. Suppose $p = 3$. In $\mathbb{Z}_9$, the elements which are relatively prime to 3 are

$$1, \quad 2, \quad 4, \quad 5, \quad 7, \quad 8.$$

There are 6 of them, and $6 = 3^2 - 3$. □

---

4. For each set below, check the axioms for a group. If an axiom is violated, give a specific counterexample.

(a) The set $\{1, 3, 7, 9\}$ under multiplication mod 10.

(b) The set of 2×2 matrices with real entries under matrix multiplication.

(c) The set of positive integers under multiplication.

(d) The set of integers under the operation $x * y = xy + 1$.

(e) The set of rational numbers under division.

(f) The following set of 2×2 matrices under matrix addition:

$$G = \left\{ \begin{bmatrix} x & x \\ y & y \end{bmatrix} \;\middle|\; x, y \in \mathbb{Z} \right\}.$$

(g) The set of all pairs of real numbers (a, b), where $a, b \neq 0$, under the operation

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

(a) Here's the multiplication table:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The table shows that set is closed under the operation. Multiplication of integers is associative, so this multiplication is associative. The element 1 is an identity for the operation. Finally, every element has an inverse: $1^{-1} = 1$, $3^{-1} = 7$, $7^{-1} = 3$, and $9^{-1} = 9$.

Therefore, the set is a group under the operation. □

(b) The set is closed under the operation, and matrix multiplication is associative. The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity element for matrix multiplication.

However, not every element has a multiplicative inverse. From linear algebra, you know that a matrix is invertible if and only if its determinant is nonzero. So, for example, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ does not have a multiplicative inverse, because its determinant is 0.

The set is *not* a group under matrix multiplication.

As an aside, this is why when people refer to the *group* of all 2×2 matrices, they *can't* mean the operation to be *multiplication*. They probably mean the operation to be matrix *addition* — and you can check that this set *is* a group under matrix addition.

In the same way, when someone refers to "the group of integers", the operation *can't* be multiplication, and most likely is addition. □

(c) The set of positive integers is closed under multiplication, multiplication of integers is associative, and the positive integer 1 is an identity element for multiplication.

However, most positive integers do not have multiplicative inverses. For example, there is no positive integer x such that $2 \cdot x = 1$.

The set is *not* a group under multiplication. □

(d) If x and y are integers, so is $xy + 1$. The set is closed under the operation.

Let $x, y, z \in \mathbb{Z}$. Then

$$(x * y) * z = (xy + 1) * z = (xy + 1)z + 1 = xyz + z + 1,$$

$$x * (y * z) = x * (yz + 1) = x(yz + 1) + 1 = xyz + x + 1.$$

These are not equal in general. In particular, note that

$$(2 * 3) * 4 = 24 + 4 + 1 = 29 \quad \text{while} \quad 2 * (3 * 4) = 24 + 2 + 1 = 27.$$

Thus, $(2 * 3) * 4 \neq 2 * (3 * 4)$. The operation is not associative.

I'll work backwards to guess an identity for the operation. If e is an identity for $*$, then in particular $e * 3 = 3$. This means that

$$e \cdot 3 + 1 = 3, \quad \text{or} \quad 3e = 2.$$

But this equation has no solutions in $\mathbb{Z}$. Hence, the operation can't have an identity element.

Since there is no identity element, I can't consider the existence of inverses.
$\mathbb{Z}$ is not a group under $*$. □

(e) Division is not a binary operation on the set of rational numbers, because it isn't defined for *all* pairs of rationals. For example, you can't divide 42 by 0. Therefore, this does not give a group structure on $\mathbb{Q}$. □

(f) If you add two elements of G, you get another element of G:

$$\begin{bmatrix} x_1 & x_1 \\ y_1 & y_1 \end{bmatrix} + \begin{bmatrix} x_2 & x_2 \\ y_2 & y_2 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 & x_1 + x_2 \\ y_1 + y_2 & y_1 + y_2 \end{bmatrix}.$$

Therefore, matrix addition is a binary operation on G.
I'll take for granted that matrix addition is associative.
The identity for matrix addition is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and this is an element of G.
Finally, if $\begin{bmatrix} x & x \\ y & y \end{bmatrix} \in G$, its additive inverse is also in G:

$$-\begin{bmatrix} x & x \\ y & y \end{bmatrix} = \begin{bmatrix} -x & -x \\ -y & -y \end{bmatrix} \in G.$$

Therefore, G is a group under matrix addition. □

(g) If a, b, c, and d are nonzero real numbers, then so are ac and bd. Therefore, the definition gives a binary operation on the set.
I have

$$[(a,b)\cdot(c,d)]\cdot(e,f) = (ac,bd)\cdot(e,f) = (ace,bdf),$$
$$(a,b)\cdot[(c,d)\cdot(e,f)] = (a,b)\cdot(ce,df) = (ace,bdf).$$

Therefore, the operation is associative.
I also have

$$(1,1)\cdot(a,b) = (a,b) \quad \text{and} \quad (a,b)\cdot(1,1) = (a,b).$$

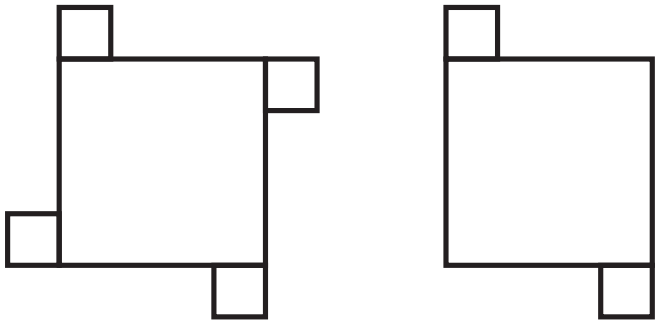
Therefore, $(1,1)$ is the identity element for the operation.
If (a,b) is in the set, then $a, b \neq 0$. Hence, $\frac{1}{a}$ and $\frac{1}{b}$ are defined. I have

$$(a,b)\cdot\left(\frac{1}{a},\frac{1}{b}\right) = (1,1) \quad \text{and} \quad \left(\frac{1}{a},\frac{1}{b}\right)\cdot(a,b) = (1,1).$$

Hence, $(a,b)^{-1} = \left(\frac{1}{a},\frac{1}{b}\right)$.
Therefore, the set is a group under the operation. □

---

5. Describe the symmetries of each of the following figures.



(a) (b)

Figure (a) has four symmetries: The identity, and rotations through 90°, 180°, and 270°.

Figure (b) has two symmetries: The identity and rotation through 180°. □

---

6. Let G be a group and let $a, b, c \in G$. Simplify the following expressions as much as possible:

(a) $a^{-1}(ab^3)^2b^{-4}$

(b) $b(a^{-1}b)^{-2}a^{-1}$.

(c) $(ab^2)^{-1}(ba^2)^{-1}$.

(d) $(abc)^2c^{-1}b^{-1}a^{-5}$.

(a)
$$a^{-1}(ab^3)^2b^{-4} = a^{-1}ab^3ab^3b^{-4} = b^3ab^{-1}. \quad \square$$

(b)
$$b(a^{-1}b)^{-2}a^{-1} = b[(a^{-1}b)^{-1}]^2a^{-1} = b(b^{-1}a)^2a^{-1} = bb^{-1}ab^{-1}aa^{-1} = ab^{-1}. \quad \square$$

(c)
$$(ab^2)^{-1}(ba^2)^{-1} = b^{-2}a^{-1}a^{-2}b^{-1} = b^{-2}a^{-3}b^{-1}. \quad \square$$

(d)
$$(abc)^2c^{-1}b^{-1}a^{-5} = (abc)(abc)c^{-1}b^{-1}a^{-5} = abcabb^{-1}a^{-5} = abcaa^{-5} = abca^{-4}. \quad \square$$

---

7. Let G be a group and let $a, b, x \in G$. Solve the following equation for x:

$$a^2b^{-1}x(ab)^2 = a^3b^{-3}aba^2b.$$

$$\begin{aligned}
a^2b^{-1}x(ab)^2 &= a^3b^{-3}aba^2b \\
ba^{-2}a^2b^{-1}x(ab)^2 &= ba^{-2}a^3b^{-3}aba^2b \\
x(ab)^2 &= bab^{-3}aba^2b \\
xabab &= bab^{-3}aba^2b \\
xababb^{-1}a^{-1}b^{-1}a^{-1} &= bab^{-3}aba^2bb^{-1}a^{-1}b^{-1}a^{-1} \\
x &= bab^{-3}abab^{-1}a^{-1} \quad \square
\end{aligned}$$

---

8. Let a and b be elements of a group G, with $a \neq b$. Suppose that the integers m and n are relatively prime. Prove that either $a^m \neq b^m$ or $a^n \neq b^n$.

Suppose on the contrary that $a \neq b$, but both $a^m = b^m$ and $a^n = b^n$. Since $(m, n) = 1$, there are integers s and t such that

$$sm + tn = 1.$$

Then

$$\begin{aligned}
(a^m)^s &= (b^m)^s \\
a^{sm} &= b^{sm}
\end{aligned}$$

Likewise,

$$\begin{aligned}
(a^n)^t &= (b^n)^t \\
a^{tn} &= b^{tn}
\end{aligned}$$

So

$$a^{sm} \cdot a^{tn} = b^{sm} \cdot b^{tn}$$
$$a^{ms+nt} = b^{ms+nt}$$
$$a = b$$

This contradicts $a \neq b$.
Hence,either $a^m \neq b^m$ or $a^n \neq b^n$. □

---

9. (a) Give an example of a finite nonabelian group.

(b) Give an example of an infinite group which is not countable.

(a) D_3, the group of symmetries of an equilateral triangle, is a nonabelian group of order 6. □

(b) $(\mathbb{R}, +)$, the group of real numbers under addition, is an infinite group of uncountable cardinality. □

---

10. Let G be a group, let $a, b \in G$, and suppose that $ab = ba$. Prove that for all $n \geq 1$,

$$ab^n = b^n a.$$

I'll use induction on n. For $n = 1$, the result says $ab = ba$, which is true by assumption.
Suppose that $n > 1$, and suppose that the result is true for $n - 1$:

$$ab^{n-1} = b^{n-1}a.$$

I need to prove the result for n. I have

$$\begin{array}{rcll} ab^n & = & ab^{n-1} \cdot b & (\text{Since } b^n = b^{n-1}b) \\ & = & b^{n-1}ab & (\text{By induction}) \\ & = & b^{n-1}ba & (\text{Since } ab = ba) \\ & = & b^n a & (\text{Since } b^n = b^{n-1}b) \end{array}$$

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

---

11. (a) Find the inverse of $\begin{bmatrix} 2 & 6 \\ 1 & 5 \end{bmatrix}$ in the group $GL(2, \mathbb{Z}_7)$.
(b) Explain why $GL(2, \mathbb{Z}_7)$ is *not* a group under addition.

(a)

$$\begin{bmatrix} 2 & 6 \\ 1 & 5 \end{bmatrix}^{-1} = (2 \cdot 5 - 6 \cdot 1)^{-1} \begin{bmatrix} 5 & 1 \\ 6 & 2 \end{bmatrix} = 4^{-1} \begin{bmatrix} 5 & 1 \\ 6 & 2 \end{bmatrix} = 2 \cdot \begin{bmatrix} 5 & 1 \\ 6 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 5 & 4 \end{bmatrix}. \quad \square$$

(b) $GL(2, \mathbb{Z}_7)$ is not closed under addition. For example,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix} \in GL(2, \mathbb{Z}_7), \quad \text{but} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \notin GL(2, \mathbb{Z}_7). \quad \square$$

---

12. In each case, a group and a subset of the group are given. Check each axiom for a subgroup as applied to the subset. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

(a) The subset $H = \{\ldots, -3\sqrt{2}, -2\sqrt{2}, -\sqrt{2}, 0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots\}$ of the group $\mathbb{R}$ of real numbers under addition.

(b) The following subset of $GL(2,\mathbb{R})$:

$$K = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \;\middle|\; ad = 1 \right\}.$$

(c) The subset J of the group $\mathbb{R}^2$ under vector addition consisting of vectors $\langle a, b\rangle$ which satisfy $a = b^2$.

(d) The subset $H = \{x \in G \mid x^2 = 1\}$ in an abelian group G.

(e) The subset $P = \{(x, y, z) \in \mathbb{Z}^3 \mid 3x + 4y = 5z\}$. ($\mathbb{Z}^3$ is a group under component-wise addition [i.e. vector addition].)

(f) The subset $K = \{A \in M(2,\mathbb{R}) \mid ABA = 0\}$, where $B \in M(2,\mathbb{R})$ is a fixed matrix and 0 denotes the 2×2 zero matrix.

(a) Elements of the subset have the form $n\sqrt{2}$, where n is an integer.
If m and n are integers, then

$$m\sqrt{2} + n\sqrt{2} = (m + n)\sqrt{2} \in H.$$

Therefore, H is closed under the group operation.
$0 = 0\sqrt{2} \in H$, so the identity element of $\mathbb{R}$ is contained in H.
Finally, if $n\sqrt{2} \in H$, its additive inverse $-n\sqrt{2}$ is also in H.
Hence, H is a subgroup of $\mathbb{R}$. □

(b) Suppose $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, \begin{bmatrix} a' & 0 \\ 0 & d' \end{bmatrix} \in K$, so $ad = 1$ and $a'd' = 1$. Their product is

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & 0 \\ 0 & d' \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ 0 & dd' \end{bmatrix}.$$

$$(aa')(dd') = (ad)(a'd') = 1 \cdot 1 = 1.$$

Hence, the product is in K. Therefore, K is closed under the operation.
The identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ of $GL(2,\mathbb{R})$ is in K, since $1 \cdot 1 = 1$.
If $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in K$, its inverse is

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{d} \end{bmatrix}.$$

Now $ad = 1$, so $\left(\frac{1}{a}\right)\left(\frac{1}{d}\right) = \frac{1}{ad} = 1$. Hence, the inverse is in K.
Therefore, K is a subgroup of $GL(2,\mathbb{R})$. □

(c) J is not closed under vector addition. $\langle 1, 1\rangle$ is in the set, since $1 = 1^2$; $\langle 4, 2\rangle$ is in the set, since $4 = 2^2$. But since $5 \neq 3^2$,

$$\langle 1, 1\rangle + \langle 4, 2\rangle = \langle 5, 3\rangle \notin J.$$

The identity vector $\langle 0, 0\rangle$ is in J, since $0 = 0^2$.
The vector $\langle 1, 1\rangle$ is in the set, since $1 = 1^2$. However, its additive inverse $-\langle 1, 1\rangle = \langle -1, -1\rangle$ is not in the set, since $-1 \neq (-1)^2$.
J is not a subgroup of $\mathbb{R}^2$. □

(d) An element is in H if it squares to the identity.

Suppose $x, y \in H$. This means that $x^2 = 1$ and $y^2 = 1$. I want to show that $xy \in H$. I'll square it and see if I get 1:

$$(xy)^2 = xyxy = xxyy = x^2y^2 = 1 \cdot 1 = 1.$$

(The second equality used the fact that G is abelian.) This proves that $xy \in H$, so H is closed under the operation.

$1^2 = 1$, so $1 \in H$.

Finally, suppose $x \in H$, so $x^2 = 1$. I want to show that $x^{-1} \in H$. I'll square it and see if I get 1:

$$(x^{-1})^2 = x^{-2} = (x^2)^{-1} = 1^{-1} = 1.$$

Therefore, $x^{-1} \in H$, and H is closed under taking inverses.

Hence, H is a subgroup of G. □

(e) Let $(x, y, z), (x', y', z') \in P$. I have to show that

$$(x, y, z) + (x', y', z') = (x + x', y + y', z + z') \in P.$$

Since $(x, y, z), (x', y', z') \in P$, I have

$$3x + 4y = 5z \quad \text{and} \quad 3x' + 4y' = 5z'.$$

So

$$(3x + 4y) + (3x' + 4y') = 5z + 5z', \quad \text{and} \quad 3(x + x') + 4(y + y') = 5(z + z').$$

Therefore, $(x + x', y + y', z + z') \in P$.

Since $3 \cdot 0 + 4 \cdot 0 = 5 \cdot 0$, it follows that $(0, 0, 0) \in P$.

Finally, suppose $(x, y, z) \in P$. I have to show that

$$-(x, y, z) = (-x, -y, -z) \in P.$$

Since $(x, y, z) \in P$, I have $3x + 4y = 5z$. So

$$-(3x + 4y) = -5z, \quad \text{and} \quad 3(-x) + 4(-y) = 5(-z).$$

Therefore, $(-x, -y, -z) \in P$.

Hence, P is a subgroup of $\mathbb{Z}^3$. □

(f) Let $A, A' \in K$. I want to show that $A + A' \in K$. Since $A, A' \in K$, I have

$$ABA = 0 \quad \text{and} \quad A'BA' = 0.$$

Hence,

$$ABA + A'BA' = 0$$
$$(A + A')B(A + A') = 0$$

Therefore, $A + A' \in K$.

The identity for matrix addition is the zero matrix 0. Since $0 \cdot B \cdot 0 = 0$, it follows that $0 \in K$.

Finally, let $A \in K$. I need to show that $-A \in K$. Since $A \in K$, I have $ABA = 0$. Therefore,

$$(-1)ABA(-1) = (-1)0(-1), \quad \text{so} \quad (-A)B(-A) = 0.$$

(In the first equality, I'm multiplying both sides of $ABA = 0$ by the **numbers** -1 and -1.) Thus, $-A \in K$.

Hence, K is a subgroup of $M(2, \mathbb{R})$. □

---

13. Suppose that G is a group, H is a subgroup of G, and $g \in G$. Let

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Prove that gHg^{-1} is a subgroup of G.

gHg^{-1} consists of all elements of the form g(something in H)g^{-1}.
Let $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, where $h_1, h_2 \in H$. Then

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1}.$$

Since $h_1h_2 \in H$ — H is a subgroup, so it's closed under products — it follows that $g(h_1h_2)g^{-1} \in gHg^{-1}$. Therefore, gHg^{-1} is closed under products.
Since $1 \in H$, $g(1)g^{-1} \in gHg^{-1}$. But $g(1)g^{-1} = 1$, so $1 \in gHg^{-1}$. Thus, gHg^{-1} contains the identity.
Suppose $ghg^{-1} \in gHg^{-1}$, where $h \in H$. The inverse is

$$(ghg^{-1})^{-1} = gh^{-1}g^{-1}.$$

$h^{-1} \in H$, since H is a subgroup (and therefore closed under taking inverses). Therefore, $gh^{-1}g^{-1} \in gHg^{-1}$, and gHg^{-1} is closed under taking inverses.
Therefore, gHg^{-1} is a subgroup of G. □

---

14. Suppose H and K are subgroups of a group G, and suppose that

$$hk = kh \quad \text{for all} \quad h \in H \quad \text{and} \quad k \in K.$$

Define

$$HK = \{hk \mid h \in H \quad \text{and} \quad k \in K\}.$$

Prove that HK is a subgroup of G.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. h_1k_1 and h_2k_2 are two typical elements of HK; I must show that their product is in HK. But by assumption, anything in H commutes with anything in K. So $k_1h_2 = h_2k_1$, and

$$(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2) \in HK.$$

Since $1 \in H$ and $1 \in K$, $1 = 1 \cdot 1 \in HK$.
Let $h \in H$ and $k \in K$. Since h^{-1} and k^{-1} commute, I have

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK.$$

Therefore, HK is a subgroup of G. □

---

15. Consider the following function $f : \mathbb{Z}_3 \to \mathbb{Z}_4$:

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 2.$$

Is f a group homomorphism?

f is not a homomorphism! For instance,

$$f(1) + f(2) = 1 + 2 = 3, \quad \text{while} \quad f(1 + 2) = f(0) = 0.$$

Beware of assuming that a simple-looking function must be a group map! □

16. In each case, determine whether the function is a homomorphism.

(a) $\mathbb{R}[x]$ is the group of polynomials with real coefficients under polynomial addition and $g : \mathbb{R}[x] \to (\mathbb{R}, +)$ is defined by

$$g(\phi(x)) = \phi(1).$$

(b) $h : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by

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

(c) $\phi : \mathbb{Z} \times \mathbb{Z} \to (\mathbb{Z}, +)$ is defined by

$$\phi(x, y) = 2x + 3y.$$

(Here $\mathbb{Z} \times \mathbb{Z}$ is a group under component-wise addition [i.e. "vector addition"], so $(a, b) + (c, d) = (a + c, b + d)$.)

(d) $\det : GL(n, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$ is the determinant function, $GL(n, \mathbb{R})$ is the group of invertible $n \times n$ real matrices under matrix multiplication, and $\mathbb{R}^*$ is the group of nonzero real numbers under multiplication.

(e) $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$ is defined by

$$f(x) = x^2 - 1.$$

(a) If $\phi(x)$ and $\psi(x)$ are polynomials, then

$$g(\phi(x) + \psi(x)) = \phi(1) + \psi(1),$$

$$g(\phi(x)) + g(\psi(x)) = \phi(1) + \psi(1).$$

Therefore, $g(\phi(x) + \psi(x)) = g(\phi(x)) + g(\psi(x))$, so g is a homomorphism.
Note that I could have used any number in place of 1. □

(b) It's often useful to check whether the function takes the identity to the identity; if it *doesn't*, then the function is not a homomorphism.

In this case, $h(0) = 0 \cdot 1 = 0$, so h takes the identity to the identity. However, this doesn't prove that h is a homomorphism.

In fact,

$$h(2 + 3) = h(5) = 5 \cdot 6 = 30, \quad \text{but} \quad h(2) + h(3) = 2 \cdot 3 + 3 \cdot 4 = 18.$$

Therefore, $h(2 + 3) \neq h(2) + h(3)$, so h is *not* a homomorphism. □

(c) Let $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$\phi((a, b) + (c, d)) = \phi(a + c, b + d) = 2(a + c) + 3(b + d) = (2a + 3b) + (2c + 3d) = \phi(a, b) + \phi(c, d).$$

Therefore, ϕ is a group map. □

(d) Let $A, B \in GL(n, \mathbb{R})$. From linear algebra, the determinant of a product is the product of the determinants, so

$$\det(AB) = (\det A)(\det B).$$

Hence, det is a group map. □

(e) I have

$$f(2 \cdot 3) = f(6) = 6^2 - 1 = 35, \quad \text{but} \quad f(2) + f(3) = (2^2 - 1) + (3^2 - 1) = 3 + 8 = 11.$$

Since $f(2 \cdot 3) \neq f(2) + f(3)$, it follows that f is not a group map. □

17. The function $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ defined by $f(x) = 3x \pmod{12}$ is a group map.

(a) Find $\ker f$.

(b) Find $\operatorname{im} f$.

(c) Find $f^{-1}(\{6\})$.

(a) $x \in \ker f$ if and only if $3x = 0 \pmod{12}$. But $3x = 0 \pmod{12}$ is equivalent to $12 \mid 3x$, or $4 \mid x$. Thus,

$$\ker f = \{0, 4, 8\}. \quad \square$$

(b)

$$\operatorname{im} f = \{0, 3, 6, 9\}. \quad \square$$

(c) $x \in f^{-1}(\{6\})$ is equivalent to $f(x) = 6$, or $3x = 6 \pmod{12}$. This is equivalent to $12 \mid 3x - 6$, or $4 \mid x - 2$. Since the elements divisible by 4 are the elements of $\ker f$, the last equation says that the elements of $f^{-1}(\{6\})$ are obtained by adding 2 to the elements of $\ker f$. Thus,

$$f^{-1}(\{6\}) = \{2, 6, 10\}. \quad \square$$

---

18. Define $f : \mathbb{R}^* \to \mathbb{R}^*$ by

$$f(x) = x^2.$$

($\mathbb{R}^*$ is the group of nonzero reals under multiplication.)

(a) Prove that f is a group map.

(b) Find $\ker f$ and $\operatorname{im} f$.

(a) Let $x, y \in \mathbb{R}^*$. Then (since $\mathbb{R}^*$ is abelian)

$$f(xy) = (xy)^2 = xyxy = x^2y^2 = f(x)f(y).$$

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

(b) The identity of $\mathbb{R}^*$ is 1. So

$$\ker f = \{x \in \mathbb{R}^* \mid f(x) = 1\} = \{x \in \mathbb{R}^* \mid x^2 = 1\} = \{1, -1\}.$$

If $x \in \mathbb{R}^*$, then $f(x) = x^2 > 0$. Thus, $f(x)$ is always a positive real number, and $\operatorname{im} f \subset \mathbb{R}^+$. Conversely, if y is a positive real number, then

$$f(\sqrt{y}) = (\sqrt{y})^2 = y.$$

Therefore, $\mathbb{R}^+ \subset \operatorname{im} f$. Hence, $\operatorname{im} f = \mathbb{R}^+$. $\square$

---

19. Define $f : \mathbb{Z}_3 \to \mathbb{Z}_8$ by $f(x) = 5x \pmod{8}$. Is f a group map?

I have

$$f(2 + 2) = f(1) = 5, \quad \text{but} \quad f(2) + f(2) = 2 + 2 = 4.$$

Since $f(2 + 2) \neq f(2) + f(2)$, it follows that f is not a group map. $\square$

---

20. Let G and H be groups, and let $\phi : G \to H$ be a group map. Let $g \in G$. Prove that if g has finite order, then the order of $\phi(g)$ divides the order of g.

Suppose that g has order n. Then $g^n = 1$, so

$$[\phi(g)]^n = \phi(g^n) = \phi(1) = 1.$$

Hence, the order of $\phi(g)$ must divide n. □

---

21. $\mathbb{R}$ is a group under the operation

$$a * b = a + b - 2.$$

Define $f : (\mathbb{R}, +) \to (\mathbb{R}, *)$ by

$$f(x) = x + 2.$$

Show that f is an isomorphism.

Let $x, y \in \mathbb{R}$. Then

$$f(x + y) = x + y + 2 \quad \text{and} \quad f(x) * f(y) = (x + 2) * (y + 2) = (x + 2) + (y + 2) - 2 = x + y + 2.$$

Hence, $f(x + y) = f(x) * f(y)$, and so f is a group map.
Define $g : (\mathbb{R}, *) \to (\mathbb{R}, +)$ by

$$g(x) = x - 2.$$

Then

$$f(g(x)) = f(x - 2) = (x - 2) + 2 = x,$$
$$g(f(x)) = g(x + 2) = (x + 2) - 2 = x.$$

Therefore, f and g are inverses, so f is bijective. Therefore, f is an isomorphism. □

---

22. Prove that if $f : G \to H$ is an invertible group map, then f^{-1} is a group map. (Thus, if f is an isomorphism, then its inverse is as well.)

Let $x, y \in H$. Since f and f^{-1} are inverses, $f(f^{-1}(x)) = x$ for all $x \in H$. In particular,

$$f\left(f^{-1}(x \cdot y)\right) = x \cdot y.$$

Using the fact that f is a group map and the inverse property again, I have

$$f\left(f^{-1}(x) \cdot f^{-1}(y)\right) = f\left(f^{-1}(x)\right) \cdot f\left(f^{-1}(y)\right) = x \cdot y.$$

Therefore,

$$f\left(f^{-1}(x \cdot y)\right) = f\left(f^{-1}(x) \cdot f^{-1}(y)\right).$$

But f is invertible, so it's injective. This means that $f(x) = f(y)$ implies $x = y$. So the last equation above gives

$$f^{-1}(x \cdot y) = f^{-1}(x) \cdot f^{-1}(y).$$

Thus, f^{-1} is a group map. □

---

23. Suppose n and x are integers, $n > 0$,

$$n \mid 2x + 5 \quad \text{and} \quad n \mid 3x + 4.$$

Prove that $n = 1$ or $n = 7$.

The idea is to make a linear combination of $2x + 5$ and $3x + 4$ where the x's cancel:

$$n \mid 3(2x + 5) - 2(3x + 4) = 7.$$

Since n is a positive integer dividing 7, it follows that $n = 1$ or $n = 7$. □

Using $x = 0$ and $x = 1$, you can see that both cases could occur.

---

24. Suppose that n and x are integers, n is odd,

$$n \mid 2x + 1 \quad \text{and} \quad n \mid 2x + 3.$$

Prove that $n = 1$.

n divides $2x + 1$ and $2x + 3$, so

$$n \mid (2x + 3) - (2x + 1) = 2.$$

But n is odd, so $n = \pm 1$. □

---

25. Find the greatest common divisor of 3462 and 118 and write it as a linear combination of 3462 and 118 with integer coefficients.

3462	-	88
118	29	3
40	2	1
38	1	1
2	19	0

The GCD of 3462 and 118 is 2, and

$$(3)(3462) + (-88)(118) = 2. \quad \square$$

---

26. Use the Extended Euclidean Algorithm to find 49^{-1} in $\mathbb{Z}_{61}$.

61	-	5
49	1	4
12	4	1
1	12	0

$$5 \cdot 49 - 4 \cdot 61 = 1$$
$$5 \cdot 49 = 1 \pmod{61}$$

Hence, $49^{-1} = 5$ in $\mathbb{Z}_{61}$. □

27. Prove that if m is an integer, then $(6m+4, 5m+3) = 1$ or 2. Give specific values of m which show that both cases can occur.

Note that

$$5 \cdot (6m+4) - 6 \cdot (5m+3) = 2.$$

Now $(6m+4, 5m+3) \mid (6m+4)$ and $(6m+4, 5m+3) \mid (5m+3)$, so

$$(6m+4, 5m+3) \mid 5 \cdot (6m+4) - 6 \cdot (5m+3) = 2.$$

But the only positive integers which divide 2 are 1 and 2, so $(6m+4, 5m+3) = 1$ or 2.
If $m = 1$, $6m+4 = 10$, $5m+3 = 8$, and $(10, 8) = 2$.
If $m = 2$, $6m+4 = 16$, $5m+3 = 13$, and $(16, 13) = 1$.
Therefore, both cases can occur. □

---

28. Prove that if $a, b \in \mathbb{Z}$, then $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$.

Since $(a,b) \mid a$ and $(a,b) \mid b$, I can write

$$a = m(a,b) \quad \text{and} \quad b = n(a,b) \quad \text{for} \quad m, n \in \mathbb{Z}.$$

I want to show that $(m,n) = 1$. There are integers $j, k \in \mathbb{Z}$ such that

$$(a,b) = ja + kb.$$

Then

$$(a,b) = jm(a,b) + kn(a,b), \quad \text{so} \quad 1 = jm + kn.$$

Hence, $(m,n) = 1$. □

---

29. If two integers differ by 1000, can they both be divisible by 7?

Suppose m and n are both divisible by 7, and $m-n = 1000$. Since $7 \mid m$ and $7 \mid n$, I have $7 \mid m-n = 1000$. This is a contradiction, since $7 \nmid 1000$. Therefore, two integers that differ by 1000 cannot both be divisible by 7. □

---

30. Find the greatest common divisor and the least common multiple of $p^3q^{10}r^2$ and p^5q^7, where p, q, and r are distinct primes.

To find the greatest common divisor, take the *smallest* power of each prime that occurs in *both numbers*:

$$(p^3q^{10}r^2, p^5q^7) = p^3q^7.$$

To find the least common multiple, take the *largest* power of each prime that occurs in *either number*:

$$[p^3q^{10}r^2, p^5q^7] = p^5q^{10}r^2. \quad \square$$

---

31. If p, q, and r are distinct prime numbers, how many positive divisors does pqr have?

A positive divisor of pqr must have the primes p, q, and r as factors. For each such divisor, either it has p as a factor or it doesn't. This gives two choices. The same is true for q and r. Hence, there are a total of $2^3 = 8$ choices, and 8 positive divisors. □

---

32. (a) For what integers n is $n^2 - 3n + 2$ prime?

(b) Calvin Butterball says: "Since n^2+2n+2 doesn't factor, n^2+2n+2 is always prime." Is Calvin correct?

(a) Suppose $n^2 - 3n + 2 = p$, where p is prime. Then $(n-1)(n-2) = p$, and there are four cases.

Case 1: $n - 1 = 1$ and $n - 2 = p$.

$n - 1 = 1$ gives $n = 2$, so $p = n - 2 = 0$. This is a contradiction, since 0 isn't prime.

Case 2: $n - 1 = -1$ and $n - 2 = -p$.

$n - 1 = -1$ gives $n = 0$, so $-p = n - 2 = -2$, and $p = 2$. This works, since 2 is prime.

Case 3: $n - 1 = p$ and $n - 2 = 1$.

$n - 2 = 1$ gives $n = 3$, so $p = n - 1 = 2$. This works, since 2 is prime.

Case 4: $n - 1 = -p$ and $n - 2 = -1$.

$n - 2 = -1$ gives $n = 1$, so $-p = n - 1 = 0$, and $p = 0$. This is a contradiction, since 0 isn't prime.

Thus, $n^2 - 3n + 2$ is prime for $n = 0$ and $n = 3$. □

(b) Calvin is wrong. For example, if $n = 2$, $n^2 + 2n + 2 = 10$, which is not prime. □

---

33. Suppose $a, b, c \in \mathbb{Z}$ and $c \mid ab$. Prove that $c \mid (a, c)(b, c)$.

There are integers w, x, y, and z such that

$$(a, c) = wa + xc \quad \text{and} \quad (b, c) = yb + zc.$$

Then

$$(a, c)(b, c) = (wa + xc)(yb + zc) = wy(ab) + (wza + xyb + xzc)c.$$

Since $c \mid ab \mid wy(ab)$ and $c \mid (wza + xyb + xzc)c$, it follows that $c \mid (a, c)(b, c)$. □

---

34. Suppose x and n are positive integers. Prove that

$$(x-1)^2 \mid x^n - nx(x-1) - 1.$$

First, I have

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

So

$$\begin{aligned} x^n - nx(x-1) - 1 &= (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) - nx(x-1) \\ &= (x-1)[(x^{n-1} + x^{n-2} + \cdots + x + 1) - nx] \end{aligned}$$

Consider the polynomial $(x^{n-1} + x^{n-2} + \cdots + x + 1) - nx$. Plugging in $x = 1$ gives

$$\overbrace{(1 + 1 + \cdot + 1)}^{n \text{ times}} - n = 0.$$

Thus, $x = 1$ is a root of $(x^{n-1} + x^{n-2} + \cdots + x + 1) - nx$, so by the Root Theorem, $x - 1$ must be a factor:

$$(x^{n-1} + x^{n-2} + \cdots + x + 1) - nx = (x - 1)p(x).$$

Thus,

$$x^n - nx(x - 1) - 1 = (x - 1) \cdot (x - 1)p(x).$$

Hence, $(x - 1)^2 \mid x^n - nx(x - 1) - 1$. □

---

35. Prove that if $n \geq 1$, then

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2.$$

For $n = 1$, I have

$$1^3 = 1 \quad \text{and} \quad \frac{1}{4} \cdot 1^2 \cdot (1 + 1)^2 = 1.$$

The result is true for $n = 1$.
Assume that the result is true for n:

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2.$$

I want to prove the result for $n + 1$:

$$1^3 + 2^3 + \cdots + n^3 + (n + 1)^3 = \frac{1}{4}(n + 1)^2(n + 2)^2.$$

I have

$$1^3 + 2^3 + \cdots + n^3 + (n + 1)^3 = \frac{1}{4}n^2(n + 1)^2. + (n + 1)^3 = (n + 1)^2 \left(\frac{1}{4}n^2 + (n + 1)\right) =$$

$$\frac{1}{4}(n + 1)^2 \left(n^2 + 4(n + 1)\right) = \frac{1}{4}(n + 1)^2 \left(n^2 + 4n + 4\right) = \frac{1}{4}(n + 1)^2(n + 2)^2.$$

This proves the result for $n = 2$, so the result is true for all $n \geq 1$, by induction. □

---

36. Prove that there is no integer x such that $78x = 61 \pmod{91}$.

Suppose that $78x = 61 \pmod{91}$. Note that $91 = 7 \cdot 13$ and $78 = 6 \cdot 13$. Multiply by 7:

$$\begin{aligned} 78x &= 61 \pmod{91} \\ 7 \cdot 78x &= 7 \cdot 61 \pmod{91} \\ 546x &= 427 \pmod{91} \\ 0 \cdot x &= 63 \pmod{91} \\ 0 &= 63 \pmod{91} \end{aligned}$$

This contradiction proves that there is no such x. □

---

37. Solve the equation $34x + 63 = 191 \pmod{225}$.

Subtracting 63 from both sides gives $34x = 128 \pmod{225}$. Note that $(34, 225) = 1$; I'll find the multiplicative inverse of 34 mod 225.

225	-	86
34	6	13
21	1	8
13	1	5
8	1	3
5	1	2
3	1	1
2	1	1
1	2	0

The table gives

$$(13)(225) + (-86)(34) = 1, \quad \text{so} \quad (-86)(34) = 1 \pmod{225}.$$

Multiply $34x = 128 \pmod{225}$ by -86:

$$(-86) \cdot 34x7 = (-86) \cdot 128 \pmod{225}$$
$$x = -11008 = 17 \pmod{225} \quad \square$$

---

38. Compute $\sum_{n=1}^{100} n! \pmod 8$.

If $n \geq 8$, then $8 \mid n!$, so $n! = 0 \pmod 8$. So

$$\sum_{n=1}^{100} n! = \sum_{n=1}^{7} n! \pmod 8.$$

However, 4!, 5!, 6!, and 7! all contain 2 and 4 as **separate** factors, so they're each divisible by 8, and hence they're each congruent to 0 mod 8. So now

$$\sum_{n=1}^{100} n! = \sum_{n=1}^{3} n! = 1! + 2! + 3! = 1 + 2 + 6 = 1 \pmod 8. \quad \square$$

---

39. Recall that

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Suppose p is an odd prime. Compute

$$\binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p-1} + \binom{p}{p} \pmod p.$$

Consider

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}.$$

For $1 \le k \le p$, there is a factor of p in the numerator, but no factor of p in the denominator. Moreover, since p is prime, I can't have two factors a and b in the denominator whose product is p. Hence,

$$\binom{p}{k} = 0 \pmod{p} \quad \text{for} \quad 1 \le k \le p.$$

It follows that

$$\binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p} = 1 + 0 + \cdots + 0 + 1 = 2 \pmod{p}. \quad \square$$

---

40. Prove that if $n \in \mathbb{Z}$, then $n^3 + 3n + 5$ is not divisible by 7.

Every integer n is congruent mod 7 to one of 0, 1, 2, 3, 4, 5, or 6. So I just need to consider these 7 cases:

$n \pmod 7$	0	1	2	3	4	5	6
$n^3 + 3n + 5 \pmod 7$	5	2	5	6	4	5	1

For all n, I have $n^3 + 3n + 5 \neq 0 \pmod 7$. Hence, if $n \in \mathbb{Z}$, then $n^3 + 3n + 5$ is not divisible by 7. $\square$

---

41. Prove that there are no integers m and n such that $11m^2 - 4n^2 = 33$.

Suppose there is a solution (m, n), so $11m^2 - 4n^2 = 33$. Reduce the equation mod 4 to obtain

$$\begin{aligned} 3m^2 &= 1 \pmod 4 \\ 3 \cdot 3m^2 &= 3 \cdot 1 \pmod 4 \\ m^2 &= 3 \pmod 4 \end{aligned}$$

Construct a table of squares mod 4:

$x \pmod 4$	0	1	2	3
$x^2 \pmod 4$	0	1	0	1

The table shows that 3 is not a square mod 4. This contradiction shows that the original equation has no solutions. $\square$

---

42. Solve the following modular equation and simplify your answer to a number in the range $\{0, 1, \ldots, 60\}$.

$$8x + 55 = 14(2x + 3) \pmod{61}.$$

$$\begin{aligned} 8x + 55 &= 14(2x + 3) \pmod{61} \\ 8x + 55 &= 28x + 42 \pmod{61} \\ 13 &= 20x \end{aligned}$$

Use the Extended Euclidean algorithm to find $20^{-1} \pmod{61}$.

61	-	3
20	3	1
1	20	0

Thus,

$$1 = 1 \cdot 61 + (-3) \cdot 20$$
$$1 = (-3) \cdot 20 \pmod{61}$$

Hence, $20^{-1} = -3 \pmod{61}$. Multiplying $20x = 13 \pmod{61}$ by -3 and simplifying, I obtain

$$(-3) \cdot 20x = (-3) \cdot 13 \pmod{61}$$
$$x = -39 \pmod{61}$$
$$x = 22 \pmod{61} \quad \square$$

---

43. (a) Prove that the following equation has no solutions:

$$6x = 7 \pmod{12}.$$

(b) Bonzo McTavish says that the following equation has no solutions:

$$2x = 6 \pmod{10}.$$

Bonzo says: "In the last problem, 6 and 12 weren't relatively prime, so you couldn't find $6^{-1} \pmod{12}$ and that's why the equation had no solutions. In this problem, 2 and 10 aren't relatively prime, so this equation has no solutions, either."

Show that Bonzo is incorrect.

(a) Suppose x satisfies $6x = 7 \pmod{12}$. Then

$$2 \cdot 6x = 2 \cdot 7 \pmod{12}$$
$$0 = 2 \pmod{12}$$

This contradiction shows that the original equation has no solutions. $\square$

(b) An easy way to check for solutions is to make a table:

x	0	1	2	3	4	5	6	7	8	9
$2x \pmod{10}$	0	2	4	6	8	0	2	4	6	8

As the table shows, $x = 3$ and $x = 8$ are solutions, so Bonzo is incorrect.

He's right that $2^{-1} \pmod{10}$ is undefined, so you can't multiply both sides by 2^{-1}. However, that only shows that you can't solve the equation **in that particular way**. $\square$

One hears only those questions for which one is able to find answers. - Friedrich Nietzsche