Mat2033 - Discrete Mathematics

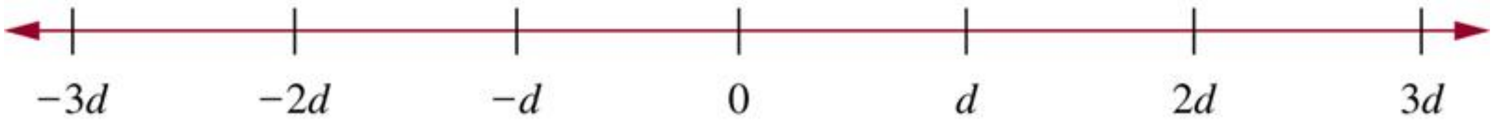
Integers and division

Integers and division

- **Number theory**: the branch of mathematics involves integers and their properties.
- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b=ac$.
- When a divides b we say that a is a factor of b and that b is a multiple of a.
- The notation $a|b$ denotes a divides b. We write $a \nmid b$ when does not divide b.

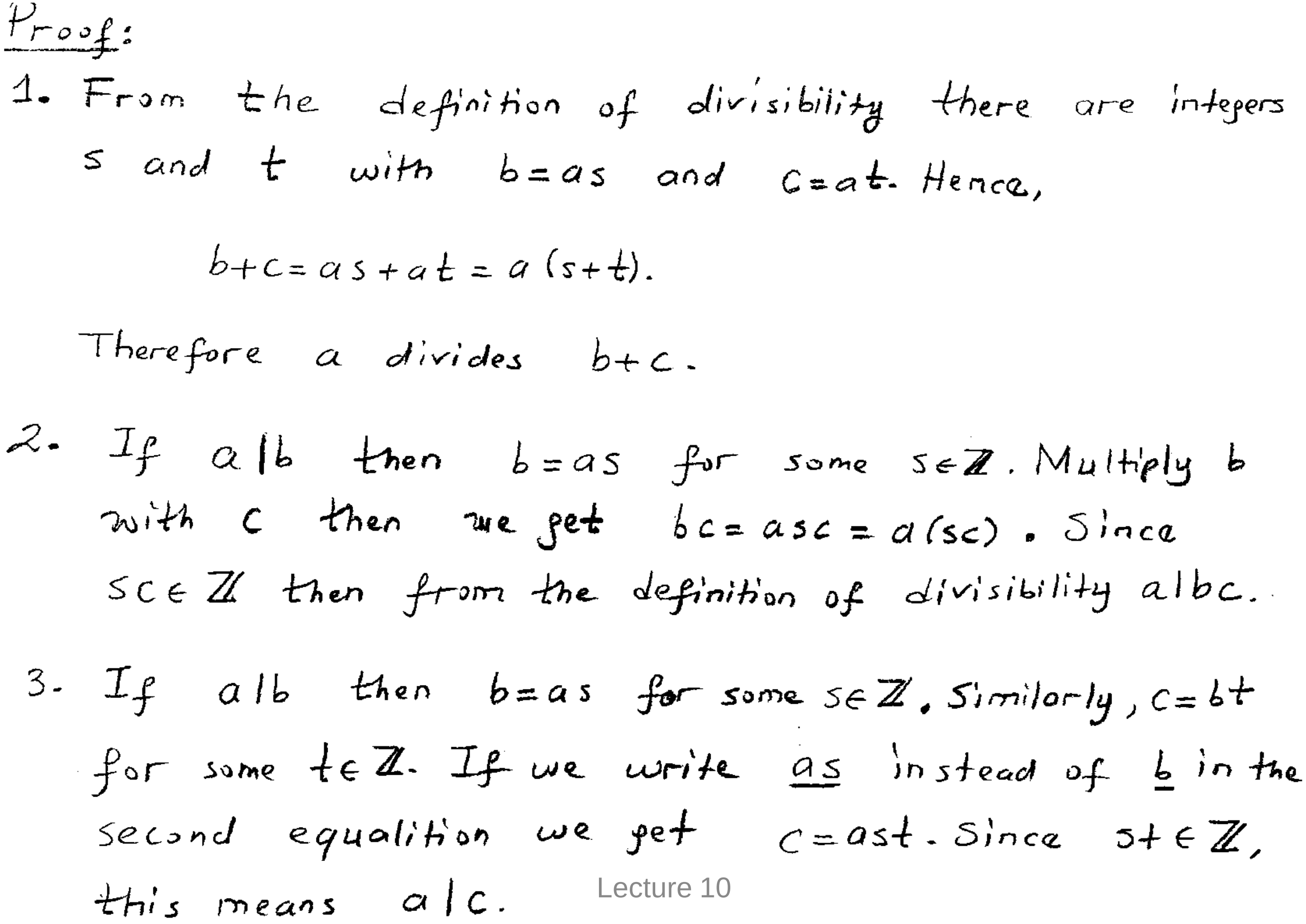
Example: Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

- The positive integers divisible by *d* are all integers of them form *dk*, where *k* is a positive integer
- Thus, there are $\lfloor n/d \rfloor$ positive integers not exceeding *n* that are divisible by *d*



Theorem 1: Let *a*, *b*, and *c* be integers, then

1. If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
2. If $a \mid b$ then $a \mid bc$ for all integers *c*
3. If $a \mid b$ and $b \mid c$, then $a \mid c$



Proof:

1. From the definition of divisibility there are integers s and t with $b=as$ and $c=at$. Hence,

$$b+c=as+at=a(s+t).$$

Therefore a divides $b+c$.

2. If $a|b$ then $b=as$ for some $s\in\mathbb{Z}$. Multiply b with c then we get $bc=asc=a(sc)$. Since $sc\in\mathbb{Z}$ then from the definition of divisibility $a|bc$.

3. If $a|b$ then $b=as$ for some $s\in\mathbb{Z}$. Similorly, $c=bt$ for some $t\in\mathbb{Z}$. If we write $\underline{as}$ instead of $\underline{b}$ in the second equalition we get $c=ast$. Since $st\in\mathbb{Z}$, this means $a|c$.

Corollary-1: If a, b and c are integers such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers.

Corollary-1: If a, b and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb+nc$ whenever m and n are integers.

Proof: By part (2) of thm-1 it follows that $a \mid mb$ and $a \mid nc$ whenever m and n are integers. By part (1) of thm-1 it follows that $a \mid mb+nc$.

The division algorithm

- Let a be integer and d be a positive integer. Then there are unique integers q and r with $0 \le r < d$, such that $a=dq+r$.
- In the equality, d is the divisor, a is the dividend, q is the quotient, r is the remainder

$$q = a \textbf{ div } d, \qquad r = a \textbf{ mod } d$$

- -11 divided by 3
- -11=3(-4)+1, -4=-11 div 3, 1=-11 mod 3
- -11=3(-3)-2, but remainder cannot be negative

Example: What are the quotient and remainder when 101 is divided by 11?

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$

Example: What are the quotient and remainder when -11 is divided by 3?

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$

Example: What are the quotient and remainder when -11 is divided by 3?

solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$

Example: What are the quotient and remainder when -11 is divided by 3?

solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Note: The remainder cannot be negative. So we cannot write in the above example

$$-11 = 3(-3) - 2$$

Since $r = -2$ does not satisfy $0 \leq r < 3$.

Example: What are the quotient and remainder when 101 is divided by 11?

Solution: $101 = 11 \cdot 9 + 2$. The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \text{ mod } 11$

Example: What are the quotient and remainder when -11 is divided by 3?

solution: $-11 = 3(-4) + 1$. The quotient is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \text{ mod } 3$.

Note: The remainder cannot be negative. So we cannot write in the above example

$$-11 = 3(-3) - 2$$

Since $r = -2$ does not satisfy $0 \leq r < 3$.

Note: a is divisible by d if and only if the remainder is zero.

Primes and greatest common divisions

- **Prime**: a positive integer *p* greater than *1* if the only positive factors of *p* are *1* and *p*
- A positive integer greater than *1* that is not prime is called **composite**

Remark: The integer n is composite if and only if there exists an integer a such that $a | n$ and $1 < a < n$.

The primes less than 100 are:

2 3 5 7 11 13 17 19 23

29 31 37 41 43 47 53 59 61

67 71 73 79 83 89 97

Theorem:(Fundamental theorem of arithmetic) Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes when the prime factors are written in order of non-decreasing size

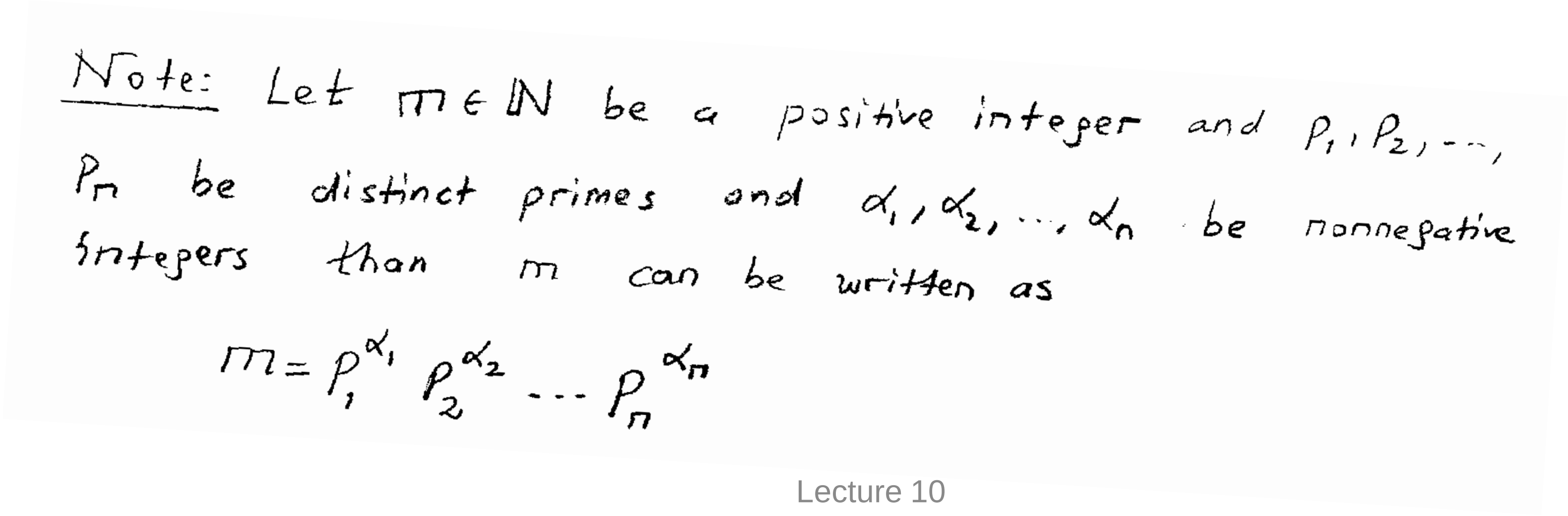
Example: Prime factorizations of integers

100=2·2·5·5= $2^2 . 5^2$

641=641

999=3·3·3·37= 3^3·37

1024=2·2·2·2·2·2·2·2·2·2= 2^{10}



Note: Let $m \in \mathbb{N}$ be a positive integer and $p_1, p_2, \dots, p_n$ be distinct primes and $\alpha_1, \alpha_2, \dots, \alpha_n$ be nonnegative integers than m can be written as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

Theorem: If *n* is a composite integer, then *n* has a prime division less than or equal to $\sqrt{n}$.

- As *n* is composite, *n* has a factor *1<a<n*, and thus *n=ab*.
- We show that $a \le \sqrt{n}$ or $b \le \sqrt{n}$ (by contraposition)
- Thus *n* has a divisor not exceeding $\sqrt{n}$.
- This divisor is either prime or by the fundamental theorem of arithmetic, has a prime divisor less than itself , and thus a prime divisor less than $\sqrt{n}$.

Note: An integer is prime if it is not divisible by any prime less than or equal to its square root.

Example: Show that 101 is prime

- The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7
- As 101 is not divisible by 2, 3, 5, 7, it follows that 101 is prime

Procedure for prime factorization

- Begin by diving *n* by successive primes, starting with *2*.
- If *n* has a prime factor, we would find a prime factor not exceeding $\sqrt{n}$.
- If no prime factor is found, then *n* is prime.
- Otherwise, if a prime factor *p* is found, continue by factoring *n/p* .
- Note that *n/p* has no prime factors less than *p*.
- If *n/p* has no prime factor greater than or equal to *p* and not exceeding its square root, then it is prime.
- Otherwise, continue by factoring *n/(pq)*.
- Continue until factorization has been reduced to a prime.

Example: Find the prime factorization of 7007.

- Start with 2, 3, 5, and then 7, 7007/7=1001
- Then, divide 1001 by successive primes, beginning with 7, and find 1001/7=143
- Continue by dividing 143 by successive primes, starting with 7, and find 143/11=13
- As 13 is prime, the procedure stops
- $7007=7\cdot7\cdot11\cdot13=7^2\cdot11\cdot13$

Theorem

Theorem: There are infinitely many primes.

- Proof by contradiction.
- Assume that there are only finitely many primes, p_1, p_2, …, p_n. Let $Q=p_1p_2…p_n+1$
- By Fundamental Theorem of Arithmetic: Q is prime or else it can be written as the product of two or more primes.

Theorem

- However, none of the primes p_j divides Q, for if p_j | Q, then p_j divides Q-p_1 p_2 … p_n =1
- Hence, there is a prime not in the list p_1,p_2,…,p_n
- This prime is either Q, if it is prime, or a prime factor for Q
- This is a contradiction as we assumed that we have listed all the primes

Greatest common divisors

- Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the **greatest common divisor** (GCD) of a and b, often denoted as $gcd(a,b)$

Greatest common divisors

- The integers *a* and *b* are **relative prime** if their GCD is 1

  gcd(10, 17)=1,

  gcd(10, 21)=1,

  gcd(10,24)=2

- The integers a_1, a_2, …, a_n are **pairwise relatively prime** if gcd(a_i, a_j)=1 whenever $1 \leq i < j \leq n$

Example: What is the common divisor of 24 and 36?

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence gcd$(24, 36) = 12$.

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $gcd(24,36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $gcd(24, 36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: The positive common divisor of 17 and 22 is 1 so 17 and 22 are relatively prime. So $gcd(17, 22) = 1$

Example: What is the common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6 and 12. Hence $\gcd(24, 36) = 12$.

Definition-5: The integers a and b are relatively prime if their greatest common divisor is 1.

Example: The positive common divisor of 17 and 22 is 1 so 17 and 22 are relatively prime. So $\gcd(17, 22) = 1$

Definition-6: The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Prime factorization and GCD

- Finding GCD

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, \quad 500 = 2^2 \cdot 5^3$$

$$\gcd(120,500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Least common multiple

- **Least common multiples** of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*, denoted as *lcm(a,b)*

Least common multiple

- Finding LCM

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, 500 = 2^2 \cdot 5^3$$

$$\operatorname{lcm}(120,500) = 2^3 \cdot 3^1 \cdot 5^3 = 8 \cdot 3 \cdot 125 = 3000$$

Theorem: Let a and b be positive integers, then

$$ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$$

Modular arithmetic

- If a and b are integers and m is a positive integer, then a is **congruent** to b modulo m if m divides a-b

- We use the notation $a \equiv b$ (mod m) to indicate that a is **congruent** to b modulo m. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$

- Let a and b be integers, m be a positive integer. Then $a \equiv b$ (mod m) if and only if a mod m = b mod m

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are not congruent modulo 6

17-5=12, we see 17≡5 (mod 6)

24-14=10, and thus $24 \not\equiv 14 \pmod{6}$

Theorem: Let m be a positive integer. The integer a and b are congruent modulo m if and only if there is an integer k such that $a=b+km$.

(→) If $a=b+km$, then $km=a-b$, and thus m divides $a-b$ and so $a \equiv b \pmod{m}$

(←) if $a \equiv b \pmod{m}$, then $m|a-b$. Thus, $a-b=km$, and so $a=b+km$

Theorem: Let m be a positive integer.

If $a\equiv b$ (mod m) and $c\equiv d$ (mod m), then

$a+c=b+d$ (mod m) and $ac\equiv bd$ (mod m).

Proof:

Since $a \equiv b$ (mod m) and $c \equiv d$ (mod m), there are integers t and s such that $b=a+sm$ and $d=c+tm$. Therefore

$b+d=(a+c)+m(s+t)$,

$bd=(a+sm)(c+tm)=ac+m(at+cs+stm)$

Hence $a+c \equiv b+d$ (mod m), and $ac \equiv bd$ (mod m)

Example: $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, so

$18=7+11 \equiv 2+1=3 \pmod 5$

$77=7\cdot 11 \equiv 2\cdot 1=2 \pmod 5$

Corollary: Let a and b be integers and m be a positive integer, then

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Proof: By definitions mod m and congruence modulo m, we know that $a \equiv (a \bmod m) \pmod{m}$ and $b \equiv (b \bmod m) \pmod{m}$. Hence

$$(a+b) \equiv ((a \bmod m) + (b \bmod m)) \pmod{m}$$
$$ab \equiv (a \bmod m)(b \bmod m) \pmod{m}$$

Theorem-9: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, then $m \mid (a-b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$. Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence m divides $a - b$, so that $a \equiv b \pmod{m}$.

Note: The set of all integers congruent to an integer a modulo m is called the congruence class of a modulo m.

Applications of Congruences

Cryptology:

Congruences have many applications to discrete mathematics and computer science. One of the most important applications of congruences involves cryptology, which is the study of secret messages. One of the earliest known uses of cryptology was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three). For instance, using this scheme the letter B is sent to E and the letter X is sent to A. This is an example of encryption, that is, the process of making a message secret.

To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25, based on its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer $f(p)$ in the set $\{0,1,2,\ldots,25\}$ with

$$f(p) = (p+3) \bmod 26$$

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by $(p+3) \bmod 26$.

Example: What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesor's cipher?

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p+3) \bmod 26$. This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13 .

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN".

To recover the original message from a secret message encrypted by the Caesar's cipher, the function f^{-1}, the inverse of f, is used. f^{-1} sends an integer p from $\{0,1,2,\ldots,25\}$ to $f^{-1}(p)=(p-3) \bmod 26$. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called decryption.

It is possible to generalize Caesar's method. For example we can shift any letter by k, so that

$$f(p)=(p+k) \bmod 26.$$

Such a cipher is called a <u>shift cipher</u>. Note that decryption can be carried out using

$$f^{-1}(p) = (p-k) \bmod 26.$$

Obviously, Caesar's method and shift ciphers do not provide a high level of security. There are various ways to enhance this method. One approach that slightly enhances the security is to use a function of the form

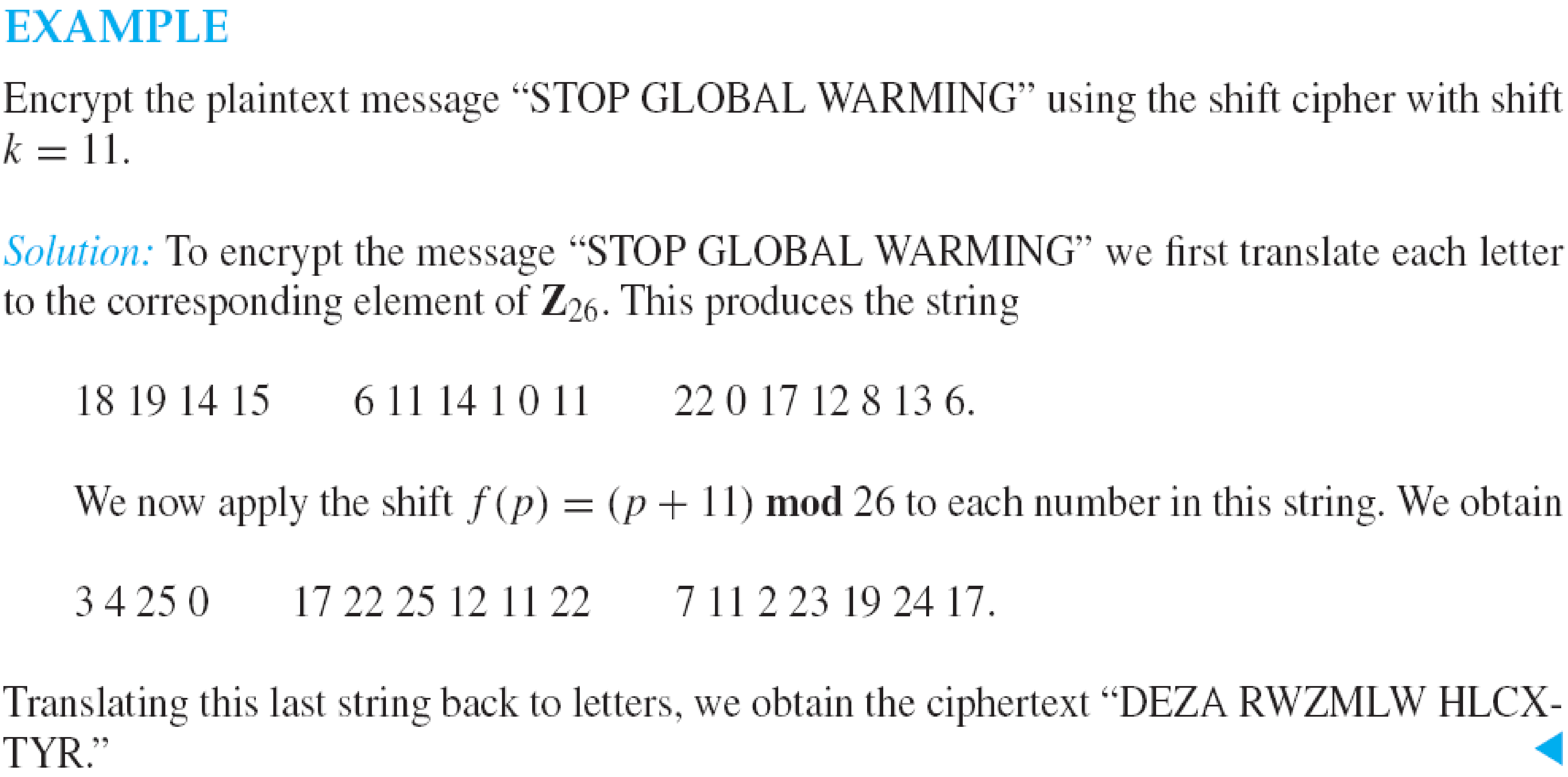
$$f(p) = (ap+b) \bmod 26$$

where a and b are integers, chosen such that f is a bijection (1-1 and onto). Such a mapping is called an <u>affine transformation</u>.

__Example:__ What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

Example: What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

Solution: 10 represents K, then $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$.
21 represents V. K is replaced by V in the encrypted message ■



EXAMPLE

Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with shift $k = 11$.

Solution: To encrypt the message "STOP GLOBAL WARMING" we first translate each letter to the corresponding element of $\mathbf{Z}_{26}$. This produces the string

$$18\ 19\ 14\ 15 \qquad 6\ 11\ 14\ 1\ 0\ 11 \qquad 22\ 0\ 17\ 12\ 8\ 13\ 6.$$

We now apply the shift $f(p) = (p + 11)$ **mod** 26 to each number in this string. We obtain

$$3\ 4\ 25\ 0 \qquad 17\ 22\ 25\ 12\ 11\ 22 \qquad 7\ 11\ 2\ 23\ 19\ 24\ 17.$$

Translating this last string back to letters, we obtain the ciphertext "DEZA RWZMLW HLCXTYR." ◀

EXAMPLE

Decrypt the ciphertext message “LEWLYPLUJL PZ H NYLHA ALHJOLY” that was encrypted with the shift cipher with shift $k = 7$.

Solution: To decrypt the ciphertext “LEWLYPLUJL PZ H NYLHA ALHJOLY” we first translate the letters back to elements of $\mathbf{Z}_{26}$. We obtain

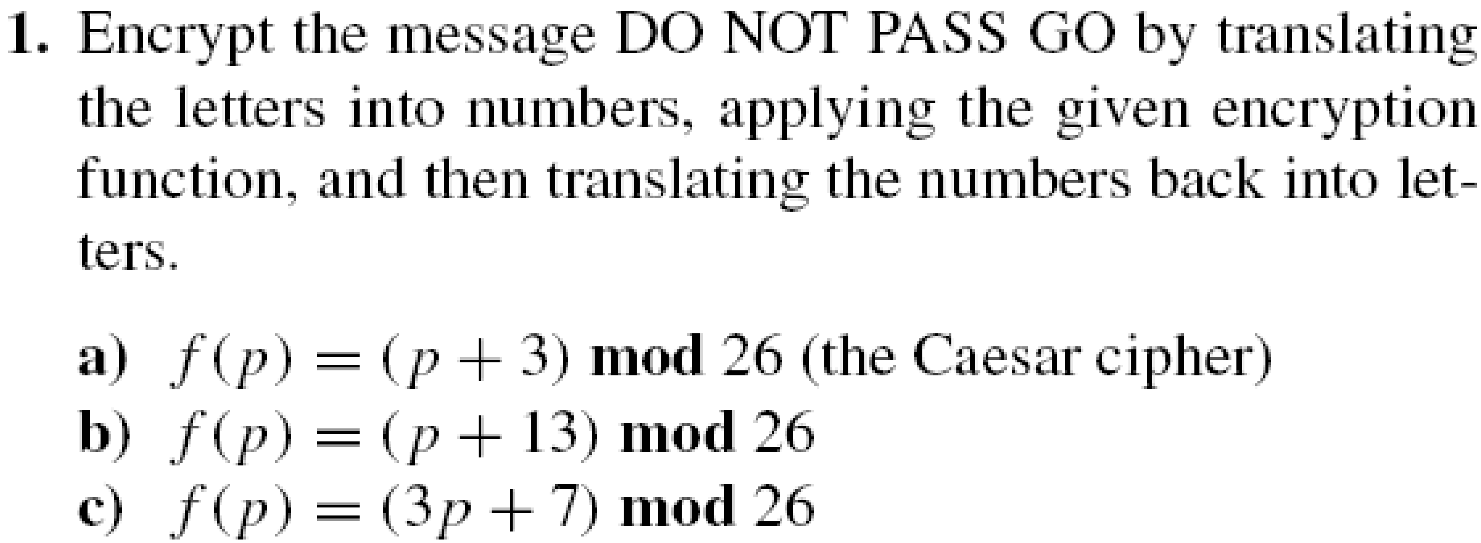
11 4 22 11 24 15 11 20 9 11   15 25   7   13 24 11 7 0   0 11 7 9 14 11 24.

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

4 23 15 4 17 8 4 13 2 4   8 18   0   6 17 4 0 19   19 4 0 2 7 4 17.

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain “EXPERIENCE IS A GREAT TEACHER.” ◀

Exercises

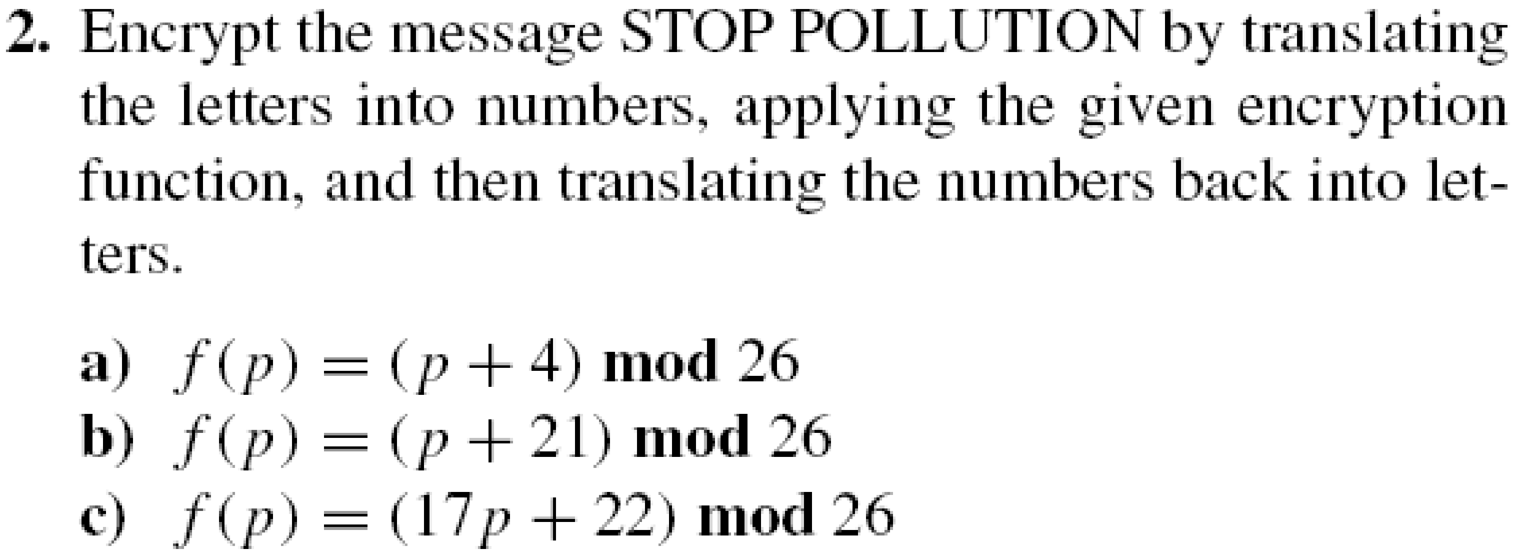


1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p + 3)$ **mod** 26 (the Caesar cipher)

b) $f(p) = (p + 13)$ **mod** 26

c) $f(p) = (3p + 7)$ **mod** 26

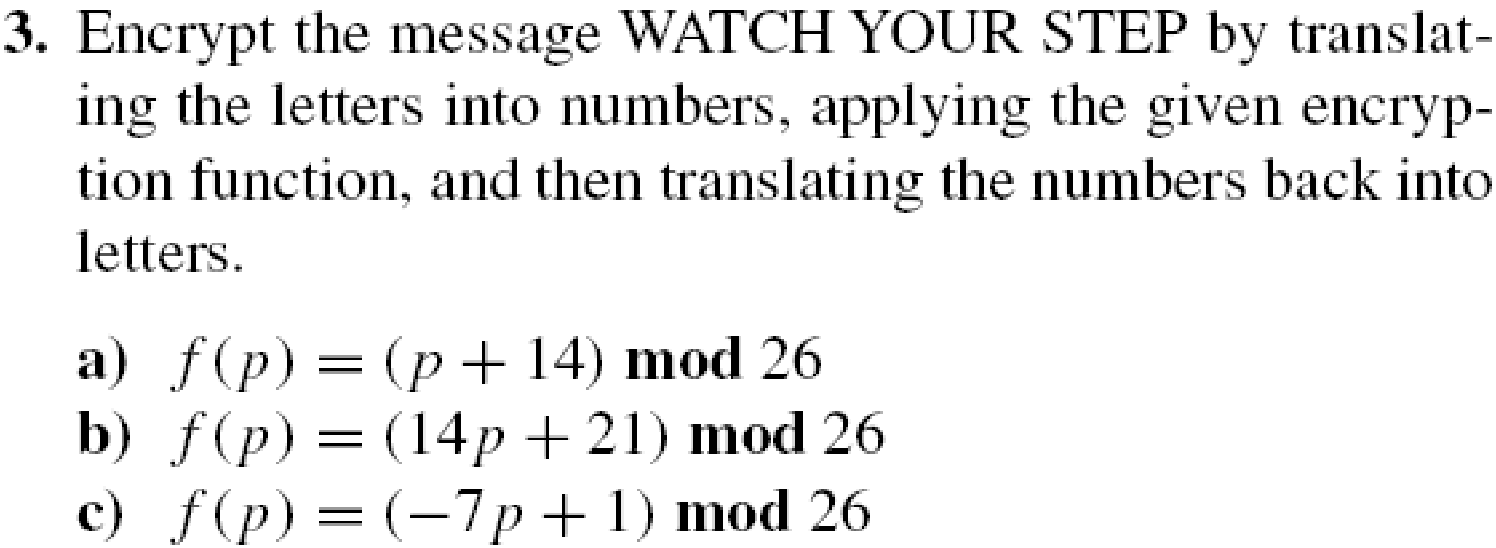


2. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p + 4) \textbf{ mod } 26$

b) $f(p) = (p + 21) \textbf{ mod } 26$

c) $f(p) = (17p + 22) \textbf{ mod } 26$

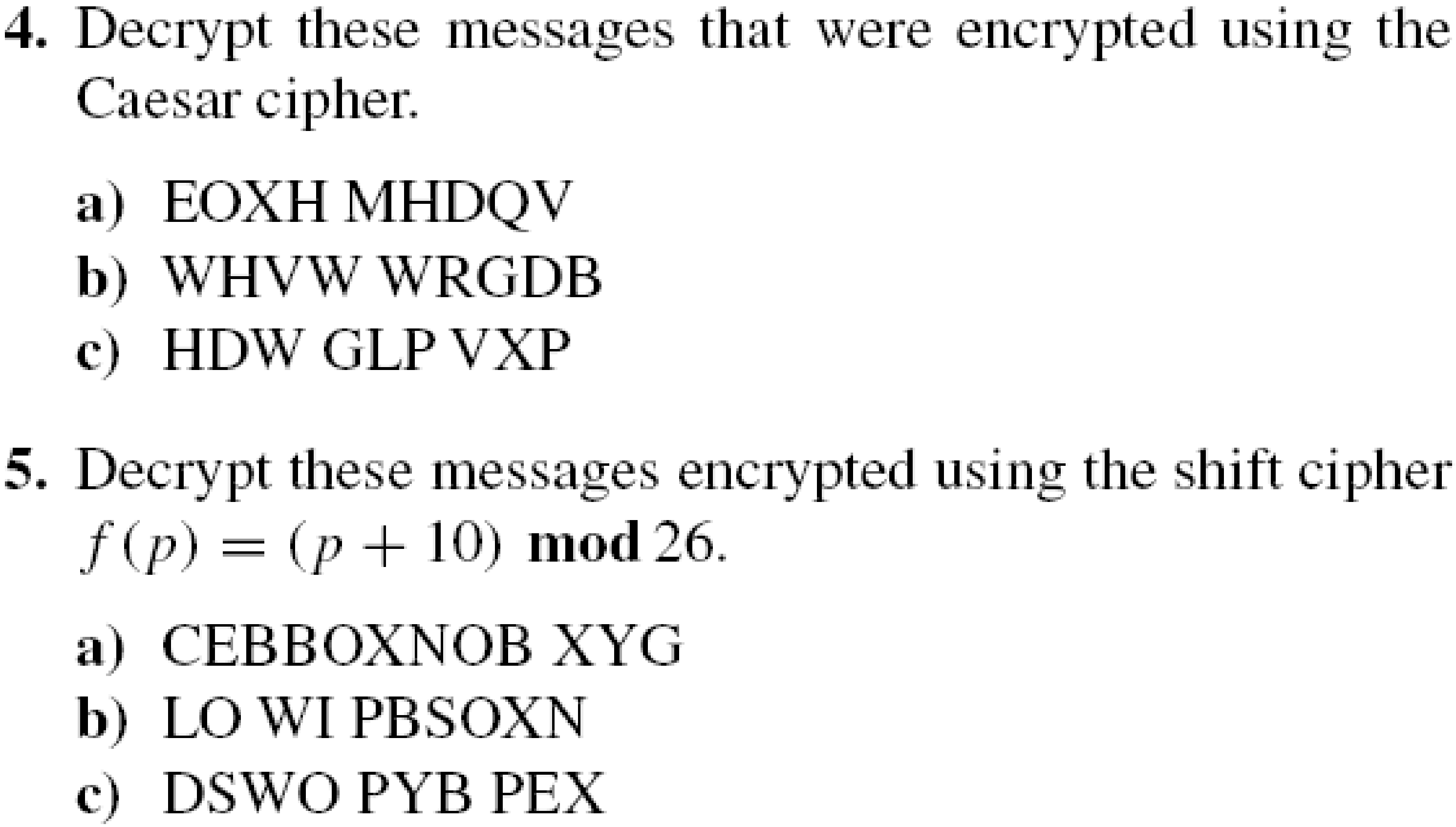


3. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p + 14)\ \mathbf{mod}\ 26$

b) $f(p) = (14p + 21)\ \mathbf{mod}\ 26$

c) $f(p) = (-7p + 1)\ \mathbf{mod}\ 26$



4. Decrypt these messages that were encrypted using the Caesar cipher.

a) EOXH MHDQV

b) WHVW WRGDB

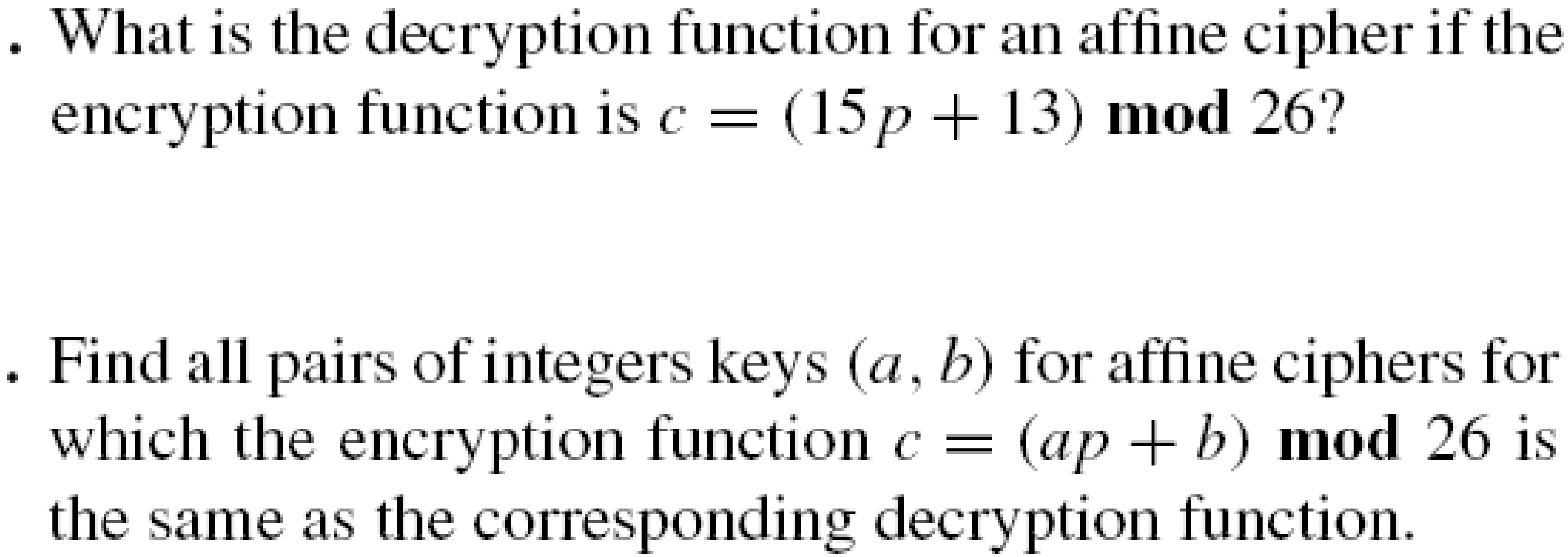
c) HDW GLP VXP

5. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10)\ \mathbf{mod}\ 26$.

a) CEBBOXNOB XYG

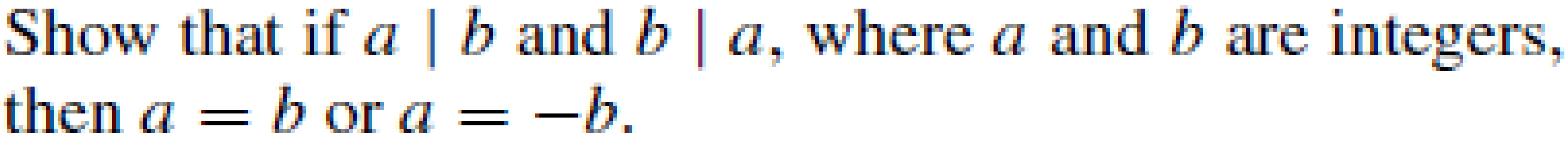
b) LO WI PBSOXN

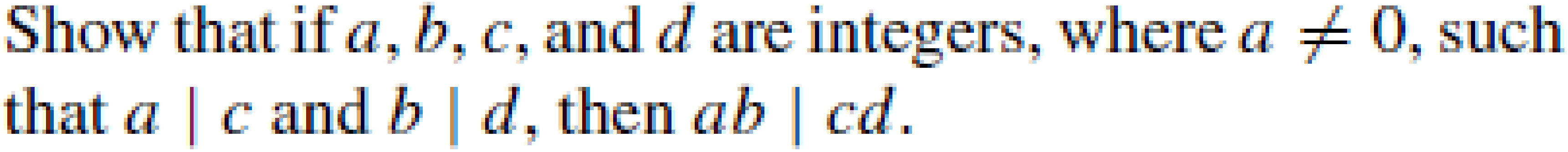
c) DSWO PYB PEX

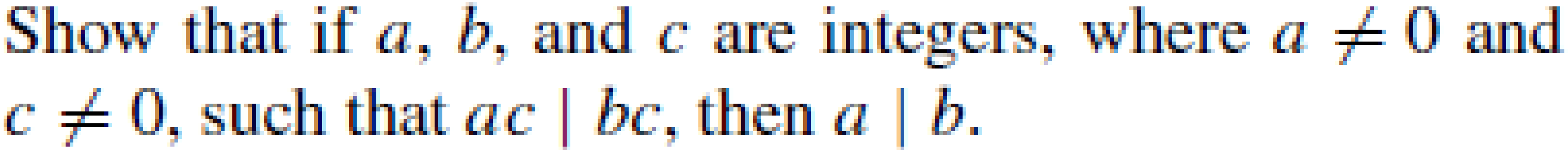


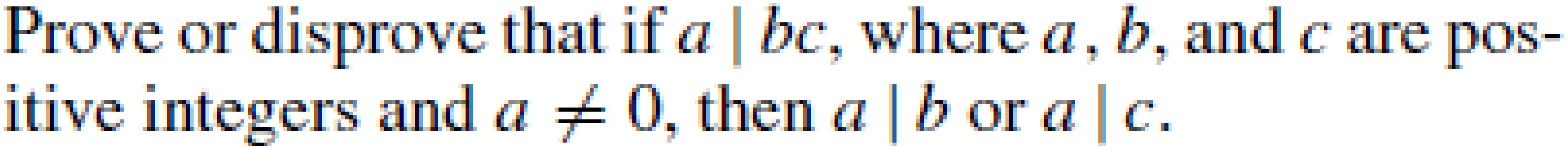
. What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13)$ **mod** 26?

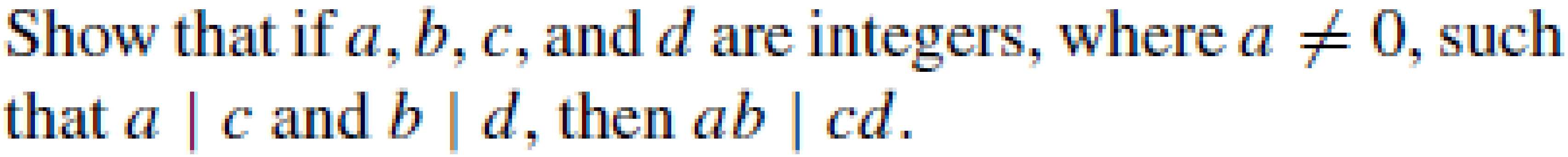
. Find all pairs of integers keys (a, b) for affine ciphers for which the encryption function $c = (ap + b)$ **mod** 26 is the same as the corresponding decryption function.

- 
  Show that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

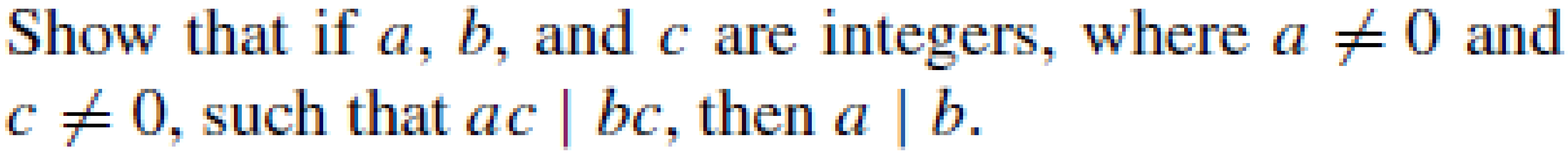
- 
  Show that if a, b, c, and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

- 
  Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

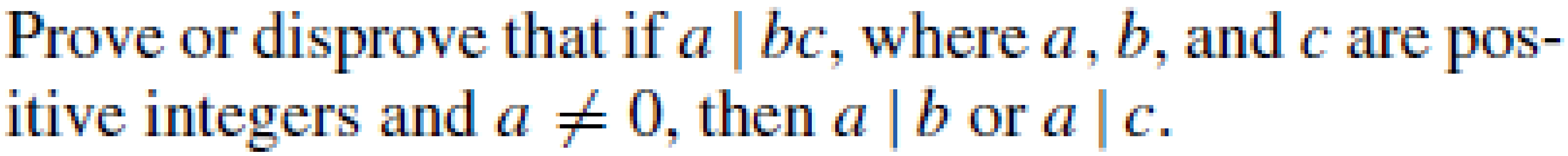
- 
  Prove or disprove that if $a \mid bc$, where a, b, and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.



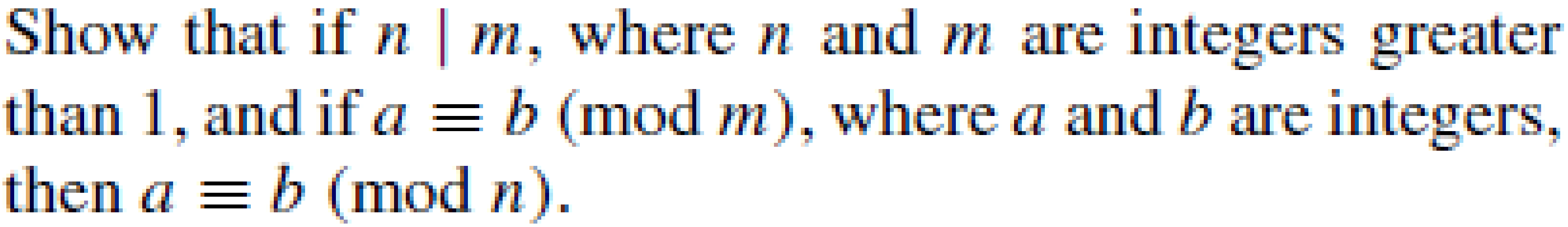
Show that if a, b, c, and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.



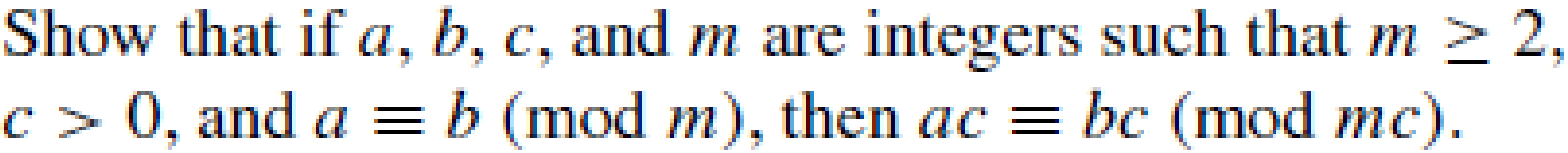
Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.



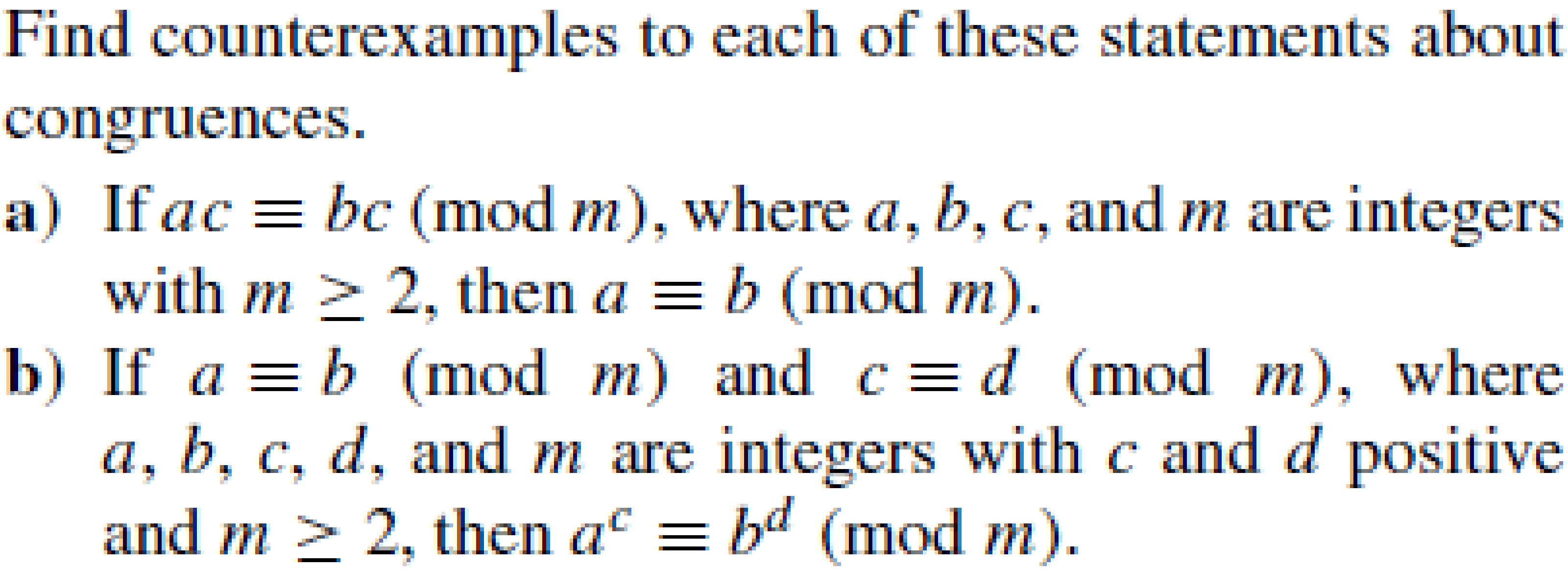
Prove or disprove that if $a \mid bc$, where a, b, and c are positive integers and $a \neq 0$, then $a \mid b$ or $a \mid c$.



Show that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.



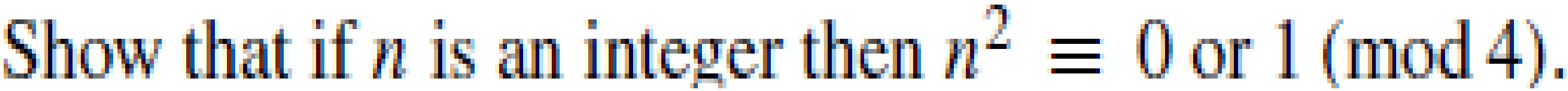
Show that if a, b, c, and m are integers such that $m \geq 2$, $c > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.



Find counterexamples to each of these statements about congruences.

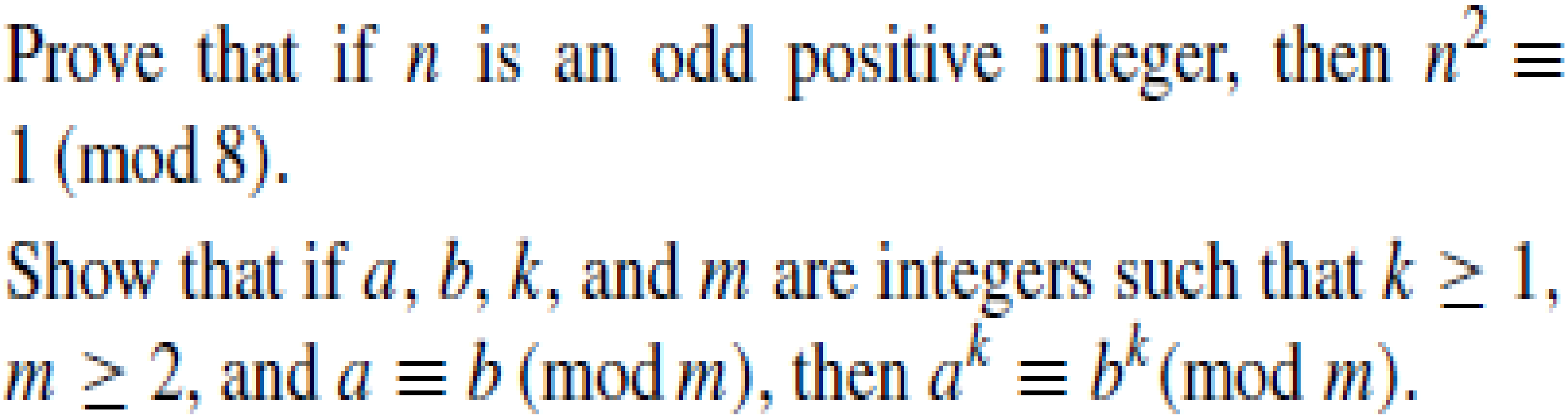
a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

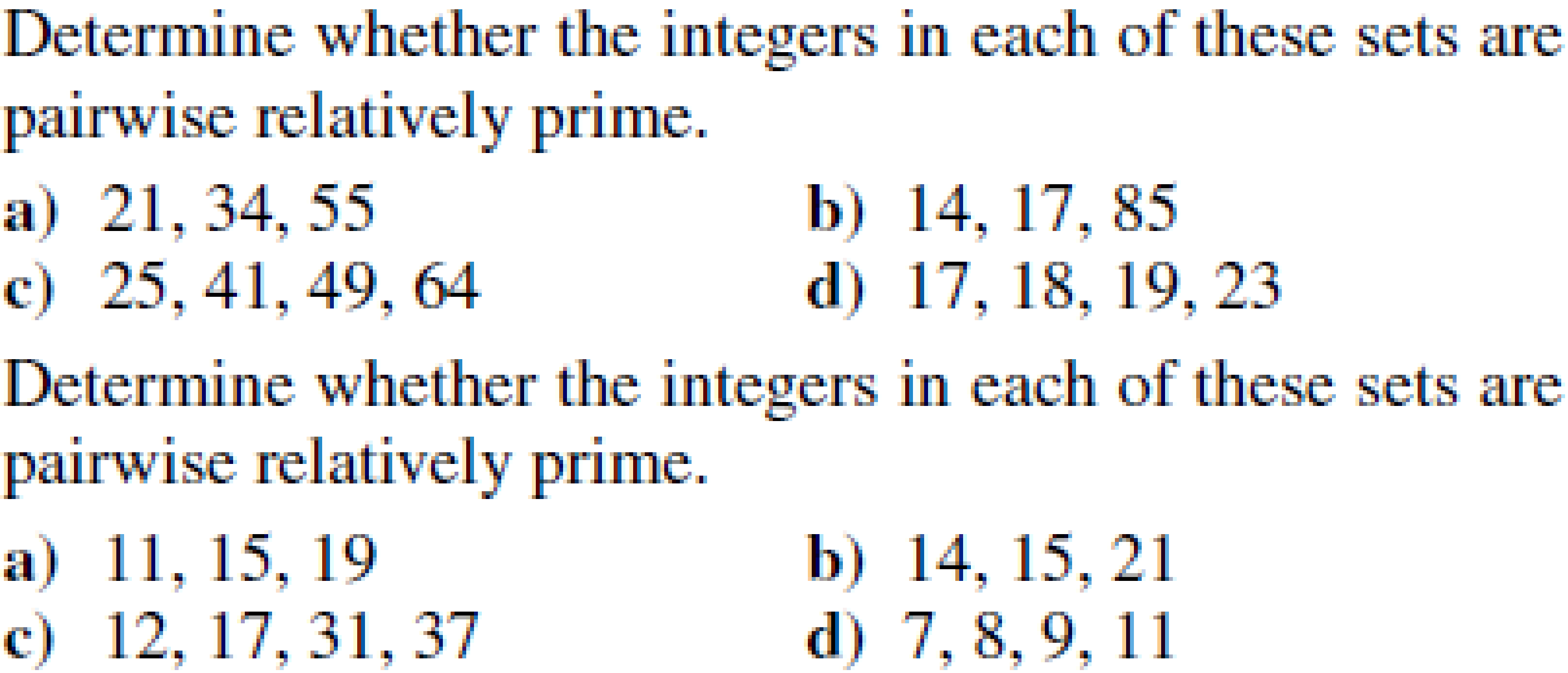
- 

  Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod{4}$.

- Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod 4$.
- Use Exercise □ to show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.



- Prove that if n is an odd positive integer, then $n^2 \equiv 1 \pmod{8}$.
- Show that if a, b, k, and m are integers such that $k \geq 1$, $m \geq 2$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.



Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55

b) 14, 17, 85

c) 25, 41, 49, 64

d) 17, 18, 19, 23

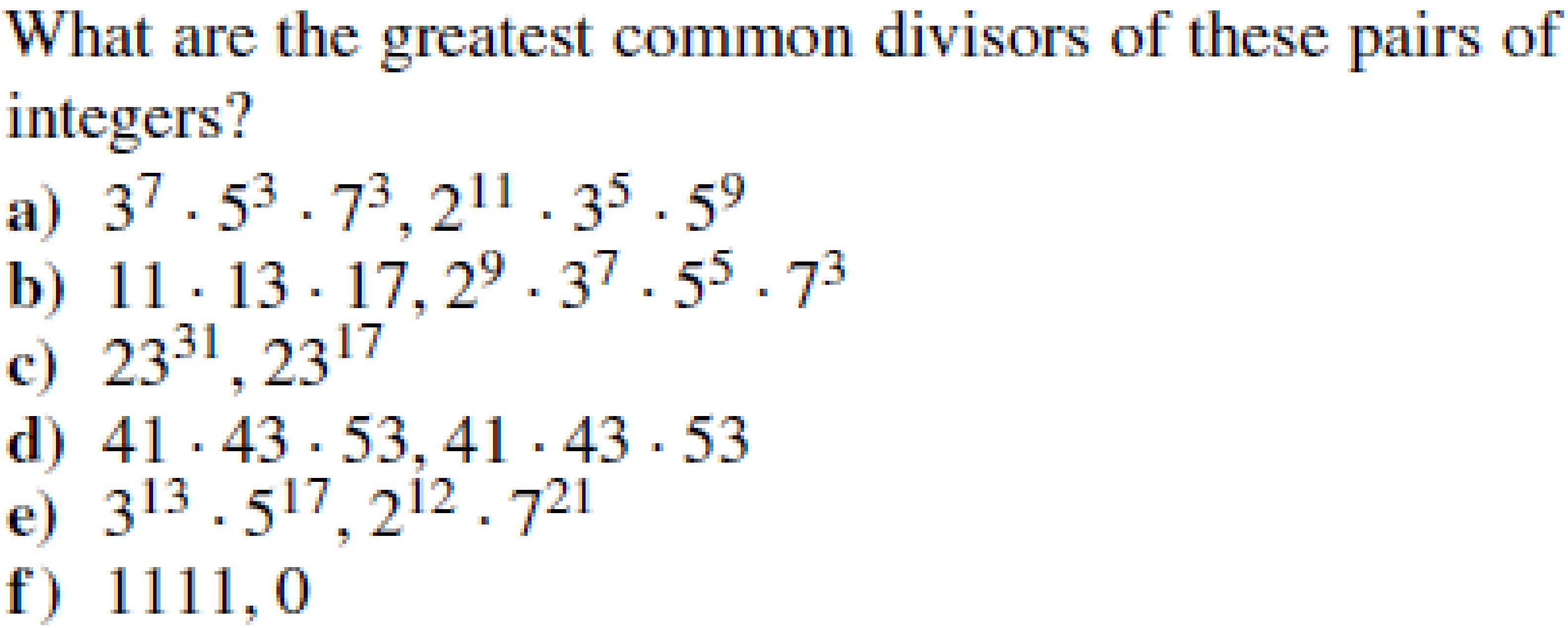
Determine whether the integers in each of these sets are pairwise relatively prime.

a) 11, 15, 19

b) 14, 15, 21

c) 12, 17, 31, 37

d) 7, 8, 9, 11



What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

c) $23^{31}, 23^{17}$

d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$

e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$

f) $1111, 0$