- Section 4.1: 1, 5, 9, 17, 21, 29, 41, 43, 44, 45, 47, 51

1. Does 17 divide each of these numbers?

a) 68 **b)** 84 **c)** 357 **d)** 1001

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

Solution:

When $a \mid b$ then we know that $b = ac$ where c is an integer. We can do the same for $b \mid a$, so $a = bc$. When looking at the equations for a and b, we can conclude that c must be 1, because if it was bigger, the other equation would not hold. If b is 2a, then a must be $\frac{1}{2}b$ but then c would not be an integer.

It is the same thing for if a or b is negative, as then it would be that $c = -1$

9. Prove that if a and b are integers and a divides b, then a is odd or b is even.

Solution:

When a devides b we know that b must be a multiple of a. We also know that an even number multiplied by an integer will always give an even number, so if b is even, then a cannot be odd. And then if a is odd, then b must also be odd.

17. Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \le c \le 12$ such that

a) $c \equiv 9a \pmod{13}$.
b) $c \equiv 11b \pmod{13}$.
c) $c \equiv a + b \pmod{13}$.
d) $c \equiv 2a + 3b \pmod{13}$.
e) $c \equiv a^2 + b^2 \pmod{13}$.
f) $c \equiv a^3 - b^3 \pmod{13}$.

21. Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if a **mod** $m = b$ **mod** m.

29. Find a **div** m and a **mod** m when

a) $a = 228$, $m = 119$.
b) $a = 9009$, $m = 223$.
c) $a = -10101$, $m = 333$.
d) $a = -765432$, $m = 38271$.

Solution:

a) 1=228 **div** 119, 109 = 228 **mod** 119

b) 40 = 9009 **div** 223, 89 = 9009 **mod** 223

c) −31 = −10101 **div** 333, 222 = −10101 **mod** 333

d) −21 = −765432 **div** 38721, 38259 = −765432 **mod** 38721

1. Does 17 divide each of these numbers?

a) 68 **b)** 84 **c)** 357 **d)** 1001

41. 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 $a \equiv b \pmod{n}$.

Solution:

When $n \mid m$ we know that m is a multiple of n. And when we say $a \equiv b(\bmod m)$ we basically say that a and b is the same distance away from a multiple of m. But since we also know that m is a multiple of n, this means that a and b must be the same distance away from a multiple of n as well.

43. 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 $a^c \equiv b^d \pmod{m}$.

Solution:

a) This is false when $m = c$. Example: $a = 19, b = 18, c = 5, m = 5$. We would then have

$$19 \cdot 5 \bmod 5 = 18 \cdot 5 \bmod 5 \Leftrightarrow 95 \bmod 5 = 90 \bmod 5 \Leftrightarrow 0 = 0$$

Which is true. But then: $19 \bmod 5 = 18 \bmod 5 \Leftrightarrow 4 = 3$ Which is false.

b) $a = -13, b = -23, c = 5, d = 15, m = 10.$

Proof:

$$-13 \bmod 10 = -23 \bmod 10 \Leftrightarrow 7 = 7$$

$$5 \bmod 10 = 15 \bmod 10 \Leftrightarrow 5 = 5$$

$$(-13)^5 \bmod 10 = (-23)^{15} \bmod 10 \Leftrightarrow -371293 \bmod 10 \approx -2.666352 \cdot 10^{20} \Leftrightarrow 7 = 3$$

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

Solution:

When you look at a table of a number of n^2 and $n^2 - (n-1)^2$ you can see an interesting pattern:

n	n^2	$n^2 - (n-1)^2$
2	4	3
3	9	5
4	16	7
5	25	9
6	36	11
7	49	13
8	64	15
9	81	17

On this table you can see that the difference between each n^2 grows by 2 for each *n*. This means that the difference is n^2 and $(n-1)^2$ is always $4 \cdot x \pm 1$. So as we can see, n^2 is always either a multiple of 4, or *a multiple of 4* plus 1.

45. Use Exercise 44 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.

Solution:

As seen on the table, n^2 is always either a multiple of 4, or *a multiple of 4* +1. *m* is always 1 below a multiple of 4, which makes it never be equal to the sum of the squares of two integers. This is because the sum of the squares of two integers will always either be 4k (when the squares of the two integers both are a multiple of 4), $4k + 1$ (when one of the squares are a multiple of 4, and the other is a multiple + 1), or $4k + 2$ (when both of the squares are a multiple of 4 + 1). So the sum of the squares of two integers will never equal $4k + 3$

47. 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 $a^k \equiv b^k \pmod{m}$.

Solution:

This is true because $a \equiv a^k (\text{mod } m)$. We know this as when you for when you take a^k, the result will still be a multiple of a. So that means that you could rewrite a^k as $a \cdot a^{k-1} \cdot a^{k-2}$.... So if we call the $a^{k-1} \cdot a^{k-2}$... l, we can write $a = m \cdot c + d$ and $a \cdot l = m \cdot c \cdot l + d$.

51. Write out the addition and multiplication tables for $\mathbf{Z}_5$ (where by addition and multiplication we mean $+_5$ and $\cdot_5$).

Dette er korrekt. eller er det