

1. For $n = 8, 27$, find all positive integers less than n and relatively prime to n .

- $n = 8 = 2^3$:

Remember, an integer a is relatively prime to 8 if $\gcd(a, 8) = 1$. If 2 divides a , then since 2 also divides 8, $\gcd(a, 8) \neq 1$. But since 2 is the only prime factor of 8, if 2 does *not* divide a , then $\gcd(a, 8) = 1$.

Thus, the set of all positive integers less than 8 and relatively prime to 8 is the set of all odd numbers:

$$\{1, 3, 5, 7\}.$$

- $n = 27 = 3^3$:

If 3 divides an integer a , then since 3 also divides 27, $\gcd(a, 27) \neq 1$. However, since 3 is the only prime factor of 27, if 3 does *not* divide a , then $\gcd(a, 27) = 1$.

Thus, the set of all positive integers less than 27 and relatively prime to 27 is the set of all positive integers which aren't multiples of 3; that is,

$$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}.$$

2. If $a = 2^4 \cdot 3^2 \cdot 5 \cdot 7^2$ and $b = 2 \cdot 3^3 \cdot 7 \cdot 11$, determine $\gcd(a, b)$ and $\text{lcm}(a, b)$.

For both of these, we use the fact that all integers have unique prime factorizations.

- Any number which divides a must consist only of factors of a .

Furthermore, it can't have more factors of 2, for instance, than a does. Thus any number which divides a must have between 0 and 4 factors of 2.

Similarly, any number which divides b must consist only of factors of b , and it can't have more factors of (for instance) 2 than b does. Thus any number that divides b must have between 0 and 1 factor of 2.

The most 2's a common divisor of both a and b could have is thus 1, and so the greatest common divisor of a and b must have exactly 1 power of 2.

Proceeding similarly, $\gcd(a, b)$ must have a factor of 3^2 (3^2 divides both a and b , but 3^3 only divides b); and a factor of 7; while 5 divides a it doesn't divide b so it can't divide the common divisor, and similarly for 11.

Thus $\gcd(a, b) = 2 \cdot 3^2 \cdot 7$.

- Any multiple of a has as some of its factors 2^4 , 3^2 , 5, and 7^2 . Similarly, any multiple of b has as some of its factors 2, 3^3 , 7, and 11.

Thus any common multiple of both a and b must have *at least* factors of 2^4 , 3^3 , 5, 7^2 , and 11. This gives us the least common multiple:

$$\mathbf{lcm(a, b)} = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11$$

3. Determine $51 \pmod{13}$.

$51 \pmod{13}$ = the remainder when 51 is divided by 13. Thus $51 \pmod{13} = 12$.

Another way to think of it: 13 goes evenly in to 52, exactly 4 times. 51 is one short of 52, so the remainder is -1. $51 \pmod{13} = -1 = 12$.

4. $\gcd(12, 35) = 1$, of course. Find integers s and t so that $1 = 12s + 35t$. Are s and t unique?

Remember to use the Euclidean Algorithm: use division repeatedly (you may need to look in your books)

•

$$35 = 2 \cdot 12 + 11 \quad \implies \quad 11 = 35 - 2 \cdot 12$$

$$12 = 1 \cdot 11 + 1 \quad \implies \quad 1 = 12 - 1 \cdot 11$$

$$1111 \cdot 1$$

Putting our results together and working backwards, we find

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ &= 12 - (35 - 2 \cdot 12) \\ &= 3 \cdot 12 - 1 \cdot 35 \end{aligned}$$

Therefore with $s = 3$ and $t = -1$, $1 = 12s + 35t$.

- Are s and t unique?

NO! It is also true that $11 \cdot 35 - 32 \cdot 12 = 385 - 384 = 1$, or in other words, $1 = 12s + 35t$ with $s = -32$ and $t = 11$.

(I just found this by fiddling around; there's probably an efficient way to find a counter-example to the uniqueness of the linear combination, but I didn't find one.)

5. Let $S = \mathbb{R}$ and define $a \sim b \iff a^2 = b^2$.

- (a) Show \sim is an equivalence relation.

I need to check:

- **Reflexivity:** For all $a \in \mathbb{R}$, is $a \sim a$?
- **Symmetry:** For all $a, b \in \mathbb{R}$ such that $a \sim b$, is it also true that $b \sim a$?
- **Transitivity:** For all $a, b, c \in \mathbb{R}$ such that $a \sim b$ and $b \sim c$, is it true that $a \sim c$?

How do those questions translate to this situation?

- **Reflexivity:** For all $a \in \mathbb{R}$, is $a \sim a$?
In other words, is $a^2 \stackrel{?}{=} a^2$? Of course!
- **Symmetry:** For all $a, b \in \mathbb{R}$ such that $a \sim b$, is it also true that $b \sim a$?
In other words, is it true that if $a^2 = b^2$, then $b^2 = a^2$? Of course!
- **Transitivity:** For all $a, b, c \in \mathbb{R}$ such that $a \sim b$ and $b \sim c$, is it true that $a \sim c$?
In other words, is it true that if $a^2 = b^2$ and $b^2 = c^2$, then $a^2 = c^2$? Of course!

Therefore the relation $a \sim b$ if $a^2 = b^2$ **is an equivalence relation.**

- (b) What are the equivalence classes?

By definition, $[a] = \{b \in \mathbb{R} | b \sim a\} = \{b \in \mathbb{R} | b^2 = a^2\} = \{a, -a\}$.

Thus, the equivalence classes of this equivalence relation are:

$$[0] = \{0\}$$

$$[1] = \{1, -1\}$$

$$[2] = \{2, -2\}$$

$$[3] = \{3, -3\}$$

etc