Find 52^{-1} in Z_{165}. Does every element in Z_{165} have an inverse?

Problem Solving - What are the terms/strategies I may need? What do I know?

Definition of an inverse:

x^{-1} such that $xx^{-1} = 1$ in the space

Z_n $= \{0, 1, 2, \dots, n-1\}$ such that $a + b$ in the space is $(a + b) mod\ n$

Definition of mod n $(a + b) mod\ n = r$ where $(a + b) = qn + r$ with $q, r \in Z$ and $0 \leq r < n$

Theorems:

If $\gcd(a, n) = 1$ then a has a multiplicative inverse in Z_n

$n\ mod\ n = 0$

Euclidean Algorithm for finding $\gcd(a, b)$

Start with finding $a = q_0 b + r_0$

Then continue to iterate $b = q_1 r_0 + r_1$

$r_0 = q_2 r_1 + r_2$

…

Continue until the remainder is 0, then we have that r_{n-1} is our GCD

Using the extended Euclid algorithm, we can always find $as + nt = \gcd(a, n)$ by working backwards from the Euclid algorithm to find the inverse of a

Find 52^{-1} in Z_{165}. Does every element in Z_{165} have an inverse?

Steps & Process – Try to answer the question writing in many steps to avoid small errors.

Here we want to find $GCD(52{,}165)$ using the Euclid Algorithm:

$$165 = 3 \times 52 + 9$$
$$52 = 5 \times 9 + 7$$
$$9 = 1 \times 7 + 2$$
$$7 = 3 \times 2 + 1$$
$$2 = 2 \times 1 + 0$$

Thus the $\gcd(52{,}165) = 1$ so we do have a multiplicative inverse of 52. To find it we use the extended Euclid Algorithm:
Ignoring the last line, and working backwards, we can see that

$$1 = 7 - 3 \times 2$$
$$1 = 7 - 3 \times (9 - 1 \times 7) \qquad = (4) \times 7 - 3 \times (9)$$
$$1 = (4) \times (52 - 5 \times 9) - 3 \times (9) \qquad = (4) \times (52) + (-23) \times 9$$
$$1 = (4) \times (52) + (-23) \times (165 - 3 \times 52) \qquad = (73) \times 52 + (-23) \times 165$$

$\Rightarrow \quad 23 \times 165 + 1 = 73 \times 52$

$\Rightarrow \quad (73 \times 52) mod\ 165 = 1$

$\Rightarrow \quad$ Thus we have our inverse $52^{-1} = 73$ under mod 165

We note that not everything has an inverse as it is impossible for 5 to have an inverse since GCD(165, 5) = 5

Find 52^{-1} in Z_{165}. Does every element in Z_{165} have an inverse?

Solidify Understanding – Explain why the steps makes sense by connecting to math you know.

Why does the Extended Euclid Algorithm work?

Why is it that if the GCD of (a, n) is not 1 then we have no a^{-1}?

Can you find all elements that do not have inverses in Z_{165}?

For Video Please click the link below:

Video