

Activity: Review of the Euclidean Algorithm

The goal of this activity is to remember how to use the Euclidean Algorithm to find the greatest common divisor of two elements in a ring (numbers or polynomials, for us) and write the gcd as a linear combination of the two elements (which Bezout's lemma tells us we can do).

Example 1 Let's find the gcd of 945 and 2415. Repeatedly use the division algorithm:

$$2415 = 945 \cdot 2 + 525$$

$$945 = 525 \cdot 1 + 420$$

$$525 = 420 \cdot 1 + 105$$

$$420 = 105 \cdot 4 + 0.$$

Check: 105 divides all the quotients and remainders, and any other divisor of 945 and 2415 would also divide 105. Therefore, $\gcd(945, 2415) = 105$.

Now work backwards to obtain numbers r and s such that $945r + 2415s = 105$.

$$\begin{aligned} 105 &= 525 + (-1) \cdot 420 \\ &= 525 + (-1) \cdot [945 + (-1) \cdot 525] \\ &= 2 \cdot 525 + (-1) \cdot 945 \\ &= 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 \\ &= 2 \cdot 2415 + (-5) \cdot 945. \end{aligned}$$

So $r = -5$ and $s = 2$. □

1. Find the greatest common divisor of 471 and 564 using the Euclidean Algorithm and then find integers r and s such that $\gcd(471, 564) = 471r + 564s$.

2. In the quotient ring $\mathbb{Z}/\langle 564 \rangle$, find an element $a + \langle 564 \rangle$ such that $(a + \langle 564 \rangle)(471 + \langle 564 \rangle) = 3 + \langle 564 \rangle$. Explain why the previous question is helpful here.

3. Is $471 + \langle 564 \rangle$ a unit in $\mathbb{Z}/\langle 564 \rangle$? Explain.

- 2