Bezout's identity and the extended Euclidean algorithm

Lesson 23 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

---

Practice problems

1. Find $\gcd(120, 48)$ and find integers x and y such that $120x + 48y = \gcd(120, 48)$.
2. Find the GCD of 81 and 57 and express it as a linear combination of the two.
3. If $\gcd(a, b) = 1$, we say a and b are relatively prime. Use the extended Euclidean algorithm to find x and y such that $17x + 13y = 1$.

Solutions

1. Find $\gcd(120, 48)$ and find integers x and y such that $120x + 48y = \gcd(120, 48)$.

   - Step 1: $120 = 2 \cdot 48 + 24$
   - Step 2: $48 = 2 \cdot 24 + 0$. The GCD is 24.
   - Step 3: From the first equation, $24 = 1 \cdot 120 - 2 \cdot 48$.
   - Step 4: Thus, $x = 1$ and $y = -2$.

   Answer: x = 1, y = -2

2. Find the GCD of 81 and 57 and express it as a linear combination of the two.

   - Step 1: $81 = 1 \cdot 57 + 24$
   - Step 2: $57 = 2 \cdot 24 + 9$
   - Step 3: $24 = 2 \cdot 9 + 6$
   - Step 4: $9 = 1 \cdot 6 + 3$
   - Step 5: $6 = 2 \cdot 3 + 0$. The GCD is 3.
   - Step 6: $3 = 9 - 1 \cdot 6$
   - Step 7: $3 = 9 - 1(24 - 2 \cdot 9) = 3 \cdot 9 - 1 \cdot 24$
   - Step 8: $3 = 3(57 - 2 \cdot 24) - 1 \cdot 24 = 3 \cdot 57 - 7 \cdot 24$
   - Step 9: $3 = 3 \cdot 57 - 7(81 - 1 \cdot 57) = 10 \cdot 57 - 7 \cdot 81$.

   Answer: 3 = (-7) \cdot 81 + 10 \cdot 57

3. If $\gcd(a, b) = 1$, we say a and b are relatively prime. Use the extended Euclidean algorithm to find x and y such that $17x + 13y = 1$.

   - Step 1: $17 = 1 \cdot 13 + 4$
   - Step 2: $13 = 3 \cdot 4 + 1$
   - Step 3: $4 = 4 \cdot 1 + 0$. The GCD is 1.
   - Step 4: $1 = 13 - 3 \cdot 4$
   - Step 5: $1 = 13 - 3(17 - 1 \cdot 13) = 4 \cdot 13 - 3 \cdot 17$.

   Answer: x = -3, y = 4
