

Math 55, Euclidean Algorithm Worksheet

Feb 12, 2013

For each pair of integers (a, b) , use the Euclidean algorithm to find their gcd. Then reverse the steps of the algorithm to find integers s and t such that $as + bt = \gcd(a, b)$.

1. $a=254, b=32$

$$254 = 7 \cdot 32 + 30$$

$$32 = 1 \cdot 30 + 2$$

$$30 = 15 \cdot 2 + 0$$

so $\gcd(254, 32) = 2$.

$$30 = 254 - 7 \cdot 32$$

$$2 = 32 - 1 \cdot 30$$

$$= 32 - (254 - 7 \cdot 32)$$

$$= 8 \cdot 32 - 254$$

so $s = -1$ and $t = 8$.

2. $a=74, b=383$

$$383 = 5 \cdot 74 + 13$$

$$74 = 5 \cdot 13 + 9$$

$$13 = 1 \cdot 9 + 4$$

$$9 = 2 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

so $\gcd(74, 383) = 1$.

$$13 = 383 - 5 \cdot 74$$

$$9 = 74 - 5 \cdot 13$$

$$= 74 - 5(383 - 5 \cdot 74)$$

$$= 26 \cdot 74 - 5 \cdot 383$$

$$4 = 13 - 9$$

$$= (383 - 5 \cdot 74) - (26 \cdot 74 - 5 \cdot 383)$$

$$= 6 \cdot 383 - 31 \cdot 74$$

$$1 = 9 - 2 \cdot 4$$

$$= (26 \cdot 74 - 5 \cdot 383) - 2(6 \cdot 383 - 31 \cdot 74)$$

$$= 88 \cdot 74 - 17 \cdot 383$$

so $s = 88$ and $t = -17$.

3. $a=7544, b=115$

$$7544 = 65 \cdot 115 + 69$$

$$115 = 1 \cdot 69 + 46$$

$$69 = 1 \cdot 46 + 23$$

$$46 = 2 \cdot 23 + 0$$

so $\gcd(7544, 115) = 23$.

$$\begin{aligned}69 &= 7544 - 65 \cdot 115 \\46 &= 115 - 69 \\&= 115 - (7544 - 65 \cdot 115) \\&= 66 \cdot 115 - 7544 \\23 &= 69 - 46 \\&= (7544 - 65 \cdot 115) - (66 \cdot 115 - 7544) \\&= 2 \cdot 7544 - 131 \cdot 115\end{aligned}$$

so $s = 2$ and $t = -131$.

4. $a=687$, $b=24$

$$\begin{aligned}687 &= 28 \cdot 24 + 15 \\24 &= 1 \cdot 15 + 9 \\15 &= 1 \cdot 9 + 6 \\9 &= 1 \cdot 6 + 3 \\6 &= 2 \cdot 3 + 0\end{aligned}$$

so $\gcd(687, 24) = 3$.

$$\begin{aligned}15 &= 687 - 28 \cdot 24 \\9 &= 24 - 15 \\&= 24 - (687 - 28 \cdot 24) \\&= 29 \cdot 24 - 687 \\6 &= 15 - 9 \\&= (687 - 28 \cdot 24) - (29 \cdot 24 - 687) \\&= 2 \cdot 687 - 57 \cdot 24 \\3 &= 9 - 6 \\&= (29 \cdot 24 - 687) - (2 \cdot 687 - 57 \cdot 24) \\&= 86 \cdot 24 - 3 \cdot 687\end{aligned}$$

so $s = -3$ and $t = 86$.

What is the inverse of $74 \pmod{383}$?

We computed above that

$$1 = 88 \cdot 74 - 17 \cdot 383$$

so

$$1 \equiv 88 \cdot 74 \pmod{383}.$$

So by definition of inverse, 88 is the inverse of $74 \pmod{383}$.