Bezout Coefficients

Marcio Woitek

Problem 1

Answer: $(7, -4)$

When we apply the extended Euclidean algorithm with $m = 19$ and $n = 11$, this is what we get:

m	n	q	r	s	t	$\hat{s}$	$\hat{t}$
19	11	1	8	1	0	0	1
11	8	1	3	0	1	1	-1
8	3	2	2	1	-1	-1	2
3	2	1	1	-1	2	3	-5
2	1	2	0	3	-5	-4	7

The desired result is in the last two columns of the last row. Specifically, the coefficient corresponding to m is the final value of $\hat{s}$, and the coefficient associated with n is the last $\hat{t}$. Therefore, $t = -4$ and $s = 7$. This has to be true, since $19 \cdot (-4) + 11 \cdot 7 = -76 + 77 = 1$.

Problem 2

Answer: No, any number of the form $24s + 32t$ where s, t are integers must be divisible by 8.

Bob is going to receive s coins from Alice. This amounts to $24s$. To make this exchange work, Bob has to give Alice t coins. In this case, Bob is losing money, which means the total is $-32t$. Since the goal is to give Bob 4 cents, the following equation must hold:

$$24s - 32t = 4. \tag{1}$$

Next, denote the LHS of this equation by T. We also introduce $t' = -t$. Using these definitions, we can write

$$T = 24s + 32t' = 8(3s + 4t'). \tag{2}$$

The last expression makes it clear that T is divisible by 8. Since 4 doesn't have this property, it's impossible to satisfy $T = 4$.

Problem 3

Answer: No such integer since $15k \bmod 21$ must be divisible by 3 for all k.

Assume it's possible to satisfy the equation we were given. In this case, we can write $15k$ as follows:

$$15k = 21q + 1, \tag{3}$$

where q is some unknown integer. $15k$ is clearly divisible by 3. Then the RHS of the above equation must also be divisible by 3. We can express this fact through the following equation:

$$(21q + 1) \bmod 3 = 0. \tag{4}$$

Notice that 21 is also divisible by 3. This allows us to write

$$(21q + 1) \bmod 3 = [(21q) \bmod 3 + 1 \bmod 3] \bmod 3 = 1. \tag{5}$$

Then we've just shown that $1 = 0$. Since this is absurd, our assumption that the original problem has a solution must be wrong.

Problem 4

Answer: $s \leftarrow s - qs'$, $t \leftarrow t - qt'$

To avoid confusion, let's denote the original m, n, q and r by m_0, n_0, q_0 and r_0. Next, imagine we're applying the extended Euclidean algorithm with $m = m_0$ and $n = n_0$. The first two steps are represented below.

m	n	q	r	s	t	$\hat{s}$	$\hat{t}$
m_0	n_0	q_0	r_0	1	0	0	1
n_0	r_0	$n_0//r_0$	$n_0\%r_0$	0	1	1	$-q_0$

Notice that, starting from the second row, we're using the extended Euclidean algorithm with $m = n_0$ and $n = r_0 = m_0 \bmod n_0$. This is the exact same situation the problem statement talks about. This table also shows us that the coefficients associated with r_0 are $\hat{s}$ and $\hat{t}$. As we know, these coefficients are updated by using the following rules:

$$\hat{s} \leftarrow s - q\hat{s}, \tag{6}$$
$$\hat{t} \leftarrow t - q\hat{t}. \tag{7}$$

Inspecting the first row of our table, we see that $\hat{s}$ and $\hat{t}$ are also related to n_0. In the problem statement, these coefficients are denoted by s' and t'. Therefore, the rules for updating the coefficients related to r_0 are

$$\hat{s} \leftarrow s - qs', \tag{8}$$
$$\hat{t} \leftarrow t - qt'. \tag{9}$$

Our notation doesn't match the one used in the options, but it has the advantage of not being confusing.