2 Euclid's Algorithm

(a) gcd(527, 323) = **17**

Step (Recursive Call)	x	y
1	527	323
2	323	204
3	204	119
4	119	85
5	85	34
6	34	17
7	17	0

And then 17 would be returned, so the greatest common divisor is 17.

(b) $5^{-1} \equiv \mathbf{11} \pmod{27}$

We would like to implement the extended Euclid's algorithm on 27 and 5.

Step (Recursive Call)	x	y	Return
1	27	5	$(1, -2, 11)$
2	5	2	$(1, 1, -2)$
3	2	1	$(1, 0, 1)$
4	1	0	$(1, 1, 0)$

And then $(1, -2, 11)$ would be returned, so we have that $\gcd(27, 5) = 1 = -2 * 27 + 11 * 5$.
Thus, $5^{-1} \equiv 11 \pmod{27}$.

(c) $x = \mathbf{17}$

Since we have that $5x + 26 \equiv 3 \pmod{27}$, so we have that $5x \equiv -23 \equiv 4 \pmod{27}$. Then, since we have from part (b) that $5^{-1} \equiv 11 \pmod{27}$, which is equivalent to $5 * 11 \equiv 1 \pmod{27}$, so we have that $5 * 11 * 4 \equiv 4 \pmod{27}$. Thus, $x = 11 * 4 = 44 \equiv 17 \pmod{27}$, so $x = 17$.

(d) Disprove

I will proceed by providing a counterexample. Consider $a = 1, b = 0, c = 1, x = 0$.
For any $x \in \mathbb{Z}$, we have that $ax = 1x = cx + 0$, which means that $ax \bmod c$ would always be 0, which implies that a has no multiplicative inverse mod c, as indicated by the hypothesis of our preposition. Then, consider $x = 0$, by definition of modular arithmetic, we have that $ax = 1 * 0 = 0 \equiv b \pmod{c}$, so $x = 0$ is a solution to the equation $ax \equiv b \pmod{c}$. Thus, $a = 1, b = 0, c = 1, x = 0$ is a counterexample.