1. (5 + 6 marks)

   a) Assume b and $m > 1$ are relatively prime. Apply Lemma 0 (which allows the gcd as an integer combination of the two numbers) to show that if $ax \equiv b \pmod{m}$ has a solution x_0 then x_0 and a must both be relatively prime to m.

Lemma 0: exists $r, s \in \mathbb{Z}$ such that $br + ms = 1$. (*) (0.5)

If $ax_0 \equiv b \pmod{m}$ then $ax_0 - b = mk$ or $b = ax_0 - mk$, (3)

so (*) $(ax_0 - mk)r + ms = 1$ becomes $a(x_0 r) + m(s - kr) = 1$

so $\gcd(x_0, m)$ and $\gcd(a, m)$ both must divide 1, so they (1.5)