Dennis Kuzminer
CSCI-UA 310-001 PS4

6.

a. $100z + 200 \equiv 93z + 171\ (mod\ 1000) \rightarrow 7z \equiv -29\ (mod\ 1000) \rightarrow 7z \equiv 971(mod\ 1000)$
$d = gcd(7, 1000) = 1 \rightarrow$ There is a unique solution from [1...n).
$z = 971t\ mod\ 1000,\ t = 7^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 7) $\rightarrow d = 1,\ s = -1,\ t = 143$
$z = 29(143)\ mod\ 1000 \rightarrow 4147\ mod\ 1000 =$ **853**

b. $115z + 130 \equiv 100z + 165\ (mod\ 1000) \rightarrow 15z \equiv 35\ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(15, 1000) = 5 \rightarrow$ There are unique solutions from [1...n), as 5|35.
$15z \equiv 35\ (mod\ 1000) \rightarrow /d \rightarrow 3z \equiv 7\ (mod\ 200)$
$z = 7t\ mod\ 200,\ t = 15^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 15) $\rightarrow d = 5,\ s = -1,\ t = 67$
$z = 469\ mod\ 200 = 69 \rightarrow$ Other solutions: 69+0, 69+200, 69+4(200), 69+2(200), 69+3(200) $\rightarrow$ **69, 269, 469, 669, 869**

c. $115z + 132 \equiv 100z + 140\ (mod\ 1000) \rightarrow 15z \equiv 8\ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(15, 1000) = 5 \rightarrow$ There are **no solutions** in [1...n), as $5 \nmid 8$.

d. $119z + 132 \equiv 113z + 140\ (mod\ 1000) \rightarrow 6z \equiv 8\ (mod\ 1000) \rightarrow d = gcd(a, n) \rightarrow$
$d = gcd(6, 1000) = 2 \rightarrow$ There are unique solutions from [1...n), as 2|8.
$6z \equiv 8\ (mod\ 1000) \rightarrow /d \rightarrow 3z \equiv 4\ (mod\ 500)$
$z = 4t\ mod\ 500,\ t = 6^{-1} mod\ 1000 \rightarrow$ ExtEuclid(1000, 6) $\rightarrow d = 2,\ s = -1,\ t = 167$
$z = 4(167)\ mod\ 500 \rightarrow 668\ mod\ 500 = 168 \rightarrow$ Other solutions: 168+0, 168+500 $\rightarrow$ **168, 668**