#1

a) GCD(82, 24)

$82 = 24(3) + 10$
$24 = 10(2) + 4$
$10 = 4(2) + 2$
$4 = 2(2) + 0$

The GCD(82,24) = 2

The remainder sequence is (82,24), (24,10), (10,4), (4,2), (2,0).

in the form (a, s, t)

1. (82, 1, 0)
2. (24, 0, 1)
3. (10, 1, -3)
4. (4, -2, 7)

$\Longrightarrow \quad 2 = 82(-2) + 24(7)$

b.) co-factors of (144, 89)

$144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 7$
$8 = 7(1) + 1$
$7 = 1(7) + 0$

gcd = 1
≡ co-prime ≡

$144 = \frac{144}{1}$

$89 = \frac{89}{1}$

The co-factors are 34 & −55

Remainder sequence
(144, 1, 0)
(89, 0, 1)
(55, 1, -1)
(34, -1, 2)
(21, 2, -3)
(13, -3, 5)
(8, 5, -8)
(5, -8, 13)
(3, 13, -2)
(2, 34, -55)
(0, -89, 144)

$\Longrightarrow \quad 1 = 144(34) + 89(-55)$

c.) We can use Lames theorem (# of steps in Euclidean is at most 5x the # of digits (in base 10) of smaller b (given h(a,b)).

A tighter upper bound can be done using Fibonacci sequence, known to produce the longest Euclidean algorithm sequence for a pair of consecutive #'s. Thus, the length of a sequence $h(F_{k+1})$ for 2 fib #'s F_k + F_{k+1} is k taking k division steps to find GCD of F_k & F_{k+1}

The upper bound for $h(250)$ is 13

Using Fib:

$1+0=1$, $1+1=2$, $2+1=3$, $3+2=5$, $5+3=8$, $8+5=13$, $13+8=21$, $21+13=34$, $34+21=55$, $55+34=89$, $89+55=144$, $144+89=233$ $\Rightarrow$ 13 steps

d.) Find $h(a,b)$ s.t. $0<b<a\leq 250$

Using the Fibonacci sequence/algorithm above the largest a,b we can get is $233+144$ (F_{13}, F_{12}). Since 233 (step 13) is our limit our lower bound is the next highest limit (F_{12}).

e.) The upper bound is closer to the true value. The true value is 13. This is because it requires 13 Fibonacci #'s to get closer to $n=250$.

#2

a.) $6x \equiv 10 \pmod{21}$

$(a,b,n) = (6,10,21)$ s.t $a=6$ $b=10$ & $n=21$
To solve linear congruence we must solve for x s.t $6x \equiv 10 \pmod{21}$
However, the GCD of of 6 & 21 is 3 & 3 does not divide by 10 thus
x DNE

b.) $4x \equiv 10 \pmod{21}$

$(a,b,n) = (4,10,21)$ s.t $a=4$, $b=10$, & $c=21$. The correct answer is
$x=13$.

$GCD(4,21) = 1$, thus we can find multiplicative inverse of 4 mod 21 & multiplying the inverse by 10 gives us solution, which modulo 21 is 13.

c.) $6x \equiv 15 \pmod{21}$

answer:
$x = 20, 6, \& \ 13 \pmod{21}$

Explanation/work: $(a,b,n) = (6,15,21)$. First we find $GCD(6,21) = 3$.
Since 3 divides 15 we have 3 solutions & can simplify our equation:
$2x \equiv 5 \pmod{7}$ ← divided everything by GCD

Next we find multiplicative inverse of $2 \pmod{7}$ using Euclidean. Once the inverse was found, it was multiplied by $5\left(\frac{15}{GCD}\right)$. The soutions are:

1. $x \equiv 20 \pmod{21}$
2. $x \equiv 20+7 \pmod{21}$
3. $x \equiv 20+2\cdot 7 \pmod{21}$

Which simplifies to

1. $x \equiv 20 \pmod{21}$
2. $x \equiv 6 \pmod{21}$
3. $x \equiv 13 \pmod{21}$

Thus $x \equiv 20, 6, \& \ 13 \pmod{21}$

#3

(a) Given the hint that a must divide 10..., we can manually check the powers of each element. The primitive roots of $\mathbb{Z}^*_{11}$ are 2, 6, 7 & 8. These #'s when raised to powers from 1 to 10 modulo 11, generate all elements $\mathbb{Z}_{11}$ without rep.

(b) The set $\mathbb{Z}^*_{12}$ consists of all integers less than 12 that are coprime to 12. The set $\mathbb{Z}^*_{12}$ consists of 1, 5, 7, + 11.

(c) To determine if 11 is in $\mathbb{Z}^*_{90}$ we need to check if 11 is coprime to 90. The element 11 is in $\mathbb{Z}^*_{90}$ because they share no common divisors except for 1. The prime factoritation of 90 is $2 \times 3^2 \times 5$ & the # 11 does not appear in there thus 11 is in $\mathbb{Z}^*_{90}$.