1. In which of the following Die Hard scenarios do the heroes survive? Justify your answer.

   (a) Target 5ℓ, jug capacities 7ℓ and 4ℓ.

   (b) Target 12ℓ, jug capacities 182ℓ and 217ℓ.

   (c) Target $\frac{1}{2}\ell$, jug capacities $6\frac{1}{4}\ell$ and $11\frac{1}{4}\ell$.

   (d) **(Optional)**Target 6ℓ, jug capacities 16ℓ, 28ℓ, and 36ℓ.

   Solution:

   (a) They survive: The GCD of 7 and 4 is 1 so any target that fits into A, including 5, is possible. The Die Hard algorithm reaches the target after the following steps:

jug A (7ℓ)	jug B (4ℓ)	action
—	4ℓ	fill B
4ℓ	—	B → A
4ℓ	4ℓ	fill B
7ℓ	1ℓ	B → A
—	1ℓ	spill A
1ℓ	—	B → A
1ℓ	4ℓ	fill B
5ℓ	—	B → A

   The algorithm took three iterations during which jug A was spilled once. At the end it must contain $3 \cdot 4 - 1 \cdot 7 = 5$ litres of water.

   (b) Since $\gcd(182, 217) = 7$ and 7 does not divide 12, they die.

   (c) We can change the measuring unit to $\frac{1}{4}\ell$. The target is 2 units with jug capacities 25 units and 45 units. Since $\gcd(25, 45) = 5$ and 5 does not divide 2, they die.

   (d) They die. We will argue that the amount of water in each jug is a multiple of 4. The proof is essentially identical to the one we gave for Lemma 2 in Lecture 4 (but the Lemma itself is not adequate as it talks about two and not three bins). Initially, every jug is empty so the amount is a multiple of 4. This property is preserved by the pouring steps because not only is the amount in each jug is a multiple of 4, but so is the remaining capacity. Since every step completely fills a jug, completely empties a jug, or transfers an amount equal to the remaining capacity of one of the jugs, the amounts will be multiples of 4 after the transition. Since 6 is not a multiple of 4, they die.

2. Apply the extended GCD algorithm to find a representation of $\gcd(a, b)$ as a combination $sa + tb$ of a and b given below. The two coefficients s and t will have different signs. Then find another combination with the signs reversed.

   (a) $a = 105$ and $b = 42$

   (b) $a = 2002$ and $b = 1881$

   Solution:

   (a) We first apply Euclid's algorithm to calculate the GCD:

$$\begin{aligned} E(105, 42) &= E(42, 21) && \text{because } 105 = 2 \cdot 42 + 21 \\ &= E(21, 0) && \text{because } 42 = 2 \cdot 21 \end{aligned}$$

Thus $\gcd(105, 42) = 21$. The desired combination comes from the first equation

$$21 = 105 - 2 \cdot 42.$$

To reverse the signs of the coefficients we add $-42 \cdot 105 + 105 \cdot 42$ to the right hand side to obtain

$$21 = (1 - 42) \cdot 105 + (-2 + 105) \cdot 42 = -41 \cdot 105 + 103 \cdot 42.$$

(b)

$$\begin{aligned} E(2002, 1881) &= E(1881, 121) && \text{because } 2002 = 1 \cdot 1881 + 121 \\ &= E(121, 66) && \text{because } 1881 = 15 \cdot 121 + 66 \\ &= E(66, 55) && \text{because } 121 = 1 \cdot 66 + 55 \\ &= E(55, 11) && \text{because } 66 = 1 \cdot 55 + 11 \\ &= E(11, 0) && \text{because } 55 = 5 \cdot 11, \end{aligned}$$

so $\gcd(1881, 121) = 11$. To find s and t we work backwards starting with the second equation from the bottom which expresses 11 as a combination of 66 and 55:

$$11 = 66 - 55$$

The previous equation expresses 55 as a combination $55 = 121 - 66$. Combining the two we get

$$11 = 66 - (121 - 66) = -121 + 2 \cdot 66$$

Moving up, $66 = 1881 - 15 \cdot 121$, from where

$$11 = -121 + 2 \cdot (1881 - 15 \cdot 121) = 2 \cdot 1881 - 31 \cdot 121.$$

Finally, the first equation gives $121 = 2002 - 1881$ and

$$11 = 2 \cdot 1881 - 31 \cdot (2002 - 1881) = -31 \cdot 2002 + 33 \cdot 1881.$$

To reverse the signs we add $1881 \cdot 2002 - 2002 \cdot 1881$ to the right-hand side and collect terms to get

$$11 = (-31 + 1881) \cdot 2002 + (33 - 2002) \cdot 1881 = 1850 \cdot 2002 - 1969 \cdot 1881.$$

3. Here is another algorithm G for calculating GCDs. It assumes the inputs a and b are positive integers.

```
$G(a, b)$ :
    if $a = b$, output $a$.
    if $a > b$, output $G(a - b, b)$
    otherwise, output $G(a, b - a)$.
```

(a) Viewing G as a state machine, show the states that the algorithm visits on inputs $a = 27$ and $b = 6$.

(b) Prove that the GCD of the two arguments stays the same throughout the execution.

(c) Use part (b) to prove that $G(a, b)$ outputs the GCD of a and b assuming that it has terminated.

(d) Prove that G always terminates (**Hint:** There is a quantity that decreases in every step.)

Solution:

(a) $(27, 6) \to (21, 6) \to (15, 6) \to G(9, 6) \to (3, 6) \to (3, 3)$. The algorithm then outputs 3.

(b) The transitions of the algorithm are of the form $(a, b) \to (a - b, b)$ or $(a, b) \to (a, b - a)$. Let's consider the first type of transition. To show that it preserves the GCD we prove that any given d divides both a and b *if and only if* d divides both $a - b$ and b. It will follow that the pairs (a, b) and $(a - b, b)$ have the same common divisors and therefore the same GCD.

First assume d divides both a and b. Then d must also divide their combination $a - b$ so it divides both $a - b$ and b.

Now assume d divides both $a - b$ and b. Then d must also divide their combination $(a - b) + b$ which equals a so d divides both a and b.

The proof for the second type of transition $(a, b) \to (a, b - a)$ is completely symmetric. Only the names of a and b are swapped there.

(c) By part (b) the GCD of the two numbers in the state remains invariant throughout the execution. The output is produced when the two numbers are equal to one another. In that case the output equals both numbers which is also their GCD. Therefore the output must equal the GCD of the two inputs.

(d) The sum of the two numbers must decrease because $(a - b) + b = a < a + b$ and $a + (b - a) = b < a + b$. As both numbers remain strictly positive (this is another invariant!) the algorithm on input a, b cannot run for more than $a + b$ steps.

4. For each of the following statements about integers, say if it is true or false. Justify your claim with a proof.

(a) If c divides $a + b$ then c divides a and c divides b.

(b) If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ then $\gcd(ab, c) = 1$.
(**Hint:** Use the connection between gcd and combinations.)

(c) For all $n \geq 1$, $\gcd(21n + 4, 14n + 3) = 1$.

Solution:

(a) False. $c = 2$, $a = 3$, $b = 5$ is a counterexample because 2 divides $3 + 5 = 8$ but 2 does not divide 3, let alone 5 also.

(b) True. Assume $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$. Then, $ap + cq = 1$ and $br + cs = 1$ for some integers p, q, r, s. We can write

$$(ap)(br) = (1 - cq)(1 - cs) = 1 + c(-q - s + csq).$$

So $1 = ab(pr) + c(q + s - csq)$ is an integer combination of ab and c. Therefore their GCD must be 1.

(c) True because 1 is a combination of $21n+4$ and $14n-3$ for all n, namely $1 = -2\cdot(21n+4)+3\cdot(14n+3)$. This combination may look mysterious but it is simply the output of extended Euclid's algorithm:

$$\begin{aligned} E(21n + 4, 14n + 3) &= E(14n + 3, 7n + 1) && \text{because } 21n + 4 = (14n + 3) + (7n + 1) \\ &= E(7n + 1, 1) && \text{because } 14n + 3 = 2 \cdot (7n + 1) + 1 \\ &= E(1, 0) && \text{because } 7n + 1 = (7n + 1) \cdot 1 \\ &= 1 \end{aligned}$$

As usual the coefficients -2 and 3 can be found by working backwards.