Problem 1.
Suppose $a$ has quotient $q$ and remainder $r$ when divided by $b$. What is the quotient and remainder of $3a$ when divided by $3b$?

Proof. Since $a = bq + r$ we have $3a = 3bq + 3r$. Since $0 \leq r < b$ we have $0 \leq 3r < 3b$. Then $3r$ is the remainder of $3a$ when divided by $3b$, and $q$ is the quotient. \hfill \Box

Problem 2.

a) Use the Euclidean algorithm to find the gcd of the following pairs of numbers: $(52, 47)$, $(124, 1024)$, $(201, 315)$

Answers: $1, 4, 3$.

b) Find at least one pair of integer solutions for each of the following equations

\begin{align*}
52x + 47y &= 1 \\
124x + 1024y &= 4 \\
201x + 315y &= 3
\end{align*}

c) Given two positive integers $a, b$, describe how to find at least one solution to the equation $ax + by = \text{gcd}(a, b)$.

Proof. Let $r_1, r_2, \ldots, r_n$ be the sequence of remainders in the euclidean algorithm applied to $a$ and $b$, with $r_n = \text{gcd}(a, b)$. We will describe how to find integers $x_i, y_i$ such that $ax_i + by_i = r_i$ for each $i$. Since $r_1 = a - bq_1$ we can set $x_1 = 1, y_1 = -q_1$. Similarly we can find $x_2, y_2$. Now suppose

\begin{align*}
ax_{k-1} + bx_k - 1 &= r_{k-1} \\
ax_k + bx_k &= r_k
\end{align*}

Let us find the next pair $x_{k+1}, y_{k+1}$. We have $r_{k-1} = r_k q_k + r_{k+1}$, and thus

\begin{align*}
r_{k+1} = r_{k-1} - r_k q_k = ax_{k-1} + bx_k - 1 - ax_k + bx_k = a(x_{k-1} - q_k x_k) + b(y_{k-1} - q_k y_k)
\end{align*}

Thus we can set $x_{k+1} = x_{k-1} - q_k x_k$ and $y_{k+1} = y_{k-1} - q_k y_k$. \hfill \Box

Problem 3.

In this problem, you can assume the conclusion of problem 2c): For any two positive integers $a, b$ there exists an integer solution $x, y$ to the equation $ax + by = \text{gcd}(a, b)$.

a) Let $a$ be an integer and $p$ be a prime number that does not divide $a$. What is $\text{gcd}(a, p)$?
Proof. Since the only positive divisors of \( p \) are 1 and \( p \), and \( p \) is not a divisor of \( a \), the gcd is 1.

b) (Euclid’s lemma) Suppose \( a, b \) are positive integers and \( p \) is prime such that \( p \mid ab \). Prove that \( p \mid a \) or \( p \mid b \). (Hint: assume that \( p \) does not divide \( a \). Then by part a) you know \( \text{gcd}(a, p) \). Use that and 2c)

Proof. Suppose \( p \) does not divide \( a \). Then \( \text{gcd}(a, p) = 1 \), and by 2c) we find integers \( x, y \) such that \( ax + py = 1 \). If we multiply this equation by \( b \) we get \( abx + pby = b \). Since \( p \mid ab \) we get that \( p \) is a divisor of \( abx + pby \), which means \( p \mid b \) and we are done.

Problem 4.
Using problem 3b), it is possible to show that any positive integer has a unique prime factorization: it can be written as a product of primes in a unique way. You can use this fact in this problem.

a) Find the smallest integer greater than 1 that has remainder 1 when divided by 2, 3, 5, 7.

Proof. If \( n \) has remainder 1 when divided by 2, 3, 5, 7, then \( n - 1 \) is divisible by 2, 3, 5, 7. Then \( n - 1 \) must have all those primes in its prime factorization, which means \( n - 1 \) is divisible by 210. Thus the smallest possible \( n \) is 211.

b) Find all such positive integers.

Proof. Since \( n - 1 \) has to be divisible by 210, and all such \( n \) work, we get \( n = 210k + 1 \) as the general expression for \( n \).