Greatest Common Divisor

Q1. Let a, b be positive numbers and let X be the set of all positive numbers r such that $xa = yb + r$ for some natural numbers x, y. Prove that the set X is exactly the set of all multiples of $gcd(a, b)$. First show that the smallest element must be $gcd(a, b)$ and any other element must be a multiple of the gcd.

Q2. Let a, b be positive numbers such that $a \bmod b \neq 0$. Let $g > 0$ be the smallest number such that $xa \bmod b = g$ for some number x. Prove that $g = gcd(a, b)$. This implies that a has a multiplicative inverse mod b if and only if $gcd(a, b) = 1$.

Q3. Consider the following definition of a function $f(n, m)$. Define $f(0, n) = n$ for all n, $f(n, m) = f(m, n)$ for all n, m and $f(n, m) = f(n \bmod m, m)$. Prove using strong induction that this defines f uniquely and that for all n, m $f(n, m) = gcd(n, m)$. This gives an algorithm for computing $gcd(n, m)$ called Euclid's algorithm. If n, m are numbers with k bits in their binary representations, find an upper bound on the number of arithmetic operations required to compute the gcd. Modify the algorithm to find x and y such that $xn = ym + gcd(n, m)$.

Q4. Another algorithm for finding the gcd is given by a different definition. Again $gcd(0, n) = gcd(n, 0) = n$ for all n, $gcd(2n, 2m) = 2gcd(n, m)$, $gcd(2n, 2m + 1) = gcd(n, 2m+1)$, $gcd(2n+1, 2m) = gcd(2n+1, m)$ and $gcd(2n+1, 2m+1) = gcd(2m+1, n-m)$ if $m \leq n$ and $gcd(2n + 1, m - n)$ otherwise. Prove that this function is well-defined and it gives exactly the gcd of n, m. This needs the fact that every number $n > 0$ is either $2m$ or $2m + 1$ for some $m < n$. This has the advantage that it uses only subtraction and division by 2, and is easier to implement in hardware.

Q5. Consider an $m \times n$ matrix A with integer entries. Let L be the set of all m-dimensional vectors v such that $v = Ax$ for some n-dimensional vector x with integer entries. The set L is called a lattice. Prove that for any such matrix A, there exists an $m \times m$ matrix B such that L is exactly the set of vectors By, where y can be any integral m-dimensional vector. Note that when A is the 1×2 matrix $[ab]$, B is the 1×1 matrix $[gcd(a, b)]$. B is called a basis for L. A challenging problem is to find a basis with "smallest" possible entries and a vector in L with smallest magnitude. This is equivalent to finding gcd if $m = 1$ but is much more difficult for arbitrary m. Try to do it for $m = 2$. The dimension of L is the smallest k such that every vector in L can be written as an integer linear combination of k m-dimensional vectors. The dimesion of L can be at most m but may be less than m. Given the matrix A, can you find an efficient algorithm to find the dimension of L?