Exercise 1: (Modular inverse)

Use the extended euclidian algorithm (`ExtendedGCD`), to program the function `ModInv[a,p]` which determines the inverse of an integer a, if it exists and return 0 otherwise.

(6 points)

Exercise 1: (Chinese remainder theorem)

Program the solution of the Chinese remainder theorem 4.10 of the lecture and test your program on the following examples:

(a) $x \equiv 112 \mod 383, \quad x \equiv 63 \mod 701$

(b) $x \equiv 41 \mod 541, \quad x \equiv 77 \mod 547, \quad x \equiv 131 \mod 557$

(c) $x \equiv 52 \mod 83, \quad x \equiv 1443 \mod 2651, \quad x \equiv 2111 \mod 9713$

(d) $x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 5 \mod 7, \quad x \equiv 7 \mod 11, \quad x \equiv 11 \mod 13.$

(10 points)