Cryptography in Networking, Exercises 2 (September 21, 2017)

1) Find the elements with multiplicative inverses in $\mathbb{Z}_{24}$. What are those inverses?

2) The input of the Extended Euclidean algorithm consists of integers $a$ and $b$. The algorithm returns a triple $(d, x, y)$ which satisfies the equation $d = \gcd(a, b) = ax + by$. The recursive version of the algorithm is short:

**Extended-Euclid $(a, b)$:**

1. if $b = 0$
   2. then return $(a, 1, b)$;
3. $(d', x', y') := \text{Extended-Euclid}(b, a \mod b)$;
4. $(d, x, y) := (d', y', x' - \lfloor a/b \rfloor y')$;
5. return $(d, x, y)$.

The following example shows how the algorithm works when the input is $a = 99$, $b = 78$:

| $a$ | $b$ | $|a/b|$ | $d$ | $x$ | $y$ |
|-----|-----|--------|-----|-----|-----|
| 99  | 78  | 1      | 3   | -11 | 14  |
| 78  | 21  | 3      | 3   | 3   | -11 |
| 21  | 15  | 1      | 3   | -2  | 3   |
| 15  | 6   | 2      | 3   | 1   | -2  |
| 6   | 3   | 2      | 3   | 0   | 1   |
| 3   | 0   | -      | 3   | 1   | 0   |

Simulate the algorithm with numbers $a = 215$ and $b = 710$. How is it possible, with the help of the algorithm, to determine the multiplicative inverse of $a$ modulo $p$ ($p$ a prime)?

3) Find all primitive roots modulo 19.

4) (a) Construct (addition and multiplication tables) the finite field $GF_f(2^3)$ using the irreducible polynomial $f(X) = X^3 + X^2 + 1$.
   
   (b) Show that this polynomial is indeed irreducible.

5) (a) Construct $GF_g(2^3)$ using the irreducible polynomial $g(X) = X^3 + X + 1$.
   
   (b) Using results from (a) and from previous exercise, try to find a mapping $h : GF_f(2^3) \rightarrow GF_g(2^3)$ such that $h$ is bijective (one-to-one) and $h$ satisfies the conditions

   i) $h(p(X) \oplus_f q(X)) = h(p(X)) \oplus_g h(q(X))$,
   
   ii) $h(p(X) \otimes_f q(X)) = h(p(X)) \otimes_g h(q(X))$,

   for all $p(X), q(X) \in GF_f(2^3)$. Such a function $h$ is called an *isomorphism* and its existence shows that the fields $GF_f(2^3)$ and $GF_g(2^3)$ are structurally identical. This implies that the only difference between the two is that elements are named in different way.

6) Let us study a linear feedback shift register (LFSR) that corresponds to the irreducible polynomial $f = X^4 + X^3 + 1$ in $\mathbb{Z}_2[X]$.

Apply the LFSR to show that the polynomial $X$ generates the whole multiplicative group in $GF_f(2^4)$. 