T-79.503 Fundamentals of Cryptology
Homework 6
October 22, 2003

1. (Stinson 5.4) Compute $\gcd(57, 93)$, and find integers s and t such that $57s + 93t = \gcd(57, 93)$.

2. (Stinson 5.7) Solve the following system of congruences:

$$\begin{aligned} 13x &\equiv 4 \bmod 99 \\ 15x &\equiv 56 \bmod 101 \end{aligned}$$

   HINT First use the EXTENDED EUCLIDEAN ALGORITHM, and then apply the Chinese remainder theorem.

3. a) Compute $\phi(100)$.
   b) Determine the two least significant decimal digits of the integer 2003^{2003}.

4. Find the cyclic multiplicative subgroups of $\mathbb{Z}_{23}$.

5. Consider the finite field $GF(2^3)$ with polynomial x^3+x+1 (see Stinson 6.4). Create the look-up table for the inversion function $z \mapsto z^{-1}$ in $GF(2^3)$.

6. Let f be the Boolean function defined by the leftmost output bit of the S-box S_1 of DES.

   a) Create a look-up table for f considered as a function of the four middle input bits by setting $x_1 = x_6 = 1$.
   b) Derive the algebraic normal form of f.
   c) Count the number of inputs $(1, x_2, x_3, x_4, x_5, 1)$, for which $f(1, x_2, x_3, x_4, x_5, 1) = x_3$ and determine the correlation between the third (from the left) input bit and the leftmost output bit on the 4th row of S_1.