T-79.503 Fundamentals of Cryptology
Homework 6
October 28, 2004

1. Compute $\gcd(9211, 4880)$, and find integers $s$ and $t$ such that $9211s + 4880t = \gcd(9211, 4880)$.

2. Solve the following system of congruences

$$\begin{aligned} 15x &\equiv 12 \pmod{2003} \\ 11x &\equiv 5 \pmod{2004} \end{aligned}$$

3. a) Compute $\phi(100)$.

   b) Determine the two least significant decimal digits of the integer $2004^{2004}$.

4. (Stinson 5.9) Suppose that $p = 2q + 1$, where $p$ and $q$ are odd primes. Suppose further that $\alpha \in \mathbb{Z}_p^*$, $\alpha \not\equiv \pm 1 \pmod{p}$. Prove that $\alpha$ is a primitive element modulo $p$ if and only if $\alpha^q \equiv -1 \pmod{p}$ .

5. Find the smallest primitive element in $\mathbb{Z}_{23}^*$. (Hint: use the result of problem 4.) What are the orders of elements 2 and 4? Give 2 and 4 as powers of the smallest primitive element.

6. It is given that

$$2^{48} \equiv 443 \pmod{1201},$$

   where 1201 is prime. Show that the element $\alpha = 443$ has multiplictive order 25 in the group $\mathbb{Z}_{1201}^*$.