Introduction to Cryptography

Homework 2

September 28, 2006

1. Assume that m and n are coprime integers; for solving the system of congruences

$$\begin{aligned} x &\equiv a \bmod m, \\ x &\equiv b \bmod n, \end{aligned}$$

compute integers r, s with $mr + ns = 1$, and put $x = ans + bmr$.

   (a) Show that this x solves the system.

   (b) Estimate the complexity of this algorithm; here you may assume that $0 \le a < m$ and $0 \le b < n$.

2. Let $f, g \in \mathbb{Z}[X]$ be polynomials. What is the complexity for computing $f + g$ and fg?

3. Let f and g be polynomials in $(\mathbb{Z}/m\mathbb{Z})[X]$. What is the complexity for computing $f + g$ and fg?

4. Prove the following rules for gcd's of natural numbers:

$$\gcd(a, b) = \begin{cases} 2\gcd(\frac{a}{2}, \frac{b}{2}) & \text{if } 2 \mid a, 2 \mid b; \\ \gcd(\frac{a}{2}, b) & \text{if } 2 \mid a, 2 \nmid b; \\ \gcd(\frac{a-b}{2}, b) & \text{if } 2 \nmid ab. \end{cases}$$

5. Show how to compute $\gcd(91, 77)$ using these rules. This algorithm is due to Stein (1961).