Algebraic Cryptography
Homework 1

Due Wednesday, 6 September 2017

Problem 1. The *Division Algorithm* states that for nonnegative integers $a, b \in \mathbb{Z}$ with $b \neq 0$ (called the *dividend* and *divisor*, there exist integers $q, r \in \mathbb{Z}$ with $0 \leq r < b$ (call the *quotient* and *remainder*) for which $a = qb + r$. Prove the Division Algorithm.

Problem 2. The *greatest common divisor* of two nonzero integers a, b is the largest positive integer which divides both a, b. We denote this $\gcd(a, b)$. A linear combination of a, b over $\mathbb{Z}$ is a quantity of the form $ax+by$ where $a, b \in \mathbb{Z}$. *Bezout's identity* asserts that the greatest common divisor of a, b is the smallest positive linear combination of a, b over $\mathbb{Z}$. Symbolically,

$$\gcd(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Prove Bezout's identity.

Problem 3. The *Euclidean Algorithm* is the following sequence of operations. Let $a, b \in \mathbb{Z}$ with $b > 0$. Repeatedly apply the Division Algorithm to the divisor and remainder of the previous division until the remainder is zero. In other words:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

For this problem:

(a) Prove that the Euclidean Algorithm terminates.

(b) Prove that the last nonzero remainder is $\gcd(a, b)$.

(c) Explain how the Euclidean Algorithm allows for the computation of the integers x, y in Bezout's identity.

Problem 4. The purpose of this problem is to analyze the efficiency of the Euclidean Algorithm. This necessitates a quick study of the Fibonacci sequence. Let $F_0 = 0$, $F_1 = 1$, and for all $n > 1$, define $F_n = F_{n-1} + F_{n-2}$; this is the *Fibonacci sequence*. In particular, the Fibonacci sequence is a linear recursion with constant coefficients. Let $\varphi = \frac{1+\sqrt{5}}{2}$ denote the *golden ratio*.

(a) Prove that the Fibonacci sequence is generated by the formula

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}},$$

and hence $F_n = \lceil \varphi^n \rceil$.

(b) Prove that that number of divisions required in the Euclidean Algorithm is at most $\log_\varphi b + 1$.

(c) Show that the above bound is optimal. That is, for any positive integer n, find positive integers a, b with $n > \log_\varphi b$ for which the Euclidean Algorithm applied to a, b requires n divisions.

Problem 5. Suppose that p, q are primes, $n = pq$ and e is a positive integer for which $\gcd(e, \operatorname{lcm}(p-1, q-1)) = 1$.

(a) Explain how to find a d for which $de \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$.

(b) Prove that $m^{ed} \equiv m \pmod{n}$. (This is Exercise 1 in Chapter 1, *hint: Fermat's Little Theorem*)

Problem 6. Exercise 4(a)–(d) of Chapter 1: Kid Krypto.