# Algebraic Cryptography
# Homework 2

Due Monday, 18 September 2017

**Problem 1.** Explain in detail the *square and multiply* algorithm for computing modular exponentiation efficiently. Use this method to compute

$$2956^{2039} \pmod{5219}.$$

Note: you can use a computer (a standard scientific calculator should suffice, otherwise you are not using an efficient algorithm!) to do each of the multiplications and modular reductions, but I should be able to see the algorithm you described at work in the example.

**Problem 2.** All the exercises for §1 of Chapter 2. There are 15, but they should each take less than 1 minute. You do not need to provide proofs.

**Problem 3.** Exercises 1,2,3 from §2 of Chapter 2. Exercise 2 does not require proofs, but the others do.

After having proven the Division Algorithm on the last homework, you now know that the proof of existence of the quotient and remainder is nonconstructive, instead relying on the well-ordering of a certain set of integers. In this homework, we will analyze an actual division method.

**Problem 4.** The *Newton–Raphson method* is a numerical method for computing the zeros of a real-valued differentiable function. The method proceeds as follows for the function $f$:

- Guess a value $x_0$ for the zero of $f$.
- for $n \geq 1$, set $x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)}$.

This numerical scheme does not always converge, but it often works in applications, and in fact, convergence is often quadratic.

Now consider the following. To calculate the quotient and remainder from a division with dividend $a$ and divisor $b$, it suffices to calculate only one or the other, because the other can be easily calculated once one is known. Moreover, the quotient is the floor of the $\frac{a}{b}$ (i.e., greatest integer less or equal to $\frac{a}{b}$). Therefore, if we can calculate $\frac{a}{b}$ sufficiently accurately, then we can compute the quotient (since it's the integer part). Moreover, $\frac{a}{b} = a \cdot \frac{1}{b}$, so if we can calculate $\frac{1}{b}$ with high precision, then we can do division by multiplication!

So, suppose we want to divide by $b$. We can approximate $\frac{1}{b}$ by applying the Newton–Raphson method to the function $f(x) := \frac{1}{x} - b$.

(a) Show that the iterations of the Newton–Rapshon method can be achieved solely with the addition and multiplication of known quantities.

(b) Define the error of the $n$-th approximant to be $e_n = bx_n - 1$. Prove that $e_{n+1} = -e_n^2$.

(c) Using the previous error calculation, what is the valid range (in terms of $b$) for your initial guess in order to ensure convergence? Explain how to easily choose an initial guess (expressed in binary).

(d) If your initial guess is good to one (binary) significant figure, how many iterations do you have to compute in order to ensure your guess is good to 500 binary significant figures (i.e., 500 bits of precision)?