MA503: Homework 5

Use wolfram alpha (or google search) for modular exponentiation.

Exercise 5.1. [6pts] Compute ALL distinct powers of 2 modulo $n = 29$ to find $\log_2(21)$.

Exercise 5.2. [2pts] Use computations done in Exercise 5.1 to solve an instance $n = 29$, $g = 2$, $A = 18$, $B = 14$ of CDH.

Exercise 5.3. [2pts] Suppose that Bob sends a message to Alice using ElGamal protocol. For public information collected by Eve $n = 29$, $g = 2$, $A = 17$, $c_1 = 6$ and $c_2 = 10$ find m. Use computations done in Exercise 5.1.

Exercise 5.4. [10pts] For $n = 37$ use the babystep-giantstep algorithm to compute $\log_2(3)$ modulo n. I expect to see the list of babysteps, the list of giantsteps, and a matching pair.

Exercise 5.5. [10pts] Use Pohlig–Hellman algorithm to compute $\log_2(19)$ modulo 37. Compute x_i's directly, by computing sufficiently many powers of g_i.

Exercise 5.6. [10pts] For $N = 43$ and $g = 5$ compute $|g|$, choose $B = 3$. Compute B-smooth powers $g^i \,\%\, 43$ for $i = 1, \ldots, 15$ and use them to compute $\log_5(2)$ and $\log_5(3)$.

A **ring** is a set R with two binary operations $+$ and $\cdot$, called **addition** and **multiplication**, that satisfy the following axioms:

(R1) (R,+) is an abelian group with identity denoted by 0.
(R2) Multiplication is associative and R contains 1 (**unity**).
(R3) $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

To check if $(R, +, \cdot)$ is a ring it is sufficient to check that $+$ and $\cdot$ are indeed binary functions on R and that all axioms (R1), (R2), (R3) are satisfied.

Exercise 5.7. [+12pts] Which of the following are rings? EXPLAIN!

(1) $(\mathbb{Z}, +, \cdot)$
(2) $(\mathbb{Z}_n, +, \cdot)$.
(3) $(U_n, +, \cdot)$.
(4) $(\mathbb{N}, +, \cdot)$.
(5) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ with standard addition and multiplication.
(6) The set of all real-valued functions $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ with $+, \cdot$ defined as follows:

$$(f + g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$