Midterm exam, November 16, 2007. TIME: 55 minutes

http://people.aub.edu.lb/∼kmakdisi/

GRADES (each problem is worth 10 points):

1	2	3	4	5	6	7	TOTAL/70

Instructions: This exam booklet is also your answer sheet; **please answer question 0 on this page, and answer questions 1–7 inside the booklet.** Calculators are allowed. In any problem, you may use part (a) to solve part (b) even if you were not able to solve part (a).

Good luck!

0. a) Your name: b) Your AUB ID#:

1. Let $a = 10500$ and $b = 3654$.

a) Find the prime factorizations of a and b, and use these to compute the GCD (a, b).

b) Find (a, b) again, this time by the Euclidean algorithm.

2. Find all integers x that simultaneously satisfy $x \equiv 2 \pmod{13}$, $x \equiv 3 \pmod{9}$.

3. Find a solution of $x^3 + x \equiv 13 \pmod{11^2}$. (There are several, but you should only find ONE.)

4. Compute the two Legendre symbols $\left(\frac{6}{37}\right)$, $\left(\frac{11}{31}\right)$ in two ways **each**:

a) using quadratic reciprocity;

b) using Euler's criterion.

5. a) Show that every $\overline{x} \in (\mathbf{Z}/20200\mathbf{Z})^*$ satisfies $\overline{x}^{100} = \overline{1}$.

b) The function $f : (\mathbf{Z}/20200\mathbf{Z})^* \to (\mathbf{Z}/20200\mathbf{Z})^*$ given by $f(\overline{x}) = \overline{x}^{17}$ is a bijection. Show this by explicitly computing a formula for the inverse function f^{-1}.

6. Let p be a prime number.

a) If $x \in \mathbf{Z}$, show that the GCD $(x, x^2 + p)$ is either 1 or p.

b) If $x, y \in \mathbf{Z}$ satisfy $y^2 = x^3 + px$, show that x is either a square or p times a square (so $x = \ell^2$ or $x = p\ell^2$ for some integer ℓ).

7. Let p be a prime number of the form $p = 4q + 1$ with q prime.

a) Show that $\left(\frac{2}{p}\right) = -1$.

b) Show that 2 is a primitive root modulo p.