TEST 1

NAME, First name :		

Duration : 70 minutes, Total of points : 20 pts

Exercise 1 (4 pts). For each statement, decide whether it is true of false. Justify (by a proof or a counterexample). Let $n \in \mathbb{N}^*$.

(1) If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, then n is prime.

(2) For all $m \in \mathbb{N}^*$, the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic.

(3) For all $a \in \mathbb{N}$, if $\left(\frac{a}{n}\right) = -1$, then a is not a square modulo n.

Exercise 2 (3 pts). Let p be an odd prime and n be a divisor of $p-1$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Show that a has an n^{th} square root if and only if $a^{\frac{p-1}{n}} = 1$.

Exercise 3 (2 pts). Is 2 a square modulo the prime number $p = 241$?

Exercise 4 (4 pts). Solve the equation $x^2 = 137 \mod 323$.
Hint. One can use that $323 = 17 \cdot 19$ and $1 = 17 \cdot 9 - 19 \cdot 8$.

Exercise 5 (3 pts). (1) How many generators of $(\mathbb{Z}/13\mathbb{Z})^\times$ are there ? List them all.

(2) Let p be an odd prime and α a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Show that all the generators are given by α^i, with i and $p-1$ coprime. Deduce the number of generators of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercise 6 (4 pts). (1) What are the primes p such that $p+2$ and $p+4$ are also prime.

(2) What are the primes p such that p divide $2^p + 1$.

(3) Let p be an odd prime. Show that there exists infinitely many n such that p divide $n2^n + 1$.