

ASSIGNMENT 9 - NUMBER THEORY, WINTER 2009
(LAST ASSIGNMENT!)

Submit by Monday, March 30, 16:00.

Solve following questions:

- (40) Factor $n = 3599$, using both Fermat's and Pollard's $p = 1$ methods. In Pollard's method you can calculate the gcd's using a computer.
- (41) The message 2401 was sent using RSA with modulus $n = 3599$ and encryption key $e = 2983$. What was the original message?

In the following questions use the method we used in class for calculating $N(x^2 + y^2 = 1)$. Namely, $N(x^2 + y^2 = 1) = \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right)\right) \left(1 + \left(\frac{b}{p}\right)\right)$, etc.

- (42) Find the number of solutions to the equation $x^2 + y^2 = 0$ over $\mathbb{F}_p$.
- (43) Find the number of solutions to the equation $x^2 + y^2 = \alpha$ over $\mathbb{F}_p$, where $\alpha \in \mathbb{F}_p$ is a non-zero constant.

The honors students need to submit also the following problem.

- (M) Find the number of solutions to the equation $Ax^2 + By^2 = \alpha$ over $\mathbb{F}_p$, where $\alpha \in \mathbb{F}_p$ is a constant and $A, B \in \mathbb{F}_p$ are non-zero constants.