3. Exercise sheet
Hand in solutions until Thursday, 26 April 2007.

Exercise 3.1 (Playing with $\mathbb{Z}_{26}$). (10 points)

We have seen that an affine cipher of $\mathbb{Z}_{26}$ is given by a scaling factor $\alpha \in \mathbb{Z}_{26}^\times$ and a shift $i \in \mathbb{Z}_{26}$ as the map $A_{\alpha,i} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $a \mapsto \alpha a + i$. Suppose we are given a suitably long cipher text $c = (c_0, c_1, c_2, \ldots, c_{\ell-1})$. For a generalized Cesar $C_i = A_{1,i}$ it is sufficient to know one plain text letter $p_j$ then $i$ is determined by $c_j = p_j + i$ as $i = c_j - p_j$. Now suppose an affine cipher was used.

How many (different) plain text letters must we know such that we can determine the key in any case?

(i) Suppose $\alpha$ is known. How many further plain text letters do we need to determine $i$?
(ii) Say 0 (ie. A) translates to 0 (ie. A), and 13 (ie. N) translates to 13 (ie. N). Does that fix $\alpha$ and $i$?
(iii) Answer the global question.

Exercise 3.2 (Counting $\mathbb{Z}_{pq}$). (10 points)

In the course we have counted the number of invertible elements of $\mathbb{Z}_{26}$ by noting that a lot of elements are even or divisible by 13 and by writing down inverses for all the others.

(i) Do the same for $\mathbb{Z}_{35}$.

Generalize the argument to $\mathbb{Z}_{pq}$ where $p$ and $q$ are two different prime numbers:

(ii) Name $q$ numbers and $p$ numbers that cannot have inverses without telling more than one number in both cases.
(iii) First, prove that \( \#\mathbb{Z}^\times_{pq} \leq (p - 1)(q - 1) \) by identifying elements which cannot be invertible.

(iv) Second, use the fact that for any \( a \in \mathbb{N}_{<pq} \) which is not a multiple of \( p \) there exist \( s, t \in \mathbb{Z} \) such that \( sa + tp = 1 \) and for any \( a \in \mathbb{N}_{<pq} \) which is not a multiple of \( q \) there exist \( s', t' \in \mathbb{Z} \) such that \( s'a + t'q = 1 \) to show that all remaining numbers have inverses.

**Exercise 3.3 (Crack Vigenère).** (10+2 points)

By mail you received a Vigenère encrypted text.

- (i) Crack it using cryptool which you find at http://www.cryptool.de/. Use the analysis options to show what is done for the basis ciphers. Explain how you did proceed.

- (ii) Describe the autocorrelation of the sample text. How does the key length become visible?

- (iii) Read the help page on autocorrelation and analysis of the Vigenère cipher. Formulate in two sentences what autocorrelation is. In one further sentence explain why this helps in finding the key length.