8. Exercise sheet
Hand in solutions until Sunday, 16 June 2013, 23:59h.

Exercise 8.1. (10 points)
Let \( p \neq q \) be prime numbers, \( N = p \cdot q, f = x \in \mathbb{Z}_N[x] \).

(i) Show that \( p^2 + q^2 \) is a unit in \( \mathbb{Z}_N \), i.e. \( \gcd(p^2 + q^2, pq) = 1 \).

(ii) Let \( u \in \mathbb{Z}_N \) be the inverse of \( p^2 + q^2 \). Show that \( f = u(px + q)(qx + p) \).

(iii) Prove that the two linear factors in (ii) are irreducible in \( \mathbb{Z}_N[x] \). Hint: Consider the situation in \( \mathbb{Z}_p \) and \( \mathbb{Z}_q \) separately.

(iv) Conclude that factoring \( N \) is polynomial-time reducible to factoring polynomials in \( \mathbb{Z}_N[x] \).

Exercise 8.2 (An inequality of norms). (3 points)
Let \( f \in \mathbb{Z}[t] \) be a polynomial of degree \( n \). Define \( \|f\|_1 := \sum_{1 \leq i \leq n} |f_i| \) and \( \|f\|_2 := (\sum_{1 \leq i \leq n} f_i^2)^{1/2} \). Let \( \sigma(f) := \# \{ i | f_i \neq 0 \} \) be the sparsity of \( f \). Show that we have \( \|f\|_1 \leq \sqrt{\sigma(f)} \cdot \|f\|_2 \). Hint: Use the Cauchy-Schwarz inequality \( \langle f, g \rangle \leq \|f\| \cdot \|g\| \), where \( f \) and \( g \) are the coefficient vectors of two polynomials of degree \( n \).

Exercise 8.3 (The Coppersmith method). (27+5 points)
In the lecture we discussed an algorithm for finding small polynomials with high-order roots.

(i) Implement the algorithm in a programming language of your choice.

(ii) Play around with the parameters of the above algorithm. In particular perform the following experiments: Set \( N = 2183, \mu = 1/2, v = 56, f = x + v \). Now compute for all \( 1 \leq k \leq 15 \) the largest \( c \geq 3 \) for which your algorithm produces you a valid result.

(iii) What do the results tell you in the context of the security of RSA primes? Explain detailed.

(iv) Perform the same experiment with other values of \( v \). +5