8. Exercise sheet
Hand in solutions until Monday, 21 December 2010, 23:59h.

Exercise 8.1 (Order-finding revisited). (5 points)
Design an order-finding quantum circuit that uses an unitary operator
\[ V \ket{j} \ket{k} = \ket{j} \ket{k + x^j \text{ rem } N} \]
instead of the \( j \)-controlled \( U \) from the course. Hint: Show that you obtain the same state as the one given in Exercise 7.4 iv) when replacing \( U \) by \( V \) and setting the second register in state \( \ket{0} \) instead of \( \ket{1} \). Conclude that you have an efficient circuit by showing that the circuit for \( V \) is polynomial-size.

Exercise 8.2 (Equivalence). (5 points)
Prove that ORDER-FINDING and FACTORING are polynomial-time equivalent. Hint: To show this you need to give two polynomial-time reductions. Note that one of them was already given in the lecture.

Exercise 8.3 (Continued fraction step). (9+4 points)
We want to simulate the post-computation of the order-finding procedure. So choose \( \tilde{\varphi} \in 2^{-t} \mathbb{Z} \) close to \( \frac{s}{r} \) and compute the convergents of its continued fraction. We should observe that the last convergent with an \( L \)-bit denominator always divides \( r \). Recall that \( L \) is the bit length of the parameter \( N \) that describes the group \( \mathbb{Z}_N^* \) and we work with \( t = n + \lceil \log_2 \left( \frac{2 + \frac{1}{n}}{2} \right) \rceil \) bits to get \( n = 2L + 1 \) accurate bits of \( s/r \). So we should pick \( \tilde{\varphi} \in \left[ \frac{s}{r} - 2^{-n-1}, \frac{s}{r} + 2^{-n-1} \right] \cap 2^{-t} \mathbb{Z} \) because the probability to find it outside all of these ranges is at most \( \varepsilon \).

Let \( r = 36 \) and consider \( \varepsilon = 2^{-10} \), choose two values \( s \in \mathbb{N}_{<r} \) at random, one coprime to \( r \) and one not coprime to \( r \), and consider the five values for \( \tilde{\varphi} \) nearest to the center of the interval, three random values in the interval, two random values somewhat outside (enlarge the interval by a factor 32, say).

For each chosen situation do the following (it might be useful to employ a computer algebra system for the following tasks):

(i) Compute the probability to observe the particular \( \tilde{\varphi} \). Also write it as \( \frac{1}{r} \) to see how large it is compared to the upper bound.

(ii) Compute the continued fraction and the convergents of \( \tilde{\varphi} \). Hint: If the continued fraction is \( [a_0, a_1, a_2, \ldots] \) then you can compute the convergents \( \frac{p_i}{q_i} \) as follows: \( p_0 = 1, q_0 = 0, p_1 = a_0, q_1 = 1, p_i = a_{i-1} \cdot p_{i-1} + p_{i-2}, q_i = a_{i-1} \cdot q_{i-1} + q_{i-2} \) for \( i > 1 \).

(iii) Pick the last convergent with \( q_i < 2^L \) and let \( r' \) be its denominator. Check whether \( r' \) divides \( r \).

Interpret your results.
Exercise 8.4 (More on continued fractions). (0+10 points)

Read chapter A4.4 in the text-book and sketch the main theorems as well as the solutions to the exercises given there.