Quantum Information Theory

Prof. John Schliemann
Dr. Paul Wenk

Tue. H33 13pm c.t. & **Thu.** H34, 3pm c.t.
Mon. 12pm c.t., H33

Sheet 5

1 Adding Qubits with the Help of the Fourier Transform ..... [9P]

The goal is to build a quantum circuit for the operation $|x\rangle \to |x+y \mod 2^n\rangle$ with y being a constant and $0 \le x < 2^n$. In contrast to the simple addition with carrier from sheet 3 we perform the addition in the Fourier space: First, we apply a quantum Fourier transform (QFT) to $|x\rangle$, apply appropriate phase shifts which implement the addition, and finally reverse the QFT.

(a) Describe every step of the above procedure. How do the operators for the controlled phase shifts look like which implement the addition? *Hint: Write down the values to be added in binary.*

(b) Plot the quantum circuit for adding x and y in the case where both consist of three qubits.

(c) For which values of y is this procedure most optimal?

2 Divisibility of Numbers ....[12P]

(a) Find all $n \in \mathbb{N}$ such that $n+1|n^2+1$.

(b) Find all $n \in \mathbb{Z}\backslash\{3\}$ such that $n-3|n^3-3$.

(c) (i) By factorizing $a^{p-1}-1$ for $p>2$ prime and $a \in \mathbb{Z}$, $p \nmid a$, show that

$$a^{\frac{p-1}{2}} \equiv \pm 1 \mod p. \tag{1}$$

(ii) Prove $20801|20^{15}-1$.
Hint: Factorize 20801 and use Fermat's little theorem and (i).

3 Prime Factorization .... [6P]

Assume $a, b \in \mathbb{N}$ with $10 \nmid a$, $10 \nmid b$ and $ab = 1000$. Determine $a+b$.

4 Zero Divisor ....[5P]

A ring R is *free of zero divisors* if $\forall_{a,b\in R}\ a \cdot b = 0 \ \Rightarrow\ a = 0 \ \vee\ b = 0$.
Show that $\mathbb{Z}/m\mathbb{Z}$ is free of zero divisors iff m is prime.