Prof. Friedrich Eisenbrand
Gennady Shmonin

Due Date: November 3, 2008

# Combinatorial Optimization

Fall 2008

Assignment Sheet 3

**Exercise 1 (Number of minimum cuts)**
How many minimum cuts, with respect to a weight function $w : E \to \mathbb{R}$, can a graph $G = (V, E)$ have?

**Exercise 2 (Fast exponentiation)**
Describe an algorithm that, given positive integers $a$, $n$ and $m$, computes the value

$$a^n \bmod m.$$

The algorithm must be polynomial in the binary encoding length of $a$, $n$ and and $m$, that is, polynomial in $\log(a+1)$, $\log(n+1)$, and $\log(m+1)$.

**Exercise 3 (Carmichael numbers)**
Let $n$ be a Carmichael number, i.e., the congruence $a^{n-1} \equiv 1 \bmod n$ holds for any $a$, which is relatively prime to $n$. Prove that

(a) $n$ is odd;

(b) $n$ is not divisible by a square of any prime;

(c) if $p$ is a prime factor of $n$, then $p-1$ divides $\frac{n}{p} - 1$.

(d) $n$ has at least three prime factors.

Conversely, if $n$ is a product of at least three distinct odd primes such that $p-1$ divides $\frac{n}{p} - 1$ for each prime factor $p$ of $n$, prove that $n$ is a Carmichael number. Find the prime factors of 1729, and show that it is a Carmichael number.

**Exercise 4 (Determinant)**
Design a polynomial-time algorithm to test if the determinant of a given integral matrix is zero.

*Hint.* Modify the Gaussian elimination procedure to guarantee that all numbers in intermediate computations remain polynomial in the input size.