Prof. Dr. Alexander Bockmayr,
Prof. Dr. Knut Reinert,
Sandro Andreotti

November 5, 2012

Algorithms

WS 2012/13

Exercises 3

1. **Modulo Arithmetic (Niveau II)** Prove the following theorem:
   For any positive intergers a and n, if $d = gcd(a, n)$ (the greatest common divisor of a and n), then
   $$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, n - d\}$$
   and thus
   $$|\langle a \rangle| = n/d$$
   ($\langle a \rangle := \{a \cdot i \mod n \mid i \in \mathbb{N}\}$).
   Hint: Use Bezout's lemma. It states that if a and b are nonzero integers with greatest common divisor d, then there exist integers x and y such that $ax + by = d$

2. **Hashing (Niveau II)** Consider a version of the division method in which $h(k) = k \mod m$, where m=$2^p - 1$ and k is a character string interpreted in radix 2^p. Show that if string x can be derived from string y by permuting its characters, then x and y hash to the same value.

3. **Expected value (Niveau I)** Proof: Define pi = Pr (exactly i probes access occupied slots)for i = 0, 1, 2, ... (Note that for $i > n, p_i = 0$). The expected number of probes is then $\sum_{i=0}^{\infty} i \cdot p_i$. Now define q_i = Pr (at least i probes access occupied slots). Show that $\sum_{i=0}^{\infty} i \cdot p_i = \sum_{i=1}^{\infty} q_i$.