Prof.Dr. W.Koepf
Dr. E. Nana Chiadjeu

Exercise to the Lecture

UNIKASSEL VERSITÄT

Exercise sheet 07 **COMPUTER ALGEBRA I** **20.06.2013**

Aufgabe 1: (Carmichael numbers)
A Carmichael number is a composite positive integer p which satisfies the congruence $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}_p$.
A number $p \in \mathbb{N}_{\geq 4}$ is a Carmichael numbers if and only if

(i) $p = p_1 \cdots p_n$ with pairwise distinct primes $p_k \in \mathbb{P}$

(ii) $p_k - 1 \mid p - 1$ for all $j = 1, \ldots, n$

(a) Let be $k \in \mathbb{N}$. Prove that if each factor of the following number

$$p = (6\,k + 1) \cdot (12\,k + 1) \cdot (18k + 1) \tag{1}$$

is prime, then p is a Carmichael number.

(b) Use equation (1) and find via *Mathematica* a Carmichael number containing at least 120 digits.

(8 Punkte)

Aufgabe 2: (Lucas Test) Let be $n \in \mathbb{N}_{\geq 3}$. The number $n \in \mathbb{P}$ if and only if there exist $a \in \mathbb{N}$, $1 < a < n$, satisfying

$$a^{n-1} \equiv 1 \mod n \quad \text{and} \quad a^{\frac{n-1}{q}} \not\equiv 1 \mod n$$

for all prime divisors q of $n - 1$.

(a) Program the previous statement (**Lucas test**) in *Mathematica* to check if a given number $n \in \mathbb{N}$ is prime or not.

(b) Which knowledge about n resp. $n - 1$ is needed, such that an application of the Lucas-Test can be efficiently executed?

(8 Punkte)

Deadline: at the latest Thursday, 27.06.2013, 08.15 h to nana@mathematik.uni-kassel.de. More informations under `http://www.mathematik.uni-kassel.de/~koepf/ca-SS2013.html`