Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://resources.mpi-inf.mpg.de/departments/d1/teaching/ws14/ComputerAlgebra

Assignment sheet 7 due: Monday, December 11

Exercise 1: Computation of e

Show that

$$\begin{pmatrix} \frac{1}{1} & \frac{1}{1} \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} \frac{1}{n} & \frac{1}{n} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{n!} & \sum_{i=1}^{n} \frac{1}{i!} \\ 0 & 1 \end{pmatrix}.$$

Derive an algorithm with running time $\tilde{O}(n)$ for computing a rational approximation $\tilde{e}$ of Euler's number e with $|\tilde{e} - e| < 2^{-n}$!

Exercise 2: Square-free part (4 points)

Let $f \in F[x]$ be a polynomial with coefficients in a field and ℓ be defined as in the Extended Euclidean Algorithm when applied to $a := f$ and $b := f'$; that is,

$$s_\ell \cdot f + t_\ell \cdot f' = \gcd(f, f').$$

Show that the $t_{\ell+1}$ from the next iteration of the algorithm is the square-free part $f^* := f/\gcd(f, f')$ of f.

Exercise 3: Extended Euclidean Algorithm (4 points)

Trace the Extended Euclidean Algorithm (use a computer algebra system of your choice) to compute the GCD of

$$f = 77400x^7 + 29655x^6 - 153746x^5 + 37585x^4 + 91875x^3 - 130916x^2 - 21076x + 51183 \quad \text{and}$$
$$g = -5040x^6 + 27906x^5 + 44950x^4 - 66745x^3 + 69052x^2 + 111509x - 98208,$$

considered as polynomials in $\mathbb{Q}[x]$ with rational coefficients. What do you observe?

Copy and paste:

```
f = 77400*x^7 + 29655*x^6 - 153746*x^5 + 37585*x^4 + 91875*x^3 - 130916*x^2 - 21076*x + 51183
g = -5040*x^6 + 27906*x^5 + 44950*x^4 - 66745*x^3 + 69052*x^2 + 111509*x - 98208
```

Exercise 4: Yun's Algorithm (4 points)

Show that Yun's Algorithm computes a square-free factorization $f = \prod_{i=1}^{m} g_i^i$, with g_i square-free and pairwise coprime, of a polynomial $f \in R[x]$, where R is a factorial ring.

Algorithm 1: Yun's Square-Free Factorization Algorithm

Input : $f \in R[x]$ primitive, R a factorial ring.
Output : A square-free factorization $f = \prod_{i=1}^{m} g_i^i$ with pairwise coprime and square-free polynomials $g_i \in R[x]$.

$u := \gcd(f, f')$, $v_1 := \frac{f}{u}$, $w_1 := \frac{f'}{u}$, $i = 1$
while $v_i \neq 1$ **do**
  Recursively define
  $g_i := \gcd(v_i, w_i - v_i')$
  $v_{i+1} := \frac{v_i}{g_i}$
  $w_{i+1} := \frac{w_i - v_i'}{g_i}$
  $i = i + 1$
$m := i - 1$
return $g_1 \dots g_m$