max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2014/15**

Computer Algebra

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

Assignment sheet 5 due: Wednesday, December 3

Exercise 1: Choosing points with large absolute value (4 points)

Let $f \in \mathbb{Z}[x]$ be an integer polynomial of degree strictly less than n with coefficients of absolute value less than 2^τ. Let further $x_1, \ldots, x_n \in \mathbb{Q}$ be n distinct rational points in the unit circle (i.e., $|x_i| \leq 1$) of bitsize τ (i.e., if $x_i = p_i/q_i$ in reduced form, then p_i and q_i are integers of absolute value less than 2^τ).

We say that the point x_i is *large* for f among $\{x_1, \ldots, x_n\}$ if

$$4|f(x_i)| \geq \max_{1 \leq j \leq n} |f(x_j)| =: \lambda.$$

- Determine the cost of finding a large point in a naive way, that is, by evaluating f at all points x_j exactly.
- Show how to find a large point in $\tilde{O}\big(n(\tau + \log \max\{1, \lambda^{-1}\})\big)$ bit operations.

  Hint: Use approximate evaluation with increasing precision.

Exercise 2: Properties of rings (4 points + 2 bonus points)

1. Show that $\mathbb{Z}[x]$ is not a principal ideal domain.
2. Give an example of an irreducible element in the ring $\mathbb{Z}[\sqrt{-13}]$ that is not prime.
3. Give an example of a (non-factorial) ring R in which Gauß' Lemma does not hold; that is, there is a polynomial $f \in R[x]$ which is irreducible over $R[x]$, but factors over $F[x]$, where F is the quotient field of R.
4. Prove: If R is a Euclidean domain, then R is also a principal ideal domain.
5. Show that $\mathbb{Q}[x_1, \ldots, x_n]$ is not a Euclidean domain for all $n \geq 2$.

Exercise 3: Square-free part (4 points)

Let $f \in \mathbb{R}[x]$ be a polynomial with real coefficients and ℓ be defined as in the description of the Extended Euclidean Algorithm given in the lecture, when applied to f and $g := f'$; 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^* of f, which is defined as $f^* := f/\gcd(f, f')$.

Exercise 4: Extended Euclidean Algorithm (4 points)

Trace the Extended Euclidean Algorithm to compute the GCD of

$f = 77400x^7 + 29655x^6 - 153746x^5 + 37585x^4 + 91875x^3 - 130916x^2 - 21076x + 51183$ 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
```