max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/comp-alg/

Assignment sheet 5 due: Monday, November 27

Exercise 1: Polynomial division with remainder (4 points)

Let

$$f = 30x^7 + 31x^6 + 32x^5 + 33x^4 + 34x^3 + 35x^2 + 36x + 37$$

and

$$g = 17x^3 + 18x^2 + 19x + 20$$

be two polynomials in $\mathbb{Z}/101[x]$.

(i) Compute $f^{-1} \bmod x^4$.

(ii) Compute q and r in $\mathbb{Z}/101[x]$ with $f = q \cdot g + r$ and $\deg r < 3 = \deg g$.

Exercise 2: Inverse in finite fields (4 points)

Let p be an arbitrary prime and a be an integer that is not divisible by p.

- Derive an algorithm to compute an integer $b \in \{1, \ldots, p^\ell - 1\}$ with $a \cdot b \equiv 1 \bmod p^\ell$, where $\ell \neq 0$ is an arbitrary given integer.

  (Hint: Use Newton iteration.)

- Compute $97^{-1} \bmod 4096$.

Exercise 3: Fast multipoint evaluation (4 points)

Trace the fast multipoint evaluation algorithm to evaluate

$$f(x) = 1 + 2x + 3x^2 + 4x^3 + 5x^4 + 6x^5 + 7x^6 + 8x^7$$

at the points $-3, -2, \ldots, 3, 4$. You may use any method of your choice for all occurring multiplications and divisions.

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

Let $f \in \mathbb{Z}[x]$ be an integer polynomial of degree less than n with coefficients of absolute value less than 2^L. Furthermore, let $x_1, \ldots, x_n \in \mathbb{Q}$ be n distinct rational points in $[0, 1]$ of bitsize ℓ (i.e., $x_i = p_i/q_i \in [0, 1]$ with integers p_i and q_i of absolute value less than 2^ℓ).

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

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

- 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 $\tilde{O}\big(n(L + \log \max\{1, \lambda^{-1}\})\big)$ bit operations.

  Hint: Use approximate multipoint evaluation with increasing precision.