UNIVERSITÄT DES SAARLANDES
Fachrichtung Mathematik
Prof. Dr. Frank-Olaf Schreyer

Universität des Saarlandes - Campus E2 4 - D-66123 Saarbrücken

Computer Algebra Summer Term 2019

Exercise Sheet 7. Hand in by Tuesday, June 4.

Exercise 1. Determine experimentally the percentage of monic polynomials of degree n in $\mathbb{F}_p[x]$ which have a linear factor.

Can you prove your observation?

Exercise 2. Prove that there are precisely $q^n - q^{n-1}$ square free monic polynomials of degree n in $\mathbb{F}_q[x]$.

Hint: Every monic polynomial f of degree n can be uniquely factored into monic polynomials $f = f_1 f_2$, where f_1 is square free and f_2 is a square.

Now consider the generating functions

$$\sum_{d\geq 0} q^d t^d, \sum_{d\geq 0} q^d t^{2d} \in \mathbb{Z}[[t]]$$

for the number of monic polynomials respectively squares of monic polynomials.

Exercise 3. Consider the primitive polynomials

$$f = 2x^6 - 9x^5 + 11x^4 - 14x^3 + 15x^2 - 6x + 6$$

and

$$g = 5x^6 + 3x^5 - x^4 - 5x^3 - 4x^2 + 8$$

in $\mathbb{Z}[x]$. Factor f and g modulo several primes, and make a guess about their factorisation in $\mathbb{Z}[x]$ (use e.g. Macaulay2). Can you prove you guess?

Exercise 4.

(1) Count the number of partitions of 5 occurring in the factorisation of about 100 randomly chosen polynomials of degree 5 in $\mathbb{F}_p[x]$ where is p is a moderate size prime p.
(2) Compare this with the factorisation in $\mathbb{Z}/q[x]$ for a fixed randomly choose primitive polynomial $f \in \mathbb{Z}[x]$ for 100 different primes q.

Compute the probability that a fixed partition of 5 occurs in case (1).