COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/03/01

EXERCISE SHEET 7

Polynomial division

Exercise 1 (8 points)**.** Prove that, for all $n \in \mathbb{N}$,

$$5 \mid (n^5 - n)\,.$$

(Hint:) you may try by induction.

Exercise 2 (9 points)**.** Solve the following systems of congruences.

(a)

$$\begin{cases} x \equiv 6 \pmod{10} \\ x \equiv 11 \pmod{15} \end{cases}$$

(b)

$$\begin{cases} x \equiv 3 \pmod{21} \\ x \equiv 11 \pmod{14} \end{cases}$$

(c)

$$\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 16 \pmod{18} \\ x \equiv 10 \pmod{15} \end{cases}$$

Exercise 3 (9 points)**.** Compute the quotient and remainder of the polynomial division between the following pairs of polynomials in $\mathbb{Q}[x]$.

(a) $2x^4 - 1$, $x^2 - 2x + 1$.

(b) $6x^4 + 3x^2 - 3$, $2x^3 + 1$.

(c) $3x^4$, $x - 1$.

Exercise 4 (9 points)**.** Compute the quotient and remainder of the polynomial division between the following pairs of polynomials in $\mathbb{Z}_{13}[x]$.

(a) $[2]x^4 - [1]$, $[3]x^2 - [2]x + [1]$.

(b) $[6]x^4 + [3]x^2 - [3]$, $[5]x^3 + [1]$.

(c) $[3]x^4$, $[2]x - [1]$.

Exercise 5 (8 points)**.** Prove that, for every $n \geq 1$, the numbers $n^4 + 3n^2 + 1$ and $n^3 + 2n$ are coprime.

Exercise 6 (8 points)**.** Let $p(x)$ be a polynomial with integer coefficients

$$p(x) = a_n x^n + \cdots + a_0 \,,$$

where $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Let $\frac{s}{t} \in \mathbb{Q}$ be a rational root of $p(x)$, where we assume that $\gcd(s,t) = 1$. Prove that s, t satisfy the following condition:

$$s \mid a_0 \quad \text{AND} \quad t \mid a_n \,.$$

(Hint:) Write explicitly the condition $p(\frac{s}{t}) = 0$. Multiply it by t^n.

Exercise 7 (9 points)**.** Find all the real solutions to the following equations.

(a) $x^3 - 6x^2 + 9x - 2 = 0$.

(b) $3x^4 - x^3 - 6x + 2 = 0$.

(c) $2x^5 + x^4 - 8x^3 - 4x^2 + 8x + 4 = 0$.

(Hint:) First, find one rational solution, by try-and-error. Exercise 6 restricts the search.