4400-001 - SPRING 2022 - WEEK 4 (2/01, 2/03)
RINGS, GROUPS, AND MODULAR ARITHMETIC

Some of these exercises can be found in Savin - Chapter 2, §4 and §5

Exercise 1 (recommended). Euler's ϕ function. Recall from the video for Week 4 - Tuesday, that for n a positive integer, $\phi(n)$ is defined to be the number of integers $0 \leq a < n$ such that $\gcd(a, n) = 1$. Equivalently, by results from last week,

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^{\times}|.$$

Explain the following formulas claimed at the end of the video.

(1) If p is prime and k is a positive integer,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

(2) If m and n are coprime, then

$$\phi(mn) = \phi(m)\phi(n)$$

(Hint: use the Chinese Remainder Theorem).

(3) If $m_1, \ldots, m_s$ are pairwise coprime (i.e. $\gcd(m_i, m_j) = 1$ for all $i \neq j$), then

$$\phi(m_1 \ldots m_s) = \phi(m_1) \ldots \phi(m_s).$$

(Hint: repeatedly apply part (2)).

You will need to know and use these formulas, even if you do not work through this exercise!

Exercise 2 (required). Congruences and Lagrange's theorem.

(1) Find the order of:
  (a) $(\mathbb{Z}/15\mathbb{Z})^{\times}$
  (b) $(\mathbb{Z}/25\mathbb{Z})^{\times}$
  (c) $(\mathbb{Z}/100\mathbb{Z})^{\times}$
  (d) $(\mathbb{Z}/1000\mathbb{Z})^{\times}$

(2) Find the last two digits of 3^{125} and 3^{9999} .

(3) Find the last two digits of 2^{9999} (Warning: 2 is not coprime to 100, so you need to be a bit more clever here! Hint: $100 = 4 \cdot 25$; apply the Chinese Remainder Theorem).

(4) Compute 3^{25} modulo 45.

(5) Find the last three digits of 7^{403}.

Exercise 3 (recommended). Solving more equations.

(1) Solve $x^{62} - 16 = 0$ in $\mathbb{Z}/31\mathbb{Z}$.

(2) Solve $19x - 11 = 0$ in $\mathbb{Z}/31\mathbb{Z}$.

(3) Solve $13x - 11 = 0$ in $\mathbb{Z}/31\mathbb{Z}$.

(4) Find all solutions to each of the following equations in the ring $\mathbb{Z}/30\mathbb{Z}$

$$21x - 24 = 0$$
$$24x - 11 = 0$$
$$11x - 24 = 0.$$

Exercise 4 (required). The Euclidean algorithm for polynomials.
Polynomial long division says that if $a(x)$ and $b(x)$ are two non-zero polynomials with coefficients in a field $\mathbb{K}$ then there are unique polynomials $q(x)$ and $r(x)$ with coefficients in $\mathbb{K}$ such that

1. $a(x) = q(x)b(x) + r(x)$, and
2. $\deg r(x) < \deg b(x)$.

The Polynomial Euclidean Algorithm and gcd equation work exactly like for integers – if $a(x), b(x) \in \mathbb{K}[x]$ then there are polynomials $s(x)$ and $t(x)$ with coefficients in $\mathbb{K}$ such that

$$a(x)s(x) + b(x)t(x) = \gcd(a(x), b(x))$$

We can find $s(x)$ and $t(x)$ by using long division as above to write

$$\begin{aligned} a(x) &= q_0(x)b(x) + r_0(x) \\ b(x) &= q_1(x)r_0(x) + r_1(x) \\ r_0(x) &= q_2(x)r_1(x) + r_2(x) \\ r_1(x) &= q_3(x)r_2(x) + r_3(x) \\ &\cdots\cdots \end{aligned}$$

The last non-zero remainder is the gcd, and we get $s(x)$ and $t(x)$ by unraveling backwards – just like the Euclidean algorithm for integers

(1) Compute $q(x)$ and $r(x)$ for the long division $a(x)/b(x)$ when
$$a(x) = 3x^3 - 5x^2 + 10x - 3, b(x) = 3x + 1.$$
(2) Carry out the polynomial Euclidean algorithm to compute the gcd in $\mathbb{Q}[x]$ of
$$a(x) = x^5 + x^4 + x^3 + 2x^2 + 1 \text{ and } b(x) = x^8 + x^7 + x^5 + x^3 + x^2 + 1.$$
and express it as $a(x)s(x) + b(x)t(x)$.
(3) Carry out the polynomial Euclidean algorithm to compute the gcd in $\mathbb{F}_3[x]$ of
$$a(x) = x^3 + x^2 + 1 \text{ and } b(x) = x^3 + x^2$$
and express it as $a(x)s(x) + b(x)t(x)$.

Exercise 5 (More difficult). Polynomial gcd and squarefree polynomials. For $\mathbb{K}$ a field and any polynomial $f(x) \in \mathbb{K}[x]$, if we write $f(x) = a_n x^n + x_{n-1}x^{n-1} + \dots a_0$, then we define the "derivative" $f'(x)$ using the standard formula

$$f'(x) = na_n x^{n-1} + (n-1)x_{n-1}x^{n-2} + \dots + a_1.$$

(Note that the traditional definition using calculus does not make sense, e.g., if $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$).

(1) Show this definition satisfies the product rule: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.
(2) A polynomial is called square free if it is not divisible by the square of a non-constant polynomial. If $f(x)$ is a non-zero polynomial, show that $f(x)$ is square free if and only if $\gcd(f(x), f'(x)) = 1$.

Exercise 6 (More difficult). Invertible elements in power series and polynomial rings. Let $\mathbb{K}$ be a field. Recall that $\mathbb{K}[x]$ denotes the ring of polynomials in the variable x with coefficients in $\mathbb{K}$. We consider also $\mathbb{K}[[x]]$, the ring of power series in the variable x with coefficients in $\mathbb{K}$ (we do not require any convergence properties, which don't make sense for general $\mathbb{K}$ – i.e., we consider "formal" power series, which cannot necessarily be interpreted as functions).

(1) What is $\mathbb{K}[x]^\times$?
(2) What is $\mathbb{K}[[x]]^\times$?