Homework 6 (due Mar. 5)

MATH 110 | Introduction to Number Theory | Winter 2023

Problem 1 (15 pts)**.** Give a counterexample to **disprove** the *unique prime factorization property* in $\mathbb{Z}/20[T]$.

Remark. Refer to Problem 4 in HW 2 for the related notions. Note that, to show your example fails the *unique prime factorization property*, you need to show your factors are *prime* (in the context of polynomials, irreducible), and not associated to either other (that is, not different by a nonzero constant factor).

Problem 2. Let p be a prime number.

(a) (5 pts) Let $f(T)$ be a polynomial modulo p of degree 2 or 3. **Prove that** $f(T)$ is irreducible if and only if $f(T)$ has no roots modulo p.

Hint. Prove the contrapositive, looking at the degrees of the divisors of $f(T)$.

(b) (5 pts) **Count** the number of monic polynomials modulo p of degree d.

(c) (5 pts) **Count** the number of monic irreducible polynomials modulo p of degree 2.

(d) (5 pts) **Count** the number of monic irreducible polynomials modulo p of degree 3.

Problem 3. Let $f(T)$ be an integer polynomial. Its *derivative* $f'(T)$ is *defined* to be the integer polynomial obtained from $f(T)$ as follows: discard the constant term, then for each positive integer n, replace T^n by nT^{n-1} (here T^0 means the constant 1). One can repeat this process to define what is the *k-th derivative* $f^{(k)}(T)$ of $f(T)$.

(a) (5 pts) Give a **formula** of the degree of $f^{(k)}(T)$ in terms of the $\deg(f)$.

Hint. First show that $\deg(f') = \deg(f) - 1$ as long as $f \neq 0$. Be aware of what will happen when $k > \deg(f)$.

(b) (5 pts) **Prove that** taking derivative is compatible with modular reduction. Namely, if two integer polynomials $f(T)$ and $g(T)$ are congruence modulo m, then $f'(T)$ and $g'(T)$ are also congruence modulo m. Here m is any modulus.