MATH 350, SPRING 2023

HOMEWORK 5, DUE MARCH 1

(1) Compute (56437534324)(2346594312) modulo 4.
(2) Compute 10! modulo 7.
(3) One of the simplest but most useful applications of modular arithmetic is to rule out solutions to diophantine equations.
  (a) Working modulo 8, prove that $x^2 + y^2 + z^2 = 8007$ has no integer solutions.
  (b) Prove that $23495x + 343453450y^3 + 3 = 2343324$ has no integer solutions.
  (c) Unfortunately, this method only works in one direction. It is known that $2x^2 + 7y^2 = 1$ has a solution modulo n for every n. Use another method to show that this equation has no integer solutions.

The equation

$$x_1^3 - 15x_1x_2x_3 + 5x_2^3 - 100x_3^3 + 750x_3x_4x_5 - 50x_4^3 - 2500x_5^3 = 0$$

has a nonzero solution modulo n for every n. The instructor for this course believes, but has not yet been able to prove, that the equation has no nonzero integer solutions.

(4) Let a_n denote the n^{th} Fibonacci number. Prove that $a_n \equiv 4^{n-1}(2^n - 1) \pmod{11}$.
(5) Prove that there are infinitely many irreducible polynomials in $\mathbb{F}_p[T]$.
(6) Prove that the number of roots of a polynomial $\mathbb{F}_p[T]$ is bounded by the degree of the polynomial. Give a counter example to show that the same statement is false in $(\mathbb{Z}/n)[T]$.
(7) This problem defines the T-*adic* absolute value on polynomials in $\mathbb{F}_p[T]$, which is *not* the same as the absolute value in the book defined using the notion of degree. For $F(T) \neq 0$, we say $|F(T)|_T = p^{-s}$ if $T^s \mid F(T)$ but $T^{s+1} \nmid F(T)$. We set $|0|_T = 0$. Prove the following three properties of $|\cdot|_T$:
  - $|F(T) - G(T)|_T = |G(T) - F(T)|_T$.
  - $|F(T) - G(T)|_T \geq 0$, with equality if and only if $F(T) = G(T)$.

  and
  - $|F(T) - G(T)|_T \leq \max\{|F(T) - H(T)|_T, |G(T) - H(T)|_T\}$.

  The last condition above is the ultra-metric inequality, so the three conditions taken together show us that the absolute value of the difference is a notion of distance (called an ultrametric). Here is some geometric intuition behind this problem: Imagine the graphs of two polynomial functions $F(T)$ and $G(T)$, and zoom in very close to the point $T = 0$. Since T^s is very small when s is large, the smaller the absolute value, the closer the two graphs are in that neighborhood.
(8) *PAR problem* #5. Let N be a positive integer written in base 10, with units digit d_0, tens digit d_1, hundreds digit d_2, etc. Let $A = D_0 - d_1 + d_2 - d_3 - \ldots$ be the alternating sum of the digits, i.e.

$$A = \sum_i (-1)^i d_i.$$

  Prove that $A \equiv N \pmod{11}$. Deduce that a palindromic number (one whose digits read the same forwards and backwards) with an even number of digits must be a multiple of 11, and show that the same need not be true for a palindromic number with an odd number of digits.