Math 104B, Winter 2019

Number Theory II, HW 5

Due Thursday February 14th by 10AM in Shubham Sinha's box.

From Niven, Zuckerman, Montgomery (5th Ed.):

- Problems (Section 9.2, page 419):

  1, 3

- Problems (Section 9.8, page 433):

  3

- Problems (Section 9.9, pages 440–441):

  2, 3, 4, 5

Problem A. Let $f(x)$ be a monic polynomial with integer coefficients:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n.$$

We say $f(x)$ is **Eisenstein** relative to a prime number p if all its coefficients $a_0, a_1, \ldots, a_{n-1}$ are multiples of p and $p^2 \nmid a_0$.

(a) If such a p exists, prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$. (This means there is no factorization $f(x) = g(x)h(x)$ with $\mathbb{Z}$-polynomials g, h of degree > 0.)

(`Hint`: Suppose $g(x) = b_0 + \cdots + x^r$ and $h(x) = c_0 + \cdots + x^s$ give a non-trivial factorization of $f(x)$. We may assume $p|b_0$ and $p \nmid c_0$ – why? Suppose $p|b_i$ for all $i = 0, \ldots, m-1$ but $p \nmid b_m$. Consider the coefficient

$$a_m = b_0c_m + b_1c_{m-1} + \cdots + b_{m-1}c_1 + b_mc_0.$$

Since $p|a_m$ by assumption, Euclid's lemma implies $p|b_m$ or $p|c_0$.)

(b) Show that the pth cyclotomic polynomial $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Z}[x]$ by verifying that $\Phi_p(x+1)$ is Eisenstein relative to the prime p. Can you make this argument work for $\Phi_{p^r}(x)$?