MATH 306 – HOMEWORK ASSIGNMENT III

1. Give the definition of Euler φ function. Let φ denote the Euler φ-function and p be a prime. Observe that

$$\varphi(p) = p - 1,$$
$$\varphi(p^a) = p^{a-1}(p-1),$$

and φ is multiplicative in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \ \text{ if } \gcd(a,b) = 1.$$

Prove that if n has the following prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, then

$$\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Compute the remainder of $3^{3^{100}}$ when it is divided by 100.

2. Observe that $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ is a field with 3 elements. Now we will construct a field taking an extension of $\mathbb{F}_3$.

a) Find an irreducible polynomial $p(x)$ of degree 2 in the polynomial ring $\mathbb{F}_3[x]$.

b) Prove that $F = \mathbb{F}_3[x]/I$ is a field, where $I = p(x)\mathbb{F}_3[x]$ is an ideal of $\mathbb{F}_3[x]$ generated by $p(x)$.

Note that $p(x)$ is irreducible polynomial in $\mathbb{F}_3[x]$, but it is reducible in F.

c) Take a root α of $p(x)$ in F and write elements of F using this root.

d) Give multiplication and addition tables of F.

3. Let α be a complex number. A polynomial $f \in \mathbb{Q}[x]$ is said to be a *minimal polynomial* for α over $\mathbb{Q}$ if

i) it is a nonzero monic polynomial in $\mathbb{Q}[x]$ such that

$$f(\alpha) = 0,$$

ii) for every nonzero polynomial $g \in \mathbb{Q}[x]$ of lower degree than f,

$$g(\alpha) \neq 0.$$

Suppose that a polynomial $f \in \mathbb{Q}[x]$ is a minimal polynomial of α. Using the division algorithm for polynomials, prove that for every polynomial $h \in \mathbb{Q}[x]$, if $h(\alpha) = 0$, then f divides h in $\mathbb{Q}[x]$.

4. Find the minimal polynomial of

$$\alpha = \frac{\sqrt{50 - 10\sqrt{5}}}{5}$$

which is the length of the side of the icosahedron in the unit sphere.

Hint: Firstly, find a polynomial in $\mathbb{Q}[x]$ which has α as a root. Is it irreducible?

5. Consider the extension field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ of $\mathbb{Q}$. Prove your answers to the following questions:

a) The extension field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ can be considered to be a vector space over $\mathbb{Q}$. What is $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}]$, that is, what is the dimension of the vector space $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ over $\mathbb{Q}$? Find a basis for the vector space $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ over $\mathbb{Q}$.

b) The element $\sqrt{5} + \sqrt{7}$ is in the field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$. Find the minimal polynomial of $\sqrt{5} + \sqrt{7}$ over $\mathbb{Q}$. What is

$$[\mathbb{Q}(\sqrt{5} + \sqrt{7}) : \mathbb{Q}]?$$

c) Do we have $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$?

d) Express the multiplicative inverse of the element

$$1 + \sqrt{5} + \sqrt{7}$$

in the field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ in terms of the basis elements you have given part **a)** (that is as a linear combination of the basis elements with rational number coefficients).

Due Date: June 5, 2014.