ASSIGNMENT 4 – ELEMENTARY NUMBER THEORY MATH 392

Eyal Goren, November 6, 1998

1. Let B be the group $\mathbb{Z}/n\mathbb{Z}$. Except for (a), the questions are for any n!
(a) For $n = 12$, write the cyclic subgroup generated by every element of B and its order.
(b) Prove that the order of the element k of B is $\frac{n}{(n,k)}$.
(c) Recall that a cyclic subgroup H of a group G is a subgroup of the form $H =< g >$, where $g \in G$. A element $g' \in G$ is callled a *generator* of H if also $< g' >= H$. Find the generators of the cyclic subgroups in (a).
(d) Recall that two groups G_1 and G_2 are isomorphic, if there exists a bijection

$$f : G_1 \longrightarrow G_2,$$

satisfying

$$f(g + g') = f(g) + f(g').$$

Prove that every finite cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some n. (By definition: G is a *cyclic group* if there exists $g \in G$ such that $G =< g >$).
(e) Prove that $\mathbb{Z}/n\mathbb{Z}$ has precisely $\phi(n)$ generators, where ϕ is Euler's function.
(f) How many elements and generators does the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by k have?
(g) Prove that for every $\ell | n$ the group $\mathbb{Z}/n\mathbb{Z}$ has a unique subgroup of order ℓ and it is cyclic.
(h) Conclude from the previous questions the formula

$$n = \sum_{d|n} \phi(d).$$

2. Find the solutions for the equation $x^2 + y^2 = -1$ in the rings $\mathbb{Z}/n\mathbb{Z}$ for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$. Formulate some conjecture based on your answer.

3. Prove that every ideal in the ring $\mathbb{Z}[\omega]$ is principal, where $\omega = \frac{-1+\sqrt{-3}}{2}$ and

$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}.$$

I suggest you imitate the proof for $\mathbb{Z}[i]$.

4. Let $d \neq 0, 1, -1$, be a square free integer (i.e., if p is a prime then $p^2 \nmid d$). An element of $\mathbb{Q}(\sqrt{d})$ is called an *algebraic integer* if it is a solution of a polynomial of the form

$$x^2 + ax + b,$$

where a, b are <u>integers</u>. Find the algebraic integers of $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{-3}]$.