Problem 1. How many ideals does the ring $\mathbb{Z}/60$ have?

Solution: Note that we have a surjective homomorphism $f : \mathbb{Z} \longrightarrow \mathbb{Z}/60$ which sends an integer n to the remainder it has upon division by 60. The kernel of this homomorphism is $60\mathbb{Z}$. By the correspondence theorem, there is a bijection between ideals of $\mathbb{Z}/60$ and those ideals of $\mathbb{Z}$ which contain $60\mathbb{Z}$. Recall now that every ideal of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for unique $m \geq 0$. Also $n\mathbb{Z} \subseteq m\mathbb{Z}$ iff $m|n$ (see Problem 1 of Homework 16). It follows that the ideals of $\mathbb{Z}$ which contain $60\mathbb{Z}$ are in bijective correspondence with positive divisors of 60. Since $60 = 2^2 \cdot 3 \cdot 5$, the number of divisors of 60 is $(2+1)(1+1)(1+1) = 12$ (in general, if $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$ is a prime factorization of n into powers of different primes then the number of positive divisors of n is $(a_1 + 1)(a_2 + 1)...(a_s + 1)$). Thus $\mathbb{Z}/60$ has 12 ideals.

Problem 2. Let I be the principal ideal $(1+3i)\mathbb{Z}[i]$ of the ring of Gaussian integers $\mathbb{Z}[i]$.

a) Prove that $\mathbb{Z} \cap I = 10\mathbb{Z}$.

b) Prove that $\mathbb{Z} + I = \mathbb{Z}[i]$.

c) Prove that $\mathbb{Z}[i]/I$ is isomorphic to $\mathbb{Z}/10$.

Solution: a) $\mathbb{Z} \cap I$ consists of integrs which are of the form $(1 + 3i)(a + bi)$ for some inetegrs a, b. But $(1+3i)(a+bi) = (a-3b)+(3a+b)i$ is an integer iff $3a+b = 0$ and then $(1 + 3i)(a + bi) = 10a$. Thus all elements of $\mathbb{Z} \cap I$ are divisible by 10, i.e. $\mathbb{Z} \cap I \subseteq 10\mathbb{Z}$. On the other hand, for any integer a we have $10a = (1+3i)(a+(-3a)i)$ so $10\mathbb{Z} \subseteq \mathbb{Z} \cap I$. It follows that $\mathbb{Z} \cap I = 10\mathbb{Z}$.

b) Let $a + bi \in \mathbb{Z}[i]$. Note that

$$a + bi = (-9a + 3b) + (1 + 3i)(a + (b - 3a)i).$$

This shows that $a + bi \in \mathbb{Z} + I$ and consequently that $\mathbb{Z} + I = \mathbb{Z}[i]$.

c) We use here the Third Isomorphism Theorem with $R = \mathbb{Z}[i]$, $I = (1 + 3i)\mathbb{Z}[i]$ and $S = \mathbb{Z}$. It asserts that $(S + I)/I$ and $S/S \cap I$ are isomorphic. But in our case $(S + I)/I = \mathbb{Z}[i]/(1 + 3i)\mathbb{Z}[i]$ and $S/S \cap I = \mathbb{Z}/10\mathbb{Z}$, which proves the result.

Problem 3. Let F be a finite field.

a) Prove that there is unique prime number p such that F contains a subring isomorphic to the field $\mathbb{Z}/p$. **Hint:** There is unique non-zero homomorphism from $\mathbb{Z}$ to F).

b) Prove that a vector space V over $\mathbb{Z}/p$ is finite iff it is finite dimensional. Prove that the number of elements of V is a power of p. **Hint.** Consider a basis of V.

c) Explain how F can be considered as a vector space over $\mathbb{Z}/p$, where p is defined in a) and conclude that the number of elements of F is a power of p.

Solution: Consider the unique non-zero homorphism $h : \mathbb{Z} \longrightarrow F$ (see Problem 1 of Homework 14). Let $n\mathbb{Z}$ be the kernel of h. By the First Isomorphism Theorem, the image of h is a subring of F isomorphic to $\mathbb{Z}/n$. Since F is a finite field, $\mathbb{Z}/n$ is a finite domain (every subring of a field is a domain). This implies that $n = p$ is a prime number (if n is not a prime then we know that $\mathbb{Z}/n$ has zero divisors). Thus F contains a subring isomorphic to the field $\mathbb{Z}/p$. Note that p is the smallest positive integer k such that $1 + 1 + .. + 1 = 0$ in F (1 is added k times). Thus p is unique.

b) Let K be any finite field. If V is a finite dimensional vector space over K of dimension d then V has a basis $e_1, ..., e_d$ which means that every element of V can be expressed in a unique way as $a_1e_1 + a_2e_2 + ... + a_de_d$ for some $a_1, ..., a_d$ in K. This means thet elements of V are in bijective correspondence with sequences $a_1, ..., a_d$ of elements of K (i.e with elements of K^d). The number of such sequences is finite and equal to $|K|^d$ (each a_i can be one of $|K|$ elements of K). Thus V is finite and has $|K|^d$ elements. If $K = \mathbb{Z}/p$ then $|K| = p$ so the number of elements of V is a power of p. Conversely, if V is finite then any subset of V is finite so V is finite dimensional over K.

c) Let K be the subring of F isomorphic to the field $\mathbb{Z}/p$. We can consider F as a vector space over K, where the addition of vectors is just the ordinary addition in F and the multiplication of elements of F (i.e. vectors) by elements of K (i.e. scalars) comes from the ordinary multiplication in F (in this manner, any filed L can be considered as a vector space over any subfield M of L). By b), the number of elemetns in F is a power of p.