

Instructor: Miklos Abert  
 Scribe: Saravanan Thiyagarajan  
 June 23, 2006 .

3. LECTURE 3

3.1. Fun Problems.

**Problem 3.1.** Given a countable graph such that every finite subgraph can be colored using  $k$  colors, can the whole graph be colored with  $k$  colors?

**Solution.** Yes. Enumerate the vertices of the graph, say  $\{v_1, v_2, \dots, v_n, \dots\}$ . Construct a tree whose vertices in the  $n$ -th level are all the  $k$ -colorings of the subgraph  $\{v_1, \dots, v_n\}$  and which has an edge between colorings if a coloring of  $\{v_1, \dots, v_n\}$  extends to a coloring of  $\{v_1, \dots, v_n, v_{n+1}\}$ . This is a tree. It is locally finite (Why?). It has infinitely many vertices (Why?). Now apply the lemma on locally finite trees proved last class.

**Problem 3.2.** Let  $n$  be a positive integer. In how many ways can  $n$  be written as the sum of two squares, up to reordering and negatives?

**Solution.** Suppose we have  $n = x^2 + y^2$ . Then in  $\mathbb{Z}[i]$ ,  $n = w\bar{w}$  where  $w = x + iy$ . Therefore it suffices to find the number of ways of writing  $n$  as such a product in  $\mathbb{Z}[i]$  up to units and conjugation (what do conjugation and multiplication by unit correspond to?).

If

$$n = 2^a \prod_{\text{primes } p_i \equiv -1 \pmod{4}} p_i^{\alpha_i} \prod_{\text{primes } q_i \equiv 1 \pmod{4}} q_i^{\beta_i}.$$

Using the factorization of Gaussian primes from the last lecture we have the following decomposition into irreducibles in  $\mathbb{Z}[i]$ :

$$n = (-i)^a (1+i)^{2a} \prod_{\text{primes } p_i \equiv -1 \pmod{4}} p_i^{\alpha_i} \prod_{\text{primes } q_i \equiv -1 \pmod{4}} v_i^{\beta_i} \bar{v}_i^{\beta_i}$$

where  $q_i = v_i \bar{v}_i$  is the Gaussian factorization unique up to units and reordering. Note that all the  $\alpha_i$  should be even (Why?). Recall that

$$(-i)^a (1+i)^{2a} = (1-i)^a (1+i)^a.$$

Hence it suffices to consider only

$$\prod_{\text{primes } q_i \equiv -1 \pmod{4}} v_i^{\beta_i} \bar{v}_i^{\beta_i}$$

which has  $\prod (\beta_i + 1)$  representations (Why?).

3.2. Residue classes and Quotient rings. We will first work with  $\mathbb{Z}$ .

Notation 3.3.

$$a \equiv b \pmod{n} \text{ if } n \mid (a - b), \quad n \neq 0$$

then we say that  $a$  is congruent to  $b$  modulo  $n$

**Lemma 3.4.**  $a_1 \equiv a_2 \pmod{n}$  and  $b_1 \equiv b_2 \pmod{n} \implies a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$  and  $a_1 b_1 \equiv a_2 b_2 \pmod{n}$ .

The proof is immediate from definitions.

**Definition 3.5.** The residue class of  $a \pmod{n} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$

By the above lemma, we can add and multiply residue classes. Check that this gives a ring structure on the set of residue classes modulo  $n$ .

*Notation 3.6.* Denote by  $\mathbb{Z}_n$  the ring of residue classes modulo  $n$ .

**Lemma 3.7.**  $\mathbb{Z}_n$  is a field iff  $n$  is prime.

This is a corollary of Lemma 3.9.

*Remark 3.8.* Note that the definitions above are valid in any principal ideal domain (Check).

**Lemma 3.9.** Suppose  $R$  is a P.I.D then  $f$  is an irreducible element in  $R$  iff the set of residue classes modulo  $f$  is a field.

*Proof.* Note that  $a \pmod f$  is invertible iff  $\gcd(a, f) = 1$ . □

From now on  $R$  will be a ring and  $I$  an ideal in  $R$ .

*Notation 3.10.*

$$a \equiv b \pmod I \text{ if } (a - b) \in I.$$

We generalize Lemma 3.4 to get:

**Lemma 3.11.**  $a_1 \equiv a_2 \pmod I$  and  $b_1 \equiv b_2 \pmod I \implies a_1 + b_1 \equiv a_2 + b_2 \pmod I$  and  $a_1 b_1 \equiv a_2 b_2 \pmod I$

**Definition 3.12.** The residue class of  $a \pmod I = \{x \in R | x \equiv a \pmod I\}$

Addition and multiplication of residue classes make sense and gives a ring structure on the set of residue classes modulo  $I$ .

**Definition 3.13.** Denote by  $R/I$  the ring of residue classes modulo  $I$ . We call this the quotient ring of  $R$  modulo  $I$ .

**Definition 3.14.** If  $R_1$  and  $R_2$  are rings, a function  $f : R_1 \rightarrow R_2$  is a homomorphism if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b).$$

$f$  is an isomorphism if it is a bijective homomorphism.

**Definition 3.15.** The kernel of the homomorphism  $f$  is  $\ker f = \{x \in R_1 | f(x) = 0\}$ .

We have the following easy lemma:

**Lemma 3.16.** The kernel of  $f$  is an ideal in  $R_1$  and  $f(R_1)$  is a subring of  $R_2$ .

**Theorem 3.17.**

$$f(R_1) \cong R_1 / \ker f.$$

We shall skip the proof of this theorem.

### 3.3. The Euler $\phi$ function.

**Definition 3.18.** For  $n \geq 1$ , let  $\phi(n)$  be the number of positive integers less than  $n$  and relatively prime to  $n$ .

We shall find an expression for  $\phi(n)$ .

**Proposition 3.19.** For  $n > 1$ ,  $n = \prod p_i^{\alpha_i}$  we have

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$$

*Proof.* Let  $n > 1$ , and  $n = \prod p_i^{\alpha_i}$  be its prime factorization.

Let

$$R = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_k}}.$$

Define

$$f : \mathbb{Z} \longrightarrow R \\ x \mapsto (x \bmod p_1^{\alpha_1}, \dots, x \bmod p_k^{\alpha_k}).$$

Then  $\ker f = (n)$  (Why?). This  $\implies \mathbb{Z}_n \cong f(\mathbb{Z}) \subset R$ .

Then we calculate the cardinalities on both sides to conclude that  $\mathbb{Z}_n$  is isomorphic to  $R$ . □

**Corollary 3.20.**  $\phi(n)$  is multiplicative.

*Proof.* Follows from the fact that the invertible elements in  $R$  are exactly the elements with invertible coordinates. □

Hence  $\phi(n) = \prod \phi(p_i^{\alpha_i})$ . Now  $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1}$  (Check).  
Hence  $\phi(n) = n \prod (1 - 1/p_i)$ .