

# Algebraic Number Theory: Problems

March 13, 2008

1. Prove the following corollary to the Chinese Remainder Theorem.

**Claim 0.1.** *Let  $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_M$  be non-zero integral ideals which are pairwise relatively prime, and let  $\alpha_1, \alpha_2, \dots, \alpha_M$  be elements of a Dedekind domain  $R$ . Then there exists  $\alpha \in R$  such that*

$$\alpha \equiv \alpha_m \pmod{\mathfrak{a}_m}; \quad m = 1, 2, \dots, M.$$

2. Algebra review: Let  $R$  be a ring and suppose  $A$  and  $B$  are ideals of  $R$ . If  $A + B = R$  we say  $A$  and  $B$  are *relatively prime*. Show that if  $A$  and  $B$  are relatively prime then  $A \cap B = AB$ .
3. Suppose  $D$  is a unique factorization domain. Show that  $D$  is integrally closed in its field of fractions.
4. Show that  $\mathbb{Z}[\sqrt{-5}]$  is a Dedekind domain, but not a principal ideal domain.
5. If  $\mathbb{Q} \subseteq K \subseteq L$  and  $K, L$  are algebraic number fields, show that  $d_K$  divides  $d_L$ .
6. Suppose  $\alpha \in \mathcal{O}_K$ , and let  $\mathfrak{a} = (\alpha)$ . What is the relationship between  $N_{K/\mathbb{Q}}(\alpha)$  and  $N(\mathfrak{a})$ ?
7. Given a fractional ideal  $\mathfrak{b}$  with

$$\mathfrak{b} = \frac{\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_M^{n_M}}{\mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_L^{m_L}},$$

where the  $\mathfrak{p}$ s and  $\mathfrak{q}$ s are distinct primes then we define the norm of  $\mathfrak{b}$  to be

$$N(\mathfrak{b}) = \prod_{m=1}^M N(\mathfrak{p}_m)^{n_m} \Big/ \prod_{\ell=1}^L N(\mathfrak{q}_\ell)^{m_\ell}.$$

We know there must exist some  $c \in K$  and some integral ideal  $\mathfrak{a} \subseteq \mathcal{O}_K$  such that  $\mathfrak{b} = c\mathfrak{a}$ . Show that the norm of  $\mathfrak{b}$  is also given by

$$N(\mathfrak{b}) = N_{K/\mathbb{Q}}(c)N(\mathfrak{a}).$$

8. Show that every prime ideal in  $\mathfrak{D}_K$  contains exactly one rational prime.
9. Given two fractional ideals  $\mathfrak{A}$  and  $\mathfrak{B}$  of  $\mathcal{O}_K$ , we say  $\mathfrak{A}$  and  $\mathfrak{B}$  are equivalent,  $\mathfrak{A} \sim \mathfrak{B}$ , if there exist  $\alpha, \beta \in \mathcal{O}_K$  such that

$$(\alpha)\mathfrak{A} = (\beta)\mathfrak{B}.$$

- (a) Show that  $\sim$  is an equivalence relation on the group of fractional ideals of  $\mathcal{O}_K$ .  
 (b) Show that if  $\mathcal{O}_K$  is a PID then all ideals are equivalent.
10. Show that  $N_{K/\mathbb{Q}}$  is a multiplicative function on  $K$ .
11. Show that for any  $x > 0$ ,  $\#\{\mathfrak{a} \subseteq \mathcal{O}_K : N(\mathfrak{a}) \leq x\} < \infty$ .
12. Let  $\mathcal{H}$  be the set of equivalence classes of ideals in a number field  $K$ . We may create a product on equivalence classes by choosing representatives  $\mathfrak{A}_1$  and  $\mathfrak{A}_2$  for equivalence classes  $\mathcal{C}_1$  and  $\mathcal{C}_2$  and then defining  $\mathcal{C}_1\mathcal{C}_2$  to be the equivalence class containing  $\mathfrak{A}_1\mathfrak{A}_2$ . Show that this product is well-defined, and that  $\mathcal{H}$  equipped with this product is an abelian group.
13. Let  $K = \mathbb{Q}(\sqrt{-d})$  where  $d$  is a square-free integer. Find an integral basis for  $K$ . (Hint: the answer depends on whether  $d$  is congruent to 0 or 1 mod 4.)
14. Prove the following theorem.

**Theorem 0.2.** Let  $K = \mathbb{Q}(\sqrt{d})$  where  $d$  is a square-free integer. Suppose  $p$  is a rational prime and let  $(p) = p\mathcal{O}_K$ .

(a) if  $p|d$  then  $(p) = (p, \sqrt{d})^2$ .

(b) if  $d$  is odd then  $(2) = \begin{cases} (2, 1 + \sqrt{d})^2 & d \equiv 3 \pmod{4}; \\ \left(2, \frac{1+\sqrt{d}}{2}\right) \left(2, \frac{1-\sqrt{d}}{2}\right) & d \equiv 1 \pmod{8}; \\ \text{prime} & \text{otherwise.} \end{cases}$

(c) if  $p$  is odd and  $p \nmid d$  then  $(p) = \begin{cases} (p, n + \sqrt{d})(p, n - \sqrt{d}) & d \equiv n^2 \pmod{p}; \\ \text{prime} & \text{otherwise.} \end{cases}$

15. Let  $K = \mathbb{Q}(\sqrt{-5})$ . Compute the norm of the ideal  $(2, 1 + \sqrt{-5}) \subseteq \mathcal{O}_K$ . Conclude that  $(2, 1 + \sqrt{-5})$  is not principal.
16. Suppose  $\mathfrak{a}, \mathfrak{b}$  and  $\mathfrak{c}$  are ideals in  $\mathcal{O}_K$  for some number field  $K$  such that

$$(\mathfrak{a}, \mathfrak{b}) = \mathcal{O}_K \quad \text{and} \quad \mathfrak{a}\mathfrak{b} = \mathfrak{c}^M,$$

for some integer  $M > 1$ . Show that there exist ideals  $\mathfrak{d}, \mathfrak{e} \subseteq \mathcal{O}_K$  such that  $\mathfrak{a} = \mathfrak{d}^M$  and  $\mathfrak{b} = \mathfrak{e}^M$ .

17. Show that the only solution to  $x^2 + 13 = y^3$  is given by  $x = 70, y = 17$ .
18. Let  $p$  be a rational prime. Show that

$$(x_1 + x_2 + \dots + x_L)^p \equiv (x_1^p + x_2^p + \dots + x_L^p) \pmod{p}.$$

19. Show that  $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$ .

20. Let  $q$  be an odd prime. Prove:

- (a) If  $q \equiv 1 \pmod{4}$ , then  $q$  is a quadratic residue mod  $p$  if and only if  $p \equiv r \pmod{q}$  where  $r$  is a quadratic residue.

(b) If  $q \equiv 3 \pmod{4}$ , then  $q$  is a quadratic residue mod  $p$  if and only if  $p \pmod{\pm b^2 \pmod{4q}}$ , where  $b$  is an odd integer relatively prime to  $q$ .

21. Show that if  $\alpha \in \mathcal{O}_K$  and  $|\alpha^{(n)}| = 1$  for all conjugates  $\alpha^{(n)}$ , then  $\alpha$  is a root of unity.
22. The *regulator* of  $K$  is defined as follows. Let  $r = r_1 + r_2 - 1$  and suppose  $\epsilon_{1,2}, \dots, \epsilon_r$  are fundamental units for  $K$ . Further assume that  $\sigma_1, \sigma_2, \dots, \sigma_{r+1}$  are embeddings of  $K$  subject to the condition that  $\sigma_{r_1+1}, \dots, \sigma_{r+1}$  represent all of the complex conjugate pairs of embeddings of  $K$ . The regulator is then given by

$$R_K = \left| \det [\log |\sigma_n(\epsilon_m)|]_{n,m=1}^r \right|.$$

Notice that the matrix in this definition does not use the embedding  $\sigma_{r+1}$ . Show that, in fact, the regulator is unchanged by replacing any embedding  $\sigma_n$  with  $\sigma_{r+1}$ . That is, the regulator can be defined using any  $r$  of the embeddings  $\sigma_1, \sigma_2, \dots, \sigma_{r+1}$ .

23. Show that the regulator  $R_K$  is independent of the choice of fundamental units. That is, suppose  $\epsilon_1, \dots, \epsilon_r$  and  $\delta_1, \dots, \delta_r$  are different sets of fundamental units. Show that

$$\det [\log |\sigma_n(\epsilon_m)|]_{n,m=1}^r = \pm \det [\log |\sigma_n(\delta_m)|]_{n,m=1}^r.$$

24. Show that if  $d \equiv 1 \pmod{4}$  is a square-free integer, then the equation

$$x^2 - dy^2 = 4$$

has infinitely many integer solutions.

25. Show that if  $d$  is a positive square-free integer, and  $K = \mathbb{Q}(\sqrt{-d})$  then,

$$U_K \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } d = 1; \\ \mathbb{Z}/6\mathbb{Z} & \text{if } d = 3; \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$