2015-11-23 Introduction to number theory Problems

References:
Kato-Kurokawa-Saito, "Number Theory 2: Introduction to Class Field Theory", American Mathematical Society.
J.S.Milne's lecture note "Algebraic Number Theory" available at
http://www.jmilne.org/math/CourseNotes/ant.html

1. Let A be a Dedekind domain, and $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension and B be the integral closure of A in L. Let $\mathfrak{p} \subset A$ be a prime ideal and $\mathfrak{p}B$ be the ideal of B generated by $\mathfrak{p} \subset A \subset B$. Let

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$$

be the prime factorization of $\mathfrak{p}B$ ($\mathfrak{q}_i$ are distinct prime ideals of B and $e_i \geq 1$).
1.1. Show that the set of prime ideals lying over $\mathfrak{p}$ is $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$.
1.2. Suppose L/K is a Galois extension. Let $\sigma \in \mathrm{Gal}(L/K)$ be an automorphism $L \overset{\cong}{\to} L$ of K algebras. Show that it induces an isomorphism $B \overset{\cong}{\to} B$ of A-algebras.
1.3. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be primes lying over $\mathfrak{p}$. Let $\sigma \in \mathrm{Gal}(L/K)$ and suppose $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.
1.3.1. Show that $e(\mathfrak{p}, \mathfrak{q}_1) = e(\mathfrak{p}, \mathfrak{q}_2)$.
1.3.2. Show that $f(\mathfrak{p}, \mathfrak{q}_1) = f(\mathfrak{p}, \mathfrak{q}_2)$.

2.1. Show that $\mathbb{Z}[\sqrt{-1}]/3\mathbb{Z}[\sqrt{-1}]$ is a 2-dimensional vector space over $\mathbb{F}_3$.
2.2. Show that $\mathbb{Z}[\sqrt{-1}]/(2+\sqrt{-1})\mathbb{Z}[\sqrt{-1}]$ is a 1-dimensional vector space over $\mathbb{F}_5$.

3. In this problem, you may use the following proposition.
Proposition: Let A be a Dedekind domain and $K = \mathrm{Frac}(A)$. Let L/K be a finite separable extension and B be the integral closure of A in L. Let $\alpha \in L$ be an element such that $L = K(\alpha)$. Let $f(T) \in K[T]$ be the monic polynomial of minimal degree such that $f(\alpha) = 0$. Suppose $B = A[\alpha]$. Then the different $\mathcal{D}(B/A)$ is equal to $(f'(\alpha))$.

Let $A = \mathbb{Z}$, $K = \mathrm{Frac}(A) = \mathbb{Q}$. Let $L = \mathbb{Q}(\sqrt{m})$ where m is a square free integer. Let B be the ring of integers of L. Recall that (see the problem sets on 2015-11-09)

$$B = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

3.1. Compute the different $\mathcal{D}(B/A)$ when $m \equiv 2, 3 (\bmod 4)$.
3.2. Compute the different $\mathcal{D}(B/A)$ when $m \equiv 1 (\bmod 4)$.

4. Let $A = \mathbb{Z}$, $K = \mathrm{Frac}(A) = \mathbb{Q}$. Let $L = \mathbb{Q}(\sqrt{m})$ where m is a square free integer. Let B be the ring of integers of L.
4.1. Let $p \in \mathbb{Z}$ be an odd prime number which does not divide m. Show that the prime ideal $p\mathbb{Z}$ is totally split in L if $\left(\dfrac{m}{p}\right) = 1$.
4.2. Let $p \in \mathbb{Z}$ be an odd prime number which does not divide m. Show that the prime ideal $p\mathbb{Z}$ is totally split in L only if $\left(\dfrac{m}{p}\right) = 1$.

5. Let u_n be the n-th Fibonacci number. For example, $u_0 = 0, u_1 = 1, u_2 = 1, u_3 = 2, \ldots$. The recursion relation $u_{n+2} = u_{n+1} + u_n$ for $n \geq 0$ is satisfied. We have

$$u_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

5.1. Let $p \neq 5$ a prime number. Suppose $m \equiv n \pmod{(p^2-1)}$. Show that $u_m \equiv u_n (\operatorname{mod} p)$. (Suggestion: consider the decomposition of p in $\mathbb{Q}(\sqrt{5})$.)
5.2. Let p be a prime number such that $p \equiv \pm 1 \pmod 5$. Suppose that $m \equiv n \pmod{(p-1)}$. Show that $u_m \equiv u_n \pmod p$. (Suggestion: consider the factorization of p in (the ring of integers of) $\mathbb{Q}(\sqrt{5})$.)

6.1.1. Let p be a prime number such that $p \equiv 3 \pmod 4$. Show that the canonical inclusion $\mathbb{Q}_p \subset \mathbb{Q}_p(\sqrt{-1})$ is not an isomorphism.
6.1.2. Show that it is the unramified extension of degree 2.
6.2. Let p be a prime number such that $p \equiv 1 \pmod 4$. Show that the canonical inclusion $\mathbb{Q}_p \subset \mathbb{Q}_p(\sqrt{-1})$ is an isomorphism.
6.3. Find the unramified extension of $\mathbb{Q}_5$ of degree 2.