Problem 1. Prove that $\beta = \sqrt{2} + \sqrt{3}$ is an algebraic integer by explicitly writing down a monic polynomial in $\mathbb{Z}[x]$ that has $\beta$ as a root.

Problem 2. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Prove that there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

Problem 3. Let $m \geq 1$ and let $\zeta$ be a primitive $m$th-root of unity, i.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for all $1 \leq j < m$. Prove that
\[
\prod_{i=0}^{m-1} \prod_{j=0, j \neq i}^{m-1} (\zeta^i - \zeta^j) = (-1)^{m-1}m^{m}.
\]

Problem 4. Let $m \neq 0$ be an integer and let $n \geq 2$ be an integer. Prove that the equation
\[
x^n + y^n = m
\]
has only finitely many solutions $x, y \in \mathbb{Z}$. Find an explicit upper bound for $\max\{|x|, |y|\}$ in terms of $m$ and $n$.

Problem 5. The \textit{content} of a polynomial
\[
f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d \in \mathbb{Z}[x]
\]
is the quantity
\[
\text{Content}(f) = \gcd(a_0, a_1, \ldots, a_d).
\]
(a) Prove that
\[
\text{Content}(fg) = \text{Content}(f)\text{Content}(g).
\]
(Hint: For every prime $p$, compute the highest power of $p$ dividing both sides of the equation.) This result is called \textit{Gauss’ Lemma}.
(b) Prove that if $f(x)$ factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[x]$.
Problem 6. Let \( p \in \mathbb{Z} \) be a prime, and let
\[
f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1} x + a_d \in \mathbb{Z}[x]
\]
be a polynomial such that
\[
p \nmid a_0, \quad p \mid a_i \text{ for } 1 \leq i \leq d, \quad p^2 \nmid a_d.
\]
Prove that \( f(x) \) is irreducible in \( \mathbb{Q}[x] \). (From the previous problem, it suffices to prove that it is irreducible in \( \mathbb{Z}[x] \).) This is called Eisenstein’s Irreducibility Criterion.

Problem 7. Let \( A \subset B \) be rings, let \( \beta \in B^* \) be a unit in \( B \), and let \( \alpha \in A[\beta] \cap A[\beta^{-1}] \). Prove that \( \alpha \) is integral over \( A \). (Hint: Find an \( n \geq 1 \) such that the \( A \)-module \( A + A\alpha + A\alpha^2 + \cdots + A\alpha^n \) is stable under multiplication by \( \alpha \).)

Problem Set # 2

Problem 8. Let \( K = \mathbb{Q}(\sqrt{2}) \).
\begin{enumerate}
\item[(a)] Prove that the ring of integers of \( K \) is \( R_K = \mathbb{Z}[\sqrt{2}] \).
\item[(b)] Compute the discriminant of \( R_K \) as a \( \mathbb{Z} \)-module.
\end{enumerate}

Problem 9. Let \( K/\mathbb{Q} \) be a number field and \( R_K \) its ring of integers.
\begin{enumerate}
\item[(a)] Let \( \alpha \in R_K \). Prove that \( \alpha \in R_K^* \) if and only if \( N_{K/\mathbb{Q}}\alpha = \pm 1 \).
\item[(b)] Let \( K = \mathbb{Q}(\sqrt{-d}) \), where \( d \geq 1 \) is a positive square-free integer. We determined the ring of integers \( R_K \) of \( K \) in class. Compute the unit group \( R_K^* \). (There are three different answers, depending on \( d \).)
\end{enumerate}

Problem 10. Let \( K/\mathbb{Q} \) be a number field and let \( a \) be an ideal of \( R_K \). Prove that \( a \cap \mathbb{Z} \neq \emptyset \).

Problem 11. Suppose that the minimal polynomial of \( \alpha \) is \( x^n + ax + b \in \mathbb{Z}[x] \), and let \( K = \mathbb{Q}(\alpha) \). Prove that
\[
D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = (-1)^{(n^2-n)/2}(n^2b^{n-1} + a^n(1-n)^{n-1}).
\]

Problem 12. (This example is due to Dedekind.) Let \( K = \mathbb{Q}(\alpha) \), where \( \alpha^3 - \alpha^2 - 2\alpha - 8 = 0 \).
\begin{enumerate}
\item[(a)] Prove that \( f(x) = x^3 - x^2 - 2x - 8 \) is irreducible over \( \mathbb{Q} \).
\item[(b)] Let \( \beta = \frac{1}{2}(\alpha^2 + \alpha) \). Prove that \( \beta^3 - 3\beta^2 - 10\beta - 9 = 0 \), and hence that \( \beta \in R_K \).
\item[(c)] Prove that \( D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -4 \cdot 503 \) and that \( D_{K/\mathbb{Q}}(1, \alpha, \beta) = -503 \). Deduce that \( \{1, \alpha, \beta\} \) is a \( \mathbb{Z} \)-basis for \( R_K \).
(d) Let $\gamma \in R_K$. Prove that $D_{K/Q}(1, \gamma, \gamma^2)$ is even.
(e) Deduce that $R_K$ has no $\mathbb{Z}$-basis of the form $\{1, \gamma, \gamma^2\}$, i.e., $R_K$ cannot be written in the form $\mathbb{Z}[\gamma]$. 

**Problem 13.** Let $K$ and $L$ be number fields that are linearly disjoint over $\mathbb{Q}$, i.e., satisfying $K \cap L = \mathbb{Q}$.

(a) Prove that $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$.
(b) Let $D = \gcd(D_K, D_L)$. Prove that the rings of integers of $K$, $L$, and $KL$ satisfy

$$R_{KL} \subset \frac{1}{D}R_K R_L.$$ 

**Problem 14.** Let $K$ be a number field with $r_1$ real embeddings and $2r_2$ complex embeddings. Prove that

$$\text{sign } D_K = (-1)^{r_2}.$$ 

**Problem Set # 3**

**Problem 15.** Show that every principal ideal domain is a Dedekind domain.

**Problem 16.** We proved in class that the ring $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}(\sqrt{-5})$, so $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain. Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

The next four problems show that the ideas of divisibility, greatest common divisor, and least common multiple are valid for ideals in a Dedekind domain $R$.

**Problem 17.**

**Definition.** The ideal $b$ divides the ideal $a$ if $b \trianglerighteq a$. We write $b \mid a$.

Prove that $b \mid a$ if and only if there is an ideal $c$ such that $a = bc$.

**Problem 18.**

**Definition.** The ideal $d$ is the greatest common divisor of $a$ and $b$ if it satisfies:

1. $d \mid a$ and $d \mid b$.
2. If $h \mid a$ and $h \mid b$, then $h \mid d$.

Prove that $\gcd(a, b)$ exists and is unique. More precisely, prove that $\gcd(a, b) = a + b$. 
Problem 19.

**Definition.** The ideal $m$ is the least common multiple of $a$ and $b$ if it satisfies:

1. $a \mid m$ and $b \mid m$.
2. If $a \mid n$ and $b \mid n$, then $m \mid n$.

Prove that $\text{lcm}(a, b)$ exists and is unique. More precisely, prove that $\text{lcm}(a, b) = a \cap b$.

Problem 20.

**Definition.** Let $p$ be a prime ideal. The valuation of $a$ at $p$ is the largest integer $e \geq 0$ such that $p^e \mid a$. We denote this quantity by $\text{ord}_p(a)$ or $v_p(a)$.

(a) Prove that $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$.

(b) Prove that $a = \prod_p p^{\text{ord}_p(a)}$.

(Note that all but finitely many factors in the product are equal to 1.)

(c) Prove that $\text{gcd}(a, b) = \prod_p p^{\min\{\text{ord}_p(a), \text{ord}_p(b)\}}$.

$\text{lcm}(a, b) = \prod p^{\max\{\text{ord}_p(a), \text{ord}_p(b)\}}$.

Problem 21. Let $K/\mathbb{Q}$ be a number fields, and let $\alpha \in R_K$ with $\alpha \neq 0$. Recall that the norm of the ideal $\alpha R_K$ is the number of elements in the quotient ring $R_K/\alpha R_K$, while the norm of the element $\alpha$ is the determinant of the linear transformation $K \to K$ defined by $\beta \mapsto \alpha \beta$. Prove that $N(\alpha R_K) = |N(\alpha)|$. 
For the next few problems, you may want to use the following theorem, which I did not prove in class. (We may go back to it, or you can look it up in any textbook on algebraic number theory if you want to see the proof.)

**Theorem 1.** Let $K/Q$ be an algebraic number field and suppose that its ring of integers can be written in the form $R_K = \mathbb{Z}[\alpha]$. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$, and let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x)$ factors in $\mathbb{F}_p[x]$ as
\[
f(x) \equiv f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_r(x)^{e_r} \pmod{p},
\]
where $f_1, \ldots, f_r$ are distinct irreducible polynomials in $\mathbb{F}_p[x]$. Then $p$ divides $N_{K/Q}p_i$ for $i = 1, 2, \ldots, r$. Further,
\[
R_K = pR_K f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}.
\]

**Problem 22.** Let $K/Q$ be an algebraic number field of degree $n$, and suppose that its ring of integers can be written in the form $R_K = \mathbb{Z}[\alpha]$. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$, and factor $f(x)$ in $R_K[x]$ as
\[
f(x) = (x - \alpha)(\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}) \quad \text{with} \quad \beta_0, \ldots, \beta_{n-1} \in R_K.
\]
(a) Prove that the dual basis to $1, \alpha, \ldots, \alpha^{n-1}$ is
\[
\frac{\beta_0}{f'(\alpha)}, \frac{\beta_1}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}.
\]
(b) Prove that the different of $K/Q$ is the principal ideal
\[
D_{K/Q} = f'(\alpha)R_K.
\]
(Use (a) and the fact, proven in class, that $D_{K/Q}^{-1}$ is generated by the dual basis.)
(c) Let $K = \mathbb{Q}(\zeta_p)$ be the field generated by a primitive $p$’th root of unity (with $p$ prime). Compute $D_{K/Q}$.

**Problem 23.** Let $K/Q$ be an algebraic number field of degree $n$, and as in the previous problem, suppose that its ring of integers can be written in the form $R_K = \mathbb{Z}[\alpha]$. Prove that if $p \mid D_{K/Q}$, then $p$ ramifies in $K$. (This is the other direction of Dedekind’s theorem, which we did not prove in class.)
Problem 24. If you want to get started on this problem before we finish this unit in class, you’ll want to use the following result, which is due to Minkowski. Let \( K/\mathbb{Q} \) be a number field of degree \( n \), and let \( 2r_2 \) be the number of complex embeddings of \( K \), i.e., maps \( K \subset \mathbb{C} \) whose image is not in \( \mathbb{R} \). Then every ideal class contains an ideal \( a \) satisfying

\[
N_{K/\mathbb{Q}} a \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r_2} \sqrt{|D_{K/\mathbb{Q}}|}.
\]

(We’ll prove this in class.)

(a) Find the class numbers of \( \mathbb{Q}(\sqrt{2}) \), \( \mathbb{Q}(\sqrt{3}) \), and \( \mathbb{Q}(\sqrt{13}) \). (These should require almost no work.)

(b) Prove that \( \mathbb{Q}(\sqrt{-5}) \) has class number 2.

(c) Prove that \( \mathbb{Q}(\sqrt{-19}) \) has class number 1.

(d) Find the class numbers of \( \mathbb{Q}(\sqrt{6}) \), \( \mathbb{Q}(\sqrt{14}) \), and \( \mathbb{Q}(\sqrt{17}) \).
Problem Set # 5

Problem 25. Let $R$ be a ring (commutative, with multiplicative identity, as usual). Let $n \geq 1$. Determine the structure of the group of units in the ring $A = R[X]/(X^n)$.

Problem 26. Let $K/\mathbb{Q}$ be a cubic field with $r_1 = r_2 = 1$. Since $K$ has a unique real embedding, we will view $K$ as being a subfield of $\mathbb{R}$.

(a) Prove that $\{\alpha \in R_K^* : \alpha > 0\}$ is an infinite cyclic group. (Hint: Dirichlet’s unit theorem tells you the rank of $R_K^*$.)

(b) Prove that every element of $\{\alpha \in R_K^* : \alpha > 0\}$ has norm 1.

(c) Let $\alpha \in R_K^*$ satisfy $\alpha > 1$. Prove that

$$|D_{K/\mathbb{Q}}| \leq 4\alpha^3 + 24.$$  

(Hint: Let $\alpha = \beta^2$ with $\beta > 0$. Then the conjugates of $\alpha$ have the form $\beta^{-1}e^{i\theta}$ and $\beta^{-1}e^{-i\theta}$. Calculate the discriminant $D(1, \alpha, \alpha^2)$ as a function of $\beta$ and $\theta$, say $F(\beta, \theta) = |D(1, \alpha, \alpha^2)|^{1/2}$. For a given $\beta$, find the minimum value of $F(\beta, \theta)$, and use this to deduce that $|D(1, \alpha, \alpha^2)| \leq 4\alpha^3 + 24$. Finally observe that $D_{K/\mathbb{Q}}$ divides $D(1, \alpha, \alpha^2)$.)

Problem 27. Let $f(x) = x^3 + 10x + 1$.

(a) Check that $f(x)$ is irreducible over $\mathbb{Q}$.

(b) Check that $f(x)$ has one real root and two complex roots. Let $\alpha$ be the real root.

(c) Prove that $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$.

(d) Prove the $\{\beta \in \mathbb{Z}[\alpha]^* : \beta > 0\}$ is a cyclic group generated by $-\alpha^{-1}$. (Problem 26 will be helpful for this part of Problem 27.)

Problem 28. Let $L/K/\mathbb{Q}$ be number fields such that

$$r_1 = [K : \mathbb{Q}] \quad \text{and} \quad r_2 = \frac{1}{2}[L : \mathbb{Q}].$$

In other words, $K$ has only real embeddings and $L$ has only complex embeddings. The terminology for this is that $K$ is totally real and $L$ is totally complex. Suppose further that $[L : K] = 2$. Then $L$ is called a CM field\(^1\). Prove that $R_K^*$ is a subgroup of finite index in $R_L^*$. Can you say anything about the index?

\(^1\)CM is an abbreviation for complex multiplication. These fields play a prominent role in the theory of abelian varieties.
Problem 29. Let $L/K$ be an abelian extension of number fields, so the Frobenius map $(p, L/K) \in \text{Gal}(L/K)$ is defined for prime ideals $p$ of $K$ that are unramified in $L$. Write $I_K(L/K)$ for the set of fractional ideals of $K$ whose factorization includes only primes that are unramified in $L$. We define a map on the group of fractional ideals $I_K(L/K)$ as follows: Given $a \in I_K(L/K)$, factor $a = \prod p_i^{t_i}$ as a product of prime ideals, and set

$$(a, L/K) = \prod (p_i, L/K)^{t_i}.$$ 

This gives a homomorphism

$$(\cdot, L/K) : I_K(L/K) \longrightarrow \text{Gal}(L/K)$$

called the reciprocity map or Artin map.

(a) Let $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. (Note that $\tau(L)$ need not equal $L$, and $\tau(K)$ need not equal $K$.) Prove that

$$(\tau(a), \tau(L)/\tau(K)) = \tau(a, L/K) \tau^{-1}.$$

(b) Let $E/L/K$ be a larger abelian extension. Let

$$\text{Res}_L : \text{Gal}(E/K) \longrightarrow \text{Gal}(L/K)$$

denote the restriction map, i.e., $\text{Res}_L(\sigma)$ is the restriction of $\sigma$ to an automorphism of $L$. Prove that

$$\text{Res}_L(a, E/K) = (a, L/K).$$

(c) Let $F/K$ be a finite extension (not necessarily Galois). Let $p$ be a prime ideal of $K$ that is unramified in $L$, and let $\mathfrak{P}$ be a prime of $F$ lying over $p$. Prove that

$$\text{Res}_L(\mathfrak{P}, LF/F) = (p, L/K)^{f(\mathfrak{P}/p)},$$

where $f(\mathfrak{P}/p)$ is the residue field degree of $\mathfrak{P}/p$.

It is also true, but quite hard to prove, that the Artin map is surjective.

Problem 30. Let $K$ be a field and let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on $K$. We say that they are equivalent if they induce the same topology on $K$, where topology is induced by the distance functions $\text{dist}_1(x, y) = |x - y|_1$, and $\text{dist}_2(x, y) = |x - y|_2$. Prove that $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there is a constant $\lambda > 0$ such that

$$|x|_1 = |x|^\lambda_2$$

for all $x \in K$. 
Problem 31. Let $K$ be a field with an absolute value $| \cdot |$. Define $K_v$ to be
$$K_v = \left\{ \text{Cauchy sequences } (\alpha_i)_{i \geq 1} \subset K \right\},$$
where the equivalence relation is
$$(\alpha_i)_{i \geq 1} \sim (\beta_i)_{i \geq 1} \iff \lim_{i \to \infty} |\alpha_i - \beta_i| = 0.$$
We make $K_v$ into a ring via
$$(\alpha_i)_{i \geq 1} + (\beta_i)_{i \geq 1} = (\alpha_i + \beta_i)_{i \geq 1} \quad \text{and} \quad (\alpha_i)_{i \geq 1} \cdot (\beta_i)_{i \geq 1} = (\alpha_i \beta_i)_{i \geq 1}.$$It’s not hard to check that $\sim$ is an equivalence relation and that these operations are well-defined and make $K_v$ into a field.

(a) Define a map $\| \cdot \| : K_v \to [0, \infty)$ by
$$\|(\alpha_i)_{i \geq 1}\| = \lim_{i \to \infty} |\alpha_i|.$$Prove that $\| \cdot \|$ is well-defined and is an absolute value on $K_v$.

(b) Prove that $(K_v, \| \cdot \|)$ is a complete field. (Roughly speaking, you need to show that a Cauchy sequence of Cauchy sequences converges to a Cauchy sequence!)
For Problems 32–34, let \((K, | \cdot |)\) be a complete non-archimedean field, let
\[ R = \{ \alpha \in K : |\alpha| \leq 1 \} \quad \text{and} \quad \mathfrak{m} = \{ \alpha \in K : |\alpha| < 1 \} \]
be the ring of integers and maximal ideal of \(K\), and let \(k = R/\mathfrak{m}\) be the residue field of \(R\).

**Problem 32.** Let \(F(x) \in R[x]\) be a monic polynomial of degree \(d \geq 1\), and let \(\bar{F} \in k[x]\) denote its reduction modulo \(\mathfrak{m}\). Suppose that the following two facts are true:

(i) \(\bar{F}\) has distinct roots in \(\bar{k}\).

(ii) \(\bar{F}(x) = g(x)h(x)\) for some monic polynomials \(g(x), h(x) \in k[x]\).

Prove that there are monic polynomials \(G(x), H(x) \in R[x]\) satisfying
\[ \deg(G) = \deg(g), \quad \deg(H) = \deg(h), \quad \text{and} \quad F(x) = G(x)H(x). \]
(This is another version of Hensel’s lemma.)

**Problem 33.** The absolute value induces a topology on \(R\) in the usual way, i.e., a basis of open sets at a point \(\alpha \in R\) consists of the balls
\[ B_r(\alpha) = \{ \beta \in R : |\beta - \alpha| < r \} \quad \text{with} \quad r > 0. \]
Using this topology, prove that \(R\) is a compact if and only if the quotient field \(R/\mathfrak{m}\) is finite.

**Problem 34.** Let \(f(x) \in K[x]\) be a monic polynomial of degree \(d\) having distinct roots in \(\bar{K}\). Prove that there exists a constant \(C_f\) so that for every monic degree \(d\) polynomial \(g(x) \in K[x]\) that is sufficiently close to \(f\) and every root \(\alpha \in K\) of \(f(x)\),
\[ \min_{\beta \in K, g(\beta) = 0} |\alpha - \beta| \leq C_f |f - g|. \]
(This result is actually true for archimedean fields, too, so you might try giving a proof that works in all cases.)

**Problem 35.** Let \(K/Q\) be a number field, let \(f(x) \in K[x]\) be a monic polynomial of degree \(d\) having distinct roots in \(\bar{K}\), and for each absolute value \(v\) on \(K\), let \(K_v\) be the completion of \(K\). Then in Problem 34 we get a constant \(C_{f,v}\). Prove that for all but finitely many \(v\), the conclusion of Problem 34 is true with \(C_{f,v} = 1\). (This is important, because in the theory of Diophantine equations there are problems where one gets an upper bound of the form \(\prod_v C_{f,v}\), so it’s important to know that this potentially infinite product has a finite value.)
Problem Set # 8

Problem 36. Let \( K/\mathbb{Q}_p \) be a finite extension with ring of integers \( R \) and maximal ideal \( \mathfrak{M} \), and let \( v : K^* \to \mathbb{Z} \) be the normalized valuation on \( K \). Also let \( L(x) \) be the power series
\[
L(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \in K[x].
\]

(a) Prove that \( L(x) \) converges for all \( x \in \mathfrak{M} \).

(b) Prove that the map
\[
R_1^* (\mathfrak{M}) \to K, \quad \alpha \mapsto L(1 - \alpha).
\]
is a homomorphism, where the group law on \( K \) is addition.

(c) Prove that if \( v(x) > v(p)/(p - 1) \), then
\[
v(L(x)) = v(x).
\]

(d) Prove that if \( N > v(p)/(p - 1) \), then the map
\[
R_1^* (\mathfrak{M}^N) \to \mathfrak{M}^N, \quad \alpha \mapsto L(1 - \alpha),
\]
is injective. Deduce that \( R_1^* (\mathfrak{M}^N) \) has no elements of finite order other than 1.

Problem 37. Let \( K/\mathbb{Q}_p \) be a finite extension and let \( L/K \) be a finite tamely ramified extension. Prove that the norm map
\[
N_{L/K} : L^* \to K^*
\]
is surjective. (You may use the fact that on the residue fields \( k_L/k_K \), which are finite fields, the norm and trace maps
\[
N : k_L^* \to k_K^* \quad \text{and} \quad \text{Trace} : k_L \to k_K
\]
are surjective.)

Problem 38. Let \( D \subset \mathbb{R}^2 \) be a bounded open set, and for each \( t > 0 \), let
\[
tD = \{(tx, ty) : (x, y) \in D\}.
\]
Prove that
\[
\lim_{t \to \infty} \frac{tD \cap \mathbb{Z}^2}{t^2} = \text{Area}(D).
\]
Generalize to arbitrary dimension.
1. We fix some notation that will be used for the next few problems. Let $K/\mathbb{Q}$ be a number field and let $C$ be a nonzero ideal class of $K$. Then for $t \geq 1$ we set

$$j(t, C) = \# \{ a \in C : a \subset R_K \text{ and } N_{K/\mathbb{Q}}a \leq t \}.$$ 

We also let

$$j(t, K) = \# \{ a \subset R_K : N_{K/\mathbb{Q}}a \leq t \}.$$ 

**Problem 39.** Fix an ideal $b \subset R_K$ that is in $C^{-1}$. Prove that $j(t, C)$ can be computed by counting principal ideals using the equation

$$j(t, C) = \{ (\alpha) : \alpha \in b \text{ and } |N_{K/\mathbb{Q}}(\alpha)| \leq tN_{K/\mathbb{Q}}b \}.$$ 

**Problem 40.** Let $K/\mathbb{Q}$ be an imaginary quadratic field, and let $w_K$ denote the number of roots of unity in $K$. Then with notation as above, prove that for every ideal class $C$,

$$\lim_{t \to \infty} \frac{j(t, C)}{t} = \frac{2\pi}{2\sqrt{D_{K/\mathbb{Q}}}}.$$ 

Use this to deduce that

$$\lim_{t \to \infty} \frac{j(t, K)}{t} = \frac{2\pi h_K}{2\sqrt{D_{K/\mathbb{Q}}}},$$

where $h_K$ is the class number of $K$.

**Problem 41.** Let $K/\mathbb{Q}$ be a real quadratic field with a fixed embedding $K \subset \mathbb{R}$, and let $u_K$ be the smallest unit in $R_K^*$ satisfying $u_K > 1$. (This unit is often called the fundamental unit.) Then with notation as above, prove that for every ideal class $C$,

$$\lim_{t \to \infty} \frac{j(t, C)}{t} = \frac{2\log u_K}{\sqrt{D_{K/\mathbb{Q}}}}.$$ 

Use this to deduce that

$$\lim_{t \to \infty} \frac{j(t, K)}{t} = \frac{2h_K \log u_K}{\sqrt{D_{K/\mathbb{Q}}}},$$

where $h_K$ is the class number of $K$. 

*E-mail address: jhs@math.brown.edu* 

**Mathematics Department, Box 1917 Brown University, Providence, RI 02912 USA**