MATH 225A PROBLEM SHEET IV
FEBRUARY 21, 2006

1. Let p be a prime and a be an integer, and let (a/p) denote the Legendre symbol. Taking a to be an integer modulo p, verify that the map from $\mathbf{F}_p^*$ to $\{\pm 1\}$ given by $a \mapsto (a/p)$ is a homomorphism. Let p be an odd prime and let z be a generator of the multiplicative group $\mathbf{F}_p^*$. Show that $z^{(p-1)/2} = -1$ and hence deduce *Euler's criterion*: For any d prime to p, $d^{(p-1)/2} \equiv (d/p) \mod p$.

2. Let p, q be distinct odd primes and let w denote a primitive pth root of unity in an extension of $\mathbf{F}_q$. For any $a \in \mathbf{F}_p^*$, define the Gauss sum (in an extension of $\mathbf{F}_q$ as

$$\tau(a) = \sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) w^{ax}.$$

Prove: (i) $\tau(a) = (a/p)\tau(1)$, (ii) $\tau(1)^q = \tau(q)$, (iii) $\tau(1)^2 = (-1)^{(p-1)/2}p$.

3. For any odd n, put $\varepsilon(n) \equiv (n-1)/2 \mod 4$. Use (2) above to show that $\tau(1)^{q-1} = (q/p)$. By evaluating $\tau(1)^{q-1} = [\tau(1)^2]^{(q-1)/2}$ in two ways, prove *the law of quadratic reciprocity*, viz.:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(q)}.$$

4. For any odd n, put $\omega(n) \equiv (n^2-1)/2 \mod 8$. Let α be a primitive 8th root of unity in an extension of $\mathbf{F}_p$, and put $\beta = \alpha + \alpha^{-1}$. Show that $\beta^2 = 2$. Using the Frobenius endomorphism $x \mapsto x^p$ and Euler's criterion to evaluate β^{p-1} in two ways, prove that $(2/p) = (-1)^{\omega(p)}$.

5. Find the class numbers of $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-6})$. Hence find all the integral solutions to

(i) $x^3 = y^2 + 2$

(ii) $x^3 = y^2 + 54$

6. For an integer n, let ζ_n denote a primitive nth root of unity.

(i) If n is not a prime power, show that $1 - \zeta_n$ is a unit of $\mathbf{Q}(\zeta_n)$.

(ii) Let p be a prime, and let $(m, p) = 1$. Show that $(1-\zeta_p)/(1-\zeta_p^m)$ is a unit of $\mathbf{Q}(\zeta_p)$.

7. Calculate the class number of $K := \mathbf{Q}(\sqrt[3]{2})$. Find a unit of infinite order in K.

(Recall that we have shown that $\mathbf{Z}(\sqrt[3]{2})$ is the ring of integers of K.)