Math 702

1. (a) Let b be an odd positive integer, and let  $a = \pm 2b$ . Show that there is a positive integer m such that the Jacobi symbol  $\left(\frac{a}{m}\right) = -1$ . [Hint: There is an m such that  $m \equiv 5 \pmod{8}$  and  $m \equiv 1 \pmod{b}$ .]

(b) Show that the same conclusion holds if instead  $a = \pm qb$ , where b is as in (a) and q is an odd prime not dividing b. [Hint: There is an n prime to q such that  $(\frac{n}{q}) = -1$ , and there is an m such that  $m \equiv 1 \pmod{4b}$ ,  $m \equiv n \pmod{q}$ .]

(c) Conclude that if  $a \in \mathbb{Z}$  is a square modulo p for every prime p, then a is a square in  $\mathbb{Z}$ .

2. Verify the assertion of Artin Reciprocity for the extension  $\mathbb{Q} \subset K = \mathbb{Q}[\sqrt{n}]$ , where  $n \in \mathbb{Z}$  is not a square. That is, show that there is a conductor c supported only at the ramified and infinite primes such that the Artin map  $\sigma : I^c \to \operatorname{Gal}(K/\mathbb{Q})$  is a surjective homomorphism with kernel equal to  $P_c \mathcal{N}(c)$ . [Hint: Use Quadratic Reciprocity, problem 1 above, and Dirichlet's theorem that every arithmetic progression  $a, a + d, a + 2d, \ldots$  with (a, d) = 1 contains (infinitely many) prime numbers.]

3. (a) Let  $X = \mathbb{P}^1$ , let  $S = \{0, \infty\}$ , and let  $f : X - S \to \mathbb{G}_m$  be the identity map. Show explicitly from the definition that  $(0) + (\infty)$  is a modulus for f.

(b) Let  $X = \mathbb{P}^1$ , let  $S = \{\infty\}$ , and let  $f : X - S \to \mathbb{G}_a$  be the identity map. Show explicitly from the definition that  $2 \cdot (\infty)$  is a modulus for f. [Hint: Make a change of variables to analyze the behavior of a rational function g at infinity.]

4. Let  $X = \mathbb{P}^1$ , let  $\mathfrak{m}$  be an effective divisor on X, and let  $X_{\mathfrak{m}}$  be the associated singular curve.

(a) Show that if  $\mathfrak{m} = (0) + (\infty)$  then  $X_{\mathfrak{m}}$  is isomorphic to the projective plane curve whose affine equation is  $y^2 = x^3 + x^2$ .

(b) Show that if  $\mathfrak{m} = 2 \cdot (\infty)$  then  $X_{\mathfrak{m}}$  is isomorphic to the projective plane curve whose affine equation is  $y^2 = x^3$ .

[Hint: Show the isomorphism away from the singular point of  $X_{\mathfrak{m}}$  and then at the local ring at the singular point.]

5. Let p, q be prime numbers (possibly equal), let G be a finite p-group, and let  $\mathbb{Q} \subset K$  be a G-Galois extension ramified only at q.

(a) Show that  $\mathbb{Q} \subset K$  is totally ramified over q. [Hint: Let I be an inertia group. Use that every proper subgroup of a p-group is contained in a proper normal subgroup, and that  $\mathbb{Q}$  has no non-trivial unramified extensions.]

(b) Show that K has no non-trivial abelian unramified extensions L of p-power degree over K. [Hint: Show that the maximal such extension is Galois over  $\mathbb{Q}$ , and then apply part (a) to this field.]

(c) Conclude that the class number of K (i.e. the order of the class group of K) is prime to p. [Hint: Use another characterization of the class group, and apply (b).]

6. Let p be an odd prime number, let G be a finite p-group, and let  $\mathbb{Q} \subset K$  be a G-Galois extension ramified only at p.

(a) Show that if G is abelian then G is cyclic of p-power order. [Hint: What particular abelian extension of  $\mathbb{Q}$  must K lie in? What is the Galois group of this extension of  $\mathbb{Q}$ ?]

(b) Show that G is cyclic of p-power order even if we don't assume that G is abelian. [Hint: Apply part (a) to  $G^{ab} = G/[G, G]$  and then apply the Burnside Basis Theorem.]

(c) Conclude that the maximal pro-*p*-group quotient of  $\pi_1(\operatorname{Spec} \mathbb{Z}[1/p])$  is  $\mathbb{Z}_p$ .