

## MATH 845: HOMEWORK 5, DUE MAY 5.

1. (a) Let  $p$  be prime. Show there exists a field  $K$  of degree 4 over  $\mathbf{Q}$ , containing  $\sqrt{5}$ , with absolute discriminant  $25p$  if and only if  $p \not\equiv 2, 3 \pmod{5}$ . Show that such a field is determined by  $p$  - call it  $K_p$ . Show that the only Galois  $K_p/\mathbf{Q}$  is for  $p = 5$ .

(b) Show that  $K_p$  is neither totally real nor totally complex if and only if  $p \equiv 3 \pmod{4}$ . If  $p \equiv 1 \pmod{8}$ , show that  $K_p$  is totally real if and only if  $p$  divides the  $(p-1)/4$ th Fibonacci number and is totally complex otherwise. If  $p \equiv 5 \pmod{8}$ , show that  $K_p$  is totally complex if  $p$  divides the  $(p-1)/4$ th Fibonacci number and totally real otherwise.

2. An elliptic curve  $E$  over  $\mathbf{Q}$  of conductor  $N$  gives rise, for each prime  $p$  not dividing  $N$ , to a Galois extension (its  $p$ -division field)  $K/\mathbf{Q}$  that is unramified at all primes dividing  $pN$ . Moreover  $\text{Gal}(K/\mathbf{Q})$  embeds in  $GL_2(\mathbf{F}_p)$  such that the image of any Frobenius element at  $q$  (a prime not dividing  $pN$ ) has trace  $q + 1 - |E(\mathbf{F}_q)|$  and determinant  $q$  (both taken modulo  $p$ ).

(a) Let  $E$  be an elliptic curve over  $\mathbf{Q}$  of conductor 11. We know that if  $p = 2$ , then  $K/\mathbf{Q}$  has ramification indices  $e_2 = 3, e_{11} = 2$ . Find  $K$ . (You cannot quote any classification of elliptic curves of conductor 11, unless you write out e.g. Wiles's proof in full). Characterize the parity of  $|E(\mathbf{F}_q)|$  as  $q$  varies.

(b) If  $E$  and  $E'$  are two non-isogenous elliptic curves over  $\mathbf{Q}$  of conductor  $N$ , then Faltings's work yields an extension  $L/\mathbf{Q}$  containing  $K$ , whose Galois group embeds in the subgroup  $H$  of  $GL_2(\mathbf{F}_p[T]/(T^2))$  consisting of matrices whose determinant is in  $\mathbf{F}_p$ . Show that in the case  $p = 2$ ,  $H \cong S_4 \times \mathbf{Z}/2$ .

$L/\mathbf{Q}$  is also ramified only at the primes dividing  $pN$ . Suppose  $N = 11$  and  $p = 2$ . Find all possible  $L$  (the result in fact implies there is only one isogeny class of elliptic curves over  $\mathbf{Q}$  of conductor 11).