Problem set 12

Exercises (4)-(8) use material we will discuss on Monday and Wednesday.

(1) Use Lenstra’s elliptic curve factorization algorithm to factor each of the numbers \( N \) using the given elliptic curve \( E \) and point \( P \). (Use PARI.)
   
   (a) \( N = 589 \), \( E: y^2 = x^3 + 4x + 9 \), \( P = (2, 5) \)
   
   (b) \( N = 28102844557 \), \( E: y^2 = x^3 + 18x - 453 \), \( P = (7, 4) \).

(2) Verify that the Weil pairing is antisymmetric, bilinear, and that \( (P, P) = 1 \). (This should take no more than 3 lines. If you want a more challenging check, try [HPS] #5.27(b).)

(3) [optional] Compute the Weil pairing on the points \( P \) and \( Q \) of Example V.E.7. (You could do it “by hand” or look up Miller algorithm in [HPS] and use that.)

(4) Show that \( N_{K/\mathbb{Q}} \) and \( Tr_{K/\mathbb{Q}} \) are independent of the choice of basis for \( K \) as a vector space over \( \mathbb{Q} \).

(5) Let \( K = \mathbb{Q}(\sqrt{2}) \) where \( \theta = \sqrt{2} \). What are \( m_\theta \) and \( [K : \mathbb{Q}] \)? What are the conjugates of \( \theta \), i.e. the other roots of \( m_\theta \)?

(6) With \( K \) as in (3), compute the norm of \( a + b\theta + c\theta^2 \) and the discriminant \( \Delta(1, \theta, \theta^2) \).

(7) Find \( \Delta(1, \sqrt{2}, \sqrt{3}, \sqrt{6}) \) where \( K = \mathbb{Q}(\theta), \theta = \sqrt{2} + \sqrt{3} \).

(8) Compute the minimal polynomial for \( \sqrt{3} + \sqrt{7} \).