

MATH 104A NUMBER THEORY - FINAL SPRING 2000

1. For the following problem you may use that 587 and 1376 are primes. Prove or disprove
  - (a) 587 is a square mod 1367,
  - (b) 585 is a square mod 1367.
2. Consider the elliptic curve  $E : y^2 = x^3 + x - 1$  and the points  $P = (1, 1)$  and  $Q = (2, -3)$  on  $E$ .
  - (a) Compute  $P + Q$  with respect to the group law on  $E$ .
  - (b) Prove or disprove that  $P$  is a torsion point on  $E$  (you may use that  $2P = Q$ ).
  - (c) Determine the primes  $p$  (if any) for which  $P$  has order 6 for the given elliptic curve  $E$  mod  $p$ . (Hint: What would be the  $y$ -coordinate of  $3P$  in this case?)
3.
  - (a) Compute the number  $y = y(x)$  as a function of  $x$  whose continued fraction expansion is  $[1, 2, 3, x]$ .
  - (b) Find the number whose continued fraction expansion is  $[\overline{1, 2, 3}]$ .
  - (c) Find the continued fraction expansion of  $\frac{11x+4}{3x+1}$  (If confused, find expansion for  $26/7$  for partial credit).
5.
  - (a) Find conditions for primes  $q$  for which 5 is a quadratic residue.
  - (b) Let  $p_1, p_2, \dots, p_k$  be primes  $\equiv -1 \pmod{5}$ . Find conditions for primes  $q$  which divide  $N = (2p_1 p_2 \dots p_k)^2 - 5$ .
  - (c) Show that there are infinitely primes  $p$  of the form  $p = 5n - 1$ . (*Hint*: Assume  $p_1, p_2, \dots, p_k$  are all the primes  $\equiv -1 \pmod{5}$ . Consider the primes  $q$  which divide  $N = (2p_1 p_2 \dots p_k)^2 - 5$ .)