Partnering problems for Programming Investigation Module: Lenstra's elliptic curve factoring algorithm

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

---

0. (0 points, does not need to be turned in) Check that your program works using examples found in our texts: Savin 13.1, Trappe-Washington 16.3, and Hoffstein, et al. 5.6.

1. (5 points) Compute the order of $P = (1, 3)$ on $y^2 = x^3 + 8 \mod 41$. *Hint:* What is $|E(41)|$? Explain how you arrived at your answer.

2. (10 points) Let $P = (2, 3)$ on $y^2 = x^3 - 10x + 21$ modulo the prime 557. Verify that $189P = O$, while $63P$ and $27P$ do not equal O. Explain why this shows that the order of P is 189. Then use the fact that P has order 189, along with Hasse's bound, to determine the number of elements in this elliptic curve group.

3. (10 points) Let E be the elliptic curve $y^2 = x^3 + 17$. The prime factors $p < q$ of the composite number $7519 = pq$ satisfy $|E(p)| = 2^6$ and $|E(q)| = 3 \cdot 37$. Therefore, the order of any point P is a power of 2 modulo p and is odd modulo q. In particular, successively doubling any point $P \neq \infty$ gives the identity element modulo p, but not modulo q.

   Factor 7519 by successively doubling (a) $P = (-1, 4)$, and (b) $P = (2, 5)$.

   You can either apply your function that computes multipes, computing multiples of a point on a curve multiple times, or use a loop to do so.

4. (5 points) Factor 363982776557 using the point $P = (2, 5)$ on the curve $y^2 = x^3 + 3x + 11$.

5. (25 points) Use Lenstra's algorithm to find a proper factorization of the following composite integers. *Required work*: List (i) the chosen elliptic curve equation, (ii) the starting point P on the curve, (iii) the resulting factor, and (iv) the multiple of P yielding this factor.

   (a) 978361
   (b) 185761
   (c) 36590977
   (d) 292403327
   (e) 867360899