

MATH 5405 - EXAM III - DUE APRIL 27, 10:45 AM

Your name:

1) (5 pts) Complete the addition table for the points $P = (-1, 0)$, $Q = (0, 1)$, $-Q = (0, -1)$, $R = (2, 3)$, $-R = (2, -3)$, and the point at infinity O on the elliptic curve $y^2 = x^3 + 1$. (This shows that these six points form a subgroup of the elliptic curve group.)

+	O	P	Q	$-Q$	R	$-R$
O	O	P	Q	$-Q$	R	$-R$
P	P	O				
Q	Q			O		
$-Q$	$-Q$		O			
R	R					O
$-R$	$-R$				O	

Enter your answers in the table. Write down detailed computation of $P + Q$ only.

2) (5 pts) Let $P = (2, 3)$ be a point on the elliptic curve $E := y^2 = x^3 - 10x + 21$ modulo the prime 557 .

- (1) Show that $189P = O$ while $63P \neq O$ and $27P \neq O$. Explain why this shows that the order of P is 189.
- (2) Use the fact that P has the order 189 and Hasse's estimate to determine - precisely - the order of $E(557)$.

The fastest way to compute mP is by consecutive squaring or doubling. Thus write down here $2P, 4P, 8P, \dots, 128P$ and then $27P, 63P$ and $189P$.

3) (5 pts) Reverse engineering. In this exercise we shall construct a composite number $n = p \cdot q$ which can be factored using the point $P = (1, 2)$ be on the curve $y^2 = x^3 - x + 4$. First, calculate $Q = 2P$ as a rational point. Next, calculate $2Q$. In order to calculate $3Q$ - do not do that - you need the slope through Q and $2Q$:

$$A = \frac{y_{2Q} - y_Q}{x_{2Q} - x_Q}.$$

Write $x_{2Q} - x_Q$ as a reduced fraction and let p be the biggest prime divisor of the numerator. Let q be the first prime number bigger than $2p$. This choice of q is not important, but it assures that the following number

$$n = p \cdot q$$

is well defined. Now use the point $P = (1, 2)$ on the curve $y^2 = x^3 - x + 4$ to factor n .

4) (5 pts) Computing the “discrete logarithm on elliptic curves”. Let $P = (-1, 4)$ be a point on the curve $y^2 = x^3 + 17$. Then $Q = (21, 3) \equiv nP \pmod{31}$ for some positive integer n . The number n is called the discrete logarithm of Q modulo 31. We shall calculate n using the giant step - baby step method. First, use Hasse’s inequality to show that the order of $E(31)$ is less than or equal to 43. Since the root of 43 is less than 7, the number n can be written as $n = i + j7$ for some i and j less than 7. Now n is determined by following two steps:

- (1) Compute and list iP modulo 31 for all $i = 1, 2, \dots, 7$.
- (2) Compute $Q - j(7P)$ for $j = 1, 2, \dots$ until it is equal to iP for some i , $1 \leq i \leq 6$.

5) (5 pts) This problem involves some steps necessary to develop a primality test for Mersenne primes using the elliptic curve E given by $y^2 = x^3 - 12x$. Let $P = (-2, 4)$ and $Q = (0, 0)$. Let ℓ be an odd prime such that $m = 2^\ell - 1$ is prime. Show that

- (1) Q is the only point of order 2 on the curve $E(m)$.
- (2) P is not obtained by doubling any point on $E(m)$.
- (3) Compute $16P$ modulo 31.