NOTE: You will be emailed a Crowdmark link for submitting the assignment on March 23. If you do not receive the link, please send an email to ajmeneze@uwaterloo.ca.

1. **Elliptic curve computations** (10 marks)

    Consider the elliptic curve $E : Y^2 = X^3 + 10X + 16$ defined over $\mathbb{Z}_{17}$.

    (a) Find $E(\mathbb{Z}_{17})$, the set of $\mathbb{Z}_{17}$-rational points on E.

    Solution, all the '=' sign are modulo by 17 $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 8, 6^2 = 2, 7^2 = 15, 8^2 = 13, 9^2 = 13, 10^2 = 15, 11^2 = 2, 12^2 = 8, 13^2 = 16, 14^2 = 9, 15^2 = 4, 16^2 = 1$

    Let $x = 0, y^2 = 16, y = \pm 4 = 4, 13$ The same for $x = 1, 2, 3, \ldots 16$ All the rational points are $\{\infty, (0, 4), (0, 13), (4, 1), (4, 16), (5, 2), (5, 15)(7, 2), (7, 15), (8, 8), (8, 9), (9, 6), (9, 11)\}$

    (b) What is $\#E(\mathbb{Z}_{17})$? (Check: $\#E(\mathbb{Z}_{17})$ is prime.)

    Solution   Its 13 and its a prime.

    (c) Find a generator of $E(\mathbb{Z}_{17})$.

    Solution   Any point except ∞ is a generator as the $\#E(\mathbb{Z}_{17})$ is prime.

    (d) Let $P = (5, 2)$, $Q = (9, 11)$, $R = (9, 6) \in E(\mathbb{Z}_{17})$. Compute the following points:

    (i) $P + Q$.

    $\lambda = \frac{11-2}{9-5} = 9 \cdot 4^{-1} = 9 \cdot 13 = -2$

    $x = (-2)^2 - 9 - 5 = 7, y = -((-2) \cdot (7 - 5) + 2) = 2$, Thus, $P + Q = (7, 2)$

    (ii) $Q + R$.

    ∞

    (iii) $2R$.

    (8,8)

    (iv) $2018R$.

    $2018R = (2018 \bmod 13)R = 3R = (4, 1)$

    (e) Determine $\log_P R$.

    Solution $2P = (7, 15), 3P = (9, 6)$ Thus, $\log_P R = 3$

2. **Point multiplication** (10 marks)

Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over $\mathbb{Z}_p$. Let $n = \#E(\mathbb{Z}_p)$, and suppose that n is prime. Design and analyze a *polynomial-time* algorithm (repeated double-and-add) which, on input p, a, b, n, $P \in E(\mathbb{Z}_p)$ and $m \in [1, n-1]$, outputs mP.

Solution   Write m in binary representation as $m_i, i = 0, 1, 2, \ldots, \lfloor \log m \rfloor$

You should make an effort to solve all the problems on your own. You are also welcome to collaborate on assignments with other students presently enrolled in CO 487/687. However, *solutions must be written up by yourself.* If you do collaborate, please *acknowledge your collaborators* in the write-up for each problem. *If you obtain a solution with help from a book, research paper, a web site, or elsewhere, please acknowledge your source.* You are *not* permitted to solicit help from online bulletin boards, chat groups, newsgroups, or solutions from previous offerings of the course.

The assignment should be submitted via Crowdmark before **11:59 pm on April 4**. Late assignments will not be accepted except in *very* special circumstances (usually a documented illness of a serious nature). A high workload because of midterm tests and assignments in other courses will *not* qualify as a special circumstance.

Instructor and TA office hours:

Monday:	1:00 pm – 2:00 pm	Alessandra Graf (MC 5029)
	3:00 pm – 5:30 pm	Alfred Menezes (MC 5026)
Tuesday:	10:30 am – 11:30 am	Priya Soundararajan (MC 5466)
	11:30 am – 12:30 pm	Sam Jaques (QNC 4114)
	1:00 pm – 2:00 pm	Luis Ruiz-Lopez (MC 5486)
	3:00 pm – 4:00 pm	Elena Bakos Lang (MC 5474)
Thursday:	2:00 pm – 3:00 pm	Chris Leonardi (MC 5494)
Friday:	1:00 pm – 3:00 pm	Alfred Menezes (MC 5026)