CS 463/563 — Cryptography for Cybersecurity
Homework 9: Elliptic Curve Cryptography

DUE DATE HERE

STUDENT NAME HERE
UIN HERE
SECTION HERE
Instructor: J. Takeshita. Institution: Old Dominion University.

This assignment has **4** questions.

Submission instructions: If you don't already have the necessary tools, then install 1) a LaTeX distribution (probably the `texlive-full` package on most Linux distributions) and 2) an IDE or other text editor suitable for LaTeX. For the latter, I suggest the use of the Kile IDE, which is available in most Linux distributions' default packages. You can also just use a web IDE such as **Overleaf**.

Download the source file(s) for this assignment. Edit the file(s) to include your solutions using the text editor or LaTeX IDE of your choice. Type your answers and personal information (e.g., name, section, etc.) into the source file at the appropriate places, and double-check that the variable `solutions` is set to be false. (I should have done this for you, but it's good to be sure.) Make sure to properly format your math! See `https://latex-tutorial.com/tutorials/` if you're not already familiar with LaTeX.

Compile the source to a PDF, either through your IDE or by using the command `pdflatex`. Make sure your compilation has no errors, and address all reasonably actionable warnings (you can ignore small things like badbox warnings, as long as they don't affect the output badly). You can toggle the variable `boilerplate` to hide these instructions, if you like.

Turn in 1) the PDF and 2) any and all `.tex` source files, `.bib` bibliography files, source code, or other artifacts. Submissions that are handwritten or typeset with other methods will not be accepted! If you wrote any software in the course of this work, please include it using the `listing` package's utilities.

Cite any external sources, and include any code you write. The use of unauthorized outside assistance, including any AI/LLM, is strictly prohibited.

A note: While it is possible and allowed to solve these questions by writing your own computer programs, you should be able to also do them by hand, as similar questions may appear on exams.

Questions:

1. Consider the equation[1] $y^2 \equiv x^3 + 5x + 11 \pmod{17}$. (25 points)
   (a) Does this equation describe an elliptic curve? Justify your answer.
   (b) List all real-valued points on this curve for $x \in \{0, 1, 2, 3\}$, i.e., all elements of the set $\{(x, y) \in \mathbb{R}^2 | (x \in \{0, 1, 2, 3\}) \wedge (y^2 \equiv x^3 + 5x + 11 \pmod{17})\}$. (The symbol $\wedge$ is the logical AND.)
   (c) List all integer-valued points on this curve, i.e., all elements of the set $\{(x, y) \in (\mathbb{Z}_{17})^2 | y^2 \equiv x^3 + 5x + 11 \pmod{17}\}$. Hint: if a given value of x implies that the corresponding y-value is not a perfect square, then no integral point with that value of x exists. Also, remember: squares have both positive and negative square roots!
   (d) Consider the points $P = (3, 6)$ and $Q = (7, 7)$ on this curve. Compute $2P + Q$.
   (e) Using Hasse's Theorem, find the upper and lower bounds for the number of points on this curve.

Answer:

(a) Yes.
$5, 11 \in \mathbb{Z}_{17}$
and
$4 * 5^3 + 27 * 11^2 \neq 0 \pmod{17}$

(b) $x = 0$ $0 + 0 + 11 \pmod{17} = \pm\sqrt{11}$
$(0, \sqrt{11}), (0, -\sqrt{11})$

$x = 1$
$y^2 = 1 + 5 + 11 = 17 \pmod{17} = 0$
$(1, 0)$

$x = 2$
$y^2 = 8 + 10 + 11 \pmod{17} = \pm\sqrt{12}$
$(2, \sqrt{12}), (2, -\sqrt{12})$

$x = 3$
$y^2 = 27 + 15 + 11 \pmod{17} = 53 \pmod{17} = \pm\sqrt{2}$
$(3, \sqrt{2}), (3, -\sqrt{2})$

$\boxed{(3, \sqrt{2}), (3, -\sqrt{2}), (2, \sqrt{12}), (2, -\sqrt{12})(1, 0), (0, \sqrt{11}), (0, -\sqrt{11})}$

[1] Technically, it's a congruence.

(c) $(1, 0)$

(d) $s_{double} = \frac{3*3^2+5}{2*6} \pmod{17} = \frac{8}{3} \pmod{}$
$s_{double} = \frac{8}{3} \pmod{17} = 8 * 3^{-1} \pmod{17} = 8 * 6 \pmod{17} = 14$
$x_3 = 14^2 - 3 - 3 \pmod{17} = 3$
$y_3 = 14(3 - 3) - 6 \pmod{17} = -6 \pmod{17} = 11$
$2P = (3, 11)$

$s_{add} = \frac{7-3}{7-11} \pmod{17} = \frac{4}{-4} = -1 \pmod{17} = 16$
$x_3 = 16^2 - 3 - 7 \pmod{17} = 8$
$y_3 = 16(3 - 8) - 11 \pmod{17} = -91 \pmod{17} = 11$
$\boxed{2P + Q = (8, 11)}$

(e) $17 + 1 - 2\sqrt{17} \leq \#E \leq 17 + 1 + 2\sqrt{17}$
$\boxed{9.75 \leq \#E \leq 26.25}$

2. What is an advantage of elliptic curve cryptography, as compared to other types of cryptographic systems we have studied? (5 points)

Answer: Elliptic curves have the same level of security as other public key encryption schemes while using smaller bit lengths. For example, for 256 bit Security in RSA, you would need bit lengths of 15360. But for Elliptic curves, you would only need a bit length of 512 to get the same security.

3. What is an actual or potential weakness or downside of elliptic curve cryptography? (5 points)

Answer: A potential weakness of elliptic curve cryptography is that it is a public key scheme which makes it rely on calculations heavily, so large amounts of encryption may slow down a program.

4. Give a new question on the topic of this week's material and its solution, suitable for inclusion in future versions of this homework assignment. Your question should be different from the other questions here – don't just change some values around! Programming problems are acceptable too, but should be nontrivial. You can use textbooks, scholarly papers, or other reputable sources of information for inspiration, but you should not directly copy someone else's work. Your question should show

me that you understand the content well enough to ask and answer an interesting question about it. Include any source code used to generate/solve the problem. (10 points)

Some free online textbooks include *The Joy of Cryptography* by Mike Rosulek (Oregon State University), or *A Graduate Course in Applied Cryptography* by Dan Boneh (Stanford University) and Victor Shoup (Offchain Labs, formerly at New York University). Your course text, *Understanding Cryptography* by Christof Paar (Universität Bochum) and Jan Pelzl (Universität Bochum), is also an excellent starting point.

Possible topics include elliptic curves and cryptographic constructions based on elliptic curves.

Answer: In words, explain how point doubling and point addition appear on a graph.

With point addition on an elliptic curve, a line is drawn between two points. That line is then extended until it touches another point on the curve . That third point that is touched is the sum of the original two points.

With point doubling on an elliptic curve, a tangent line is drawn at a point. That tangent line is then extended until it touches another point on the curve. That second point that is touched is the doubled value of the original point.