Virtual Class, Week 10

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

Greetings, everyone! Here are the instructions for MATH 601 this week:

1. Remember that the the **Extended Euclidean Algorithm/RSA** Programming Investigation Module is **due this Friday**, on April 10.

2. **Read the full lecture notes** for Week 10 in the **Daily Update**. Use Sections 11.4 and 12.1 of Savin as an additional reference, but though some interesting motivation is recorded there, *be careful* – Section 12.1 has several typos in the formulas presented!

3. Access Blackboard, and **watch the instructional videos** entitled:

   (a) Quadratic sieve factoring algorithm

   (b) Elliptic curve group law

4. Complete the following **homework problems** and submit your solutions to Gradescope by **next Tuesday** (4/14). As usual, show all your steps in each problem.

   1. (10 points) Compute 255^2 and 317^2 modulo 64777. Use these to factor 64777.
   2. (10 points) Use the Quadratic sieve method to factor 7097.
   3. (10 points) An RSA-encrypted message reads 4110 where $e = 7$ and the modulus is $m = 30227$. Use the Quadratic sieve method to factor m and decrypt the message. Express the final answer in terms of the nine letter alphabet from the lecture notes.
   4. (10 points) Complete the addition table below where $P = (-1, 0)$, $Q = (0, 1)$, and $R = (2, 3)$, are points on the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{R}$. (This shows that these six points form a subgroup.)

$+$	∞	P	Q	$-Q$	R	$-R$
∞						
P						
Q						
$-Q$						
R						
$-R$						

Hint: If you find that a line is tangent to some point S on the elliptic curve, and there are no other points on the intersection of the curve with the tangent line, then S is considered to have multiplicity 3 on E, i.e., $S+S+S = 3S = O$. To verify this, either use the addition formula applies to $S+S$, and you should find that $S+S = -S$, or you can plug the equation for the tangent line into the elliptic curve equation, and check that the x-coordinate is triple root of the resulting cubic equation.

5. (10 points) Let $P = (1, 3)$ on the elliptic curve $y^2 = x^3 + 8$ over $\mathbb{R}$. Compute $2P$ and $4P$ by hand.

5. Access **Virtual Office Hours** on Blackboard with any questions.

6. Interested in delving deeper into this week's topics?

- Mathematician Carl Pomerance wrote in 1985: Pomerance created the algorithm!!

  > The quadratic sieve algorithm is currently the method of choice to factor very large numbers with no small factors. In the hands of the Sandia National Laboratories team of James Davis and Diane Holdridge, it has held the record for the largest hard number factored since mid-1983. As of writing, the largest number it has cracked is the 71-digit number $(10^{71} - 1)/9$, taking 9 hours on the Cray XMP computer at Los Alamos, New Mexico.

  See his interesting paper on the history of the quadratic sieve algorithm, which also includes some suggested improvements on the method!

- Graph the elliptic curves $y^2 = f(x)$, for the following $f(x)$ on Wolfram Alpha or other graphing software to see the beautiful ways that their shapes can change:

$$x^2 + 1,\ x^2 - x + 1,\ x^3 - x^2,\ x^3 - x,\ x^3 + x,\ x^3, x^3 + x^2.$$

  We will investigate elliptic curves like the last two next time!