Virtual Class, Week 9

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

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

1. **Read the full lecture notes** for Week 9 in the **Daily Update**. Use Sections 11.2 and 11.3 of Savin as an additional reference.

2. Access Blackboard, and **watch the instructional videos** entitled

   (a) Pollard's $p-1$ factoring algorithm

   (b) The finite field with p^2 elements

   (c) The $p+1$ factoring algorithm

3. Complete the following **homework problems** and submit your solutions to Gradescope by **next Tuesday** (4/7). As usual, show all your steps in each problem. If you use *fast exponentiation*, point this out and omit the actual calculation.

   1. (10 points) Use Pollard's $p-1$ factoring algorithm to factor 4883.
   2. (10 points) Use Pollard's $p-1$ factoring algorithm to factor $618\,240\,007\,109\,027\,021$.
   3. (10 points) Factor 5251 using the $p+1$ factoring algorithm with $z = 1 + 2i$.
   4. (10 points) Factor 3953 using the $p+1$ factoring algorithm with $z = 2 + i$.

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

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

   - Check out how to break RSA in some cases by investigating Proposition 46 and its proof in Savin 11.3.
   - Our $p+1$ factoring algorithm is only one variant. Read the Wikipedia article on *Williams's p + 1 algorithm*, and follow related links if you're interested!
   - Try the following challenge problem for fun: Explain why the $p-1$ factoring algorithm will find a *proper* factor of $n = 23 \cdot 61$ with $2 \leq a \leq 22$.

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