Math 5/440 Homework 3
Due Wednesday November 7, 2:45 pm

You can turn in your homework on CoCalc by uploading a scanned handwritten or typed pdf, and a sage worksheet for computations and functions. It will be a good idea to bring a printed copy of your homework to class however, to use during the homework presentations!

Please make note of which problems you are required to do computationally [by hand] or [using SageMath]. For [by hand] problems, you may not use software. For [using SageMath] problems, make sure your computational work is clearly explained.

1. (in book # 3.4) [using sagemath] You and Nikita wish to agree on a secret key using the Diffie-Hellman key exchange. Nikita announces that $p = 3793$ and $g = 7$. Nikita secretly chooses a number $n < p$ and tells you that $g^n \equiv 454 \pmod{p}$. You choose the random number $m = 1208$. What is the secret key?

2. [using sagemath] You are spying on Michael and Nikita who are establishing a Diffie-Hellman key exchange. Nikita sends the following data to Michael

   $p = 27437$
   $g = 7$
   $g^m \equiv 15184 \pmod{p}$.

   Michael responds to Nikita with

   $g^n \equiv 21666 \pmod{p}$.

   You intercept both transmissions. Crack their code. What is Nikita and Michael’s shared secret key $s$ modulo $p$?

3. [using sagemath] Nikita underestimated you as an adversary, and decided to use small numbers for her RSA cryptosystem out of laziness... In particular, she published the following public key:

   $(250600531, 11784151)$.

   (a) Determine Nikita’s secret decryption key $d$.

   (b) You intercept the following encoded message to Nikita: 198581849, 79320434, 174186286. Decode the secret message!

4. (in book # 3.6) [using sagemath] In this problem, you will “crack” an RSA cryptosystem. What is the secret decoding number $d$ for the RSA cryptosystem with public key

   $(n, e) = (5352381469067, 4240501142039)$?
5. (in book # 4.1) [by hand] Calculate the following by hand:
\[
\left(\frac{3}{97}\right), \left(\frac{3}{389}\right), \left(\frac{22}{11}\right), \left(\frac{5!}{7}\right).
\]

6. (in book # 4.3) [by hand] Use Gauss' Quadratic Reciprocity Law (Thm. 4.1.7 in book) to prove that for \( p \geq 5 \) prime,
\[
\left(\frac{3}{p}\right) = \begin{cases} 
1 & \text{if } p \equiv 1, 11 \pmod{12} \\
-1 & \text{if } p \equiv 5, 7 \pmod{12}.
\end{cases}
\]

7. (Double Points!) [by hand] Use Gauss' Quadratic Reciprocity Law (Thm. 4.1.7 in book) and the above problem to prove that there are infinitely many primes of the form \( 3x + 1 \).

[Hint: Modify Euclid’s proof by considering \( N = 4(p_1 \cdots p_n)^2 + 3 \) for a specified set of primes \( p_1, \ldots, p_n \). First show that \( N \) can only have prime divisors \( q \geq 5 \) with \( q \equiv 2 \pmod{3} \). Then use quadratic reciprocity and the above problem to deduce what \( q \) must look like modulo 12 to derive a contradiction. Explain all of your steps very clearly!]