CMPS/MATH 2170 Discrete Mathematics – Fall 14

10/29/14

7. Homework

Due Monday **11/10/14** at the beginning of class

Remember, you are allowed to turn in homeworks in groups of two.

1. **Perfect Number (5 points)**
   A positive integer is called *perfect* if it equals the sum of its positive divisors other than itself.

   (a) (2 point) Show that 6 and 28 are perfect.

   (b) (3 points) Show that $2^{p-1}(2^p - 1)$ is a perfect number, when $2^p - 1$ is prime.
   (Hint: Use the formula for the geometric series.)

2. **GCD (4 points)**

   (a) (2 points) Use the Euclidean algorithm to find $gcd(4125, 2205)$.

   (b) (2 point) Find $lcm(4125, 2205)$ and verify that
   $gcd(4125, 2205) \cdot lcm(4125, 2205) = 4125 \cdot 2205$.

3. **Inverse (5 points)**
   Prove that an inverse of a modulo m does not exist if $gcd(a, m) > 1$.
   (Hint: Use that there is a common divisor of a and m. You may want to consider a proof by contradiction.)

4. **Linear Congruence (2 points)**
   Solve the congruence $2x \equiv 7 \pmod{17}$.

5. **RSA (8 points)**
   The following problem walks you through the cryptanalysis of a message sent with the RSA cryptosystem. Suppose two people are communicating, call them Carola and Ellis, and Carola sends Ellis a message with RSA. She accidentally forwards you a copy of this message:

   > "AYPJRVYAYLHA, I've encrypted the cipher key with your RSA public key, and the encrypted cypher key is 107"

   You know Carola is notorious for having poor security practices – she sends messages with a *shift cipher*. This allows her to use a single encrypted number (the *cipher key*) to encode a whole text message as follows: Every letter is represented by a number between 1-26 ($A \equiv 1 \pmod{26}, B \equiv 2 \pmod{26}, \ldots, Z \equiv 0 \equiv 26 \pmod{26}$), and every letter is encoded by adding a cipher key, modulo 26, to it. Note that this modulo 26 is just for wrap-around purposes and has nothing to do with RSA. Carola's message "AYPJRVYAYLHA" does not make any sense, so it is obviously shifted with some key. So, if you can find the cipher key, you can subtract it from each letter above, modulo 26, and you will retrieve the original message.

Flip over to back page $\Longrightarrow$

You go to Ellis' website and look up his RSA public key and see that it is $(53, 115)$. You notice that Ellis' public key is $e = 53$ and he has chosen $n = 115$, which is a shockingly low number (he must be very bad at crypto, too), so you suspect you can break the cryptosystem, and you hope the message has some important secret information. We will break the system and find the message, step by step.

(a) (1 point) n is small – factor it into prime numbers, and find p, q prime such that $p \cdot q = n$. Our inability to do this step for sufficiently large n is what protects the security of RSA.

(b) (1 point) The exponents work modulo $\phi(n)$, so find $\phi(n) = (p - 1)(q - 1)$.

(c) (2 points) Ellis' public key is $e = 53$ with $n = 115$, so his private key must be the inverse of 53 modulo $\phi(n)$. Find it.

(d) (3 points) Now you have Ellis' private key, d. Use it to decrypt the cipher key. (Here, the message is 107, the encrypted cipher key. Remember, the clear text you are looking for should be the ciphertext $y = 107$, raised to Ellis' private key, which you found in the last step, reduced modulo $n = 115$.

(e) (1 point) Now that you have the cipher key, subtract it from every letter (represented by a number) in the original message, convert each to a letter, and write the final message.