EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai

HW 4

Due Feb 18

1. Modulo arithmetic practice

1. Use Euclid's algorithm (page 3 of note 5) to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.
2. Use the extended Euclid algorithm (page 4 of note 5) to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.
3. Find $x \pmod{27}$ if $5x + 26 \equiv 3 \bmod 27$. You can use the result computed in 2.
4. True or false? Assume a, b, and c are integers and $c > 0$. If a has no multiplicative inverse mod c, then $ax \equiv b \bmod c$ has no solution. Explain your answer.

2. With these results comes great responsibility...

For the following problems, you must both calculate the answers and show your work.

1. What is $2^{2013} \bmod 11$? *(Hint: There's a little theorem from class which you may find useful here. Of course, if you prefer, you can always just play around and (re-)discover the relevant pattern for yourself.)*
2. What is $2^{(5^{2013})} \bmod 11$?

3. How many bottles of tea and juice?

Jacob is preparing for a large party. He spent exactly \$125 on tea and juice. If tea costs \$3.70 per bottle and juice costs \$4.30 per bottle, how many bottles of tea and juice did Jacob buy? Prove that there is only one solution.

4. Fibonacci numbers

Recall that the Fibonacci numbers are defined by

- $F(0) = 0$
- $F(1) = 1$
- For $n \geq 2$, $F(n) = F(n-1) + F(n-2)$

Prove that for any $n \in \mathbb{N}$, $\gcd(F(n+3) + F(n+1), F(n+2) + F(n)) = 1$.

5. Check digits: books and credit cards In this problem, we'll look at two real-world applications of check-digits.

In the first part, we'll look at International Standard Book Numbers (ISBNs). These are 10-digit codes $(d_1 d_2 \ldots d_{10})$ which are assigned by the publisher. These 10 digits contain information about the language, the publisher, and the number assigned to the book by the publisher. Additionally, the last digit d_{10} is a "check digit" selected so that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \mod 11$. (*Note that the letter X is used to represent the number 10 in the check digit.*)

1. Suppose you have very worn copy of the (recommended) textbook for this class. You want to list it for sale online but you can only read the first nine digits: 0-07-288008-? (the dashes are only there for readability). What is the last digit? Please show your work, even if you actually have a copy of the textbook.
2. Wikipedia says that you can determine the check digit by computing $\sum_{i=1}^{9} i \cdot d_i \mod 11$. Show that Wikipedia's description is equivalent to the above description.
3. Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.
4. Can you *switch* any two digits in an ISBN and still have it be a valid ISBN? For example, could 012345678X and 015342678X both be valid ISBNs?
5. Now we'll look at another checksum formula: the Luhn formula (also known as the Luhn algorithm). This formula is used to verify the validity of credit card numbers. You can read more about it and see an example at `http://en.wikipedia.org/wiki/Luhn_algorithm` The algorithm is as follows:
   (a) Double each even-positioned digit, when counting from *right to left*.
   (b) Determine the sum of the digits from each of the products in step (a).
   (c) Sum the numbers from step (b). Find the sum of the unaffected digits (odd-positioned digits) in the original number. Combine these sums.
   (d) Verify the account number by determining if the sum from step (c) is equivalent to 0 mod 10.

   For clarification, an example from Wikipedia is shown below. In this example, $x = 3$ is the check digit.

Account number	7	9	9	2	7	3	9	8	7	1	x
Double every other	7	18	9	4	7	6	9	16	7	2	x
Sum of digits	7	9	9	4	7	6	9	7	7	2	=67

   Using the Luhn algorithm, determine the check digit x for the following number: $601143871005123x$.
6. Can this algorithm detect if any two digits are switched? If not, which will it miss and why? *(Hint: you may look on Wikipedia to get started but explain the answer in your own words.)*

6. OpRSA Anonymous is running a website and needs to be able to securely receive information from people with something interesting to say about a certain potential target. Your job is to help them set up a crypto-system to accomplish this task.

1. Anonymous first generates two large primes, p and q. They pick $p = 13$ and $q = 19$ (though in reality these should be 512-bit numbers). They then computes $N = pq$. Anonymous chooses e from $\{37, 38, 39\}$. Only one of these values is legitimate; which one? (N, e) is then the public key.
2. Anonymous needs to generate a private key, d, which will be kept as a secret. Help Anonymous find d and explain your calculation.
3. Brain wants to send Anonymous the message $x = 102$. How does he encrypt his message using the public key and what is the result?
4. Anonymous receives the encrypted message $y = 141$ from Candy, another informant. What is the unencrypted message that Candy sent?
5. Try encrypting several other messages (you're free to choose, as long as they're valid). Do you see anything wrong with this crypto-system? (In the real world, Anonymous is a lot smarter than this.)

7. Because the Moth just doesn't cut it

Gandalf the Grey (a good wizard) wanders about on his merry adventures but frequently runs into some troubles with goblins and orcs along the way. Always being the well-prepared wizard that he is, Gandalf has enlisted the service of the Great Eagles to fly him out of sticky situations at a moment's notice. To do this, he broadcasts a short message detailing his dilemma and a nearby eagle will come to his aid.

While this is all well and good, Saruman the White (an evil wizard) wants in on this eagle concierge service. The eagles can no longer trust just any distress call they receive! Gandalf needs you (a cryptography master) to help him devise a simple scheme that will allow the eagles to verify his identity whenever he broadcasts a message out. Not only that, but the eagles need to know when the message they receive from Gandalf has been tampered with.

Once you have devised this scheme, Gandalf will tell it to the eagle lord Gwaihir, who will relay it out to the rest of the world (they are loudmouths so they can't keep a secret).

To summarize:

(a) Gandalf broadcasts a message m to all of Middle-Earth.

(b) He is able to attach to the message an extra piece of information s that verifies his identity (i.e. cannot be forged) to whomever receives it.

(c) If the message has been modified in transit, recipients of the modified message should be able to detect that it is not original.

(d) Everyone in Middle-Earth knows the scheme (i.e. the algorithm itself is not a secret)

Your job in this problem is to devise an algorithm (like RSA) that meets the above criteria. In your answer, you should formally prove that Gandalf's messages can be successfully verified. You do not need to formally prove (though it should still be the case) that it is difficult to forge/tamper with messages, but you should provide some informal justification.