CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

HW 4

Due: Tuesdy, October 1, 2019 at 10 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

Note: *This homework consists of two parts. The first part (questions 1-6) will be graded and will determine your score for this homework. The second part (questions 7-8) will be graded if you submit them, but will not affect your homework score in any way. You are strongly advised to attempt all the questions in the first part. You should attempt the problems in the second part only if you are interested and have time to spare.*

For each problem, justify all your answers unless otherwise specified.

Part 1: Required Problems

1 The Last Digit

In each case show your work and justify your answers.

(a) If $9k+5$ and $2k+1$ have the same last digit for some natural number k, find the last digit of k.

(b) If $S = \sum_{i=1}^{19} i!$, then find the last digit of S^2.

(c) Denote the last digit of a natural number a by b. Show that the last digit of a^n is the same as the last digit of b^n where is $n \geq 1$ is a natural number.

(d) Inspired by part (c), show that the last digit of a^{4k+1} for all natural numbers k is the same as the last digit of a. [Euler's Theorem is not allowed.]

2 Modular Arithmetic Problems

In each case show your work and justify your answers.

(a) For natural numbers a, show that $7a+3$ and $5a+2$ are coprime.

(b) What is $3^{48} \pmod{11}$?

(c) Solve $x^2+x \equiv 2 \pmod{4}$.

(d) If $17x^{12}+5x^7-14x^{40} \equiv 6 \pmod{7}$, find x.

(e) If $a+4c \equiv 2b \pmod{21}$, simplify $100a+10b+c \pmod{21}$.

In parts (c), (d), and (e) give your solutions as integers mod m.

3 Check Digits: ISBN

In this problem, we'll look at a real-world applications of check-digits.

International Standard Book Numbers (ISBNs) 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 $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \pmod{11}$. (*Note that the letter X is used to represent the number 10 in the check digit.*)

(a) Suppose you have a 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? Show your work.

(b) Wikipedia says that you can determine the check digit by computing $\sum_{i=1}^{9} i \cdot d_i \pmod{11}$. Show that Wikipedia's description is equivalent to the above description.

(c) 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.

(d) 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? Explain.

4 Product of Two

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > p/2$, i.e. $(\forall x \in S)(1 \leq x \leq p-1)$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.

5 RSA with Just One Prime

Given the message $x \in \{0,1,\ldots,N-1\}$ and $N = pq$, where p and q are prime numbers, conventional RSA encrypts x with $y = E(x) \equiv x^e \pmod{N}$. The decryption is done by $D(y) \equiv y^d \pmod{}$

N), where d is the inverse of $e \pmod{(p-1)(q-1)}$.

Alice is trying to send a message to Bob, and as usual, Eve is trying to decipher what the message is. One day, Bob gets lazy and tells Alice that he will now use $N = p$, where p is a 1024-bit prime number, as part of his public key. He tells Alice that it's okay, since Eve will have to try out 2^{1024} combinations to guess x. It is very likely that Eve will not find out the secret message in a reasonable amount of time! In this problem, we will see whether Bob is right or wrong. Assume that Eve has found out about this new setup and that she knows the public key.

Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{p}$, and $D(y) \equiv y^d \pmod{p}$. Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.

(a) Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve compute d in the decryption function? If so, by what algorithm and approximately how many iterations does it take for it to terminate?

(c) Given part (b), how would Eve recover x and what algorithm would she use? Approximately how many iterations does it take to terminate?

(d) Based on the previous parts, can Eve recover the original message in a reasonable amount of time? Explain.

6 RSA for Midterm Scores

Alice wants to tell Bob her midterm score, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her midterm score.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's midterm score is. How did she do it?

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

Note: *This concludes the first part of the homework. The problems below are optional, will not affect your score, and should be attempted only if you have time to spare.*

Part 2: Optional Problems

7 Just Can't Wait

Joel lives in Berkeley. He mainly commutes by public transport, i.e., bus and BART. He hates waiting while transferring, and he usually plans his trip so that he can get on his next vehicle immediately after he gets off the previous one (zero transfer time, i.e. if he gets off his previous vehicle at 7:00am he gets on his next vehicle at 7:00am). Tomorrow, Joel needs to take an AC Transit bus from his home stop to the Downtown Berkeley BART station, then take BART into San Francisco.

(a) The bus arrives at Joel's home stop every 22 minutes from 6:05am onwards, and it takes 10 minutes to get to the Downtown Berkeley BART station. The train arrives at the station every 8 minutes from 4:25am onwards. What time is the earliest bus he can take to be able to transfer to the train immediately? Show your work. (Find the answer without listing all the schedules.)

(b) Joel has to take a Muni bus after he gets off the train in San Francisco. The commute time on BART is 33 minutes, and the Muni bus arrives at the San Francisco BART station every 17 minutes from 7:12am onwards. What time is the earliest bus he could take from Berkeley to ensure zero transfer time for both transfers? If all bus/BART services stop just before midnight, is it the only bus he can take that day? Show your work.

8 Quantum Factoring

We're pretty sure that classical computers can't break RSA (because it is hard to factor large numbers on them), but we know that quantum computers theoretically could. In this question, we will prove a fact that is a key part of Shor's Algorithm, a quantum algorithm for factoring large numbers quickly[1].

Let $N = pq$ where p, q are primes throughout this question.

(a) Prove that, for all $a \in \mathbb{N}$, there are only four possible values for $gcd(a, N)$.

(b) Using part (a), prove that, if $r^2 \equiv 1 \mod N$ and $r \not\equiv \pm 1 \pmod N$ (i.e. r is a "nontrivial square root of 1" mod N), then $gcd(r-1, N)$ is one of the prime factors of N.
Hint: $r^2 = 1 \mod N$ *can be rewritten as* $r^2 - 1 = 0 \mod N$ *or* $(r+1)(r-1) = 0 \mod N$.

[1] Read more at `https://en.wikipedia.org/wiki/Shors_algorithm`.