CSCI 0220 Discrete Structures and Probability C. Klivans

Homework 5

Due: Tuesday, 10 Mar 2015

All homeworks are due at 11:00PM in the CS22 bin on the CIT second floor, next to the Fishbowl.

Include our cover sheet or equivalent, write your *full name* and CS login on each page of your homework, label all work with the problem number, and staple the entire handin before submitting it.

Be sure to fully explain your reasoning and show all work for full credit. Consult the style guide for more information.

Problem 5.1

The caterpillar has decided that blowing smoke rings is not a subtle enough means of communication for his more sensitive messages, so he has decided to send and receive messages using RSA encryption. The caterpillar has chosen the public key (35, 5) with the numbering scheme $A = 1, B = 2, \ldots, Z = 26$, and Alice has decided to send her most recent correspondence using the caterpillar's encryption scheme. The Dormouse, who already took CS22 and therefore knows everything there is to know about RSA encryption, wants to intercept these messages using the public key and his basic knowledge of prime numbers. Fortunately for him, the caterpillar has chosen a public key which is far too small to be secure!

a. Find the caterpillar's decryption exponent. *(Hint: Find ϕ first.)*

b. Decrypt Alice's message:

$$(8, 10, 17, 11)$$

c. Encrypt the following message to replace Alice's message:

$$SAFE$$

Problem 5.2

Prove that $\frac{21n+4}{14n+3}$ is irreducible by proving that $\gcd(21n + 4, 14n + 3) = 1$ for all $n \in \mathbb{Z}^+$.

Problem 5.3

a. Compute the remainder when $2^{1111} + 3^{2222} + 4^{3333} + 5^{4444}$ is divided by 11. Show all steps.

b. Prove by induction that $2^{2^n} + 3^{2^n} + 5^{2^n} \equiv 0 \pmod{19}$ for all integers $n \geq 1$.
(*Hint*: Use two base cases. Why might this be helpful?)

Problem 5.4

Alice arrives at a tea party and finds that everyone has been drinking magical potions. There are only two types of potions: a truth potion and lie potion, causing the consumer to only tell the truth and only tell lies, respectively. There are five people at the party and everyone only drank one type of potion. Using what each person told Alice, figure out who drank which type of potion. Justify your answers.

- Mock Turtle: "I saw Bill the Lizard drink the lying potion."
- The Dormouse: "Either The White Rabbit or Mock Turtle drank the lying potion. . . maybe both!"
- The White Rabbit: "The Dormouse drank the lying potion and Bill the Lizard drank the truth potion."
- The Mad Hatter: "Of The White Rabbit and Bill the Lizard, exactly one drank the truth potion."
- Bill the Lizard: "The Dormouse and The White Rabbit both drank the truth potion."

Problem 5.5

Alice, the Hatter, the Queen of Hearts, and the Cheshire Cat are playing an *extremely fun* card game which has the following rules:

(1) The Queen of Hearts loses if and only if Alice plays her best card.

(2) If Alice gets up for a cup of tea, then the Queen of Hearts beheads the Hatter.

(3) If the Queen of Hearts beheads the Hatter, then the Cheshire Cat scratches her.

(4) Alice gets up for a cup of tea if and only if she does not play her best card.

(5) If the Cheshire Cat scratches the Queen of Hearts, then Alice does not play her best card.

(6) Every player must either win or lose.

(7) If the Hatter is not beheaded, then he wins.

(8) Only one player can win.

a. Prove that the Queen of Hearts wins if and only if she beheads the Hatter.

b. Prove that Alice plays her best card if and only if the Cheshire Cat does not scratch the Queen of Hearts.

c. Prove that Alice cannot win.