CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Dinh, Psomas, and Ye Discussion 6C

1. Woah There is a simple rule to test if a number n is divisible by 11: if the difference between the sum of the odd numbered digits of n (1st, 3rd, 5th...) and the sum of the even numbered digits of n (2nd, 4th...) is divisible by 11, then n is divisible by 11. Prove this using what you know about modular math.

2. RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e,N_1),\ldots,(e,N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(7,35)$ and $(7,77)$ as well as the corresponding transmissions. How can Eve use this knowledge to break the encryption?

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3,5\times 23)$, $(3,11\times 17)$, and $(3,29\times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.

3. Chinese Remainder Theorem

(1) You're a CalSo leader and you're trying to keep track of the number of high schoolers and family you have in your group. You can't remember the exact count, but you see that when they walk in rows of 5, there are two left, and when they walk in rows of 7, 3 are left. Also, as they walk through Sproul double file (rows of 2), you see that no people are left over. How many people are in your group?

(2) There is a rare event observable in Berkeley: the simultaneous arrival of 3 Bear Transit buses at Cory Hall. You're playing tour guide for friends visiting from unnamed East coast schools and wish to show them this phenomenon, so the day before you start waiting at the station at noon and make note of how long it takes for a bus arrives and ask how long it takes for that bus to return (make a round-trip). You find that one bus arrives in 14 minutes and will return in 21 minutes. Another arrives in 18 minutes and will return in 19 minutes. The last bus arrives in 5 minutes and will take 10(!) minutes to return. Assuming the same arrival times tomorrow, what time between 8:00am and 8:00pm should you and your friends be at the station to watch this event? Note 21*19*10 = 3990.

4. Diophantine

A father's age is one less than twice that of his son, and the digits AB making up the father's age are the reverse of the son's age, BA. How old are father and son?