CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Dinh, Psomas, and YeDiscussion templateC Sol

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.

Let n be written as $a_k a_{k-1} \cdots a_1 a_0$ where the a_i are base-10 numbers. Then $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$. Note that $10 \equiv -1 \mod 11$ so we can write

$$n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0 \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0 \mod 11$$

which is the alternating sum of the digits.

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?

Yes. Note that gcd(77, 35) = 7. She can figure out the gcd of the two numbers using the gcd algorithm, and then divide 35 by 7, getting 5. Then she knows that the p and q corresponding to the first transmission are 7 and 5, and can 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.

Since none of the N's have common factors, she cannot find a gcd to divide out of any of the N's. Hence the approach above does not work.

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?

Let x be the number of people. We start off with the system of linear congruences

$$x = 2 (mod\ 5)$$
$$x = 3 (mod\ 7)$$
$$x = 0 (mod\ 2)$$

From CRT,

$$\begin{aligned} x &= 2\frac{70}{5}\left[\frac{70}{5}^{-1}\right]_5 + 3\frac{70}{7}\left[\frac{70}{7}^{-1}\right]_7 + 0\frac{70}{2}\left[\frac{70}{2}^{-1}\right]_2 (mod\ 70) \\ &= 2(14)(4) + 3(10)(5) (mod\ 70) \\ &= 42 + 10 (mod\ 70) = 52 \end{aligned}$$

Thus, there are 52 people.

(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.

$$x = 14 (mod\ 21)$$
$$x = 18 (mod\ 19)$$
$$x = 5 (mod\ 10)$$

From CRT,

$$\begin{aligned} x &= 14\frac{3990}{21}\left[\frac{3990}{21}^{-1}\right]_{21} + 18\frac{3990}{19}\left[\frac{3990}{19}^{-1}\right]_{19} + 5\frac{3990}{10}\left[\frac{3990}{10}^{-1}\right]_{10} (mod\ 3990) \\ &= 14(190)[1^{-1}]_{21} + 18(210)[1^{-1}]_{19} + 2(399)[9^{-1}]_{10} (mod\ 3990) \\ &= 14(190)(1) + 18(210)(1) + 5(399)(9) (mod\ 3990) \\ &= 2660 + 3780 + 17955 (mod\ 3990) = 24395 (mod\ 3990) = 455 (mod\ 3990) \end{aligned}$$

So we can expect the buses to simultaneously arrive in every 455 minutes, or 7 hours and 35 minutes. This occurs at 7:35 pm.

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?

We can set up the following Diophantine equation: $10A + B = 2(10B + A) - 1 \rightarrow 19B - 8A = 1$. EGCD gives us $A = 7$ and $B = 3$, so the father is 73 while the son is 37. Note that it follows that $Ax + By = c$ has solutions iff $\gcd(x, y) | c$