CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

HW 4

1 Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

2 Amaze Your Friends

(a) You want to trick your friends into thinking you can perform mental arithmetic with very large numbers. What are the last digits of the following numbers?

i. 11^{2017}

ii. 9^{10001}

iii. $3^{987654321}$

(b) You know that you can quickly tell a number n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. Prove that you can use this trick to quickly calculate if a number is divisible by 9.

3 Euclid's Algorithm

(a) Use Euclid's algorithm in the lecture note to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

(b) Use the extended Euclid's algorithm in the lecture note to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

(c) Find $x \pmod{27}$ if $5x + 26 \equiv 3 \bmod 27$. You can use the result computed in (b).

(d) 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.

4 Solution for $ax \equiv b \bmod m$

In the lecture notes, we proved that when $\gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \bmod m$ has exactly one solution x (modulo m). The proof of the unique multiplicative inverse (theorem 5.2) actually proved that when $\gcd(m,a) = 1$, the solution of $ax \equiv b \bmod m$ with unknown variable x is unique. Now let's consider the case where $\gcd(m,a) > 1$ and see why there is no unique solution in this case. Let's consider the general solution of $ax \equiv b \bmod m$ with $\gcd(m,a) > 1$.

(a) Let $\gcd(m,a) = d$. Prove that $ax \equiv b \bmod m$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \bmod d$.

(b) Let $\gcd(m,a) = d$. Assume $b \equiv 0 \bmod d$. Prove that $ax \equiv b \bmod m$ has exactly d solutions (modulo m).

(c) Solve for x: $77x \equiv 35 \bmod 42$.

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

(a) 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.

(b) 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.

(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?