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.

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. (Signature here)

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.

Solution:

(a) i. 11 is always 1 mod 10, so the answer to (a) is 1.

ii. 9 is its own inverse mod 10, therefore, if 9 is raised to an odd power, the number will be 9 mod 10. So the answer is 9.

iii. $3^4 = 9^2 = 1 \bmod 10$. We see that the exponent $987654321 = 1 \bmod 4$ so the answer is 3.

(b) Let n be written as $a_k a_{k-1} \cdots a_1 a_0$ where the a_i are digits, base-10. We can write

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10 a_1 + a_0 \\ &= (10^k - 1)a_k + (10^{k-1} - 1)a_{k-1} + \cdots + (10-1)a_1 + \sum_{i=0}^{k} a_i. \end{aligned}$$

The first few terms are all divisible 9; they're all of the form $99\cdots99 \cdot a_i$. So if the sum at the end is divisible by 9, then n is too and vice versa.

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.

Solution:

(a) The values of x and y of all recursive calls are (you can get full credits without the column of x mod y):

Function Calls	(x, y)	x mod y
#1	$(527, 323)$	204
#2	$(323, 204)$	119
#3	$(204, 119)$	85
#4	$(119, 85)$	34
#5	$(85, 34)$	17
#6	$(34, 17)$	0
#7	$(17, 0)$	—

Therefore, $\gcd(527, 323) = 17$.

(b) To compute the multiplicative inverse of 5 mod 27, we first call `extended-gcd(27,5)`. Note that `(x div y)` in the pseudocode means $\left\lfloor \frac{x}{y} \right\rfloor$. The values of x and y of all recursive calls are (you can get full credits without the columns of x div y and x mod y):

Function Calls	(x, y)	x div y	x mod y
#1	$(27, 5)$	5	2
#2	$(5, 2)$	2	1
#3	$(2, 1)$	2	0
#4	$(1, 0)$	—	—

The returned values of all recursive calls are:

Function Calls	(d,a,b)	Returned Values
#4	—	$(1,1,0)$
#3	$(1,1,0)$	$(1,0,1)$
#2	$(1,0,1)$	$(1,1,-2)$
#1	$(1,1,-2)$	$(1,-2,11)$

Therefore, we get $1 = (-2) \times 27 + 11 \times 5$ and

$$1 = (-2) \times 27 + 11 \times 5 \equiv 11 \times 5 \mod 27,$$

so the multiplicative inverse of 5 mod 27 is 11.

(c)

$$\begin{aligned} 5x + 26 \equiv 3 \mod 27 &\Rightarrow 5x \equiv 3 - 26 \mod 27 \\ &\Rightarrow 5x \equiv -23 \mod 27 \\ &\Rightarrow 5x \equiv 4 \mod 27 \\ &\Rightarrow 11 \times 5x \equiv 11 \times 4 \mod 27 \\ &\Rightarrow x \equiv 44 \mod 27 \\ &\Rightarrow x \equiv 17 \mod 27. \end{aligned}$$

(d) False. We can have a counterexample: $a = 3$, $b = 6$, and $c = 12$, so a has no multiplicative inverse mod c (because $a = 3$ and $c = 12$ are not relatively prime). However, $3x \equiv 6 \mod 12$ has solutions $x = 2, 6, 10 \mod 12$.

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

In the lecture notes, we proved that when $\gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \mod m$ 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 $ax \equiv b \mod m$ 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 $ax \equiv b \mod m$ with $\gcd(m,a) > 1$.

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

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

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

Solution:

(a) Necessary condition ($ax \equiv b \bmod m$ has a solution $\implies b \equiv 0 \bmod d$):
If $ax \equiv b \bmod m$ has a solution, we can write $ax = my + b$ for some $x, y \in \mathbb{Z}$.
Since d is the greatest common divisor of m and a, we know that $d|a$ and $d|m$. Therefore d divides $ax - my = b$, or equivalently, $b \equiv 0 \bmod d$.

Sufficient condition ($b \equiv 0 \bmod d \implies ax \equiv b \bmod m$ has a solution):
Consider the congruent equation $(a/d)x \equiv b/d \bmod m/d$. Since $\gcd(m,a) = d$, we know that $\gcd(m/d, a/d) = 1$.
Therefore $(a/d)x \equiv (b/d) \bmod m/d$ has a solution, or equivalently, $\exists x, y \in \mathbb{Z}$, such that $(a/d)x = (m/d)y + b/d$.
$\implies ax = my + b$.
$\implies x$ is a solution for $ax \equiv b \bmod m$.

Another proof for $b \equiv 0 \bmod d \implies ax \equiv b \bmod m$ has a solution:
If $d|b$, we can write $b = kd$ for some $k \in \mathbb{Z}$. Since $\gcd(m,a) = d$, $\exists w, y \in \mathbb{Z}$, such that $aw + my = d$. Multiplying both sides by k, we get $kaw + kmy = kd = b$. So

$$\begin{aligned} akw + mky &\equiv b \bmod m, \\ akw &\equiv b \bmod m. \end{aligned}$$

Then, kw is a solution of $ax \equiv b \bmod m$.

(b) From the proof of sufficient condition in part(a), we have shown that if x satisfies $(a/d)x \equiv b/d \bmod m/d$, then x also satisfies $ax \equiv b \bmod m$. How about the reverse?
If x satisfies $ax \equiv b \bmod m$, then

$$\begin{aligned} & ax = my + b \text{ for some } y \in \mathbb{Z}, \\ \implies & \frac{a}{d}x = \frac{m}{d}y + \frac{b}{d}, \\ \implies & x \text{ satisfies } \frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}. \end{aligned}$$

We conclude the above proof as the following Lemma:
Lemma: $\forall x \in \mathbb{Z}$, x satisfies $(a/d)x \equiv b/d \bmod m/d$ if and only if x satisfies $ax \equiv b \bmod m$.

Let x_0 be the unique solution (modulo m/d) of $(a/d)x \equiv b/d \bmod m/d$, denoting as $x \equiv x_0 \bmod m/d$. Any $x \in \mathbb{Z}$ that satisfies $(a/d)x \equiv b/d \bmod m/d$ must be of the form $x = x_0 + k(m/d)$ for some $k \in \mathbb{Z}$.
By the above Lemma, any $x \in \mathbb{Z}$ that satisfies $ax \equiv b \bmod m$ will also be of the form $x = x_0 + k(m/d)$. Now we will show that there are only d distinct solutions (modulo m) for $ax \equiv b \bmod m$ among $x = x_0 + k(m/d)$ $\forall k \in \mathbb{Z}$.
Two solutions, $x_1 = x_0 + k_1(m/d)$ and $x_2 = x_0 + k_2(m/d)$, are the same in modulo m if and

only if

$$x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \mod m \iff (k_1-k_2)\frac{m}{d} \equiv 0 \mod m,$$
$$\iff (k_1-k_2)\frac{m}{d} = qm \text{ for some } q \in \mathbb{Z},$$
$$\iff (k_1-k_2)m = qmd,$$
$$\iff k_1 - k_2 = qd.$$

The above argument proved that two solutions with the form of $x = x_0 + k(m/d)$ are equal mod m if and only if $k_1 \equiv k_2 \mod d$. Without loss of generality, we can construct solutions by letting $k \in \{0, 1, \ldots, d-1\}$. To be very specific, the d distinct solutions of $ax \equiv b \mod m$ are

$$x \equiv x_0 + k\frac{m}{d} \mod m, \quad k = 0, 1, \ldots, d-1.$$

(c) Since $\gcd(77, 42) = 7$ and $35 \equiv 0 \mod 7$, we can find a unique solution from $(77/7)x \equiv 35/7 \mod 42/7$:

$$11x \equiv 5 \mod 6$$
$$-1x \equiv -1 \mod 6 \quad \text{(because } 11 \equiv -1 \mod 6 \text{ and } 5 \equiv -1 \mod 6\text{)}$$
$$x \equiv 1 \mod 6$$

The solution of $(77/7)x \equiv 35/7 \mod 42/7$ is $x \equiv 1 \mod 6$. Based on part (b), the solutions of $77x \equiv 35 \mod 42$ are

$$x \equiv 1 + 6k \mod 42, \quad k = 0, 1, \ldots, 6.$$

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?

Solution:

(a) $1\cdot 0+2\cdot 0+3\cdot 7+4\cdot 2+5\cdot 8+6\cdot 8+7\cdot 0+8\cdot 0+9\cdot 8+10\cdot d_{10} = 189+10d_{10} \equiv 2+10d_{10} \mod 11$. From the definition of the check digit, we know that $2+10d_{10} \equiv 0 \mod 11$ so $10d_{10} = 9 \mod 11$. From here, we can quickly see that $d_{10} = 2$.

(b) It is sufficient to show that $d_{10} = \sum_{i=1}^{9} i \cdot d_i \mod 11$ is a valid check digit (that is, that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 \mod 11$). To see this, we note that

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot d_i &= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot d_{10} \\
&= \sum_{i=1}^{9} i \cdot d_i + 10 \cdot \sum_{i=1}^{9} i \cdot d_i \\
&= (1+10) \cdot \sum_{i=1}^{9} i \cdot d_i \\
&\equiv 0 \mod 11.
\end{aligned}$$

(c) Suppose that the correct digits are d_i (for $1 \le i \le 10$) and that the new digits are f_i. Since the question asks about a single substitution error, we will assume without loss of generality that the kth digit has been changed, i.e. $f_k = d_k + e$ for some $-10 \le e \le 10$ (note that a digit can be 10 or X, and additionally $e \neq 0$ since that would be the case where the digit is not changed). All of the other f_i are equal to d_i. That is,

$$f_i = \begin{cases} d_k + e, & i = k, \\ d_i, & \text{otherwise.} \end{cases}$$

Then we can write:

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot f_i &= \sum_{i=1}^{10} i \cdot d_i + k \cdot e \\
&\equiv 0 + k \cdot e \mod 11,
\end{aligned}$$

where the second line comes from the fact that d_i are the correct digits and the definition of the checksum formula. We know that if $k \cdot e$ is not equivalent to 0 mod 11, then the error will be detected. Since 11 is prime, $1 \leq k \leq 10$, $-10 \leq e \leq 10$, and $e \neq 0$ the error will be detected.

(d) Let's suppose that digits k and m are switched and all of the rest are left unchanged. We will write

$$f_i = \begin{cases} d_k, & i = m \\ d_m, & i = k \\ d_i, & \text{otherwise} \end{cases}$$

where $d_k \neq d_m$ (if they are equal, it's as if you never switched them so of course it will still be valid). Then we can write:

$$\begin{aligned}
\sum_{i=1}^{10} i \cdot f_i &= k \cdot d_m + m \cdot d_k + \sum_{i \neq k,m} i \cdot d_i \\
&= (k-m+m)d_m + (m-k+k)d_k + \sum_{i \neq k,m} i \cdot d_i && \text{note that } k-m+m=k \\
&= (k-m) \cdot d_m + (m-k) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i && \text{bring like terms into the summation} \\
&= (k-m) \cdot d_m - (k-m) \cdot d_k + \sum_{i=1}^{10} i \cdot d_i \\
&= (k-m) \cdot (d_m - d_k) + \sum_{i=1}^{10} i \cdot d_i && \text{combine like terms} \\
&\equiv (k-m) \cdot (d_m - d_k) \mod 11 && \text{by the definition of the check digit}
\end{aligned}$$

Since we know that $-9 \leq k-m \leq 9$, $k-m \neq 0$, $d_m - d_k \neq 0$, and 11 is prime, we know that this will not be equivalent to 0 mod 11, thus an error will be detected.