COMP 2711 Discrete Mathematical Tools for CS
2014 Fall Semester – Solution to Written Assignment # 5
Distributed: Oct 22, 2014 – Due: Oct 29, 2014

Problem 1: What is 37 mod 17? What is -4 mod 17? What is -37 mod 17? When answering these questions please also give the associated values q and r in the representation $m = qn + r$.

SOLUTION: $37 \bmod 17 = 3$; $q = 2, r = 3 : 37 = 2 \cdot 17 + 3$.
$-4 \bmod 17 = 13$; $q = -1, r = 13 : -4 = -1 \cdot 17 + 13$.
$-37 \bmod 17 = 14$; $q = -3, r = 14 : -37 = -3 \cdot 17 + 14$.

Problem 2: Encrypt the message `COMPUTER SCIENCE` using a Caesar cipher in which each letter is shifted four places to the left.

SOLUTION: `YKILQPAN OYEAJYA`.
If you shifted it to the right instead of the left you would get `GSQTYXIV WGMIRGI`.

Problem 3: A Caesar cipher with shift k letters (to the left or to the right) has been executed on some original plaintext message. The resulting ciphertext is `SZH SLCO HLD ESTD EZ OPNZOP`. What is k and what was the original message?

SOLUTION: $k = 11$.
`HOW HARD WAS THIS TO DECODE`.
(In solving this decryption problem, we assume that the message is written in English and is grammatically correct. It is usually good to start with the very short words of only one to two characters in length, if any. The shorter a word, the fewer the number of possibilities. The position in which a word occurs in the sentence also limits the search (or guess) significantly. Once you make a guess on decrypting a certain character by shifting, you can try to decrypt other words in the same way to see if they form legal English words. If this is unsuccessful, the process is repeated by making a new guess. There exist more sophisticated decryption methods based on frequency analysis, but that is beyond the scope of this course.)

Problem 4: It is easy to see that 0, 5, 10, and 15 are all solutions to the equation

$$4 \cdot_{20} x = 0.$$

Are there any integral values of a and b, with $1 \leq a < 20$ and $1 \leq b < 20$, for which the equation $a \cdot_{20} x = b$ does *not* have any solutions in Z_{20}? If

there are, give one set of values for a and b and explain how you know that there are no solutions to $a \cdot_{20} x = b$. If there are not, explain how you know this. (You could write out the entire Z_{20} multiplication table to justify your answer, but this is not necessary)

SOLUTION: When $a = 2$ and $b = 5$, the equation $2 \cdot_{20} x = 5$ does not have any solutions in Z_{20} because $2x$ is even and so is $2x \bmod 20$. There does not exist any $x \in Z_{20}$ such that $2x \bmod 20 = 5$.

Problem 5: (a) Write the $\cdot_9$ multiplication table for Z_9.

(b) Which non-zero elements in Z_9 have a multiplicative inverse? Which do not?

SOLUTION: (a)

Z_9	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

(b)

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

Problem 6: Does there exist an x in Z_{147} that solves

$$12 \cdot_{147} x = 7?$$

If yes, give the value of x (it is not necessary to show your work).
If no, prove that such an x does not exist.

SOLUTION: *No. If* $12._{147}x = 7$ *then there is some integer* q *such that*

$$12x = 147q + 7$$

or

$$3(4x - 49q) = 7.$$

Since the left side of this equation is divisible by 3 *and the right side isnt, this is impossible.*

Problem 7: (Challenge Problem) (a) Two integers x and y are said to be *congruent modulo n, ($n > 1$)* if and only if

$$(x \bmod n) = (y \bmod n).$$

When this is the case, we write $x \equiv y \pmod{n}$. Suppose that

$$x \equiv y \pmod{n} \qquad \text{and} \qquad a \equiv b \pmod{n}.$$

Prove that

$$ax \equiv by \pmod{n}.$$

(b) Prove that for every integer n,

$$n^5 \equiv n^3 \pmod{8}.$$

SOLUTION: (a) By Euclid's division theorem there are q_1, r_1, q_2, r_2 with $0 \leq r_1 < n$ and $0 \leq r_2 < n$ such that

$$x = q_1 n + r_1 \qquad \text{and} \qquad y = q_2 n + r_2;$$

furthermore $x \bmod n = r_1$ and $y \bmod n = r_2$.

Saying that $x \equiv y \pmod{n}$ is equivalent to writing $r_1 = r_2$, and then

$$x - y = (q_1 - q_2)n.$$

So, $x \equiv y \pmod{n}$ is equivalent to saying that there is some p_1 such that $x - y = p_1 n$. Similarly, $a \equiv b \pmod{n}$ is equivalent to saying that there is some p_2 such that $a - b = p_2 n$.

In this case

$$\begin{aligned} ax &= (b + p_2 n)(y + p_1 n) \\ &= by + n(bp_1 + p_2 y + p_1 p_2 n). \end{aligned}$$

But then $ax - by = np_3$ for $p_3 = bp_1 + p_2 y + p_1 p_2 n$ and thus

$$ax \equiv by \bmod n.$$

(b) This problem is equivalent to showing that

$$(n^5 - n^3) \bmod 8 = 0$$

for all n. First notice that, for all integers k,

$$(n + 8k)^3 = n^3 + 3n^2(8k) + 3n(8k)^2 + (8k)^3.$$

Since every term on the right hand side, except possibly n^3, is divisible by 8, we find that, for all k,

$$(n+8k)^3 \equiv n^3 \pmod 8.$$

Similarly,

$$(n+8k)^5 = \sum_{i=0}^{5} \binom{5}{i} n^i 8^{5-i} k^{5-i}.$$

Since every term on the right hand side is divisible by 8 except, possibly, when $i = 5$, we find that, for all integers k,

$$(n+8k)^5 \equiv n^5 \pmod 8.$$

Combining, we find that, for all integers k,

$$(n+8k)^5 - n^3 \equiv n^5 - n^3 \pmod 8.$$

Since every integer n can be written in the form $n + 8k$, to prove that $(n^5 - n^3) \equiv 0 \pmod 8$ for *all* integers n, we therefore only need to prove $(n^5 - n^3) \bmod 8 = 0$, i.e., that $8|(n^5 - n^3)$, for $n = 0, 1, 2, 3, 4, 5, 6, 7$. This can be seen by substituting in the values:

$$\begin{array}{rcrcl}
0^5 - 0^3 & = & 0 & = & 0 \cdot 8 \\
1^5 - 1^3 & = & 0 & = & 0 \cdot 8 \\
2^5 - 2^3 & = & 24 & = & 3 \cdot 8 \\
3^5 - 3^3 & = & 216 & = & 27 \cdot 8 \\
4^5 - 4^3 & = & 960 & = & 120 \cdot 8 \\
5^5 - 5^3 & = & 3000 & = & 375 \cdot 8 \\
6^5 - 6^3 & = & 7560 & = & 945 \cdot 8 \\
7^5 - 7^3 & = & 16464 & = & 2058 \cdot 8
\end{array}$$

An alternative method of proving (b), i.e., that $(n^5 - n^3) \equiv 0 \pmod n$, for *all* integers n, to consider the two cases

1. n is even
2. n is odd

separately.

When n is even, $n = 2k$ for some integer k and

$$\begin{array}{rcl}
n^5 - n^3 & = & (2k)^5 - (2k)^3 \\
& = & 8k^3(4k^2 - 1)
\end{array}$$

Thus, $n^5 - n^3 \bmod 8 = 0$.

When n is odd, $n = 2k + 1$ for some integer k. Then

$$\begin{aligned} n^5 - n^3 &= (2k+1)^5 - (2k+1)^3 \\ &= (2k+1)^3((2k+1)^2 - 1) \\ &= (2k+1)^3(4k^2 + 4k) \\ &= (2k+1)^3 \cdot 4k(k+1) \end{aligned}$$

Since either k or $k+1$ must be even, $4k(k+1)$ is divisible by 8 for all k. Thus, $(2k+1)^3 \cdot 4k(k+1)$ is divisible by 8 so, when n is odd. $n^5 - n^3 \bmod 8 = 0$.

Combining the even and odd cases proves (b).