COMP 2711 Discrete Mathematical Tools for CS
2014 Fall Semester – Solution to Written Assignment # 6
Distributed: Nov 5, 2014 – Due: Nov 12, 2014

At the top of your solution, please write your (i) name, (ii) student ID #, (iii) email address and (iv) tutorial section.
Some Notes:

- Please write clearly and briefly. For all questions you should also provide a short explanation as to *how* you derived the solution. That is, if the solution is 20, you shouldn't just write down 20. You need to explain *why* it's 20.

- Please follow the guidelines on doing your own work and avoiding plagiarism given on the class home page. Don't forget to *acknowledge* individuals who assisted you, or sources where you found solutions.

- Some of these problems are taken (some modified) from the textbook.

- Please make a *copy* of your assignment before submitting it. If we can't find your paper in the submission pile, we will ask you to resubmit the copy.

- Your solutions can be submitted before 5PM of the due date, in the collection bin in front of Room 4213A.

Problem 1: Does there exist an x in Z_{79} that solves

$$53 \cdot_{79} x = 1?$$

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: *Yes. $x = 3$ solves the equation.*
One way to find this would be to use the Extended GCD algorithm to calculate

$$1 = 3 \cdot 53 - 2 \cdot 79.$$

Problem 2: *Consider the system of equations*

$$x \bmod 13 = 5,$$
$$x \bmod 11 = 9.$$

(a) How many solutions with x between 0 and 142 are there to the system of equations. What are these solutions?

(b) How many solutions with x between 143 and 428 are there to the system of equations. What are these solutions?

(c) How many solutions with x between 143 and 470 are there to the system of equations. What are these solutions?

SOLUTION: *(a) Since 13 and 11 are relatively prime, the Chinese Remainder Theorem tells us that there is exactly one solution $\bar{x}$ for $0 \le \bar{x} \le 11 \cdot 13 - 1 = 142$. Calculation shows that $13 \cdot_{11} 6 = 1$ and $11 \cdot_{13} 6 = 1$. Setting $y = 5 \cdot 11 \cdot 6 + 9 \cdot 6 \cdot 13 = 1032$ gives*

$$y \bmod 13 = 5,$$
$$y \bmod 11 = 9$$

Setting $\bar{x} = y \bmod 143 = 31$ gives the solution.

(b) Note that

$$x \bmod 13 = (x \bmod 143) \bmod 13$$
$$x \bmod 11 = (x \bmod 143) \bmod 11$$

This implies that x is a solution to the system of equations if and only if

$$x = \bar{x} + 143q$$

where $\bar{x}$ is the unique solution between 0 and 142 and q is an integer.

In our particular case, this means finding for how many different q it's possible for

$$x = 31 + 143q$$

to be between 143 and $428 = 143 \cdot 3 - 1$. The answer is 2 ($q = 1$, and $q = 2$) and the solutions are $x = 174, 317$.

(c) Following the answer to question 2, we now want to find for how many different q it's possible for

$$x = 31 + 143q$$

to be between 143 and $470 = 143 \cdot 3 + 41$. The answer is 3 ($q = 1$, $q = 2$ and $q = 3$) and the solutions are $x = 174, 317, 460$.

Problem 3: *(a) Show that exactly $(p-1)(q-1)$ elements in Z_{pq} have multiplicative inverses when p and q are primes.*

(b) $10 = 2 \cdot 5$ and 7 are relatively prime. How many elements in Z_{70} have multiplicative inverses?

The number of elements which have multiplicative inverses is not $(10 - 1)(7 - 1)$. Explain why your reasoning for part (a) doesn't work for 10, 7. (Do not just say that 10 is not prime. Explain why the reasoning for part (a) works when p and q are both prime but is not valid when p and q are relatively prime but not prime.)

SOLUTION: *(a) $(p-1)(q-1) = pq - (p+q-1)$: By Corollary 2.16, a has an inverse if and only if $\gcd(a, pq) = 1$. Any a that is divisible by p has $\gcd(a, pq) = p$. There are q such a's. In a similar way, any b that is divisible by q has $\gcd(b, pq) = q$. There are p such b's. Because p and q are primes, if $\gcd(a, pq) \neq 1$, then it is either p or q, and so a is a multiple of p or q. Together, there are $p + q - 1$ elements in Z_{pq} that do not have inverses. (We get $p + q - 1$ because pq is counted twice: both as divisible by p and as divisible by q.)*

(b) 24 elements in Z_{70} have multiplicative inverses.
Because p and q were prime in part (a), we knew that we had counted all cases in which $\gcd(a, pq) \neq 1$. But here in part (b) additionally all multiples b of 2 and 5 (the prime factors of 10) will have $\gcd(b, pq) > 1$.

Problem 4: *Suppose when applying RSA that, $p = 29$, $q = 37$, and $e = 19$.*
(a) What are the values of n and d?
(b) Show how to encrypt the message $M = 100$, and then how to decrypt the resulting message. Use repeated squaring *for the encrypting and decrypting.*

SOLUTION: *(a) $n = pq = 1073$. Applying the extended* GCD *algorithm, or by experimenting, you see that $d = 955$.*
(b) Let

$$
\begin{aligned}
a_0 &= 100 \bmod 1073 = 100 \\
a_1 &= 100^2 \bmod 1073 = 343 \\
a_2 &= 100^4 \bmod 1073 = (100^2 \bmod 1073)^2 \bmod 1073 = 343^2 \bmod 1073 = 692 \\
a_3 &= 100^8 \bmod 1073 = (100^4 \bmod 1073)^2 \bmod 1073 = 692^2 \bmod 1073 = 306 \\
a_4 &= 100^{16} \bmod 1073 = (100^8 \bmod 1073)^2 \bmod 1073 = 306^2 \bmod 1073 = 285
\end{aligned}
$$

Since $19 = 16 + 2 + 1$, then

$$
\begin{aligned}
a_1 \cdot a_0 \bmod 1073 &= 343 \cdot 100 \bmod 1073 = 1037 \\
100^{19} \bmod 1073 &= a_4 \cdot a_1 \cdot a_0 \bmod 1073 \\
&= a_4 \cdot (a_1 \cdot a_0 \bmod 1073) \bmod 1073 \\
&= 285 \cdot 1037 \bmod 1073 \\
&= 470.
\end{aligned}
$$

To reverse the process, let

$$
\begin{aligned}
b_0 &= 470 \bmod 1073 = 470 \\
b_1 &= 470^2 \bmod 1073 = 935 \\
b_2 &= 470^4 \bmod 1073 = (470^2 \bmod 1073)^2 \bmod 1073 = 935^2 \bmod 1073 = 803
\end{aligned}
$$

$$b_3 = 470^8 \bmod 1073 = (470^4 \bmod 1073)^2 \bmod 1073 = 803^2 \bmod 1073 = 1009$$
$$b_4 = 470^{16} \bmod 1073 = (470^8 \bmod 1073)^2 \bmod 1073 = 1009^2 \bmod 1073 = 877$$
$$b_5 = 470^{32} \bmod 1073 = (470^{16} \bmod 1073)^2 \bmod 1073 = 877^2 \bmod 1073 = 861$$
$$b_6 = 470^{64} \bmod 1073 = (470^{32} \bmod 1073)^2 \bmod 1073 = 861^2 \bmod 1073 = 951$$
$$b_7 = 470^{128} \bmod 1073 = (470^{64} \bmod 1073)^2 \bmod 1073 = 951^2 \bmod 1073 = 935$$
$$b_8 = 470^{256} \bmod 1073 = (470^{128} \bmod 1073)^2 \bmod 1073 = 935^2 \bmod 1073 = 803$$
$$b_9 = 470^{512} \bmod 1073 = (470^{256} \bmod 1073)^2 \bmod 1073 = 803^2 \bmod 1073 = 1009$$

Since $955 = 512 + 256 + 128 + 32 + 16 + 8 + 2 + 1$, *then*

$$
\begin{aligned}
b_1 \cdot b_0 \bmod 1073 &= 935 \cdot 470 \bmod 1073 = 593 \\
b_3 \cdot b_1 \cdot b_0 \bmod 1073 &= b_3 \cdot (b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 1009 \cdot 593 \bmod 1073 = 676 \\
b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073 &= b_4 \cdot (b_3 \cdot b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 877 \cdot 676 \bmod 1073 = 556 \\
b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073 &= b_5 \cdot (b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 861 \cdot 556 \bmod 1073 = 158 \\
b_7 \cdot b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073 &= b_7 \cdot (b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 935 \cdot 158 \bmod 1073 = 729 \\
b_8 \cdot b_7 \cdot b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073 &= b_8 \cdot (b_7 \cdot b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 803 \cdot 729 \bmod 1073 = 602 \\
470^{955} \bmod 1073 &= b_9 \cdot b_8 \cdot b_7 \cdot b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073 \\
&= b_9 \cdot (b_8 \cdot b_7 \cdot b_5 \cdot b_4 \cdot b_3 \cdot b_1 \cdot b_0 \bmod 1073) \bmod 1073 \\
&= 1009 \cdot 602 \bmod 1073 \\
&= 100.
\end{aligned}
$$

Problem 5: *Compute each of the following. Show or explain your work. Do not use a calculator or computer.*

1. $15^{96} \bmod 97$.

2. $67^{72} \bmod 73$.

3. $67^{73} \bmod 73$.

SOLUTION: 97 *and* 73 *are prime numbers. Use Fermat's Little Theorem to get the following:*

1. $15^{96} \bmod 97 = 1$.

2. $67^{72} \bmod 73 = 1$.

3. $67^{73} \bmod 73 = 67 \cdot 67^{72} \bmod 73 = 67 \cdot 1 = 67.$

Problem 6: (Challenge Problem) *Consider the following equations:*

$$\begin{aligned}
x \quad \bmod \quad 3 &= 2 \\
x \quad \bmod \quad 5 &= 3 \\
x \quad \bmod \quad 11 &= 4 \\
x \quad \bmod \quad 16 &= 5.
\end{aligned}$$

Let $M = 3 \cdot 5 \cdot 11 \cdot 16 = 2640$.
(i) Show that there is an integer x in Z_M that satisfies all of the equations simultaneously and state the value of x.
(ii) Prove that x is unique.

SOLUTION: *Let $m_1 = 3$, $m_2 = 5$, $m_3 = 11$, and $m_4 = 16$. Further let $M_1 = 2640/3 = 880$, $M_2 = 2640/5 = 528$, $M_3 = 2640/11 = 240$, and $M_4 = 2640/16 = 165$.*

It is clear that, for each i, m_i and M_i are relatively prime. Let N_i be such that $N_i * M_i = 1 \bmod m_i$. Using the extended GCD algorithm, we get $N_1 = 1$, $N_2 = 2$, $N_3 = 5$, and $N_4 = 13$.

Let $y = 2 \cdot M_1 \cdot N_1 + 3 \cdot M_2 \cdot N_2 + 4 \cdot M_3 \cdot N_3 + 5 \cdot M_4 \cdot N_4$. It is easy to verify that y satisfies the above system of equations. For example,

$$\begin{aligned}
y \bmod 3 &= (2 \cdot M_1 \cdot N_1 + 3 \cdot M_2 \cdot N_2 + 4 \cdot M_3 \cdot N_3 + 5 \cdot M_4 \cdot N_4) \bmod m_1 \\
&= (2 \cdot M_1 \cdot N_1) \bmod m_1 = 2.
\end{aligned}$$

Plugging in the M_i, N_i values gives

$$y = 2 \cdot 880 \cdot 1 + 3 \cdot 528 \cdot 2 + 4 \cdot 240 \cdot 5 + 5 \cdot 165 \cdot 13 = 20453.$$

Setting
$$x = y \bmod M = 20453 \bmod 2640 = 1973$$

gives x in Z_M that satisfies all the equations.

Uniqueness*: Suppose x' and x'' are two solutions, both in Z_M. Then $x' = x'' \bmod m_i$, for each i $(0 < i \le 4)$. That is $m_i | (x' - x'')$ for each i $(0 < i \le 4)$.*

Since $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4$ and the m_i's are relatively prime in pairs, those imply $M | (x' - x'')$. So we have $x' = x'' \bmod M$ and hence $x' = x''$.

Problem 7: (Challenge Problem) *For each of the following two problems, state whether there is an $x \in Z_{150}$ that satisfies the two equations. If no solution x exists, prove it. If x does exist, list* all *solutions and prove that you have found all of them.*

Note that 10 and 15 are not relatively prime, so you may not use the Chinese Remainder Theorem to solve the problem directly.

(a) Find all solutions for the following system of equations in Z_{150}:

$$x \mod 10 = 2$$
$$x \mod 15 = 4.$$

(b) Find all solutions for the following system of equations in Z_{150}:

$$x \mod 10 = 9$$
$$x \mod 15 = 4.$$

SOLUTION: *(a) Transforming the modular equations into normal equations, we get*

$$x = 2 + 10k, \quad x = 4 + 15l$$

for some integers k and l. Note that $5 = \gcd(15, 10)$. Taking $\mod 5$ of both equations gives

$$x \mod 5 = (2 + 10k) \mod 5 = 2$$

and

$$x \mod 5 = (4 + 15l) \mod 5 = 4$$

leading to a contradiction. So, no solution is possible.

(b) Again transforming the modular equations into normal equations, we get

$$x = 9 + 10k, \quad x = 4 + 15l$$

for some integers k and l.

Note that if we take $\mod 5$ of both equations we get $x \mod 5 = 4$, so it is possible that a solution exists.

Setting the two representations of x to be equal gives

$$9 + 10k = 4 + 15l.$$

Simplifying, this gives $5 = 5(3l - 2k)$ or

$$3l - 2k = 1.$$

One possible way to proceed is use brute force to check all possible values of k, l that satisfy this equation and also

$$0 \le 9 + 10k < 150, \qquad 0 \le 4 + 15l < 150.$$

Another method is to realize that (why) if y and y' satisfy the modular equations then $(y \bmod 30) = (y' \bmod 30)$. Also, if y is any solution to the equations, then, for all t, $y + 30t$ also satisfies the equations. So, it would be enough to find a solution $x \in Z_{30}$ that solves the given equations.

Since we already know $x \bmod 5 = 4$, if we could determine $x \bmod 6$ we could use the CRT for this.

Note that

$$
\begin{aligned}
x \bmod 6 &= (9 + 10k) \bmod 6 \\
&= (3 + 2(3k + 2k)) \bmod 6 \\
&= (3 + 2 \cdot 2k)) \bmod 6 \\
&= (3 + 2(3l - 1)) \bmod 6 \\
&= 1
\end{aligned}
$$

We now use the CRT to find that the unique $x \in Z_{5 \cdot 6}$ that satisfies $x \bmod 5 = 4$ and $x \bmod 6 = 1$ is $x = 19$. So, the solutions to the equations are exactly the values $x + 30t$ that fall in Z_{150}, i.e., $x = 19, 49, 79, 109, 139$.