TMA4140 - Homework Set 5
RETTES

Henry S. Sjøen & Toralf Tokheim

October 8, 2018

Contents

1 Chapter 4.4

1.1 Exercise 21

Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 1(mod2)$, $x \equiv 2(mod3)$, $x \equiv (mod5)$, and $x \equiv 4(mod11)$.

We need to find all solutions to the system of congruences.

First congruence can be written as:

$$\begin{aligned} x &\equiv 1(mod2) \\ x &= 2m+1 \end{aligned} \tag{1}$$

Second congruence can be written as:

$$\begin{aligned} x &\equiv 2(mod3) \\ x &= 3m+2 \end{aligned} \tag{2}$$

Third congruence can be written as:

$$\begin{aligned} x &\equiv 2(mod5) \\ x &= 3m+2 \end{aligned} \tag{3}$$

And the final congruence can be written as:

$$\begin{aligned} x &\equiv 4(mod11) \\ x &= 11m+4 \end{aligned} \tag{4}$$

Using the Chinese theorem, we can find the L.C.D for $2, 3, 5$ and 11.

$LCD = 2x3x5x11 = 330$

Thus, $x = 330k + I$ where I is $1, 2, 3, 4$ for $mod2, 3, 5, 11$.

Then $8, 13, 18, K, 323, K$ are numbers divided by 5 where we get remainder 3.

$8, 13, 18, K, 323, K$ can be divided by 5 to get remainder 3. If the number is 232 it satisfies all the cases for divisor 2. $323 = 2(161) + 1$. Thus the remainder is 1.

For divisor 3,$323 = 3(107) + 2$. Thus the remainder is 2.

For divisor 11, $323 = 11(29) + 4$. Thus the remainder is 4.

And the solution of the provided system of congruences is $x = 232+330k$.

Fermat's theorem
If p is prime and a is an integer not divisible by p, then $ap - 1 \equiv 1(mod p)$.

1.2 Exercise 33

Use Fermat's little theorem to find $7^{121} mod 13$.

By Fermat's theorem, $7^{12} \equiv 1(mod13)$ So to find $7^{121}(mod13)$ we have to compute

$$\begin{aligned} 7^{121} &= (7^{12})^{10} \cdot 7(mod13) \\ &\equiv (7^{12})^{10}(mod13) \cdot 7(mod13) \\ &\equiv 1(mod13) \cdot 7(mod13) \\ &\equiv 7(mod13) \end{aligned} \tag{5}$$

Answer is $7(mod13)$

1.3 Exercise 37a

Show that $2^{340} \equiv 1(mod11)$ by Fermat's little theorem and noting that $2^{340} = (2^{10})^{34}$.

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1(modp)$.

So $2^{10} \equiv 1(mod11)$

$$\begin{aligned} 2^{340} &= (2^{10})^{34} \\ &\equiv (2^{10})^{34}(mod11) \\ &\equiv 1(mod11) \end{aligned} \tag{6}$$

2 Chapter 4.5

2.1 Exercise 12

Find the sequence of pseudorandom numbers generated by the power generator with $p = 11$, $d = 2$, and seed $x_0 = 3$.

Let's use the formulae

$$\begin{aligned} x_{n+1} &= x_n^d mod p \\ x_{n+1} &= x_n^2 mod 11 \end{aligned} \tag{7}$$

Where $p = 11, d = 2, x_0 = 3$

So the sequence can be generated as

$$\begin{aligned} x_1 &= 3^2 mod 11 \\ &\equiv 9 mod 11 \\ x_2 &= 9^2 mod 11 \\ &\equiv 4 mod 11 \\ x_2 &= 4^2 mod 11 \\ &\equiv 5 mod 11 \\ x_2 &= 5^2 mod 11 \\ &\equiv 3 mod 11 \end{aligned} \tag{8}$$

Then the sequence repeats... So the Sequence is $3, 9, 4, 5, 3, 9, 4, 5$...

3 Chapter 6.1

3.1 Exercise 27

A committee is formed consisting of one representative from each of the 50 states in the United States, where the representative from a state is either the governor or one of the two senators from that state. How many ways are there to form this committee?

The number of different possible committees are $3^{50} = 7,178979877e23$

3.2 Exercise 44

How many ways are there to seat four of a group of ten people around a circular table where two seatings are considered the same when everyone has the same immediate left and immediate right neighbor?

The number of ways of seating a group of 4 people from the 10 people are

$$10 * 9 * 8 * 7 = 5040 \tag{9}$$

But our number should be less than this because we don't count all the possible arrangements. We here get 4 of the same seating arrangements that we have remove... The required number of ways are therefore

$$\frac{5040}{4} = 1260 \tag{10}$$

4 Chapter 6.2

4.1 Exercise 10

Let $(x_i, y_i), i = 1, 2, 3, 4, 5,$be a set of five distinct points with integer coordinates in the xy plane. Show that the midpoint of the line joining at least one pair of these points has integer coordinates.

The middle point of two co-ordinates (x_i, y_i) and (x_j, y_j) is $(\frac{x_i+x_j}{2}, \frac{y_i+y_j}{2})$. For the co-ordinates mid-point to be an integer, (x_i, y_i) and (x_j, y_j) needs to be even number and hence should have the same parity.

Similarly, y_i and y_j have same parit. There are four possible cases of the parity of pair of integers: $(odd, odd), (odd, even), (even, odd), (even, even)$.

By *pigeon hole principle*, since there are four integer pairs, at least two of them needs to have same parity and hence will have mid-point having integer coordinates.

4.2 Exercise 16

How many numbers must be selected from the set $1, 3, 5, 7, 9, 11, 13, 15$ to guarantee that at least one pair of these numbers add up to 16? Best case only two: $1 + 15 = 16$ but worst case?

To completely guarantee that at least one pair of the numbers add up to 16, we need to pick at least 5 numbers from the set.

4.3 Exercise 18

Suppose that there are nine students in a discrete mathematics class at a small college. We can list all possible (Male, Female)-combinations as shown in figure 4.3 on the following page.

a) Show that the class must have at least five male students or at least five female students.

$$(0,9),(1,8),(2,7),(3,6),(4,5),(5,4)(6,3),(7,2),(8,1),(9,0) \tag{11}$$

In the order (Male, Female)

Considering only two kind of genders, Male and Female. If there are 3 male, then the remaning 6 students must be female and vise versa.

b) Show that the class must have at least three male students or at least seven female students.
Same as for the exercise above. If 2 male, then the remaning 7 must be female. If more than 2 male, then the statement is still valid.

5 Chapter 6.3

A coin is flipped 10 times where each flip comes up either heads or tails. How many possible outcomes...

5.1 Exercise 19a

...are there in total?
$2^{10} = 1024$

5.2 Exercise 19b

...contain exactly two heads?
$C(10,2) = 45$

5.3 Exercise 19c

...contain at most three tails?

$$\begin{aligned} &C(10,1) + C(10,2) + C(10,3) \\ &= 1 + 10 + 45 + 120 \\ &= 176 \end{aligned} \tag{12}$$