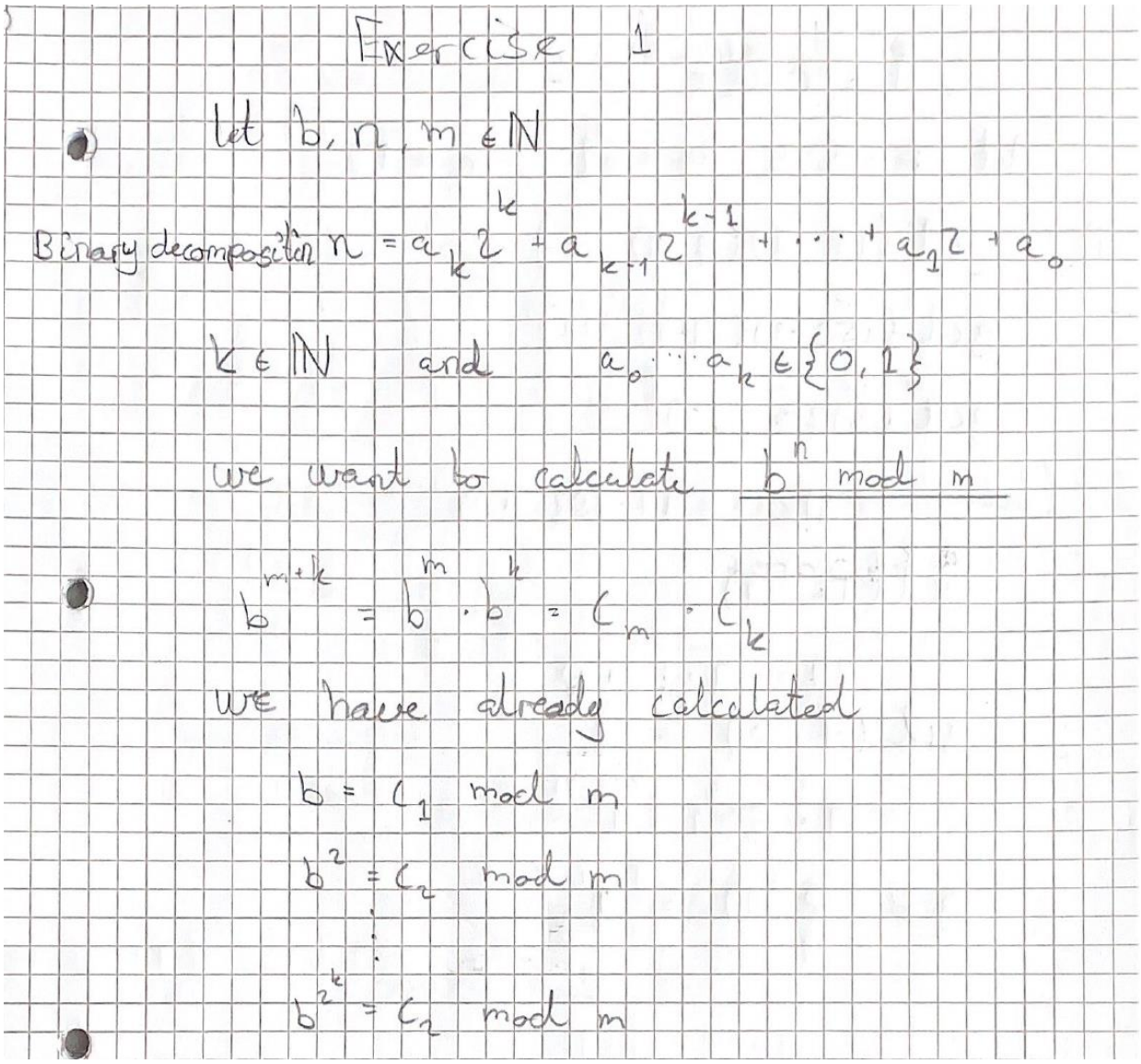
MAT-1005: Discrete mathematics

Assignment 2

Amund H. Strøm

October 27, 2021



Rest of the exercise on the next page →

Lets say we have $3^{200} \bmod 50$

Binary for $200 = 11001000$

$200 = 128 + 64 + 8$

$b = 3$

$n = 200$

$m = 50$

- we have already calculated

$b^8 = C_4 \bmod m$

↳ $3^8 = 11 \bmod 50$

$b^{64} = C_7 \bmod m$

↳ $3^{64} = 31 \bmod 50$

$b^{128} = C_8 \bmod m$

↳ $3^{128} = 11 \bmod 50$

$= 3^{200} \bmod 50$

$= 3^{128+64+8} \bmod 50$

$= 3^{128} \cdot 3^{64} \cdot 3^8 \bmod 50$

$\equiv 11 \cdot 31 \cdot 11 \bmod 50$

$\equiv 3751 \bmod 50$

$\equiv 1$

Exercise 2

Let $p = 53$, $q = 61$, $e = 17$

i) $\gcd((p-1)(q-1), e)$

$\gcd((53-1)(61-1), 17)$

$\gcd(3120, 17)$

$3120 = 17 \cdot 183 + 9$

$\gcd(17, 9)$

$17 = 9 \cdot 1 + 8$

$\gcd(9, 8) = 1$

$9 = 8 \cdot 1 + 1$

$\gcd(8, 1) = \underline{1}$

Exercise 2

ii) Let $P = 53$, $q = 61$, $e = 17$

Public key $(P \cdot q, e) \rightarrow (n, e)$

$(53 \cdot 61, 17)$

$(3233, 17)$

Padding Scheme : (Position in alphabet) - 1

↳ UPLOAD

2015 1114 0003 → M

Encryption: $M^e \bmod n$

↳

$2015^{17} \bmod 3233 \equiv 2545$

$1114^{17} \bmod 3233 \equiv 2757$

$0003^{17} \bmod 3233 \equiv 1211$

The encrypted message is:

2545 2757 1211

Exercise 2

iii) Let $P = 53$, $q = 61$, $e = 17$

find d

$d \cdot e = \gcd((P-1)(q-1), e) \bmod (P-1)(q-1)$

$d \cdot 17 = \gcd(3120, 17) \bmod 3120$

$d \cdot 17 = 1 \bmod 3120$

this means $17d + 3120k = 1$
for integers d, k

$3120 = 17 \cdot 183 + 9$

$17 = 9 \cdot 1 + 8$

$9 = 8 \cdot 1 + 1$

Expres 1 as a linear combination of 17 and 3120

$1 = 9 - 1 \cdot 8$
$= 9 - 1 \cdot (17 - 9)$
$= 2 \cdot 9 - 17$
$= 2 \cdot (3120 - 17 \cdot 183) - 17$
$= 2 \cdot 3120 - 367 \cdot 17$

$d = -367$ and $k = 2$

<u>So $d \equiv -367 \equiv 2753 \bmod 3120$</u>

Exercise 2

iv) Let $p = 53$, $q = 61$, $e = 17$, $d = 2753$

$M^d \bmod n$

$3195^{2753} \bmod 3233 = 1816$

$2038^{2753} \bmod 3233 = 2008$

$2460^{2753} \bmod 3233 = 1717$

$2550^{2753} \bmod 3233 = 0411$

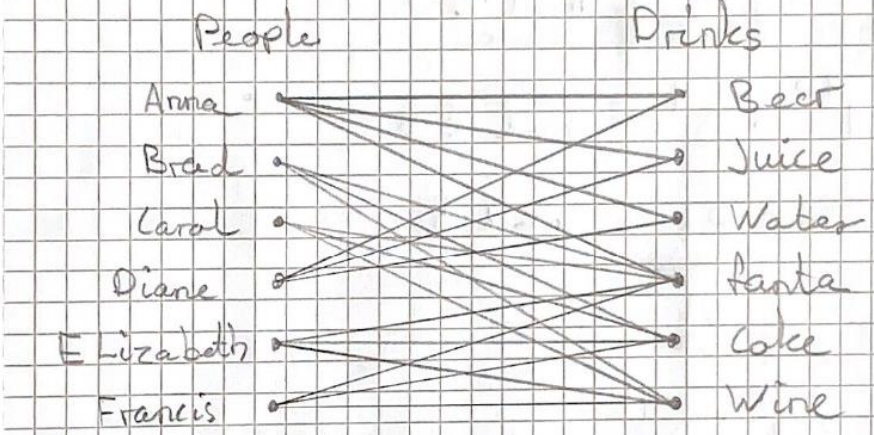
S Q U I R R E L

18 16 20 08 17 17 04 11

Exercise 3

i)

Anna : beer, Juice, Water, fanta
Brad : Coke, wine, fanta
Carol : wine, fanta, coke
Diane : Water, Juice, beer
Elizabeth : fanta, coke, wine
Francis : wine, coke, fanta

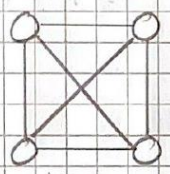


ii) there is no perfect match, since there are 4 people (Brad, Carol, Elizabeth, Francis) willing to drink 3 drinks (fanta, coke, Wine). If we reach Halls Marriage Theroem, this is true.

Exercise 4 a)

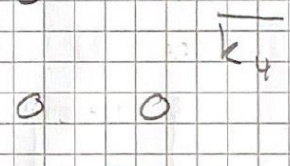
i) describe $\overline{K_n}$

if we take K_4 it will look like this:



K_4

and $\overline{K_4}$ will look like this:



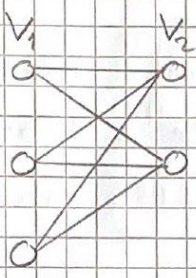
$\overline{K_4}$

this is true for any K_n and $\overline{K_n}$. because K_n has all the possible edges, so $\overline{K_n}$ will have no edges

Exercise 4 a)

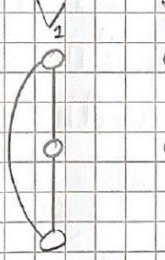
ii) Describe $\overline{K_{m,n}}$

if we take $K_{3,2}$ it will look like this:



$K_{3,2}$ it will connect every possible edge between V_1 and V_2

$\overline{K_{3,2}}$ will look like this:

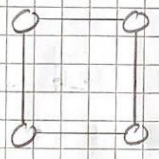


$\overline{K_{3,2}}$ it will connect the vertices in V_1 with eachother, and the vertices in V_2 with eachother. This is true for any $K_{m,n}$ and $\overline{K_{m,n}}$

Exercise 4 a)

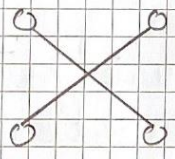
iii) Describe $\overline{C_n}$

if we take C_4 it will look like this:



C_4 it will make a "circle" around the vertices with edges

$\overline{C_4}$ will look like this:



$\overline{C_4}$ it will connect the vertices inside the "circle" with edges

This is true for any C_n and $\overline{C_n}$

Exercise 4 c)

G has e edges

$\bar{G}$ has $\bar{e}$ edges

↳ $e + \bar{e} = n \rightarrow \bar{e} = n - e$

n is the number of edges in K_v

K_v has this many edges

$= 0 + 1 + \dots + (V-1)$

we can replace this with a different version of Gauss formula:

$= \frac{V(V-1)}{2}$

now we replace n with this formula $\bar{e} = \frac{V(V-1)}{2} - e$

if G has V vertices and e edges, $\bar{G}$ has $\bar{e}$ edges: $\bar{e} = \frac{V(V-1)}{2} - e$

Exercise 4 b)

if we recall the formula in

4 c) $\bar{e} = \frac{V(V-1)}{2} - e$

G have 15 edges and $\bar{G}$ have 13 edges, how many vertices does G have?

$$\bar{e} = \frac{V(V-1)}{2} - e$$

$$\frac{V(V-1)}{2} = \bar{e} + e \quad | \cdot 2$$

$$V(V-1) = 2(\bar{e} + e)$$

$$V^2 - V = 2(\bar{e} + e)$$

it is easier to just solve it here

$$V^2 - V = 2(13 + 15)$$

$$V^2 - V = 56$$

$$8^2 - 8 = 56$$

G have 8 vertices

$$64 - 8 = 56$$

$$56 = 56$$

Exercise 5

i) $3^{304} \mod 50$

$= (3^{10})^{30} \cdot 3^4 \mod 50$

$= 1^{30} \cdot 3^4 \mod 50$

$= 81 \mod 50$

$= \underline{31}$

Exercise 5

ii) if $n \in \mathbb{Z}^+$ then $42 \mid n^7 - n$

$42 = 7 \cdot 3 \cdot 2$

$7 \mid n^7 - n$ → Fermat's Theroem

$n^7 = n \mod 7$

$n^7 - n = 0 \mod 7$

$7 \mid n^7 - n$

$2 \mid n^7 - n$ if n is even

↳ $(\text{even})^7 - \text{even}$

$= \text{even} - \text{even}$

$= \text{even}$

if n is odd

↳ $(\text{odd})^7 - \text{odd}$

$= \text{odd} - \text{odd}$

$= \text{even}$

$3 \mid n^3 - n$

Since $n^3 - n$ is a factor of $n^7 - n$. 3 must divide $n^7 - n$

$(n^7 - n) \div (n^3 - n) = n^5 + n^2 + 1$

$-(n^7 - n^5)$

$n^5 - n$

$-(n^5 - n^3)$

$n^3 - n$

$-(n^3 - n)$

0

Since 7, 2, and 3 divides $n^7 - n$.
42 must divide $n^7 - n$