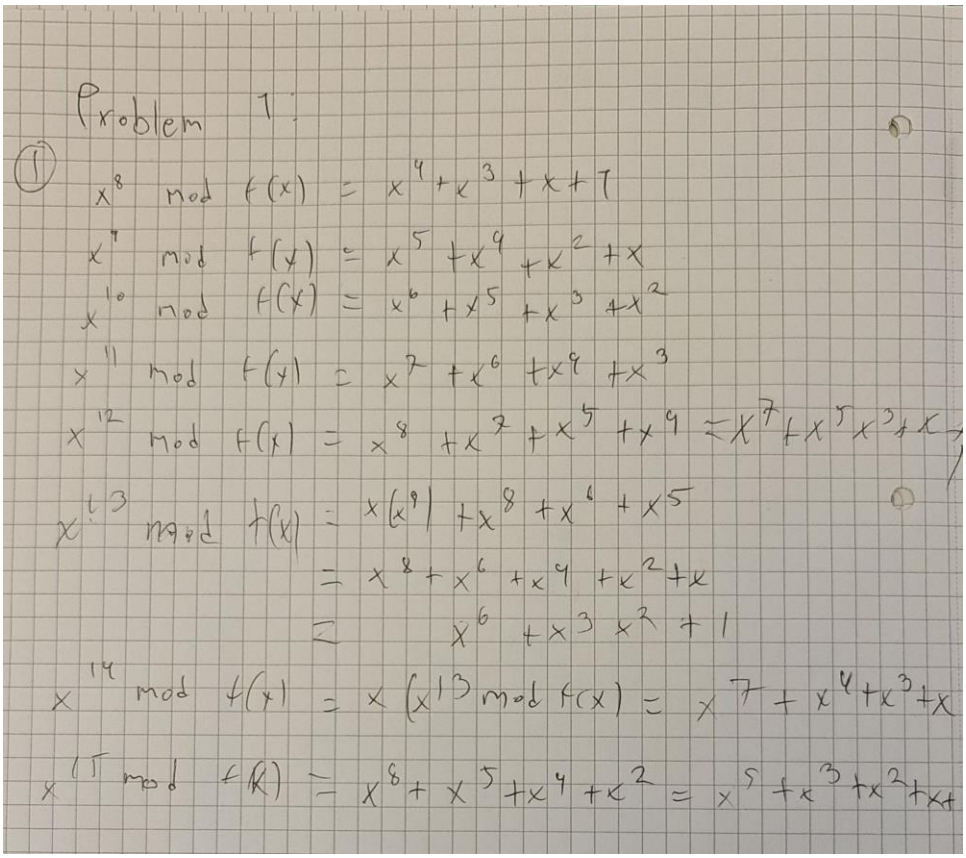
INF143A Assignment 2

Sigmund Volden

Problem 1:

1)

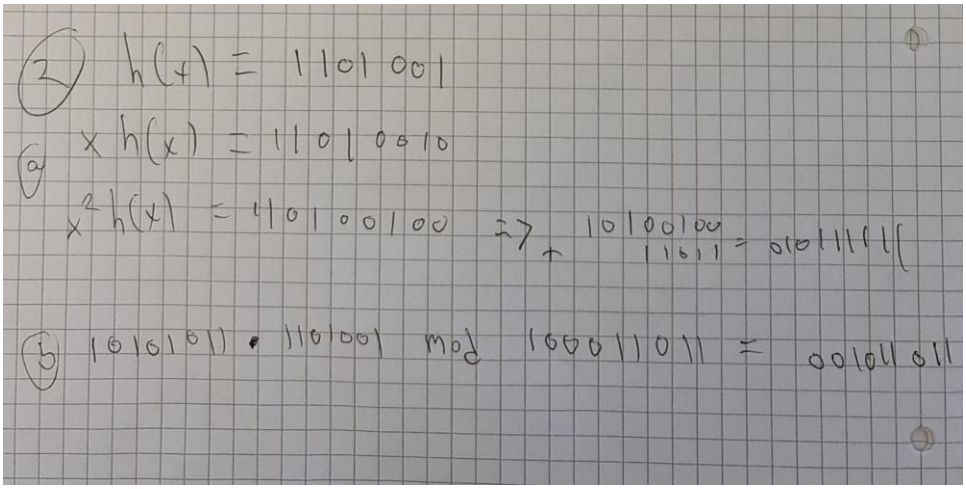
x^8 mod f(x) = 000011011
x^9 mod f(x) = 000110110
x^10 mod f(x) = 001101100
x^11 mod f(x) = 011011000
x^12 mod f(x) = 010101011
x^13 mod f(x) = 001001101
x^14 mod f(x) = 010011010
x^15 mod f(x) = 000101111



2)

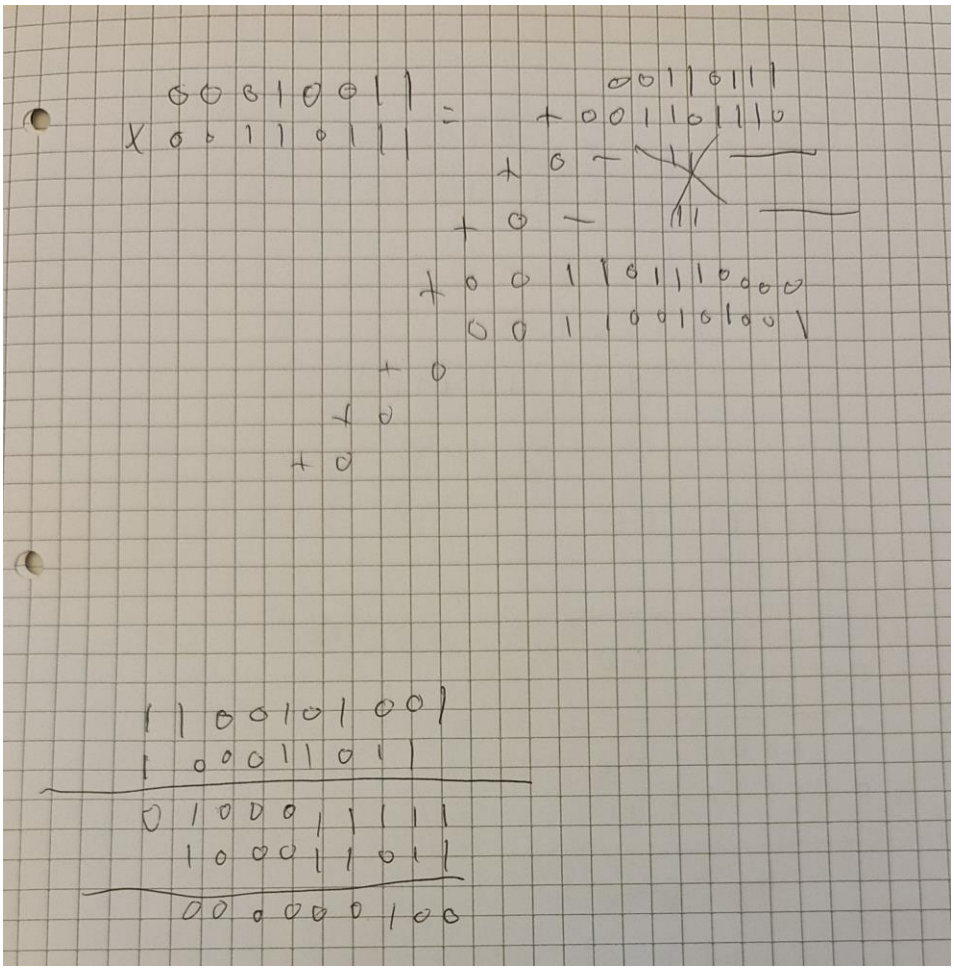
H(x) = 1101001
x*h(x) = 11010010
x^2*h(x) = 110100100

H(x) mod f(x) = 1101001
x*h(x) mod f(x) = 11010010
x^2*h(x) mod f(x) = 010111111

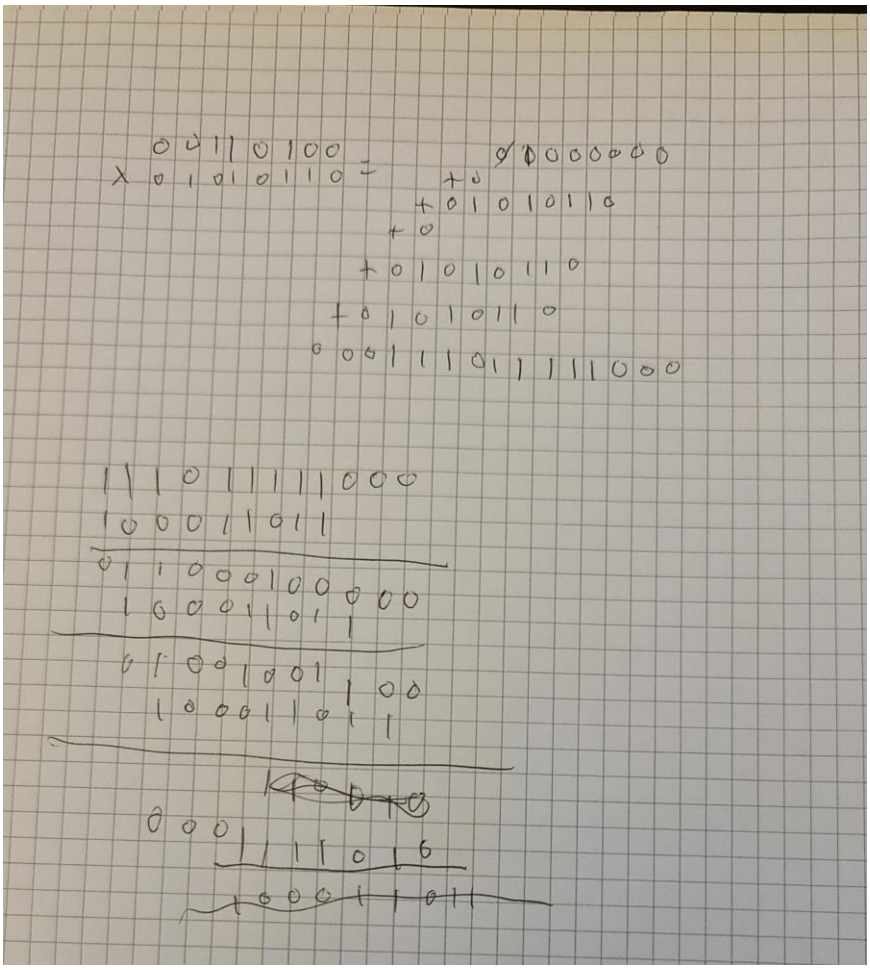


3)

0x13*0x37 mod f(x) = 000000100



0x34*0x56 mod f(x) = 001111010



Problem 2:

Script

Problem 3:

1)

The exponent 33 in binary form is 100001.

Starting with the base 5, and the first operation is just that number.

1 -----> 5

0 -----> 5^2 %77 = 25

0 -----> 25^2 % 77 = 9

0 -----> 9^2 % 77 = 4

0 -----> 4^2 % 77 = 16

1 ----> (16^2 % 77 * 5 % 77) % 77 = 25 * 5 mod 77 = 48

2)

With a = 3, for p = 67 to be prime:

=> a^(p-1) equivalent to 1 mod 67

Which means a^66 equivalent to 1 mod 67.. 66 in binary is 1000010

So, basically we can do the same thing, and if the answer is 1 then it is a prime number:

1 ----> 3

0 ----> 9

0 ----> 81 % 67 = 14

0 ----> 14^2 % 67 = 62

0 ----> 62^2 % 67 = 25

1 ----> (25^2 % 67 * 3 % 67) % 67 = 66

0 ----> 66^2 % 67 = 1

So it is prime.

3)

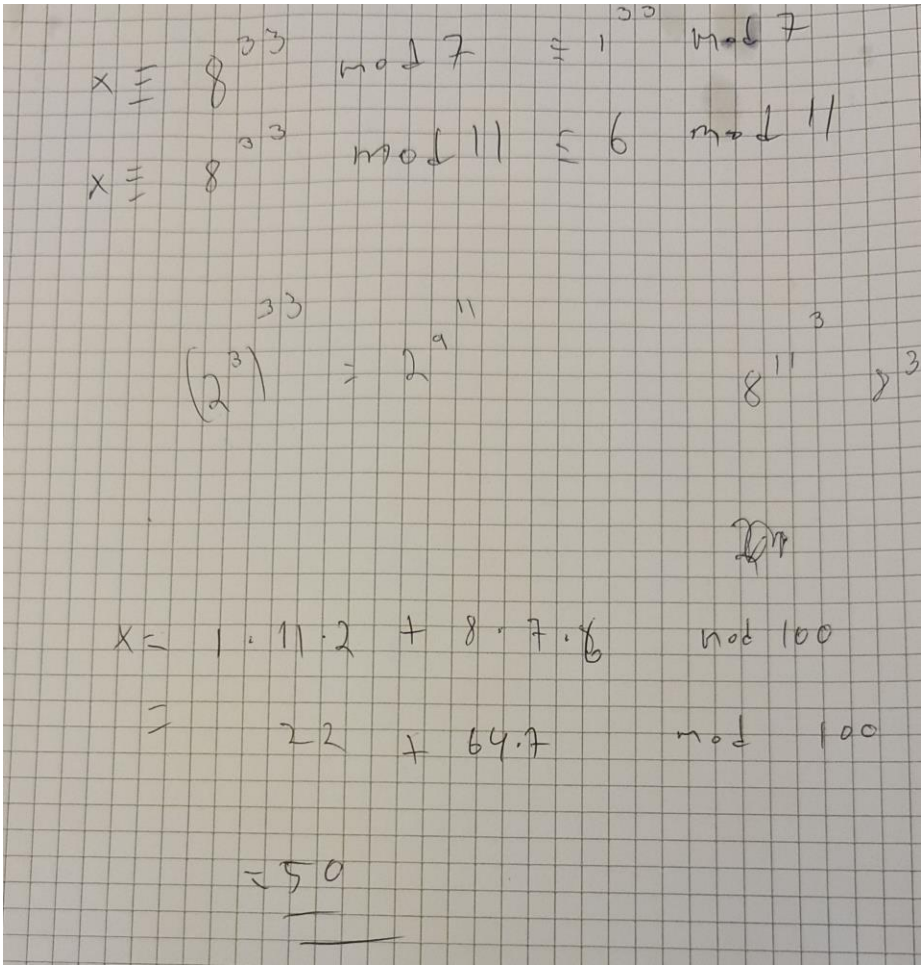
P=7

Q=11

Actually, in the calculation for x it should be 1*11*2 + 6*7*8.

Here: a is 1, q is 11 and invQ is 2.
B is 6, p is 7 and invP is 8.

So p * invP + q * invQ = 56 + 22 = 78 is equivalent to 1 mod 77



Problem 4:

script

Problem 5:

script