

# INF143A Assignment 2

Sigmund Volden

Problem 1:

1)

$$x^8 \bmod f(x) = 000011011$$

$$x^9 \bmod f(x) = 000110110$$

$$x^{10} \bmod f(x) = 001101100$$

$$x^{11} \bmod f(x) = 011011000$$

$$x^{12} \bmod f(x) = 010101011$$

$$x^{13} \bmod f(x) = 001001101$$

$$x^{14} \bmod f(x) = 010011010$$

$$x^{15} \bmod f(x) = 000101111$$

Problem 1:

①

$$x^8 \bmod f(x) = x^4 + x^3 + x + 7$$

$$x^9 \bmod f(x) = x^5 + x^4 + x^2 + x$$

$$x^{10} \bmod f(x) = x^6 + x^5 + x^3 + x^2$$

$$x^{11} \bmod f(x) = x^7 + x^6 + x^4 + x^3$$

$$x^{12} \bmod f(x) = x^8 + x^7 + x^5 + x^4 = x^7 + x^5 + x^3 + x$$

$$x^{13} \bmod f(x) = x(x^9) + x^8 + x^6 + x^5$$

$$= x^8 + x^6 + x^4 + x^2 + x$$

$$= x^6 + x^3 + x^2 + 1$$

$$x^{14} \bmod f(x) = x(x^{13} \bmod f(x)) = x^7 + x^4 + x^3 + x$$

$$x^{15} \bmod f(x) = x^8 + x^5 + x^4 + x^2 = x^5 + x^3 + x^2 + x$$

2)

$$H(x) = 1101001$$

$$x \cdot h(x) = 11010010$$

$$x^2 \cdot h(x) = 110100100$$

$$H(x) \bmod f(x) = 1101001$$

$$x \cdot h(x) \bmod f(x) = 11010010$$

$$x^2 \cdot h(x) \bmod f(x) = 01011111$$

(2)  $h(x) = 1101001$   
 (a)  $x \cdot h(x) = 11010010$   
 $x^2 \cdot h(x) = 110100100 \Rightarrow \begin{array}{r} 10100100 \\ 11011 \\ \hline 01011111 \end{array}$   
 (b)  $10101011 \cdot 1101001 \bmod 100011011 = 001011011$

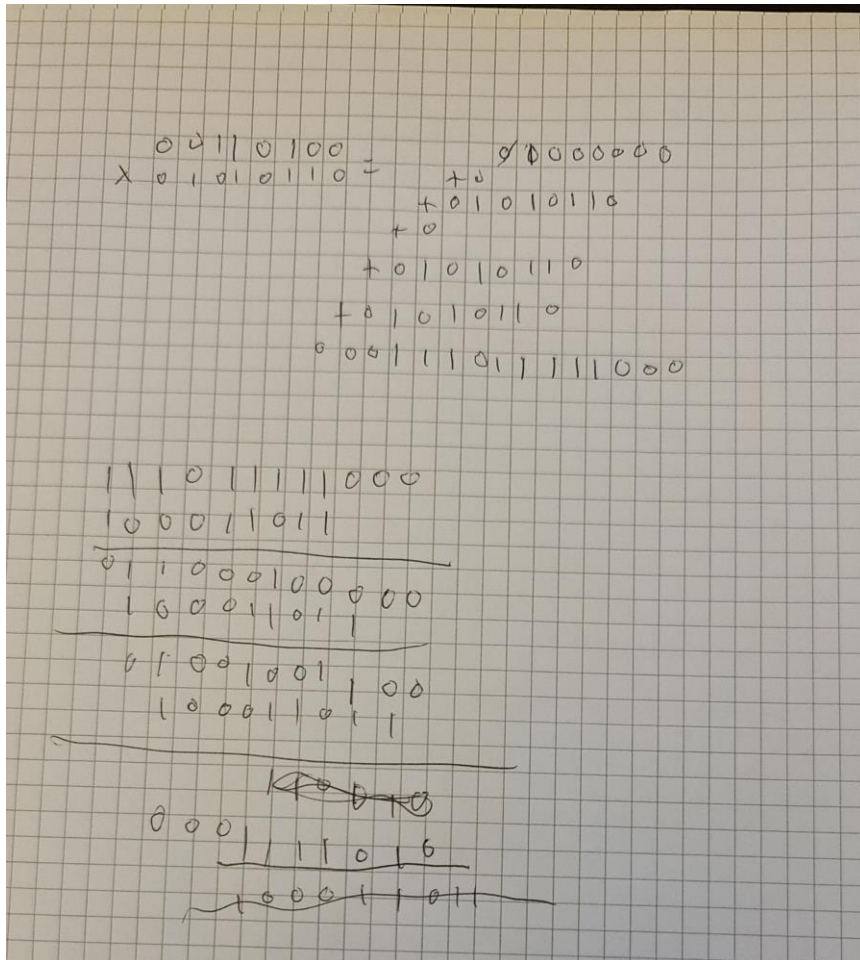
3)

$$0x13 \cdot 0x37 \bmod f(x) = 000000100$$

$$\begin{array}{r} 00010011 \\ \times 00110111 \\ \hline 00110111 \\ 00010011 \\ \hline 00000000 \\ 00000000 \\ \hline 00000000 \\ 00000000 \\ \hline 00000000 \\ 00000000 \\ \hline 00000000 \end{array}$$

$$\begin{array}{r} 110010100 \\ 100011011 \\ \hline 010001111 \\ 100011011 \\ \hline 000000100 \end{array}$$

$$0x34 * 0x56 \bmod f(x) = 001111010$$



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 ----->  $25^2 \% 77 = 9$

$$0 \text{ ----> } 9^2 \% 77 = 4$$

$$0 \text{ ----> } 4^2 \% 77 = 16$$

$$1 \text{ ----> } (16^2 \% 77 * 5 \% 77) \% 77 = 25 * 5 \bmod 77 = 48$$

2)

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

$$\Rightarrow a^{(p-1)} \text{ equivalent to } 1 \bmod 67$$

Which means  $a^{66}$  equivalent to  $1 \bmod 67$ .. 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:

$$1 \text{ ----> } 3$$

$$0 \text{ ----> } 9$$

$$0 \text{ ----> } 81 \% 67 = 14$$

$$0 \text{ ----> } 14^2 \% 67 = 62$$

$$0 \text{ ----> } 62^2 \% 67 = 25$$

$$1 \text{ ----> } (25^2 \% 67 * 3 \% 67) \% 67 = 66$$

$$0 \text{ ----> } 66^2 \% 67 = 1$$

So it is prime.

3)

$P=7$

$Q=11$

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

Here:  $a$  is 1,  $q$  is 11 and  $\text{inv}Q$  is 2.

$B$  is 6,  $p$  is 7 and  $\text{inv}P$  is 8.

So  $p \cdot \text{inv}P + q \cdot \text{inv}Q = 56 + 22 = 78$  is equivalent to 1 mod 77

Handwritten work on grid paper:

$$\begin{aligned} x &\equiv 8^{33} \pmod{7} \equiv 1^{33} \pmod{7} \\ x &\equiv 8^{33} \pmod{11} \equiv 6 \pmod{11} \end{aligned}$$
  
$$\begin{aligned} (2^3)^{33} &= 2^{99} & 8^{11} &= 2^{33} \end{aligned}$$
  

Or

$$\begin{aligned} x &= 1 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 8 \pmod{100} \\ &= 22 + 64 \cdot 7 \pmod{100} \\ &= 50 \end{aligned}$$

Problem 4:

script

Problem 5:

script