Lecture NS1 2018 revision

Chapter 2

1. Modular arithmetic: Addition/subtraction and multiplication

   $11 \ \mathbf{mod}\ 8 = 3;\ 15\ \mathbf{mod}\ 8 = 7$

   $[(11\ \mathbf{mod}\ 8) + (15\ \mathbf{mod}\ 8)]\ \mathbf{mod}\ 8 = 10\ \mathbf{mod}\ 8 = 2$

   $(11 + 15)\ \mathbf{mod}\ 8 = 26\ \mathbf{mod}\ 8 = 2$

   $[(11\ \mathbf{mod}\ 8) - (15\ \mathbf{mod}\ 8)]\ \mathbf{mod}\ 8 = -4\ \mathbf{mod}\ 8 = 4$

   $(11 - 15)\ \mathbf{mod}\ 8 = -4\ \mathbf{mod}\ 8 = 4$

   $[(11\ \mathbf{mod}\ 8) * (15\ \mathbf{mod}\ 8)]\ \mathbf{mod}\ 8 = 21\ \mathbf{mod}\ 8 = 5$

   $(11 * 15)\ \mathbf{mod}\ 8 = 165\ \mathbf{mod}\ 8 = 5$

   $(49 * 53)\ \mathbf{mod}\ 47 = 49\ \mathbf{mod}\ 47\ \mathrm{mod}{*}\ 53\ \mathbf{mod}\ 47 = 2*6 = 12$

2. State the following three theorems:
   a. Fermat
   b. Euler
   c. Chinese reminder theorem

3. Describe the Euclidean algorithm. Write a relevant pseudo-code

4. What is the Euler totient function

5. Calculate x that satisfies the following equations:
   - knowing that $30 = 2 \cdot 3 \cdot 5$: $x = 1 \bmod 2; x = 2 \bmod 3; x = 3 \bmod 5$
   - knowing that $105 = 3 \cdot 5 \cdot 7$: $x = 2 \bmod 3; x = 4 \bmod 5; x = 3 \bmod 7$

   Show your working

Chapter 5

1. Develop a set of tables similar to the following tables for GF(5).

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(d) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(e) Multiplication modulo 7

w	0	1	2	3	4	5	6
$-w$	0	6	5	4	3	2	1
w^{-1}	—	1	4	5	2	3	6

(f) Additive and multiplicative inverses modulo 7

Answer:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

w	$-w$	w^{-1}
0	0	—
1	4	1
2	3	3
3	2	2
4	1	4

Polynomial arithmetic in GF(2^8),

2. The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials:

$$f(x) = x^5 + x^4 + x + 1 \quad \text{and} \quad g(x) = x^5 + x^2 + 1$$

Give the result of $h(x) = f(x) * g(x) \bmod m(x)$.

Show your working. **Using polynomial notation:**

The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$\begin{aligned} f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2 \end{aligned}$$

$$\begin{aligned} f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\ &\quad + x^7 + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{array}{r|l}
 & x^5 + x^3 \\ \hline
x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
 & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \cline{2-2}
 & x^{11} + x^4 + x^3 \\
 & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \cline{2-2}
 & x^7 + x^6 + 1
\end{array}$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

It is much easier to repeat the above calculations using the binary notation:

7 6 5 4 3 2 1 0

f(x) 1010111

g(x) 10000011

1010111

1010111

1010111

f(x)·g(x) 10101101111001

13 12 11 10 9 8 7 6 5 4 3 2 1 0

divide by m(x) 100011011

5 4 3 2 1 0

101000

100011011 / 10101101111001

100011011

00100000011

100011011

h(x) 0000 $\boxed{11011001}$

7 6 5 4 3 2 1 0