

Imperial College London  
Department of Computing

**Network Security (430)**

Un-assessed Coursework 1

Answer the following questions, consulting Chapter 7 of *W. Stallings, Cryptography and Network Security*. Avoid using a calculator unless suggested to do so.

0. (i)  $-26 \pmod{7}$   
(ii)  $-371 \pmod{8}$
1. (i)  $22 + 16 \pmod{5}$   
(ii)  $39 * 83 \pmod{5}$   
(iii)  $5^4 \pmod{7}$   
(iv)  $3^5 \pmod{7}$
2.  $\gcd(540, 168)$  (You may use a calculator for this question)
3. By trying each possible multiplication with a “candidate inverse” work out the following (i.e. don’t use Euclid’s extended algorithm):
  - (i)  $3^{-1} \pmod{7}$
  - (ii)  $7^{-1} \pmod{9}$
  - (iii)  $5^{-1} \pmod{11}$
  - (iii)  $2^{-1} \pmod{4}$
4. Using Euclid’s extended algorithm work out: (Do this question last if you find it time consuming.)
  - (i)  $7^{-1} \pmod{9}$
  - (ii)  $7^{-1} \pmod{19}$
5. Divide  $x^5 - x^4 + x^3$  by  $x^3 + x^2 - x + 2$  producing the quotient and remainder.
6. Divide  $x^6 + x^5 + x^2 + x$  by  $x^3 + x^2 + 1$  over the field  $GF(2)$  producing the quotient and remainder.
7. Given  $f(x) = x^7 + x^6 + 1$ ,  $g(x) = x^2 + x$ ,  $m(x) = x^8 + x^4 + x^3 + x + 1$   
What is  $f(x)*g(x) \pmod{m(x)}$  over the field  $GF(2^8)$

Imperial College London  
Department of Computing

**Network Security (430)**

Un-assessed Coursework  
Solutions

0. (i)  $-26 \pmod{7} = 2$  i.e.  $-4*7 + 2 = -26$ .  
To calculate use  $7 - (26 \pmod{7}) = 7 - 5 = 2$   
(ii)  $-371 \pmod{8} = 8 - (371 \pmod{8}) = 8 - 3 = 5$  i.e.  $-47*8+5 = -371$
1. (i)  $22+16 = 3 \pmod{5}$   
Although you could do  $22+16 = 38$ , then  $38 = 3 \pmod{5}$   
A simpler approach is  $22 = 2 \pmod{5}$ ,  $16 = 1 \pmod{5}$ , then  $2+1 = 3 \pmod{5}$
- (ii)  $39*83 = 2 \pmod{5}$   
 $39 = 4 \pmod{5}$ ,  $83 = 3 \pmod{5}$   
 $4*3 = 12 = 2 \pmod{5}$
- (iii)  $5^4 = 2 \pmod{7}$  ^ is exponentiation here  
 $5*5 = 25 = 4 \pmod{7}$   
 $4*4 = 16 = 2 \pmod{7}$
- (iv)  $3^5 = 5 \pmod{7}$   
 $3*3 = 9 = 2 \pmod{7}$   
 $2*2 = 4 \pmod{7}$   
 $4*3 = 12 = 5 \pmod{7}$
2.  $\gcd(540, 168) = \gcd(36, 168) = \gcd(36, 24) = \gcd(12, 24) = \gcd(12, 0) = 12$   
i.e.  
 $\gcd(540, 168) = \gcd(540 \pmod{168}, 168) = \gcd(36, 168)$   
 $\gcd(36, 168) = \gcd(36, 168 \pmod{36}) = \gcd(36, 24)$   
 $\gcd(36, 24) = \gcd(36 \pmod{24}, 24) = \gcd(12, 24)$   
 $\gcd(12, 24) = \gcd(12, 24 \pmod{12}) = \gcd(12, 0) = 12$
3. (i)  $3^{-1} = 5 \pmod{7}$  i.e.  $3*2 = 6 \pmod{7}$  failure  
 $3*3 = 9 = 2 \pmod{7}$  failure  
 $3*4 = 12 = 5 \pmod{7}$  failure  
 $3*5 = 15 = 1 \pmod{7}$  success
- (ii)  $7^{-1} = 4 \pmod{9}$  i.e.  $7*2 = 14 = 5 \pmod{9}$  failure  
 $7*3 = 21 = 3 \pmod{9}$  failure  
 $7*4 = 28 = 1 \pmod{9}$  success
- (iii)  $5^{-1} = 9 \pmod{11}$  i.e.  $5*9 = 45 = 1 \pmod{11}$
- (iv)  $2^{-1} \pmod{4}$ ? No solution. You should be able to see why!

4. (i)  $7^{-1} \pmod{9}$  Here's a concise tabular way of performing the computation:

Let's do columns A and B first:

A	B	C	Comments
9 (from Q)		0 (always)	
7 (from Q)	1	1 (always)	Given PrevColA=9, ColA=7 work out $9 = 7*1+2$ Set ColB=1 and NextColA=2
2	3		Given PrevColA=7, ColA=2 work out $7 = 2*3+1$ Set ColB=3 and NextColA=1
1	2		Given PrevColA=2, ColA=1 work out $2 = 1*2+0$ Set ColB=2 and stop since ColA=1

Now let's complete column C

A	B	C	Comments
9 (from Q)		0 (always)	
7 (from Q)	1	1 (always)	
2	3	8	$ColC = PrevPrevColC - PrevColB * PrevColC$ $0 - 1 * 1 = -1 = 8 \pmod{9}$
1	2	4	$ColC = PrevPrevColC - PrevColB * PrevColC$ $1 - 3 * 8 = -23 = 4 \pmod{9}$

Answer is final value in column C = 4

- (ii)  $7^{-1} \pmod{19}$

A	B	C	Comments
19 (from Q)		0 (always)	
7 (from Q)	2	1 (always)	Given PrevColA=19, ColA=7 work out $19 = 7*2+5$ Set ColB=2 and NextColA=5
5	1		Given PrevColA=7, ColA=5 work out $7 = 5*1+2$ Set ColB=1 and NextColA=2
2	2		Given PrevColA=5, ColA=2 work out $5 = 2*2+1$ Set ColB=2 and NextColA=1
1	1		Given PrevColA=2, ColA=1 work out $2 = 1*1+1$ Set ColB=1 and stop since ColA=1

Now let's do Col C

A	B	C	Comments
19 (from Q)		0 (always)	
7 (from Q)	2	1 (always)	
5	1	17	$ColC = PrevPrevColC - PrevColB * PrevColC$ $0 - 2 * 1 = -2 = 17 \pmod{19}$
2	2	3	$ColC = PrevPrevColC - PrevColB * PrevColC$ $1 - 1 * 17 = -16 = 3 \pmod{19}$
1	1	11	$ColC = PrevPrevColC - PrevColB * PrevColC$ $17 - 2 * 3 = 11 \pmod{9}$

Answer is final value in column C = 11

5.

$$\begin{array}{r}
 \phantom{x^3+x^2-x+2} \quad \underline{x^2-2x+4} \\
 x^3+x^2-x+2 \mid x^5-x^4+x^3 \\
 \phantom{x^3+x^2-x+2} \quad \underline{x^5+x^4-x^3+2x^2} \\
 \phantom{x^3+x^2-x+2} \quad \phantom{x^5+x^4-x^3+2x^2} \quad \underline{-2x^4+2x^3-2x^2} \\
 \phantom{x^3+x^2-x+2} \quad \phantom{x^5+x^4-x^3+2x^2} \quad \phantom{-2x^4+2x^3-2x^2} \quad \underline{-2x^4-2x^3+2x^2-4x} \\
 \phantom{x^3+x^2-x+2} \quad \phantom{x^5+x^4-x^3+2x^2} \quad \phantom{-2x^4+2x^3-2x^2} \quad \phantom{-2x^4-2x^3+2x^2-4x} \quad \underline{4x^3-4x^2+4x} \\
 \phantom{x^3+x^2-x+2} \quad \phantom{x^5+x^4-x^3+2x^2} \quad \phantom{-2x^4+2x^3-2x^2} \quad \phantom{-2x^4-2x^3+2x^2-4x} \quad \phantom{4x^3-4x^2+4x} \quad \underline{4x^3+4x^2-4x+8} \\
 \phantom{x^3+x^2-x+2} \quad \phantom{x^5+x^4-x^3+2x^2} \quad \phantom{-2x^4+2x^3-2x^2} \quad \phantom{-2x^4-2x^3+2x^2-4x} \quad \phantom{4x^3-4x^2+4x} \quad \phantom{4x^3+4x^2-4x+8} \quad \underline{-8x^2-8}
 \end{array}$$

Quotient =  $x^2-2x+4$     Remainder =  $-8x^2-8$

6.

$$\begin{array}{r}
 \phantom{x^3+x^2+1} \quad \underline{x^3+1} \\
 x^3+x^2+1 \mid x^6+x^5 \quad +x^2+x \\
 \phantom{x^3+x^2+1} \quad \underline{x^6+x^5+x^3} \\
 \phantom{x^3+x^2+1} \quad \phantom{x^6+x^5+x^3} \quad \underline{x^3+x^2+x} \\
 \phantom{x^3+x^2+1} \quad \phantom{x^6+x^5+x^3} \quad \phantom{x^3+x^2+x} \quad \underline{x^3+x^2+1} \\
 \phantom{x^3+x^2+1} \quad \phantom{x^6+x^5+x^3} \quad \phantom{x^3+x^2+x} \quad \phantom{x^3+x^2+1} \quad \underline{x+1}
 \end{array}$$

Quotient =  $x^3+1$     Remainder =  $x+1$

7.

$$\begin{aligned}
 f(x) * g(x) &= (x^7 + x^6 + 1)(x^2 + x) \\
 &= (x^9 + x^8 + x^2) + (x^8 + x^7 + x) \\
 &= x^9 + x^8 + x^7 + x^2 + x
 \end{aligned}$$

Divide this by  $m(x) = x^8 + x^4 + x^3 + x + 1$

$$\begin{array}{r}
 \phantom{x^8+x^4+x^3+x+1} \quad \underline{x} \\
 x^8+x^4+x^3+x+1 \mid x^9+x^7 \quad +x^2+x \\
 \phantom{x^8+x^4+x^3+x+1} \quad \underline{x^9 \quad +x^5+x^4+x^2+x} \\
 \phantom{x^8+x^4+x^3+x+1} \quad \phantom{x^9 \quad +x^5+x^4+x^2+x} \quad \underline{x^7+x^5+x^4}
 \end{array}$$

Result = Remainder =  $x^7 + x^5 + x^4$