Sheet 1 crypto

(4.6) $5X \equiv 4 \bmod 3$

$5X \equiv 1 \bmod 3$

$5X + 3y = 1$

x	y	q	r
1	0	-	5
0	1	1	3
1	-1	1	2
-1	2	2	1

$5(-1) + 3(2) = 1$

Solution : $x = -1$

4.6 (b) $7x \equiv 6 \mod 5$

$7x \equiv 1 \mod 5$

$7x + 5y = 1$

x	y	q	r
1	0	-	7
0	1	1	5
1	-1	2	2
-2	3	2	1

$7(-2) + 5(3) = 1$

Solution $x = -2$

4.7 (a) 2

(b) -1

(c) 1

4.19

(a) $1234x \equiv 1 \mod 4321$

$1234x + 4321y = 1$

x	y	q	r
1	0	-	1234
0	1	0	4321
1	0	3	1234
-3	1	1	619
4	-1	1	615
-7	2	153	4
1075	-307	1	3
-1082	309		1

$1234(-1082) + 4321(309) = 1$

Solution: -1082

4.19 (b) $24140 \bmod 40902$

$24140x \equiv 1 \bmod 40902$

$24140x + 40902y = 1$

x	y	q	r
0	1	-	40902
1	0	1	24140
-1	1	1	16762
2	-1	2	7378
-5	3	3	2006
17	-10	1	1360
-22	13	2	646
61	-36	9	68
-571	337	2	34
1203	-710		0

24140 has No Multiplicative inverse mod 40902

4.24 المفروض بأن طريقة حل السؤال
دا إننا نشوف الـ prime ولا لا
عن طريق إننا نقسم على كل الأرقام
اللي أصغر منه أو على الأقل لـ $\sqrt{f(x)}$

يعني x^3+1 المفروض تقسم على :-

1
$$\boxed{\begin{array}{l} x \\ x+1 \\ x^2 \\ x^2+1 \\ x^2+x \\ x^2+x+1 \\ x^3 \end{array}}$$
x^3+1

بس دا صعب فاللي هنعمله إننا هنحاول
نشوف كل واحدة فيهم أقدر أعملها factorization ولا لا

4.24 (a) x^3+1 $\underline{GF(2)}$

$$x^3+1 = (x+1)(x^2+x+1)$$

$$(x+1)(x^2+x+1) = x^3+\cancel{x^2}+\cancel{x}+\cancel{x^2}+\cancel{x}+1$$
$$= x^3+1$$

reducible

4.24 (b) x^3+x^2+1 irreducible

(c) $x^4+1 = (x^2+1)(x^2+1)$

$(x^2+1)(x^2+1) = x^4+2x^2+1$ mod 2

$= x^4+1$

reducible

4.25 (a) x^3+x+1 , x^2+x+1

$$
\begin{array}{r|l}
 & x+1 \\
x^2+x+1 & x^3+x+1 \\
 & x^3+x^2+x \\
 & x^2+1 \\
 & x^2+x+1 \\
 & x
\end{array}
$$

	q	r
x^3+x+1, x^2+x+1	$x+1$	x
x^2+x+1, x	$x+1$	1

$$
\begin{array}{r|l}
 & x+1 \\
x & x^2+x+1 \\
 & x^2 \\
 & x+1 \\
 & x \\
 & 1
\end{array}
$$

$Gcd(x^3+x+1, x^2+x+1) = 1$

(4.25) $x^3 - x + 1$ & x^2+1 GF(3)

		a	r
x^3-x+1, x^2+1		x	$x+1$
$x^2+1, x+1$		$x+2$	2
$x+1, 2$			1

$$\begin{array}{r|l} & x \\ \hline x^2+1 & x^3+2x+1 \\ & x^3+x \\ \hline & x+1 \end{array}$$

$$\begin{array}{r|l} & x+2 \\ \hline x+1 & x^2+1 \\ & x^2+x \\ \hline & 2x+1 \\ & 2x+2 \\ \hline & -1 = 2 \end{array}$$

GCD = 1

GF(3)

$-1 \rightsquigarrow 2$

$-2 \rightsquigarrow 1$

$\frac{1}{2} \rightsquigarrow 2$

$$\begin{array}{r|l} & 2x \\ \hline 2 & x+1 \\ & x \\ \hline & 1 \end{array}$$

(4.25) $x^5+x^4+x^3-x^2-x+1,\ x^3+x^2+x+1$ GF(3)

$$\begin{array}{r|l} & x^2 \\ \hline x^3+x^2+x+1 & x^5+x^4+x^3+2x^2+2x+1 \\ & x^5+x^4+x^3+x^2 \\ \hline & x^2+2x+1 \end{array}$$

$$\begin{array}{r|l} & x+2 \\ \hline x^2+2x+1 & x^3+x^2+x+1 \\ & x^3+2x^2+x \\ \hline & 2x^2+1 \\ & 2x^2+x+2 \\ \hline & 2x+2 \end{array}$$

gcd = $2x+2$

last non zero reminder

$$\begin{array}{r|l} & 2x+2 \\ \hline 2x+2 & x^2+2x+1 \\ & x^2+x \\ \hline & x+1 \\ & x+1 \\ \hline & 0 \end{array}$$

CamScanner

GF(2)

4.26 $(x^7+x+1)f(x)+(x^8+x^4+x^3+x+1)g(x)=1$

$$x^7+x+1 \;\overline{\big)\, x^8+x^4+x^3+x+1}^{\;x}$$

$$x^8+x^2+x$$

$$\overline{x^4+x^3+x^2+1}$$

$$x^4+x^3+x^2+1 \;\overline{\big)\, x^7+x+1}^{\;x^3+x^2+1}$$

$$x^7+x^6+x^5+x^3$$

$$\overline{x^6+x^5+x^3+x+1}$$

$$x^6+x^5+x^4+x^2$$

$$\overline{x^4+x^3+x^2+x+1}$$

$$x^4+x^3+x^2+1$$

$$\overline{x}$$

$$x \;\overline{\big)\, x^4+x^3+x^2+1}^{\;x^3+x^2+x}$$

$$x^4$$

$$\overline{x^3+x^2+1}$$

$$x^3$$

$$\overline{x^2+1}$$

$$x^2$$

$$\overline{1}$$

g(x)	f(x)	q	r
1	0	–	$x^8+x^4+x^3+x+1$
0	1	x	x^7+x+1
	x	x^3+x^2+1	$x^4+x^3+x^2+1$
	x^4+x^3+x+1	x^3+x^2+x	x
	$\boxed{x^7}$		1

مش محتاجينه

$$x-(x^4+x^3+x+1).(x^3+x^2+x) =$$

$$
\begin{array}{l}
x^7+x^6+x^5 \\
+\quad x^6+x^5+x^4 \\
+\quad x^4+x^3+x^2 \\
+\quad x^3+x^2+x \\
+\quad x \\
\hline
x^7
\end{array}
$$

multipliCative inverse $= x^7$

(4.27)

$$(x^3+x+1)\,f(x) = 1 \bmod m(x)$$

$$\begin{array}{r|l} & \quad x \\ \hline x^3+x+1 & x^4+x+1 \\ & x^4+x^2+x \\ \hline & x^2+1 \end{array}$$

$$\begin{array}{r|l} & \quad x \\ \hline x^2+1 & x^3+x+1 \\ & x^3+x \\ \hline & 1 \end{array}$$

$$(x^3+x+1)\,f(x) + m(x)\,g(x) = 1$$

$f(x)$	$g(x)$	q	r
0	1	-	x^4+x+1
1	0	x	x^3+x+1
x		x	x^2+1
$1+x^2$			1

x

$(x^3+x+1)f(x) \bmod m(x)$

$(x^3+x+1)(1+x^2) = x^3+x+1+x^5+x^3+x^2$

$= (x^5+x^2+x+1) \bmod m(x)$

$$
\begin{array}{r|l}
 & x \\
\hline
x^4+x+1 & x^5+x^2+x+1 \\
 & x^5+x^2+x \\
\hline
 & 1
\end{array}
$$

reminder