FLAG - TD Feb. 13, 23

III.4 (exam question)

$A_1 = \mathbb{F}_3[x] / \langle x^2+1 \rangle$ $x^2 = -1 = 2$ mod 3

$\rightarrow \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$

Addition table is easy, all sums in mod 3.

None of sum will have degree > 2.

multiplication table

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

$x^2 = 2$

$2x^2 = 2 \cdot 2$

$= 1$

$x^2 = 2$

$x(2x+2) = 2x + 2x^2$ or

$= 2x + 1$

FLAG - TD 13. Feb. 23

Problem III.5

1. $4+5$ in $\mathbb{F}_7$, $4+5 = 9 = 2$.

   4×5 in $\mathbb{F}_7$, $4 \times 5 = 20 = 6$

2. Inverse of 23 in $\mathbb{F}_{31}$

   $23^{-1} \bmod 31$! EEA(23, 31)

   $23^{-1} \bmod 31$

   $= -4 = \underline{27}$

i	r	q	u	v
0	31		1	0
1	23	1	0	1
	8	2	1	-1
	7	1	-2	3
	1	7	3	-4
	0			

$$\begin{array}{r} 1 \\ 23 \overline{)31} \\ 23 \\ \hline 8 \end{array} \qquad \begin{array}{r} 2 \\ 8 \overline{)23} \\ 16 \\ \hline 7 \end{array}$$

$(31 \cdot 3) + (23)(-4) = 1$

3. $\mathbb{F}_9 = \mathbb{F}_3[X] / (x^2+1)$ there exists exactly 9 elements in $\mathbb{F}_9$.

   $= \{ax+b\}$, $a, b \in \mathbb{F}_3$ $\{0, 1, 2, x, x+1, x+2, 2x+1, 2x+2, 2x\} = \mathbb{F}_9$.

   $\mathbb{F}_3 = \{0, 1, 2\}$

$P(0) = 1$

$P(1) = 2$

$P(2) = 5 = 2$

$3 \bmod 3 = 0 \quad 4 \bmod 3 = 1$

$(2+2x)+(1+2x) = 3+4x = x$

$(2+2x)\times(1+2x) = 4x^2+4x+2x+2 = 4x^2+6x+2 \bmod 3$

in $\mathbb{F}_a = \mathbb{F}_3[x]/(x^2+1) \quad = 4x^2+2 = x^2+2 = 1$

$(x^2+1=0)$

$f(x) = q(x)\cdot P(x) + r(x) \qquad \deg(r) < \deg(P(x))$

$f(x) = P(x)$ in $R/P(x)$

ex $\quad x^3+x^2+1 = q(x^2+1)+r \qquad \deg(r) < 2$

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

$= \underbrace{(x+1)(x^2+1)}_{\text{take mod } x^2+1} + 2x = 2x$

- Compute $\gcd(f, g)$, $f = 3x^3 + x + 1$, $g = x^2 + 1$ in $\mathbb{Z}/7\mathbb{Z}$ ($\Rightarrow$ mod 7)

i	r	q	u	v
0	$3x^3 + x + 1$	–	1	0
1	$x^2 + 1$	$3x$	0	1
2	$5x + 1$	$3x + 5$	1	$4x$
3	3	$4x + 5$	$4x + 2$	$3x + 1$
4	0	–	–	–

$q_1 = 3x^3 + x + 1 \,/\, x^2 + 1 \mod 7$

$= 3x \mod 7 = \boxed{3x}$

$$\begin{array}{r} 3x \\ x^2+1 \overline{)\,3x^3 + x + 1} \\ -(3x^3 + 3x) \\ \hline -2x + 1 \end{array}$$

$r_2 = (-2x + 1) \mod 7 = 5x + 1$

$-2 \mod 7 = 5$

$1 \mod 7 = 1$

$q_2 = x^2 + 1 \,/\, 5x + 1 \mod 7$

$= \frac{1}{5}x - \frac{1}{25} \mod 7 = 3x + 5$

$$\begin{array}{r} \frac{1}{5}x - \frac{1}{25} \\ 5x+1 \overline{)\,x^2 + 1} \\ -(x^2 + \frac{1}{5}x) \\ \hline -\frac{1}{5}x + 1 \\ -(-\frac{1}{5}x - \frac{1}{25}) \\ \hline \frac{26}{25} = r_3 \end{array}$$

$5^{-1} \mod 7 = 3$

$25^{-1} \mod 7 = 2$

$(-25)^{-1} \mod 7 = -2 \mod 7 = 5$

$V_2 = V_0 - q_1 V_1$

$= 0 - q_1 V_1 = -3x \mod 7$

$= \boxed{4x}$

$r_3 = {}^{26}/_{25} \bmod 7 = 26 \cdot (25)^{-1} \bmod 7 = 5 \cdot 2 \bmod 7 = \boxed{3}$

$(25)^{-1} \bmod 7 = 2$

$26 \bmod 7 = 5$

$q_3 = {}^{5x+1}/_{3} \bmod 7$

$= {}^{5}/_{3}x + {}^{1}/_{3} \bmod 7 = 4x + 5$

$5 \cdot 5 \bmod 7 = 4$

$3^{-1} \bmod 7 = -2 \bmod 7$

$= 5$

$5/3x + 1/3$

$3 \overline{)\, 5x + 1}$

$-5x$

1

-1

0

$u_3 = u_1 - q_2 u_2$

$= 0 - (3x+5) \cdot 1$

$= -3x - 5 \bmod 7$

$= 4x + 2$

$v_3 = v_1 - q_2 v_2$

$= 1 - 4x \cdot 1$

$= -4x + 1 \bmod 7$

$= 3x + 1$

$\gcd(f, g) = 3$ in $\mathbb{Z}/7\mathbb{Z}$