FLAG-TD Feb.06.23

- Compute gcd & cofactors of...,
  1) $a = 224$, $b = 91$
  2) $a = 25$, $b = 31$.

1). Use EEA.

$\frac{a}{b} = 224/91$

$i = 1$

$q_1 = 2, \ r_2 = 42$.

$u_2 = 1 - 0 = 1$.

$V_2 = 0 - 1 \cdot 2 = -2$.

$i = 2$.

$91/42 = 2, r\,7$.

$q_2 = 2, \ r_3 = 7$

$u_3 = 1 - 2 = -1$

$V_3 = \underline{1} - (-2)(2) = 5$

$$\begin{array}{r} 2 \\ 91\overline{)224} \\ 182 \\ \hline 42 \end{array}$$

$$\begin{array}{r} 2 \\ 42\overline{)91} \\ 84 \\ \hline 7 \end{array}$$

$i = 3$.

$r_2/r_3 = 42/7 = 6$

$q_3 = 6 \quad r_4 = 0$

$u_4 = -1 - 6 \cdot (-1) = 5$

$V_4 = (-2) - 5 \cdot 6 = -32$

i	r	q	u	v
0	224	-	1	0
1	91	2	0	1
2	42	2	1	-2
3	$\boxed{7}$	6	-2	5
4	0	-		

$$\boxed{u_{i-1} \cdot r_0 + V_{i-1} \cdot r_1 = r_{i-1}.}$$

$-2 \cdot 225 + 5 \cdot 91 =$ should be 7.

$-448 + 455 = 7$.

· Use EEA

$a = 25, \ b = 31$

you swap a and b if $a < b$.

$$\begin{array}{r} 1 \\ 31\overline{)25} \\ 31 \\ \hline \end{array}$$

i	r	q	u	v
0	31		1	0
1	25	1	0	1
2	6	4	1	-1
3	$\boxed{1}$	6	$\boxed{-4}$	$\boxed{5}$
4	0			

$i=1$

$u_2 = u_0 - q_1 u_1 = 1 - 1 \cdot 0 = 1$

$V_2 = V_0 - q_1 V_1 = 0 - 1 \cdot 1 = -1$

$i=2$

$25/6 = 4 \ r \ 1$

$u_3 = U_1 - q_2 u_2 = 0 - 4 \cdot 1 = -4$

$V_3 = V_1 - q_2 V_2 = 1 - (-1)(4) = 5$

$i=3$

$6/1 = 6 \ r \ 0$

$25 \cdot 5 + 31(-4) = 1$

$\gcd(25, 31) = 1$

$25 \times 5 = 1 \bmod 31$

$31(-4) = 1 \bmod 25$

$5 = 25^{-1} \bmod 31$.

---

if a, b coprime, i.e. $\gcd(a,b) = 1$

$\exists \, a^{-1} \bmod b$, if p is prime $\exists \, a^{-1} \bmod p$

$\forall a < p$

$\mathbb{Z}/n\mathbb{Z} = \{0, 1 \dots, n-1\}$

n : prime.

- Addition / substraction
- Multiplication
- Inverssion (only if n is prime)
  (non-zero elements)

$\mathbb{Z}/n\mathbb{Z}$ is finite field.

FLAG-TD Feb. 06. 23

- Compute $a^{-1} \bmod b$.

  $a = 17$, $b = 19$.

you want $19 \cdot u + 17 \cdot v = \gcd(19, 17)$

$v = 17^{-1} \bmod 19$.

EEA

i	r	q	u	v
0	19.		1	0
1	17	1	0	1.
2	2.	8	1	-1.
3	$\boxed{1}$	2	-8	9
4	0			

$i = 1$.

$19/17 = 1 \text{ r } 2$.

$u_2 = u_0 - q_1 u_1 = 1 - 0 = 1$

$v_2 = v_0 - q_1 v_1 = 0 - 1 \cdot 1 = -1$.

$i = 2$.

$17/2 = 8$

$u_3 = u_1 - q_2 u_2 = 0 - 8 = -8$

$v_3 = v_1 - q_2 v_2 = 1 - 8(-1) = 9$.

$i = 3$

$2/1 = 2$ r

$19(-8) + 17(9) = 1$

$9 = 17^{-1} \bmod 19$.

$\Rightarrow$ $r_0 \cdot u_{i-1} + r_1 v_{i-1} = \gcd(r_0, r_1) = r_{i-1}$

$v_{i-1} = r_1^{-1} \bmod r_0$

$\swarrow$ $u_{i-1} = r_0^{-1} \bmod r_1$

$\gcd(a, b) = u \cdot a + v \cdot b$

if a, b are coprime meaning $\gcd(a, b) = 1$.

$1 = u \cdot a + vb$

$\hookrightarrow$ mod b

$1 = u \cdot a \Rightarrow u = a^{-1} \bmod b$

'Compute gcd & cofactor

$f = x^3+2x^2-x-2$

$g = x^2+1$

i	r	q	u	v
0	f		1	0
1	g.	$(x+2)$	0	1.
2	$(-2x-4)$	$(-\frac{1}{2}x+1)$	1	$(-x-2)$
3.	$\boxed{5}$	$(-\frac{2}{5}x-\frac{4}{5})$	$(\frac{1}{2}x-1)$	$(-\frac{1}{2}x^2+3)$
4	0			

$i=1$

$f/g = x+2$

$u_2 = u_0 - q_1u_1$

$= 1 - (x+2)\cdot 0$

$= 1$

$V_2 = V_0 - q_1V_1$

$= 0 - (x+2)(1)$

$= (-x-2)$

$$\begin{array}{r} x+2 \\ x^2+1\overline{)\,x^3+2x^2-x-2} \\ -(x^3+0x^2+x) \\ \hline 2x^2-2x-2 \\ -(2x^2+0x+2) \\ \hline -2x-4 \end{array}$$

$i=3$

$(-2x-4)/5 = -\frac{2}{5}x - 4/5$

$i=2$

$g/-2x-4 = -\frac{1}{2}x+1$

$r\ 5$

$u_3 = u_1 - q_2u_2$

$= 0 - (-\frac{1}{2}x+1)\cdot(1)$

$= \frac{1}{2}x - 1$

$V_3 = V_1 - q_2V_2 = 1 - (-\frac{1}{2}x+1)(-x-2)$

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

$= 1 - \frac{1}{2}x^2 + 2 = -\frac{1}{2}x^2+3$

$$\begin{array}{r} -x/2+1 \\ -2x-4\overline{)\,x^2+1} \\ -(x^2+2x) \\ \hline -2x+1 \\ -(-2x-4) \\ \hline 5 \end{array}$$

$$\begin{array}{r} -\frac{2}{5}x-\frac{4}{5} \\ 5\overline{)\,-2x-4} \\ -(-2x\quad) \\ \hline -4 \\ -(-4) \\ \hline 0 \end{array}$$

$\gcd(f,g) = 5$

$(x^3+2x^2-x-2)(\frac{1}{2}x-1)$

$+ (x^2+1)(-\frac{1}{2}x^2+3) = 5$

$d = \gcd(f,g)$, $f,g \in \Bbbk[x]$

$\deg(d) \le \deg(f)$ $\quad \deg(d) \le \deg(g)$

FLAG - TD   Feb. 06. 23

- f, g are coprime if $d = \gcd(f, g)$ and $\deg(d) = 0$

$$u \cdot f + v \cdot g = \gcd(f, g)$$

mod g

$$u \cdot f = d$$

$$u(x) = f^{-1}(x) \bmod g(x).$$

$\frac{1}{a} \bmod 7 \Rightarrow a^{-1} \bmod 7$

can be compute by using EEA on 7 and a.

· $\mathbb{Z}/7\mathbb{Z} \Rightarrow \bmod 7$

Compute gcd of $f = 3x^3 + x + 1$ $g = x^2 + 1$

$\frac{5}{4}\left(-\frac{8}{5}x\right)^{2}$

$-2x$

i	r	q	u	v
0	f		1	0
1	g	$3x$	0	1
2	$(-5x+1)$	$(3x+2$	1	$4x$
3				
4	0			

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

<u>i=1</u>

$f/g = q_1 \; r_2$

$= 3x, \; -2x + 1$

$u_2 = u_0 - q_1 u_1$

$= 1 - 3x \cdot 0 = 1$

$v_2 = v_0 - q_1 v_1$

$= 0 - 3x \cdot 1 = -3x$

$$\begin{array}{r} -\frac{1}{2}x - \frac{1}{4} \\ -2x+1 \overline{) \, x^2 + 1} \\ -(x^2 - \frac{1}{2}x) \\ \hline \frac{1}{2}x + 1 \\ -(\frac{1}{2}x - \frac{1}{4}) \\ \hline \frac{5}{4} \end{array}$$

<u>i=2</u>

$g/(-2x+1) = q_2 \; r_3 = -\frac{1}{2}x - \frac{1}{4}, \; \frac{5}{4}$

$u_3 = u_1 - q_2 u_2 = 0 - \left(-\frac{1}{2}x - \frac{1}{4}\right) \cdot 1$

$= \frac{1}{2}x + \frac{1}{4}$

$v_3 = v_1 - q_2 v_2 = 1 - \left(-\frac{1}{2}x - \frac{1}{4}\right)(-3x)$

$= 1 - \left(\frac{3}{2}x^2 + \frac{3}{4}x\right)$

<u>i=3</u>

$$\begin{array}{r} -\frac{8}{5}x + \frac{4}{5} \\ \frac{5}{4} \overline{) \, -2x + 1} \\ -(-2x + 1) \\ \hline 0 \end{array} - q_3$$

$0 \rightarrow r_4$

$r_3 = 5/4$

$5/4 \bmod 7$

$5 \cdot (4)^{-1} \bmod 7$

EEA on $\begin{matrix} a = 4 \\ b = 7 \end{matrix}$

$\frac{1}{25} \bmod 7 \Rightarrow$ do EEA on $\begin{matrix} a = 25 \\ b = 7 \end{matrix}$

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