11.8. (3) $a(x)$, $b(x)$ 是 F_2 上多项式. 试计算 $s(x)$, $t(x)$, 使 $s(x)a(x)+t(x)\cdot b(x)=(a(x),b(x))$.

① $a(x)=x^2+x+1$, $b(x)=x^8+x^4+x^3+x+1$

解: $b(x)=x^8+x^4+x^3+x+1=(x^6+x^5+x^3)a(x)+x+1$

6+5+3
2+1+0 | 8+4+3+1+0
8+7+6
7+6+4+3+1+0
7+6+5
5+4+3+1+0
5+4+3
1+0

$a(x)=x^2+x+1=x\cdot(x+1)+1$

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

$\therefore (a(x),b(x))=1$

$1=a(x)-x(x+1)$

$=a(x)-x(b(x)-(x^6+x^5+x^3)a(x))$

$=(x^7+x^6+x^4+1)a(x)-x\,b(x)$

$s(x)=(x^7+x^6+x^4+1)$, $t(x)=-x$

② $a(x)=x^3+x+1$, $b(x)=x^8+x^4+x^3+x+1$

$b(x)=x^8+x^4+x^3+x+1=(x^5+x^3+x^2+1)\cdot a(x)+x^2$.

5+3+2+0
3+1+0 | 8+4+3+1+0
8+6+5
6+5+4+3+1+0
6+4+3
5+1+0
5+3+2
3+2+1+0
3+1+0
2

$a(x)=1\cdot x^2+x+1$

$x^2=x\cdot(x+1)+x$

$x+1=1\cdot x+1$

$1=x+1-x$

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

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

$=(a(x)-x^2)(x+1)-x^2$

$=(x+1)(a(x))-x\cdot x^2$

$=(x+1)(a(x))-x\cdot(b(x)-(x^5+x^3+x^2+1)a(x))$

$=(x^6+x^4+x^3+1)(a(x))-x\,b(x)$

$s(x)=(x^6+x^4+x^3+1)$

$t(x)=-x$

③ $a(x)=x^4+x+1$, $b(x)=x^8+x^4+x^3+x+1$

$b(x)=(x^4+x)\cdot a(x)+x^3+x^2+1$.

4+1
4+1+0 | 8+4+3+1+0
8+5+4
5+3+1+0
5+2+1
3+2+0

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

$a(x)=(x+1)\cdot(x^3+x^2+1)+x^2$

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

$1=x^3+x^2+1-(x+1)\cdot x^2$

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

$=x^2\cdot(x^3+x^2+1)-(x+1)a(x)$

$=x^2(b(x)-(x^4+x)a(x))-(x+1)a(x)$

$=x^2\cdot b(x)-(x^6+x^3+x+1)a(x)$

$s(x)=x^2$

$t(x)=x^6+x^3+x+1$

E7.8 计算 $(a(x), b(x))$. $a(x) = x^{15}+1$, $b(x) = x^8+x^4+x^3+x^2+1$.

$$\begin{array}{l} \quad 7+3+2+1 \\ 8+4+3+2+0 \mid 15+0 \\ \quad 15+11+10+9+7 \\ \hline \quad \cancel{11}+10+9+\cancel{7}+0 \\ \quad \cancel{11}+\cancel{7}+6+5+3 \\ \hline \quad 10+9+\cancel{6}+\cancel{5}+3+0 \\ \quad 10+6+5+4+2 \\ \hline \quad 8+4+3+2+0 \\ \quad 8+5+4+3+1 \\ \hline \quad 5+2+1+0 \end{array}$$

$b(x) = (x^7+x^3+x^2+x)$ ~~...~~ $a(x)$ $+ x^5+x^2+x+1$

$$\begin{array}{l} \quad 3+0 \\ 5+2+1+0 \mid 8+4+3+2+0 \\ \quad 8+5+4+3 \\ \hline \quad 5+2+0 \\ \quad 5+2+1+0 \\ \hline \quad 1 \end{array}$$

$b(x) = (x^3+1)\cdot(x^5+x^2+x+1)+1$

$x^5+x^2+x+1 = (x^4+x+1)\cdot x + 1$

$\therefore (a(x), b(x)) = 1$

② $a(x) = x^7+1$, $b(x) = x^8+x^4+x^3+x+1$

$$\begin{array}{l} \quad 1+0 \\ 7+0 \mid 8+4+3+1+0 \\ \quad 8+1 \\ \hline \quad 4+3+0 \end{array}$$

$$\begin{array}{l} \quad 3+2+1+0 \\ 4+3+0 \mid 7+0 \\ \quad 7+6+3 \\ \hline \quad 6+3+0 \\ \quad 6+5+2 \\ \hline \quad 5+3+2+0 \\ \quad 5+4+1 \\ \hline \quad 4+3+2+1+0 \\ \quad 4+3+0 \\ \hline \quad 2+1 \end{array}$$

$b(x) = x\cdot a(x) + x^4+x^3+1$

$a(x) = (x^3+x^2+x+1)\cdot(x^4+x^3+1) + x^2+1$

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

$$\begin{array}{l} \quad 2+1+0 \\ 2+0 \mid 4+3+0 \\ \quad 4+2 \\ \hline \quad 3+2+0 \\ \quad 3+1 \\ \hline \quad 2+1+0 \\ \quad 2+0 \\ \hline \quad 1 \end{array}$$

$x^2+1 = x\cdot x + 1$

故 $(a(x), b(x)) = 1$

例证明：$f(x) = x^8+x^4+x^3+x+1$ 为数域 F_2 上的不可约多项式。只需对 $\deg \le 4$ 的不可约多项式进行试除，即对 x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$ 进行试除，结果发现均不可整除，则 $f(x) = x^8+x^4+x^3+x+1$ 为数域 F_2 上的不可约多项式

则 $F_{2^8} = F_2[x]/f(x)$ 满足多项式域的定义，是一个有限域。

1101. 设 $a(x)=x^6+x^4+x^2+x+1$　$b(x)=x^7+x+1$.

在 $R_{2^8}=F_2[x]/(x^8+x^4+x^3+x+1)$ 中计算 $a(x)+b(x)$, $a(x)\cdot b(x)$, $a(x)^2$, $a(x)^{-1}$, $b(x)^{-1}$.

解：$a(x)+b(x)=x^7+x^6+x^4+x^2$

$a(x)\cdot b(x)=x^{13}+x^7+x^6+x^{11}+x^5+x^4+x^9+x^3+x^2+x^8+x^2+x$
$+x^7+x+1$

$=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3=x^7+x^6$

$5+3$

$8+4+3+1+0 \mid 13+11+9+8+6+5+4+3$

$13+9+8+6+5$

$11+4+3$

$11+7+6+4+3$

$7+6$

$a(x)^2=x^{12}+x^8+x^4+x^2+1$

$=x^7+x^5+x^2+1$

4

$8+4+3+1+0 \mid 12+8+4+2+0$

$12+8+7+5+4$

$7+5+2+0$

$3+1$ $5+3$

$+8+6+4+2$

$1+0$

$8+4+3+1+0 \mid 9+8+7+6+5+4+3+2$

$9+5+4+2+1$

$8+7+6+3+1$

$8+4+3+1+0$

$7+6+4+2+1+0$

$x^8+x^4+x^3+x+1=(x^6+x^4+x^2+x+1)(x^2+1)+x^4$

$2+0$

$6+4+2+1+0 \mid 8+4+3+1+0$

$8+6+4+3+2$

$6+2+1+0$

$6+4+2+1+0$

4

$x^6+x^4+x^2+x+1=(x^2+1)\cdot x^4+x^2+x+1$

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

$2+1$

$2+1+0 \mid 4$

$4+3+2$

$3+2$

$3+2+1$

$x^2+x+1=(x+1)\cdot x+1$

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

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

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

$=(x^3+x+1)(x^6+x^4+x^2+x+1)-(x^2+1)x^4$

$-(x+1)x^4$

$=(x^3+x+1)(x^6+x^4+x^2+x+1)-(x^5+x^2)x^4$

$=(x^3+x+1)(x^6+x^4+x^2+x+1)-(x^4+x^2)(x^8+x^4+x^3+x+1-$
$(x^6+x^4+x^2+x+1))$

$=(x^5+x^3+x^2+x+1)(x^6+x^4+x^2+x+1)-(x^5+x^2)(x^8+x^4+x^3+x+1)$

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

$x^8+x^4+x^3+x+1=x\cdot(x^7+x+1)+x^4+x^3+x^2+1$

$x^7+x+1=(x^3+x^2+x)(x^4+x^3+x^2+1)+x$

$3+2+1$

$4+3+2+0 \mid 7+1+0$

$7+6+5+3$

$6+5+3+1+0$

$6+5+4+2$

$4+3+2+1+0$

$(x^4+x^3+x^2+1)=(x^3+x^2+x)\cdot x+1$

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

$=(x^4+x^3+x^2+1)-(x^7+x+1-(x^3+x^2+x)(x^4+x^3+x^2+1))(x^3+x^2+x)$

$=(x^6+x^4+x^2+1)(x^4+x^3+x^2+1)-(x^3+x^2+x)(x^7+x+1)$

$=(x^6+x^4+x^2+1)(x^8+x^4+x^3+x+1-x(x^7+x+1))-(x^3+x^2+x)(x^7+x+1)$

$=(x^6+x^4+x^2+1)(x^4+x^3+x^2+1)-(x^3+x^2)(x^8+x^4+x^3+x+1)(x^7+x+1)$

$\therefore b(x)^{-1}=x^7+x^6+x^4+\ldots$