

## 연 습 문 제 (3.2)

1. 보기 3.2.4 의 이산로그표를 이용하여 다음과 같은 정수  $a$  를 구하여라.

$$(1) a \equiv g^{11} \pmod{37}, \quad 1 \leq a < 37$$

$$(2) a \equiv g^{20} g^{23} \pmod{37}, \quad 1 \leq a < 37$$

[풀이] (1) 아래 이산로그표에 의하여

$$a \equiv g^{11} \pmod{37} \equiv 13, \quad 1 \leq a < 37$$

이므로  $a = 13$  이다.

$$(2) a \equiv g^{20} g^{23} = g^{43} \pmod{37} \text{ 이고 } g^{36} \equiv 1 \pmod{37} \text{ 이므로}$$

$$a \equiv g^{20} g^{23} = g^{43} \equiv g^7 \equiv 17 \pmod{37}, \quad 1 \leq a < 37$$

이고 따라서  $a = 17$  이다.

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\text{ind}_g a$	0	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7
$a$	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
$\text{ind}_g a$	17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8

2. 정수  $g = 3$  은 법 17 에 관한 원시근이고, 또는  $g$  를 밑으로 가지는 법 17 에 관한 이산로그표는 다음과 같다.

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_g a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

이 표를 이용하여 다음과 같은 정수  $a$  를 구하여라.

$$(1) a \equiv g^{11} \pmod{17}, \quad 1 \leq a < 17$$

$$(2) a \equiv (g^{10})^3 \pmod{17}, \quad 1 \leq a < 17$$

$$(3) g^{13} a \equiv 1 \pmod{17}, \quad 1 \leq a < 17$$

[풀이] (1)  $a \equiv g^{11} \equiv 7 \pmod{17}$ ,  $1 \leq a < 17$  이므로  $a = 7$  이다.

$$(2) a \equiv (g^{10})^3 \equiv g^{30} \equiv g^{14} \equiv 2 \pmod{17}, \quad 1 \leq a < 17$$

이므로  $a = 2$  이다.

$$(3) g^{13} a \equiv 1 = g^{16} \pmod{17}, \quad 1 \leq a < 17 \text{ 이므로}$$

$$a \equiv g^3 \equiv 10 \pmod{17}, \quad 1 \leq a < 17$$

이고, 따라서  $a = 10$  이다.

3. 정수  $g = 6$  가 법 11 에 관한 원시근임을 밝히고,  $g$  를 밑으로 가지는 법 11 에 관한 이산로그표를 만들어라.

그리고, 이 이산로그표를 이용하여 다음 물음에 답하여라.

$$(1) 6^e \equiv 8 \pmod{11}, \quad 1 \leq e < 11 \text{ 인 정수 } e \text{ 를 구하여라.}$$

$$(2) a \equiv 6^{19} \pmod{11}, \quad 1 \leq a < 11 \text{ 인 정수 } a \text{ 를 구하여라.}$$

$$(3) a \equiv 3^7 \pmod{11}, \quad 1 \leq a < 11 \text{ 인 정수 } a \text{ 를 구하여라.}$$

[풀이] 정수  $g = 6$  는 법 11 에 관한 원시근이다. 실제로, 다음이 성립한다.

$$g^1 \equiv 6, \quad g^2 \equiv 3, \quad g^3 \equiv 7, \quad g^4 \equiv 9, \quad g^5 \equiv 10 \pmod{11}$$

$$g^6 \equiv 5, \quad g^7 \equiv 8, \quad g^8 \equiv 4, \quad g^9 \equiv 2, \quad g^{10} \equiv 1 = g^0 \pmod{11}$$

따라서  $g$  를 밑으로 가지는 법 11 에 관한 이산로그표는 다음과 같다.

$a$	1	2	3	4	5	6	7	8	9	10	$\pmod{11}$
$\text{ind}_g a$	0	9	2	8	6	1	3	7	4	5	$\pmod{10}$

$$(1) 6^e \equiv 8 \pmod{11}, \quad 1 \leq e < 11 \text{ 일 때, } e = 7 \text{ 이다.}$$

$$(2) a \equiv 6^{19} \pmod{11}, \quad 1 \leq a < 11 \text{ 일 때, } a \equiv 6^{19} \equiv 6^9 \pmod{11}$$

이므로  $a = 2$  이다.

$$(3) a \equiv 3^7 \pmod{11}, \quad 1 \leq a < 11 \text{ 일 때,}$$

$$a \equiv 3^7 \equiv (g^2)^7 \equiv g^{14} \equiv g^4 \equiv 9 \pmod{11}$$

이므로  $a = 9$  이다.

## 연 습 문 제 (3.3)

1.  $m = 187 = 11 \cdot 17$  일 때,  $e = 7$  에 대하여

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 \leq d < \varphi(m)$$

인 정수  $d$  를 구하여라.

[풀이] 먼저  $m = 187 = 11 \cdot 17$  이므로  $\varphi(m)$  은 다음과 같다.

$$\varphi(m) = \varphi(11) \varphi(17) = 10 \cdot 16 = 160$$

그리고,  $e = 7$  일 때 유클리드의 알고리즘  
(정리 1.2.5)에 의하여

$$160(-1) + 7 \cdot 23 = 1$$

이므로

$$7 \cdot 23 \equiv 1 \pmod{160}$$

이고, 따라서  $d = 23$  이다.

$$\begin{array}{r|rr|r} 22 & 160 & 7 & 1 \\ & 154 & 6 & \\ 6 & \underline{6} & 1 & \\ & 6 & & \\ & \underline{0} & & \end{array}$$

22	1		
1	0	1	-1
0	1	-22	23

2.  $m = 323 = 17 \cdot 19$  일 때,  $e = 55$  에 대하여

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 \leq d < \varphi(m)$$

인 정수  $d$  를 구하여라.

[풀이] 먼저  $m = 323 = 17 \cdot 19$  이므로

$$\varphi(m) = \varphi(17) \varphi(19) = 16 \cdot 18 = 288$$

이고, 또  $e = 55$  일 때 다음이 성립한다.

$$288 \cdot 17 + 55 \cdot (-89) = 1$$

따라서

$$55 \cdot (-89) \equiv 1 \pmod{288}$$

$$\text{즉, } 55 \cdot 199 \equiv 1 \pmod{288}$$

이므로  $d = 199$  이다.

$$\begin{array}{r|rr|r} 5 & 288 & 55 & 4 \\ & 275 & 52 & \\ 4 & \underline{13} & 3 & 3 \\ & 12 & 3 & \\ & \underline{1} & 0 & \end{array}$$

5	4	4		
1	0	1	-4	17
0	1	-5	21	-89

4. 중국인의 나머지 정리를 이용하여 다음 연립일차합동식의 해를 구하여라.

$$(1) \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad (2) \begin{cases} x \equiv 10 \pmod{11} \\ x \equiv 3 \pmod{13} \end{cases}$$

[답] 정리 1.3.7을 이용한다.

$$(1) x \equiv 23 \pmod{35}$$

$$(2) x \equiv 120 \pmod{143}$$

5. 중국인의 나머지 정리를 이용하여 다음 연립일차합동식의 해를 구하여라.

$$(1) \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases} \quad (2) \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases}$$

[풀이] (1) 정리 1.3.8을 이용한다.

이제

$$M_1 = 5 \cdot 7 = 35, \quad M_2 = 3 \cdot 7 = 21, \quad M_3 = 3 \cdot 5 = 15$$

이라고 하면

$$35 \cdot 2 \equiv 1 \pmod{3},$$

$$21 \cdot 1 \equiv 1 \pmod{5},$$

$$15 \cdot 1 \equiv 1 \pmod{7}$$

이므로 구하는 해는 다음과 같다.

$$\begin{aligned} x \equiv u &\equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 15 \cdot 1 \cdot 4 \\ &\equiv 140 + 21 + 60 \\ &\equiv 11 \pmod{105} \end{aligned}$$

$$(2) x \equiv 103 \pmod{385}$$

## 연 습 문 제 (3.4)

1. 다음은  $g = 2$  를 밑으로 가지는 법  $p = 37$  에 관한 이산로그표이다.

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\text{ind}_g a$	0	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7
$a$	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
$\text{ind}_g a$	17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8
	19	18	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67

위의 이산로그표를 이용하여 다음 물음에 답하여라.

(1)  $r = 15$  일 때,  $d \equiv g^r \pmod{37}$ ,  $1 \leq d < 37$  인 정수  $d$  를 구하여라.

(2)  $s = 22$ ,  $a = 19$  일 때,

$$b \equiv g^s \pmod{37}, \quad 1 \leq b < 37$$

$$c \equiv ad^s \pmod{37}, \quad 1 \leq c < 37$$

인 정수  $b, c$  를 구하고  $b^{-r}c \equiv a \pmod{37}$  임을 확인하여라.

[풀이] (1)  $d \equiv g^r \equiv g^{15} \equiv 23 \pmod{37}$  이므로  $d = 23$  이다.

(2) 먼저

$$b \equiv g^s \equiv g^{22} \equiv 21 \pmod{37}$$

이므로  $b = 21$  이다. 그리고,

$$c \equiv ad^s \equiv a(g^r)^s \equiv 19 \cdot g^{15 \cdot 22}$$

이고, 또  $15 \cdot 22 \equiv 330 \equiv 6 \pmod{36}$  이므로

$$c \equiv 19 \cdot g^6 \equiv 19 \cdot 27 \equiv 32 \pmod{37}$$

이고 따라서  $c = 32$  이다.

또한, 다음이 성립한다.

$$\begin{aligned} b^{-r}c &\equiv 21^{-15}32 \equiv 21^{21} \cdot 32 \equiv (g^{22})^{21} \cdot g^5 \\ &\equiv g^{467} \equiv g^{35} \equiv 19 \equiv a \pmod{37} \end{aligned}$$

## 연 습 문 제 (3.5)

1. 보기 3.5.5 에서  $p = 83$ ,  $q = 41$ ,  $g_1 = 4$ ,  $r = 5$ ,  $a = 7$  일 때 다음 물음에 답하여라.

- (1)  $d_1 \equiv g_1^r \pmod{p}$ ,  $1 \leq d_1 < p$  인 정수  $d_1$  를 구하여라.
- (2)  $s \equiv a^r \pmod{p}$ ,  $1 \leq s < p$  인 정수  $s$  를 구하여라.
- (3)  $rr^{-1} \equiv 1 \pmod{q}$ ,  $1 \leq r^{-1} < q$  인 정수  $r^{-1}$  를 구하여라.
- (4)  $k_1 = 4$ ,  $k_2 = 3$  일 때,

$$c \equiv s^{k_1} d_1^{k_2} \pmod{p}, \quad 1 \leq c < p$$

$$e \equiv c^{r^{-1}} \pmod{p}, \quad 1 \leq e < p$$

인 정수  $c, e$  를 구하여  $a^{k_1} g_1^{k_2} \equiv e \pmod{p}$  임을 확인하여라.

[풀이] (1)  $d_1 \equiv g_1^r \equiv 4^5 = 1024 \equiv 28 \pmod{83}$  이므로  $d_1 = 28$  이다.

$$(2) s \equiv a^r \equiv 7^5 \equiv 7^2 \cdot 7^3 = 49 \cdot 11 \equiv 539 \equiv 41 \pmod{83}$$

이므로  $s = 41$  이다.

(3) 유클리드의 알고리즘(정리 1.2.5) 에 의하여

$$41 \cdot 1 + 5 \cdot (-8) = 1$$

$$5 \cdot (-8) \equiv 1 \pmod{41}$$

이므로  $5 \cdot 33 \equiv 1 \pmod{41}$  이다.

따라서  $r^{-1} = 33$  이다.

(4)  $k_1 = 4$ ,  $k_2 = 3$  일 때,

$$c \equiv s^{k_1} d_1^{k_2} \equiv 41^4 \cdot 28^3 \equiv 21^2 \cdot 40$$

$$\equiv 26 \cdot 40 \equiv 1040 \equiv 44 \pmod{83}$$

$$e \equiv 44^{33} \equiv (44^3)^{11} \equiv 26^{11} \equiv 31 \pmod{83}$$

이므로  $c = 44$ ,  $e = 31$  이다. 그리고 다음이 성립한다.

$$a^{k_1} g_1^{k_2} \equiv 7^4 \cdot 4^3 \equiv 2401 \cdot 64$$

$$\equiv 77 \cdot 64 \equiv 4928 \equiv 31 \equiv e \pmod{83}$$

8
1 0 1
0 1 -8

$$\begin{array}{r|rr} 8 & 41 & 5 \\ & 40 & 5 \\ \hline & 1 & 0 \end{array} \quad \begin{array}{l} 5 \\ 5 \\ 0 \end{array}$$

8
1 0 1
0 1 -8

2. 두 홀수인 素數  $p = 2q + 1 = 23$ ,  $q = 11$  에 대하여  $\text{ord}_p 2 = 11 = q$  임을 이용하여 다음 물음에 답하여라(보기 3.5.4 참조).

(1)  $g_1 = 2$ ,  $r = 13$  일 때

$$d_1 \equiv g_1^r \pmod{p}, \quad 1 \leq d_1 < p$$

인 정수  $d_1$  을 구하여라.

(2)  $a = 18$  일 때,

$$s \equiv a^r \pmod{p}, \quad 1 \leq s < p$$

인 정수  $s$  를 구하여라.

(3)  $rr^{-1} \equiv 1 \pmod{q}$ ,  $1 \leq r^{-1} < q$  인 정수  $r^{-1}$  를 구하여라.

(4)  $k_1 = 8$ ,  $k_2 = 9$  일 때,

$$c \equiv s^{k_1} d_1^{k_2} \pmod{p}, \quad 1 \leq c < p$$

$$e \equiv c^{r^{-1}} \pmod{p}, \quad 1 \leq e < p$$

인 정수  $c, e$  를 구하여  $a^{k_1} g_1^{k_2} \equiv e \pmod{p}$  임을 확인하여라.

[풀이] (1)  $\text{ord}_{23} 2 = 11 = q$  즉  $2^{11} \equiv 1 \pmod{23}$  이므로

$$d_1 \equiv g_1^r \equiv 2^{13} \equiv 2^{11} \cdot 2^2 = 1 \cdot 2^2 \equiv 4 \pmod{23}$$

이고 따라서  $d_1 = 4$  이다.

(2)  $a = 18$  일 때,

$$\begin{aligned} s &\equiv a^r \equiv 18^{13} \equiv (2^6)^{13} \equiv 2^{78} \\ &\equiv (2^{11})^7 \cdot 2 \equiv 1^7 \cdot 2 \equiv 2 \pmod{23} \end{aligned}$$

이므로  $s = 2$  이다.

(3) 유클리드의 알고리즘에 의하여 다음이 성립한다.

$$13 \cdot 6 + 11 \cdot 7 = 1,$$

$$13 \cdot 6 \equiv 1 \pmod{11}$$

따라서  $r^{-1} = 6$  이다.

(4)  $k_1 = 8, k_2 = 9$  일 때,

$$\begin{aligned} c &\equiv s^{k_1} d_1^{k_2} \equiv 2^8 \cdot 4^9 \\ &\equiv 2^{26} \equiv (2^{11})^2 \cdot 2^4 \equiv 2^4 \equiv 16 \pmod{23} \end{aligned}$$

이므로  $c = 16$  이다. 또,

$$\begin{aligned} e &\equiv 16^6 \equiv 2^{24} \\ &\equiv (2^{11})^2 \cdot 2^2 \equiv 2^2 \equiv 4 \pmod{23} \end{aligned}$$

이므로  $e = 4$  이다.

그리고, 다음이 성립한다.

$$\begin{aligned} a^{k_1} g_1^{k_2} &\equiv 18^8 \cdot 2^9 \equiv 2^6 \cdot 2^9 \equiv 2^{13} \\ &\equiv 2^{11} \cdot 2^2 \equiv 4 \equiv e \pmod{23} \end{aligned}$$



## 연 습 문 제 (3.6)

1. 이차합동식  $x^2 \equiv 7 \pmod{103}$ 의 해가 존재하는지를 판정하여라.

[풀이] 정리 3.6.6에 의하여 다음이 성립한다.

$$\begin{aligned} \left( \frac{7}{103} \right) &= (-1)^{\frac{7-1}{2} \frac{103-1}{2}} \left( \frac{103}{7} \right) = - \left( \frac{103}{7} \right) \\ &= - \left( \frac{5}{7} \right) = (-1)(-1)^{\frac{5-1}{2} \frac{7-1}{2}} \left( \frac{7}{5} \right) \\ &= - \left( \frac{2}{5} \right) = (-1)(-1)^{\frac{25-1}{8}} = 1 \end{aligned}$$

따라서 이차합동식  $x^2 \equiv 7 \pmod{103}$ 의 해는 존재한다.

2. 양의 정수  $m = 11 \cdot 19$ 에 대하여 이차합동식  $x^2 \equiv 2^2 \pmod{m}$ 의 해를 구하여라.

[풀이] 이차합동식  $x^2 \equiv 2^2 \pmod{m}$ 는 다음 연립합동식과 동치이다.

$$\begin{cases} x^2 \equiv 2^2 \pmod{11} \\ x^2 \equiv 2^2 \pmod{19} \end{cases}$$

그런데 이차합동식  $x^2 \equiv 2^2 \pmod{11}$ 의 해는  $x \equiv \pm 2 \pmod{11}$ 이고 또 이차합동식  $x^2 \equiv 2^2 \pmod{19}$ 의 해는  $x \equiv \pm 2 \pmod{19}$ 이므로, 이차합동식  $x^2 \equiv 2^2 \pmod{m}$ 의 해는 다음 네 연립일차합동식의 해를 구하여 얻는다.

$$\begin{array}{ll} \textcircled{1} \begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 2 \pmod{19} \end{cases} & \textcircled{2} \begin{cases} x \equiv -2 \pmod{11} \\ x \equiv 2 \pmod{19} \end{cases} \\ \textcircled{3} \begin{cases} x \equiv -2 \pmod{11} \\ x \equiv -2 \pmod{19} \end{cases} & \textcircled{4} \begin{cases} x \equiv 2 \pmod{11} \\ x \equiv -2 \pmod{19} \end{cases} \end{array}$$

그런데, 이들 네 연립이차합동식의 해는 중국인의 나머지 정리(정리 1.3.8)를 이용하여 구한다.

실제로, 유클리드의 알고리즘에 의하여

$$19 \cdot (-4) + 11 \cdot 7 = 1$$

이므로 이들 네 연립이차합동식의 해는 다음과 같다.

$$\begin{aligned} x &\equiv 19 \cdot (-4) \cdot 2 + 11 \cdot 7 \cdot 2 \equiv 2 \pmod{209}, \\ x &\equiv 19 \cdot (-4) \cdot (-2) + 11 \cdot 7 \cdot 2 \equiv 97 \pmod{209}, \\ x &\equiv -2 \equiv 207 \pmod{209}, \\ x &\equiv -97 \equiv 112 \pmod{209} \end{aligned}$$

$$\begin{array}{r|rr|r} 1 & 19 & 11 & 1 \\ & \underline{11} & \underline{-8} & \\ 2 & 8 & 3 & 1 \\ & \underline{6} & \underline{2} & \\ 2 & 2 & 1 & \\ & \underline{2} & & \\ & 0 & & \end{array}$$

1	1	2	1		
1	0	1	-1	3	-4
0	1	-1	2	-5	7

3. 이차합동식  $x^2 \equiv 860 \pmod{11021}$  에서  $11021 = 103 \cdot 107$  이고 따라서 이 이차합동식은 다음 연립합동식과 동치이다.

$$\begin{cases} x^2 \equiv 860 \equiv 36 \equiv 6^2 \pmod{103} \\ x^2 \equiv 860 \equiv 4 \equiv 2^2 \pmod{107} \end{cases}$$

이 사실을 이용하여 다음 물음에 답하여라.

- (1) 주어진 이차합동식의 해

$$x \equiv \pm x_1 \pmod{m}, x \equiv \pm x_2 \pmod{m}$$

를 구하여라.

- (2)  $(x_1 + x_2, 11021) = 103$  또는  $107$  임을 확인하여라.

- (3) 다음이 성립함을 확인하여라.

$$\begin{aligned} \left(\frac{6}{103}\right) &= -1, & \left(\frac{-6}{103}\right) &= 1, \\ \left(\frac{2}{107}\right) &= -1, & \left(\frac{-2}{107}\right) &= 1 \end{aligned}$$

- (4) 이차합동식  $x^2 \equiv 860 \pmod{11021}$  의 해 중에서 이차잉여인 해는

$$x \equiv 19012 \pmod{11021}$$

임을 밝혀라.

[풀이] (1) 두 이차합동식

$$x^2 \equiv 860 \equiv 36 \equiv 6^2 \pmod{103},$$

$$x^2 \equiv 860 \equiv 4 \equiv 2^2 \pmod{107}$$

의 해는 각각  $x \equiv \pm 6 \pmod{103}$ ,  $x \equiv \pm 2 \pmod{107}$  이다.

이제 다음 네 연립일차합동식의 해를 구해 보자.

$$\textcircled{1} \begin{cases} x \equiv 6 \pmod{103} \\ x \equiv 2 \pmod{107} \end{cases} \quad \textcircled{2} \begin{cases} x \equiv -6 \pmod{103} \\ x \equiv 2 \pmod{107} \end{cases}$$

$$\textcircled{3} \begin{cases} x \equiv -6 \pmod{103} \\ x \equiv -2 \pmod{107} \end{cases} \quad \textcircled{4} \begin{cases} x \equiv 6 \pmod{103} \\ x \equiv -2 \pmod{107} \end{cases}$$

유클리드 알고리즘을 이용하여

$$107N_1 + 103N_2 = 1$$

인 정수  $N_1, N_2$  를 구하면  $N_1 = 26$ ,  $N_2 = -27$  이므로

$$x_1 = 107 \cdot 26 \cdot 6 + 103 \cdot (-27) \cdot 2 = 11130,$$

$$x_2 = 107 \cdot 26 \cdot (-6) + 103 \cdot (-27) \cdot 2 = -22254$$

이라고 놓으면, 위의 네 연립일차합동식의 해는 각각 다음과 같다.

$$x \equiv x_1 \equiv 11130 \equiv 109 \pmod{11021},$$

$$x \equiv x_2 \equiv -22254 \equiv -212 \pmod{11021},$$

$$x \equiv -x_2 \equiv 22254 \equiv 212 \pmod{11021},$$

$$x \equiv -x_1 \equiv -109 \equiv 10912 \pmod{11021}$$

이것이  $x^2 \equiv 860 \pmod{11021}$  의 4 개의 해이다.

(2) 위의 결과에 의하여 다음이 성립한다.

$$x_1 + x_2 = 11130 - 22254 = -11124, \quad (x_1 + x_2, 11021) = 103$$

$$x_1 - x_2 = 11130 + 22254 = 33384, \quad (x_1 - x_2, 11021) = 107$$

(3) 따름정리 3.6.7 과 정리 3.6.4를 이용하여 다음 결과를 얻는다.

여기서  $103 \equiv 3 \pmod{4}$ ,  $107 \equiv 3 \pmod{4}$  이다.

$$\begin{aligned} \left(\frac{6}{103}\right) &= \left(\frac{2}{103}\right)\left(\frac{3}{103}\right) = (-1) \\ &= \left(\frac{3}{103}\right) = -\left(\frac{103}{3}\right) = -\left(\frac{1}{3}\right) = -1, \\ \left(\frac{2}{107}\right) &= (-1)^{\frac{107^2-1}{8}} = -1 \\ \left(\frac{-6}{103}\right) &= 1, \quad \left(\frac{-2}{107}\right) = 1 \end{aligned}$$

(4) 이차합동식  $x^2 \equiv 860 \pmod{11021}$  의 해 중에서 이차잉여인 해

$$x \equiv x_0 \pmod{11021}$$

는 다음 연립일차합동식의 해이다.

$$\begin{cases} x \equiv -6 \pmod{103} \\ x \equiv -2 \pmod{107} \end{cases}$$

따라서 앞의 결과에 의하여 구하는 해는 다음과 같다.

$$x \equiv x_0 \equiv -x_1 \equiv 10912 \pmod{11021}$$