$2^h(h>2)$ を法とする既約剰余系

補題 1 素数 p について，$e>1,(k,p)=1$ のとき

$$(1+kp^e)^p = 1+k'p^{e+1} \tag{1}$$

と表され,

$$(k',p)=1$$

である.

[証明](1) の左辺を展開すると

$$\begin{aligned}(1+kp^e)^p &= 1+kp^{e+1}+k^2\frac{p^{2e+1}(p-1)}{2}+\cdots+k^pp^{ep}\\ &= 1+p^{e+1}\left(k+k^2\frac{p^e(p-1)}{2}+k^3\frac{p^{2e}(p-1)(p-2)}{6}+\cdots+k^pp^{ep-e-1}\right)\end{aligned}$$

$k'=k+k^2\dfrac{p^e(p-1)}{2}+k^3\dfrac{p^{2e}(p-1)(p-2)}{6}+\cdots+k^pp^{ep-e-1}$ とおくと，$e>1$ なので

$$k\equiv k' \pmod p$$

$$\therefore (k',p)=1$$

[証明おわり]

補題 2 m が a に対応する指数であるとき,

$$a^0(=1),a,a^2,a^3,\cdots,a^{m-1} \tag{2}$$

は全て不合同である.

[証明] もし $a^h\equiv a^k(h>k)$ ならば $a^k(a^{h-k}-1)\equiv 0$ つまり $a^{h-k}\equiv 1$ となり，m より小さい指数で 1 が実現してしまうこととなりこれは矛盾である. [証明おわり]

定理 1 $2^h(h>2)$ を法とするとき，$\phi(2^h)=2^{h-1}$ の規約類は次の数によって代表される.

$$(-1)^\alpha 3^\beta,\quad \begin{pmatrix}\alpha=0,1\\ \beta=0,1,2,\cdots,2^{h-2}-1\end{pmatrix}$$

[証明] 補題 1 より

$$\begin{aligned}3^2 &= 1+1\cdot 2^3\\ 3^{2^2} &= (1+2^3)^2 = 1+k'2^4,\quad (k',2)=1,\\ 3^{2^3} &= (1+2^3)^{2^2} = \left(1+k'2^4\right)^2 = 1+k''2^5,\quad (k'',2)=1,\\ 3^{2^4} &= (1+2^3)^{2^3} = \left(1+k''2^5\right)^2 = 1+k'''2^6,\quad (k''',p)=1,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ 3^{2^{h-2}} &= (1+2^3)^{2^{h-1}} = \left(1+k^{(h-4)}2^{h-1}\right)^2 = 1+k^{(h-3)}2^h,\quad \left(k^{(h-3)},2\right)=1\end{aligned}$$

つまり，3 は 2^{h-2} 乗して始めて $1(\mathrm{mod}\ 2^h)$ となる．つまり指数 2^{h-2} に対応する．補題 2 より

$$3^\beta, (\beta = 0, 1, 2, \cdots, 2^{h-2} - 1) \tag{3}$$

は全て不合同である．また 2^h を法とする既約類，つまり奇数は全てで

$$2^{h-1}\text{個}$$

であるが，(3) は 2^{h-2} 個つまり半分しかない．またこれらは $8n+1$ または $8n+3$ の形をしていることがわかる．残りの奇数は

$$-3^\beta$$

によって代表される．したがって全ての既約類は，

$$(-1)^\alpha 3^\beta, \quad \left(\begin{array}{l} \alpha = 0, 1 \\ \beta = 0, 1, 2, \cdots, 2^{h-2} - 1 \end{array} \right)$$

によって代表される． [証明おわり]

$$a = (-1)^\alpha 3^\beta$$

とおくと，二つの指数として次のようなものを定義することができる．

$$\mathrm{Ind}^{(1)} a = \alpha \pmod 2, \quad \mathrm{Ind}^{(2)} a = \beta \pmod{2^{h-2}}$$

通常の指数と違って底というものは存在しない．$b = (-1)^{\alpha'} 3^{\beta'}$ とおくことにより次の性質を容易に導くことができる．

$$\begin{aligned} \mathrm{Ind}^{(1)}(ab) &\equiv \mathrm{Ind}^{(1)} a + \mathrm{Ind}^{(1)} b \pmod 2 \\ \mathrm{Ind}^{(2)}(ab) &\equiv \mathrm{Ind}^{(2)} a + \mathrm{Ind}^{(2)} b \pmod{2^{h-2}} \end{aligned}$$

また

$$\begin{aligned} \mathrm{Ind}^{(1)}(a^n) &\equiv n\mathrm{Ind}^{(1)} a \pmod 2 \\ \mathrm{Ind}^{(2)}(a^n) &\equiv n\mathrm{Ind}^{(2)} a \pmod{2^{h-2}} \end{aligned}$$

法 $32 = 2^5$ を例にとって指数表を作ってみよう．

$$1, 3, 3^2 = 9, 3^3 = 27, 3^4 = 81 \equiv 17, 3^5 \equiv 51 \equiv 19, 3^6 \equiv 57 \equiv 25, 3^7 \equiv 75 \equiv 11$$

$$-1 \equiv 31, -3 \equiv 29, -3^2 \equiv 23, -3^3 = 5, -3^4 \equiv 15, -3^5 \equiv 13, -3^6 \equiv 7, -3^7 \equiv 21$$

$$N \equiv (-1)^{I^{(1)}} 3^{I^{(2)}} \pmod{32}$$

N	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
$I^{(1)}$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
$I^{(2)}$	0	1	3	6	2	7	5	4	4	5	7	2	6	3	1	0

この表によって $9x = 13 \pmod{32}$ を解いてみる．

$$\mathrm{Ind}^{(1)}9 + \mathrm{Ind}^{(1)}x \equiv \mathrm{Ind}^{(1)}13 \pmod{2}$$
$$\mathrm{Ind}^{(2)}9 + \mathrm{Ind}^{(2)}x \equiv \mathrm{Ind}^{(2)}13 \pmod{8}$$

よって表から

$$\mathrm{Ind}^{(1)}x \equiv 1 \pmod{2}$$
$$\mathrm{Ind}^{(2)}x \equiv 3 \pmod{8}$$
$$\therefore \quad x \equiv 5 \pmod{32}$$

問題 1 α は奇数とする．$h \geq 3$ ならば，$x^2 \equiv a \pmod{2^h}$ は $a \equiv 1 \pmod{8}$ のときに限って解を有する．またそのとき四つの解を有する．このことを証明せよ．

[解] 指数を用いると，

$$2\mathrm{Ind}^{(1)}x \equiv \mathrm{Ind}^{(1)}a \pmod{2} \tag{4}$$
$$2\mathrm{Ind}^{(2)}x \equiv \mathrm{Ind}^{(2)}a \pmod{2^{h-2}} \tag{5}$$

解があるための条件は，

$$\mathrm{Ind}^{(1)}a \equiv 0 \pmod{2}$$
$$\mathrm{Ind}^{(2)}a \equiv 0 \pmod{2}$$

すなわち，

$$a \equiv 3^{2f} \pmod{2^h}$$

と表せる．つまりこれは 2^h の既約剰余系のうちの半分のさらに半分つまり 4 分の 1 を表している．これらはすべて，

$$a = 8n + 1$$

の形で表せるものばかりであり，つまりは

$$a \equiv 1 \pmod{8}$$

である．(4) の解は 2 つであり，

$$\mathrm{Ind}^{(1)}x = 0, 1$$

(5) の解も 2 つであり，

$$\mathrm{Ind}^{(2)}x = \frac{1}{2}\mathrm{Ind}^{(2)}a, \frac{1}{2}\mathrm{Ind}^{(2)}a + 2^{h-3}$$

つまり x の解は四つである． [証明おわり]

実際

$$x^2 \equiv 1 \pmod{2^h, h \geq 3}$$

の解は

$$x \equiv \pm 1, \pm 1 + 2^{h-1}$$

である．

参考文献

[1] 高木貞治『初等整数論講義第 2 版』（共立出版社，1997 年）