# 指数 (Index)

文字は全て整数とする．$p$ は素数とする．

**定義 1** $p$ を法とする原始根のうちの一つを $r$ とする．$a \not\equiv 0 \pmod{p}$ である任意の $a$ について

$$r^{\alpha} \equiv a \pmod{p} \tag{1}$$

を満たす $\alpha$ を $r$ を底としての $a$ の**指数** (Index) といい，

$$\alpha \equiv \mathrm{Ind}_r a \pmod{p-1}$$

と表す．標数と呼ぶこともある．底が明らかな場合は Ind. と書くこともある．

当然のことながら次の定理が成り立つ．

**定理 1**

$$a \equiv b \pmod{p} \Longleftrightarrow \mathrm{Ind}.a \equiv \mathrm{Ind}.b \pmod{p-1}$$

指数法則がもともと成り立っているので，対数と同様の性質をもつ．

**定理 2**

$$\mathrm{Ind}.ab \equiv \mathrm{Ind}.a + \mathrm{Ind}.b \pmod{p-1}$$

$$\mathrm{Ind}.a^n \equiv n\mathrm{Ind}.a \pmod{p-1}$$

[証明略]

数値計算において対数表が便利であったのと同様に，合同式においても指数表を用いれば計算が容易である．底の変換に関しても対数と同様である．

**定理 3**

$$\mathrm{Ind}_{r'} a \equiv \mathrm{Ind}_{r'} r \mathrm{Ind}_r a \pmod{p-1}$$

指数表においては底がある一つの原始根に定めてあるので，他の原始根を使いたい場合はこの変換を行えばよい．$p = 19$ の指数表を表 1 に示す．

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha$ | 0 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |

表 1

この表は $\alpha = 1$ のところを見ると $a = 10$ となっているところから底が 10 であることがわかる．実際 19 の原始根は 2,3,10,13,14,15 の 6 個であるので，底の取り方によって指数表の内容が変る．他の原始根が必要であれば既知の原始根を $p-1$ と互いに素である数で累乗してやれば求めることができる．また，$a$ が小さい順に並んだ表もあれば，$\alpha$ が順に並んでいるものもある．上下が逆になっているものもある．どちらにしても 0 のあるほうが指数である．

指数表を使っていくつかの問題を解いてみよう．使用する表は表 1 である．つまり $p = 19, r = 10$ とする．

**問題 1** 指数を求めよ.

(1) Ind.155
(2) Ind.(-1)

[解]

(1) Ind.155=Ind.3=5
(2) ind.(-1)=Ind.(18)=9

**問題 2** 次の式を満たす $x$ を求めよ.

(1) $\mathrm{Ind}.x = 7$
(2) $\mathrm{Ind}.x = -1$

[解]

(1) 表より $x = 15$
(2) $\mathrm{Ind}.x \equiv 17$ より $x = 2$

**問題 3** 次の合同式を解け.

(1) $13x \equiv 7 \pmod{19}$
(2) $x^2 \equiv 15$
(3) $x^2 \equiv 17$
(4) $x^2 + 9x \equiv 5$
(5) $x^3 \equiv 7$

[解]

(1) $\mathrm{Ind}.13x \equiv \mathrm{Ind}.7$
$\mathrm{Ind}.13 + \mathrm{Ind}.x \equiv \mathrm{Ind}.7$
$13 + \mathrm{Ind}.x \equiv 12$
$\mathrm{Ind}.x \equiv -1$
$\mathrm{Ind}.x \equiv 17$
$x \equiv 2 \pmod{19}$
(2) $2\mathrm{Ind}.x = \mathrm{Ind}.15$
$2\mathrm{Ind}.x = 7 \pmod{18}$
18 を法とする場合，左辺は必ず偶数となるため，解なし.
(3) $2\mathrm{Ind}.x \equiv \mathrm{Ind}.17$
$2\mathrm{Ind}.x \equiv 8 \pmod{18}$
$\mathrm{Ind}.x \equiv 4 \pmod{9}$
$\mathrm{Ind}.x \equiv 4, 13( \pmod{18}$
$x \equiv 6, 13 \pmod{19}$
(4) $x^2 - 10x \equiv 5$
$x^2 - 10x + 25 \equiv 30$
$(x-5)^2 \equiv 11$
$2\mathrm{Ind}.(x-5) \equiv \mathrm{Ind}.11$
$2\mathrm{Ind}.(x-5) \equiv 6 \pmod{18}$
$\mathrm{Ind}.(x-5) \equiv 3 \pmod{9}$
$\mathrm{Ind}.(x-5) \equiv 3, 12 \pmod{18}$
$x - 5 \equiv 12, 7 \pmod{19}$

(5) $3\mathrm{Ind}.x \equiv \mathrm{Ind}.7 \pmod{18}$
$3\mathrm{Ind}.x \equiv 12 \pmod{18}$
$\mathrm{Ind}.x \equiv 4 \pmod{6}$
$\mathrm{Ind}.x \equiv 4, 10, 16 \pmod{18}$
$x \equiv 6, 9, 4 \pmod{19}$

**定理 4** 奇素数 $p$ を法として，任意の底について

$$\mathrm{Ind}.(-1) = \frac{p-1}{2}$$

[証明]

$$r^{p-1} - 1 = \left(r^{\frac{p-1}{2}} + 1\right)\left(r^{\frac{p-1}{2}} - 1\right) \equiv 0$$

$r$ は原始根だから

$$r^{\frac{p-1}{2}} \not\equiv 1$$

$$\therefore r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

[証明おわり]

**定理 5** $k$ が $p-1$ で割り切れないとき

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

[証明]$p$ を法とする原始根を $r$ とすると，

$$r0, r, r^2, \cdots, r^{p-2}$$

は $p$ を法とする既約剰余系をなす．よって，左辺は順序が変るが次のように変形できる．

$$1 + r^k + (r^2)^k + \cdots + (r^{p-2})^k = 1 + r^k + r^{2k} + \cdots + r^{(p-2)k}$$

初項 1，公比 $r^k$ の等比級数なので，左辺はさらに変形できて

$$\frac{r^{k(p-1)} - 1}{r^k - 1}$$

$r^{p-1} \equiv 1$ であり，かつ $k$ は $p-1$ の倍数ではないので分母は 0 にはならない．

$$\therefore \text{左辺} \equiv 0$$

[証明おわり]

**定理 6** （Wilson の定理）$p$ が素数ならば

$$(p-1)! \equiv -1 \pmod{p}$$

[証明]$p = 2$ のときは明らかに成り立つ．奇素数 $p$ を法とする原始根を $r$ とすると，定理 5 の証明と同様に，順序は変るが

$$\begin{aligned}(p-1)! &\equiv 1 \times r \times r^2 \times \cdots \times r^{p-2} \\ &= r^{1+2+3+\cdots+(p-1)} \\ &= r^{\frac{(p-1)(p-2)}{2}} \\ &= \left(r^{\frac{p-1}{2}}\right)^{p-2} \\ &\equiv (-1)^{p-2}\end{aligned}$$

$p-2$ は奇数なので

$$(p-1)! \equiv -1$$

[証明おわり]

**定理 7** $a$ が $p$ で割り切れないとき，合同式

$$x^n \equiv a \pmod{p}$$

が解を有するための必要十分条件は

$$a^f \equiv 1 \pmod{p}$$

である．ただし $f = \dfrac{p-1}{(n, p-1)}$.

[証明]$p$ を法とする原始根を $r$ とすると，

$$x^n \equiv a \pmod{p}$$

$$\Updownarrow$$

$$n\mathrm{Ind}.x \equiv \mathrm{Ind}.a \pmod{p-1}$$

$\mathrm{Ind}.x = X, \mathrm{Ind}.a = A$ とすると，この合同式の解の有無は

$$nX \equiv A \pmod{p-1}$$

の解の有無と同値．この合同式が解をもつ条件は

$$A \equiv k(n, p-1) \pmod{p-1}$$

と表せることである．つまり

$$\mathrm{Ind}.a \equiv k(n, p-1) \pmod{p-1}$$

$$\Updownarrow$$

$$a \equiv r^{k(n,p-1)} \pmod{p}$$

$$\Updownarrow$$

$$a^f \equiv r^{k(n,p-1)\frac{p-1}{(n,p-1)}} \pmod{p}$$

$$\Updownarrow$$

$$a^f \equiv r^{k(p-1)} \pmod{p}$$

$$\Updownarrow$$

$$a^f \equiv 1 \pmod{p}$$

[証明おわり]

解があるとき，その解の個数は $(n, p-1)$ 個 である．

合同式 $x^n \equiv a \pmod{p}$ が解をもつとき $a$ を $p$ の $n$ **冪剰余**という．解をもたないとき $a$ を $p$ の**非剰余** という．$p$ の $n$ **冪剰余**の個数は $f = \dfrac{p-1}{(n, p-1)}$ 個 である．

指数という命名は果たして妥当であろうか．対数に対する指数と同じであるために大変紛らわしい．Index と Exponent の訳語と考えれば，あるいは前者が指数にふさわしく，後者が不適切なのかも知れない．とくに $a$ の指数と言った場合，整数論とそれ以外では違うものを指すことになるのではないだろうか．どちらにしても Ind と log が類似しているだけに釈然としないものを感じる．

## 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）