整 数 の 性 質

整数の集合は，「負の整数」，「0」，「正の整数(自然数)」の 3 つに分類することができ，

$$\underbrace{\{\cdots,\ -3,\ -2,\ -1\}}_{\text{負の整数}},\ \{0\},\ \underbrace{\{1,\ 2,\ 3,\ \cdots\}}_{\text{正の整数(自然数)}}$$

ここでは，このような『整数』の性質について学んでいくわけですが，小学校以来ずっと慣れ親しんできている題材ですので，皆さんがすでに知っている知識，当たり前だと思っている性質が多数出てきます。これらを体系的にまとめていきながら，様々な問題を解くための基礎事項を学んでいきます。

なお，本プリントでは整数の集合を $\mathbb{Z}$ と表し，自然数の集合を $\mathbb{N}$ と表します。

$$\mathbb{Z}=\{\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots\},\ \mathbb{N}=\{1,\ 2,\ 3,\ \cdots\}$$

($\mathbb{Z}$ はドイツ語の『Zahlen』，$\mathbb{N}$ は英語の『Natural number』の頭文字)

§1　約数と倍数

ある整数 N が $N=ak$ $(a,\ k\in\mathbb{Z},\ a\neq 0)$ と表されるとき，N は a の**倍数**，a は N の**約数**または**因数**という。例えば，$6=2\times 3$ なので，6 は 2，3 の倍数，2，3 は 6 の約数または因数となる。
なお，$k=0$ のとき $N=0$ となることから，**0 はすべての数の倍数**となることが分かる。

例 1　次の整数の正の約数をすべて求めなさい。

(1)　24　　　　(2)　29

(1)　$24=1\times 24,\ 2\times 12,\ 3\times 8,\ 4\times 6$ より，
24 の約数は 1，2，3，4，6，8，12，24 の 8 個となる。

(2)　$29=1\times 29$ より，
29 の約数は 1，29 の 2 個となる。

(1)において，約数 2 を見つけると，$24=2\times 12$ より約数 12 が見つかります。同様に，約数 3 を見つければ 8 も同時に見つかるというわけです。つまり一般的には，整数 n の約数を見つけるには，$\sqrt{n}$ 以下の自然数について調べれば十分ということが分かります。

例 2　3 桁の自然数 N が次の整数の倍数となるための条件を求めなさい。

(1)　2 の倍数　　(2)　3 の倍数　　(3)　4 の倍数　　(4)　5 の倍数

自然数 N は $N = 100a + 10b + c$ $\left(a,\ b,\ c \in \mathbb{Z},\ 1 \leqq a \leqq 9,\ 0 \leqq b \leqq 9,\ 0 \leqq c \leqq 9\right)$ と表せる。

(1)　$N = 2(50a + 5b) + c$

$2(50a + 5b)$ は 2 の倍数となるので，N が 2 の倍数になるには，c が 2 の倍数となればよい。

つまり，1 の位が 2 の倍数となればよい。

(2)　$N = 3(33a + 3b) + a + b + c$

$3(33a + 3b)$ は 3 の倍数となるので，N が 3 の倍数になるには，$a + b + c$ が 3 の倍数となればよい。

つまり，各位の和が 3 の倍数となればよい。

(3)　$N = 4 \cdot 25a + 10b + c$

$4 \cdot 25a$ は 4 の倍数となるので，N が 4 の倍数になるには，$10b + c$ が 4 の倍数となればよい。

つまり，下 2 桁が 4 の倍数となればよい。

(4)　$N = 5(20a + 2b) + c$

$5(20a + 2b)$ は 5 の倍数となるので，N が 5 の倍数になるには，c が 5 の倍数となればよい。

つまり，1 の位が 5 の倍数となればよい。

なお，この 例 2 では 3 桁の自然数においての証明だったが，一般的に n 桁としても同じように証明することができる。また，(2)において，$N = 9(11a + b) + a + b + c$ とすることで，9 の倍数になる条件も 3 の倍数となる条件と同じになることが分かる。

○　素数

1とその数自身でしか割り切れない数を**素数**といい，素数の積の形で表される自然数を**合成数**という。なお，1は素数にも合成数にも含まれない。
まずは素数の性質の確認から見ていきましょう。

①　素数は無数に存在する

これは素数が有限であると仮定し，矛盾を導くことで解決します。

証明
素数が有限個であると仮定する。今それらを a_1，a_2，a_3，…，a_n とおく。
このとき，自然数 $q = a_1a_2a_3 \ \cdots \ a_n + 1$ について考える。
（ｉ）　q が素数であるとき
　このとき，q は a_1，a_2，a_3，…，a_n のどれとも異なるので新たな素数となり，仮定に反する
（ⅱ）　q が素数でないとき
　このとき，q は素数 a_1，a_2，a_3，…，a_n のどれかで割り切れなくてはならないが，どれで割っても必ず1余ってしまうので，q は素数となる。
　これは「q が素数でない」としたことに反する。
以上より素数は無数に存在する。

②　素数の見つけ方

実は素数は，どのようなパターンで出現するかが分かっていません。ですので，ある自然数が素数であることを調べるには，素因数がないかをひたすら割って調べる**力技**しかないのです。
ある整数以下の素数を見つけるには，**『エラトステネスのふるい』**という便利な方法があります。
これは自然数の書かれた表の中から，

（Step1）　まず，2の倍数を消去する。
（Step2）　次に，残っている数の中で最小の数の倍数，つまり3の倍数を消去する。
（Step3）　次に，残っている数の中で最小の数の倍数，つまり5の倍数を消去する。

⋮

これを繰り返していき，最後に残った数が全て素数となります。大変地道な方法ではありますが，確実に素数を見つけることができるので有効です。
では，さっそく120以下の素数を見つけてみて下さい。

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	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	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

エラトステネス（紀元前275年～紀元前194年）

○　素因数分解

ある自然数の素数の因数を**素因数**といい，ある自然数を素数のみの積で表すことを**素因数分解**という。なお，素因数分解には**「積の順序を考えなければ１通りに定まる」**という性質がある。例えば，60 を素因数分解すると，$60 = 2^2 \cdot 3 \cdot 5$ となるが，分解の仕方はこの 1 通りのみということである。

なお，1 を素数に含まないのはこの「素因数分解に一意性」を保つためである。仮に，1 を素数に含めてしまうと，$60 = 2^2 \cdot 3 \cdot 5 = 1 \cdot 2^2 \cdot 3 \cdot 5 = 1^2 \cdot 2^2 \cdot 3 \cdot 5 = \ \cdots$ というように分解の仕方が複数出てきてしまう。

例 3　整数 72 の正の約数の個数と，正の約数全部の和を求めなさい。

まず，この問題を考える前に，少し先の内容を紹介しておきます。
それは，a^0 の値です。これは，$a^1 \to a^2 \to a^3 \to\ \cdots$ というように，指数の値が増えていくと，数は a 倍になります。逆に指数が減っていくと，数は $\frac{1}{a}$ 倍になります。つまり，a^1 を $\frac{1}{a}$ 倍した数が a^0 というわけです。このことから，$a^0 = 1$ になることが分かります。

$$a^0,\ \underset{\times\frac{1}{a}}{\overset{\times a}{\rightleftarrows}}\ a^1,\ \underset{\times\frac{1}{a}}{\overset{\times a}{\rightleftarrows}}\ a^2, \cdots$$

72 は $2^3 \cdot 3^2$ と素因数分解できるので，72 の約数は素因数 2 と 3 のみで構成されていることが分かります。そして，$2^0 = 3^0 = 1$ であることを考慮すると，72 の約数は $2^a 3^b\ (0 \leqq a \leqq 3,\ 0 \leqq b \leqq 2)$ と表されることが分かります。あとは，$(a,\ b)$ の組み合わせが何通りあればよいかを考えればよいだけです。

$72 = 2^3 \cdot 3^2$ より，72 の正の約数は

$$2^a 3^b\ (0 \leqq a \leqq 3,\ 0 \leqq b \leqq 2)$$

と表すことができる。a の選び方は 4 通り，b の選び方は 3 通りあるので，
72 の約数は全部で $4 \times 3 = 12$ 個ある。

また，正の約数全部の和は

$$\begin{aligned} &2^0 3^0 + 2^0 3^1 + 2^0 3^2 + 2^1 3^0 + 2^1 3^1 + 2^1 3^2 + 2^2 3^0 + 2^2 3^1 + 2^2 3^2 + 2^3 3^0 + 2^3 3^1 + 2^3 3^2 \\ &\quad = 2^0(3^0 + 3^1 + 3^2) + 2^1(3^0 + 3^1 + 3^2) + 2^2(3^0 + 3^1 + 3^2) + 2^3(3^0 + 3^1 + 3^2) \\ &\quad = (2^0 + 2^1 + 2^2 + 2^3)(3^0 + 3^1 + 3^2) \\ &\quad = 15 \cdot 13 = 195 \end{aligned}$$

例 4　1 から 32 までの自然数の積を P とする。次の各問いに答えなさい。

（1）　P は何回 2 で割り切れますか。　　　（2）　P の末尾にはいくつ続けて 0 が並びますか。

（1）　1，2，3，⋯ ，31，32 の中で，

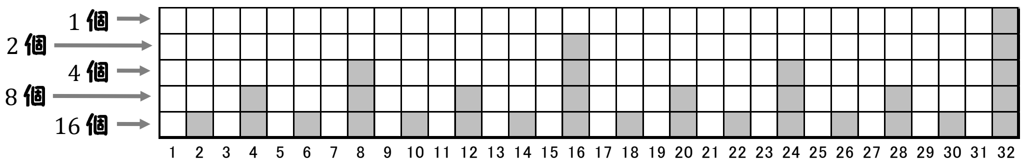
2 で割り切れる数は 16 個，2^2 で割り切れる数は 8 個，2^3 で割り切れる数は 4 個

2^4 で割り切れる数は 2 個，2^5 で割り切れる数は 1 個

よって，P が 2 で割り切れる回数は，$1+2+4+8+16=31$ 回

(1)は結局，1 から 32 までの自然数の中で，素因数 2 がいくつ含まれているかを聞かれています。つまり，下の表における色のついた部分を数えていけば終わりです。
この解答では，色のついている部分を横方向に見ながら数えています。

1 から 32 までに含まれる素因数 2 の個数



(2)は結局，10 で何回割れるかを聞かれています。$10=2\times5$ ですから，2 と 5 で何回割れるかを調べれば解決します。

（2）　1，2，3，⋯ ，31，32 の中で，

5 で割り切れる数は 6 個，5^2 で割り切れる数は 1 個

よって，P が 5 で割り切れる回数は，$1+6=7$ 回

このことと，(1)の結果から P は次のように素因数分解できる。

$$P=2^{31}\cdot3^a\cdot5^7\cdot7^b\cdots\ \left(a,\ b \text{ はある自然数}\right)$$

これより，$P=(2\cdot5)^7\cdot2^{24}\cdot3^a\cdot7^b\cdots=10^7\cdot2^{24}\cdot3^a\cdot7^b\cdots$

よって，P は末尾に 0 が 7 個並ぶことが分かる。

§2　最大公約数と最小公倍数

2 つ以上の整数において，それらに共通する約数を**公約数**といい，そのうち最大のものを**最大公約数**(greatest common divisor)という。最大公約数が 1 であるとき，それらの数は**互いに素**という。

また，2 つ以上の整数において，それらに共通する倍数を**公倍数**といい，そのうち最小のものを**最小公倍数**(least common multiple)という。

例 5　次の数の組の最大公約数と最小公倍数を求めなさい。

(1)　360，420　　　　(2)　130，231

素因数分解することで考えていきます。

(1)　$360 = 2^3 \cdot 3^2 \cdot 5$，$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$

これより，2 数に共通する因数は 2^2，3，5 なので，公約数は

$$2^a 3^b 5^c \ (0 \leqq a \leqq 2,\ 0 \leqq b \leqq 1,\ 0 \leqq c \leqq 1)$$

と表すことができる。このうち最大のものは，$2^2 \cdot 3 \cdot 5 = 60$ となる。

また，$360 = 60 \cdot 6$，$420 = 60 \cdot 7$ の公倍数のうちで最小のものは，$60 \cdot 6 \cdot 7 = 2520$

以上より，最大公約数は 60，最小公倍数は 2520

(2)　$130 = 2 \cdot 5 \cdot 13$，$231 = 3 \cdot 7 \cdot 11$

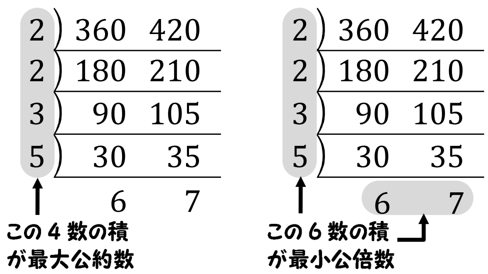
これより，2 数に共通する素因数は存在しない。

つまり，公約数は 1 のみなので，最大公約数は 1 となる。

また，最小公倍数は $130 \cdot 231 = 30030$ となる。

130 と 231 は互いに素

最小公倍数と最大公約数は右のように，2 数を共通因数で次々と割っていくことで求めてもよい。横に並べられた数の積が最大公約数で，横と下に並べられた数の積が最小公倍数となる。



また一般的には，2 数 a，b の最大公約数を G，最小公倍数を L とし，

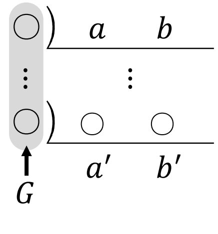
$$a = a'G,\ b = b'G \ \ (a',\ b' \text{ は互いに素})$$

とおくと，$L = a'b'G$ が成り立つ。

さらに

$$ab = a'b'G^2 = LG$$

が成り立つことが分かる。



例 6　自然数 n に対して，n と $2n+1$ が互いに素であることを示しなさい。

解①

n と $2n+1$ の最大公約数を $g(\geqq 1)$ とすると，

$n=ag$，$2n+1=bg$　$\left(a,\ b\right.$ は互いに素$\left.\right)$ とおける。

2 式から n を消去すると，

$$2ag+1=bg \quad \Leftrightarrow \quad (b-2a)g=1$$

$b-2a$ は整数より，g は 1 の約数となる。

これより，$g=1$ となるので，n と $2n+1$ は互いに素となる。

互いに素とは「2 数が 1 以外の公約数を持たない」ということです。このような否定的な命題を証明する際に便利なのが背理法です。

解②

n と $2n+1$ の素数 p を公約数に持つと仮定する。

このとき，$n=ap$　$2n+1=bp$ とおける。

2 式から n を消去すると，

$$2ap+1=bp \quad \Leftrightarrow \quad (b-2a)p=1$$

$b-2a$ は整数より，p は 1 の約数となり，これは p が素数であることに矛盾する。

以上より，n と $2n+1$ は互いに素となる。

§3　割り算の余りの性質

13 を 5 で割ったとき，商は 2，余りは 3 となるが，これは次のような式で表すことができる。

$$13 = 5 \cdot 2 + 3$$

このことを一般化すると，2 整数 a，b に対して，a を b で割ったときの商を q，余りを r とすると，a，b，q，r には次のような関係がある。

$$a = bq + r \ (0 \leqq r \leqq b - 1)$$

ここでは，割り算の余りに注目することで，様々な性質を調べていきます。

例 7　自然数 n に対して，$3n + 2$ が 5 で割り切れるような n を求めなさい。

まずは，n に自然数を片っ端から代入してみます。

$n = 1$ を代入すると，$3 \cdot 1 + 2 = 5$　適する。　　$n = 2$ を代入すると，$3 \cdot 2 + 2 = 8$　不適。
$n = 3$ を代入すると，$3 \cdot 3 + 2 = 11$　不適。　　$n = 4$ を代入すると，$3 \cdot 4 + 2 = 14$　不適。
$n = 5$ を代入すると，$3 \cdot 5 + 2 = 17$　不適。　　$n = 6$ を代入すると，$3 \cdot 6 + 2 = 20$　適する。
$n = 7$ を代入すると，$3 \cdot 7 + 2 = 23$　不適。　　$n = 8$ を代入すると，$3 \cdot 8 + 2 = 26$　不適。
⋮

代入していくとで，確実に答えを求めることはできますが，**すべての自然数について**調べることは残念ながらできません。つまり，この解法では永久に答えにたどり着くことができないのです。
そこで，自然数を 5 で割った余りでグループ分けをして，グループごとに調べていきます。

余り $0 \Rightarrow \{5,\ 10,\ 15,\ 20,\ 25,\ \cdots\} = \{5k | k$ は 0 以上の整数$\}$
余り $1 \Rightarrow \{1,\ 6,\ 11,\ 16,\ 21,\ \cdots\} = \{5k + 1 | k$ は 0 以上の整数$\}$
余り $2 \Rightarrow \{2,\ 7,\ 12,\ 17,\ 22,\ \cdots\} = \{5k + 2 | k$ は 0 以上の整数$\}$
余り $3 \Rightarrow \{3,\ 8,\ 13,\ 18,\ 23,\ \cdots\} = \{5k + 3 | k$ は 0 以上の整数$\}$
余り $4 \Rightarrow \{4,\ 9,\ 14,\ 19,\ 24,\ \cdots\} = \{5k + 4 | k$ は 0 以上の整数$\}$

k を 0 以上の整数とする。
$n = 5k$ を代入すると，$3 \cdot 5k + 2 = 15k + 2 = 5 \cdot 3k + 2$　不適。
$n = 5k + 1$ を代入すると，$3(5k + 1) + 2 = 15k + 5 = 5(3k + 1)$　適する。
$n = 5k + 2$ を代入すると，$3(5k + 2) + 2 = 15k + 8 = 5(3k + 1) + 3$　不適。
$n = 5k + 3$ を代入すると，$3(5k + 3) + 2 = 15k + 11 = 5(3k + 2) + 1$　不適。
$n = 5k + 4$ を代入すると，$3(5k + 4) + 2 = 15k + 14 = 5(3k + 2) + 4$　不適。
よって，$n = 5k + 1$ のとき，$3n + 2$ は 5 で割り切れる。

以上より，余り 1 のグループ $\{1,\ 6,\ 11,\ 16,\ 21,\ \cdots\}$ に含まれる整数がすべて答えになることが分かります。このように，ある数で割った余りで整数をグループ分けすることで，効率よくすべての整数について調べることができるわけです。なお，5 で割った余りのグループは次のように分けても構いません。

$$n = 5k,\ 5k - 1,\ 5k - 2,\ 5k - 3,\ 5k - 4\ (k \text{ は自然数})$$

○　合同式

2 つの整数 a，b と自然数 p に対して，差 $a-b$ が p で割り切れるとき，『a と b は p を法として合同』といい，

$$a \equiv b \pmod{p}$$

と表す。このような式を**合同式**という。

例　$4 \equiv 2 \pmod{2}$，$1 \equiv 7 \pmod{3}$，$2 \equiv -2 \pmod{4}$

差 $a-b$ が p で割り切れるということは，a，b を p で割った余りは等しいということを表している。
（上の例から，-2 を 4 で割った余りは 2 とみなすことができる。）

それでは，ここで合同式の性質について見ていこう。

合同式の性質

① $a \equiv a \pmod{p}$
② $a \equiv b \pmod{p}$ ならば，$b \equiv a \pmod{p}$
③ $a \equiv b \pmod{p}$，$b \equiv c \pmod{p}$ ならば，$a \equiv c \pmod{p}$

証明　両辺の差をとり，それが p の倍数であることを示せばよい。
① $a-a=0$ となり，0 は p の倍数なので成立している。
② $a \equiv b \pmod{p}$ より，$a-b=kp\ (k \in \mathbb{Z})$
　このとき，$b-a=-(a-b)=-kp$ となり，これは p の倍数である。
③ $a \equiv b \pmod{p}$，$b \equiv c \pmod{p}$ より，$a-b=kp$，$b-c=k'p\ (k,\ k' \in \mathbb{Z})$
　このとき，$a-c=a-b+b-c=kp+k'p=p(k+k')$ となり，これは p の倍数である。

また，合同式の計算法則は次のようになっている。

合同式の計算

自然数 p と整数 a，a'，b，b' に対して，$a \equiv a' \pmod{p}$，$b \equiv b' \pmod{p}$ が成り立つとき，
① $a \pm b \equiv a' \pm b' \pmod{p}$　（復号同順）
② $ab \equiv a'b' \pmod{p}$
③ $a^m \equiv (a')^m \pmod{p}$　$(m \in \mathbb{N})$

証明　上と同様，両辺の差をとり，それが p の倍数であることを示す。
$a \equiv a' \pmod{p}$，$b \equiv b' \pmod{p}$ より，$a-a'=kp$，$b-b'=k'p\ (k,\ k' \in \mathbb{Z})$
① $a \pm b-(a' \pm b')=(a-a') \pm (b-b')=kp \pm k'p=p(k \pm k')$（複号同順）
　これは p の倍数である。
② $ab-a'b'=ab-a'b+a'b-a'b'=b(a-a')+a'(b-b')=b \cdot kp+a' \cdot k'p=p(bk+a'k')$
　これは p の倍数である。
③ ②の性質を繰り返し用いると，

$$a \equiv a' \ \Rightarrow\ a^2 \equiv (a')^2 \ \Rightarrow\ a^3 \equiv (a')^3 \ \Rightarrow\ a^4 \equiv (a')^4 \ \Rightarrow\ \cdots \ \Rightarrow\ a^m \equiv (a')^m \pmod{p}$$

以上のように，和・差・積に関しては等号「=」のときと同じように計算することができる。
つまり，$a \equiv b \pmod{p}$ の両辺に同じ数を足しても，引いても，かけても構わないということである。
ただし，**商に関しては成り立たない場合がある**ので注意が必要である。
実際，$8 \equiv 2 \pmod{3}$ のときは両辺 2 で割ると，$4 \equiv 1 \pmod{3}$ は成立するが，
$8 \equiv 2 \pmod{6}$ のときは両辺 2 で割ると，$4 \equiv 1 \pmod{6}$ は成立していない。

例 8　自然数 n に対して，$3n+2$ が 5 で割り切れるような n を求めなさい。

例 7 と同じ問題ですが，合同式を用いると解答がシンプルになります。

以下 mod 5 で考える。
$n \equiv 0$ のとき　$3n+2 \equiv 3 \cdot 0+2 \equiv 2$
$n \equiv 1$ のとき　$3n+2 \equiv 3 \cdot 1+2 \equiv 5 \equiv 0$
$n \equiv 2$ のとき　$3n+2 \equiv 3 \cdot 2+2 \equiv 8 \equiv 3$
$n \equiv 3$ のとき　$3n+2 \equiv 3 \cdot 3+2 \equiv 11 \equiv 1$
$n \equiv 4$ のとき　$3n+2 \equiv 3 \cdot 4+2 \equiv 14 \equiv 4$
以上より，$n \equiv 1$ のとき，$3n+2$ は 5 で割り切れる。

例 9　30^{20} を 7 で割った余りを求めなさい。

30^{20} を計算して，それを 7 で割るのは現実的ではありません。このようなときに合同式は威力を発揮します。

以下，mod 7 で考える。
$30 \equiv 2$ より，$30^{20} \equiv 2^{20}$
$2^{20} = (2^3)^6 \cdot 2^2 = 8^6 \cdot 2^2$
$8 \equiv 1$ より，$8^6 \cdot 2^2 \equiv 1^6 \cdot 2^2 \equiv 4$
よって，余りは 4 となる。

例 10　次の合同式を満たす x を求めなさい。

(1)　$x+5\equiv 1 \pmod 3$　　(2)　$2x\equiv 7 \pmod 3$

最終的には $x\equiv a \pmod p$　$(0\leqq a\leqq p-1)$ という形で答えます。

解①

以下，mod 3 で考える。

(1)　$x+5\equiv 1$ の両辺から 5 を引くと，$x\equiv -4$

$-4\equiv 2$ より，$x\equiv 2 \pmod 3$

(2)　$2x\equiv 7$

両辺を 2 倍すると，$4x\equiv 14$

$4\equiv 1$ より，$4x\equiv 14 \iff x\equiv 14$

$14\equiv 2$ より，$x\equiv 2 \pmod 3$

解②

以下，mod 3 で考える。

(1)　$x+5\equiv 1$ の両辺に 1 を足すと，$x+6\equiv 2$

$6\equiv 0$ より，$x\equiv 2 \pmod 3$

(2)　$2x\equiv 7$

両辺に 2 を足すと，$2x+2\equiv 9$

$9\equiv 01$ より，$2(x+1)\equiv 0$

2 と 3 は互いに素より，$x+1\equiv 0$

よって，$x\equiv 2 \pmod 3$

合同式の計算において，割り算は使いにくいので，その代わりに掛け算を使うとうまくいく。
また，解②のように引き算の代わりに，足し算を使ってもよい。

なお，この問題の答えは，必ず $x\equiv 0$，$x\equiv 1$，$x\equiv 2 \pmod 3$ のどれかになるので，
与式の x に 0，1，2 をすべて代入して求めてもよい。

§4　ユークリッド互除法

ここでは，素因数分解を使わずに，最大公約数を求める方法を紹介する。
以下，2数 a，b の最大公約数を $\gcd(a,\ b)$ と表すこととする。

ユークリッド互除法

a，$b(\neq 0)$ を整数とし，a を b で割ったときの商を q，余りを r とする。つまり，$a = bq + r$ を満たしているとき，

$$\gcd(a,\ b) = \gcd(b,\ r)$$

が成り立つ。

証明　$\gcd(a,\ b) = d$，$\gcd(b,\ r) = d'$ とする。

(ｉ)　$d \geqq d'$ を示す。

d' は b，r の公約数より，$bq + r$ の約数である。つまり，a の約数。
これより，d' は a，b の公約数でもある。
a，b の最大公約数を d なので，$d \geqq d'$

(ii)　$d \leqq d'$ を示す。

$r = a - bq$
d は a，b の公約数より，$a - bq$ の約数である。つまり，r の約数。
これより，d は b，r の公約数でもある。
b，r の最大公約数を d' なので，$d \leqq d'$

(ｉ)，(ii)より，$d = d'$

これを用いると，大きな2数の最大公約数も確実に求めることができる。

例 11　3913 と 9191 の最大公約数を求めなさい。

以下，2数a，b の最大公約数を $\gcd(a,\ b)$ と表す。

$9191 = 2 \cdot 3913 + 1365$　　$3913 = 2 \cdot 1365 + 1183$　　$1365 = 1 \cdot 1183 + 182$

$1183 = 6 \cdot 182 + 91$　　$182 = 2 \cdot 91 + 0$

よって，$\gcd(9191,\ 3913) = \gcd(3913,\ 1365) = \gcd(1365,\ 1183) = \gcd(1183,\ 182)$
$= \gcd(182,\ 91) = \gcd(91,\ 0)$

となるので，最大公約数は 91 となる。

なお，ユークリッド互除法を用いると，例 6（n と $2n+1$ は互いに素となることを示しなさい）は以下のように簡単に示すことができる。
$2n + 1 = 2 \times n + 1$ より，$2n + 1$ と n の最大公約数は，n と 1 の最大公約数と等しい。
これより，$2n + 1$ と n の最大公約数は 1 となるので，n と $2n + 1$ は互いに素となる。

§5　不定方程式

方程式の数より，変数の数が多い方程式を不定方程式という。

ここでは，整数係数の不定方程式のうち有名なものをいくつか紹介していく。

○　1次不定方程式

ここでは，$ax+by+c=0$ という形の不定方程式を考えていく。

例12　x，y 整数のとき，方程式 $2x+3y=1$ を解きなさい。

この方程式を満たす整数解は無限にありますので，答えは文字を用いて表していきます。

$2x+3y=1$　…①

$x=-1$，$y=1$ は方程式①の解の1つとなるので，$2(-1)+3\cdot 1=1$　…②

①－② より，$2x-2(-1)+3y-3\cdot 1=1-1 \iff 2(x+1)+3(y-1)=0$

$\iff 2(x+1)=-3(y-1)$　…③

ここで，右辺は3の倍数なので，左辺も3の倍数となる。

2，3は互いに素なので，$x+1$ は3の倍数となる。

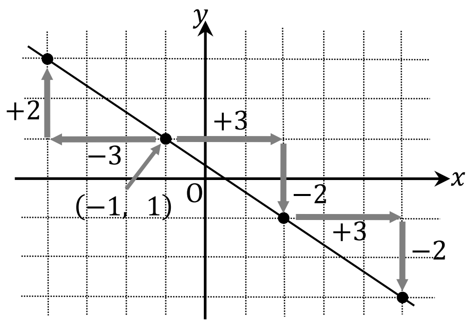
つまり，$x+1=3k \iff x=3k-1$ $(k\in\mathbb{Z})$

③に代入すると，$2\cdot 3k=-3(y-1) \iff y-1=-2k \iff y=-2k+1$

以上より，$\begin{cases} x=3k-1 \\ y=-2k+1 \end{cases}$ $(k\in\mathbb{Z})$

少し分かりにくい解答かもしれないが，座標平面上に $2x+3y=1$ のグラフをかいてみると状況をつかみやすい。

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



これより，グラフは右図のようになる。そして，この方程式の解は直線上の格子点(x 座標，y 座標がともに整数の点)となっている。そして，直線上の格子点は次の手順で見つけることができる。

(手順①)　まず，格子点を1つだけみつける。今それを $(-1,\ 1)$ とする。

(手順②)　この直線の傾きが $-\dfrac{2}{3}$ なので，「右に3，下に2」または「左に3，上に2」進むと次の格子点が見つかる。

このことから，格子点の x 座標は-1 から3ずつ離れたところ，つまり $x=3k-1$ $(k\in\mathbb{Z})$ となり，y 座標は1から2ずつ離れたところ，つまり $y=-2k+1$ $(k\in\mathbb{Z})$ となる。

この考え方を，グラフを用いずに表すと，上記のような解答になる。

なお，**答えの表し方は最初の解の選び方により変わってくる**が，どの表し方であっても，k にすべての整数を代入すれば，同じ集合となるので特に問題はない。

例 13　x，y 整数のとき，方程式 $23x+17y=1$ を解きなさい。

$23x+17y=1\quad\cdots①$

$x=3$，$y=-4$ は方程式①の解の 1 つとなるので，$23\cdot 3+17(-4)=1\quad\cdots②$

① − ② より，$23x-23\cdot 3+17y-17(-4)=1-1\quad\Leftrightarrow\quad 23(x-3)+17(y+4)=0$

$\Leftrightarrow\quad 23(x-3)=-17(y+4)\quad\cdots③$

ここで，右辺は 17 の倍数なので，左辺も 17 の倍数となる。

23，17 は互いに素なので，$x-3$ は 17 の倍数となる。

つまり，$x-3=17k\quad\Leftrightarrow\quad x=17k+3\ (k\in\mathbb{Z})$

③に代入すると，$23\cdot 17k=-17(y+4)\quad\Leftrightarrow\quad y+4=-23k\quad\Leftrightarrow\quad y=-23k-4$

以上より，$\begin{cases}x=17k+3\\ y=-23k-4\end{cases}\ (k\in\mathbb{Z})$

1 次不定方程式の解答における最大のポイントは**「解の 1 つを自力で見つける」**というところであるが，本問の場合，例 12 に比べると係数が大きいので見つけにくい。そこで，ここでは 1 次不定方程式の解の 1 つを，確実に見つける方法を紹介しておこう。

まずは，23，17 に**ユークリッド互除法**を用いていく。

$23=1\cdot 17+6\quad\Leftrightarrow\quad 6=23-1\cdot 17\quad\cdots①$

$17=2\cdot 6+5\quad\Leftrightarrow\quad 5=17-2\cdot 6\quad\cdots②$

$6=1\cdot 5+1\quad\Leftrightarrow\quad 1=6-1\cdot 5\quad\cdots③$

②，③より，5 を消去すると，$1=6-1\cdot(17-2\cdot 6)\quad\Leftrightarrow\quad 1=3\cdot 6-17$

この式に①を代入して，6 を消去すると，$1=3(23-1\cdot 17)-17\quad\Leftrightarrow\quad 1=3\cdot 23-4\cdot 17$

この式と，$23x+17y=1$ を比べることにより，解の 1 つが $x=3$，$y=-4$ と分かる。

このように，ユークリッド互除法により求まった式を**「(余り) =」の形に変形し,余りを次々と消去**していくことで，最終的に 1 次不定方程式の解を求めることができる。

また，ここでのポイントは，17 と 23 の最大公約数が 1 になっているということである。最大公約数が 1 だからこそ「1 =」の形を作ることができ，最終的に $23\cdot\bigcirc+17\cdot\square=1$ に変形することができる。

一般的に，1 次不定方程式 $ax+by=1$ は，a，b の最大公約数が 1 のとき，ユークリッド互除法を用いることにより，必ず解を 1 つ見つけることができる。

例 14　x，y 整数のとき，方程式 $159x+71y=1$ を解きなさい。

$\gcd(159,\ 71)=1$ なので，ユークリッド互除法を用いれば解が求まります。

$159=2\cdot 71+17 \iff 17=159-2\cdot 71 \quad \cdots①$

$71=4\cdot 17+3 \iff 3=71-4\cdot 17 \quad \cdots②$

$17=5\cdot 3+2 \iff 2=17-5\cdot 3 \quad \cdots③$

$3=1\cdot 2+1 \iff 1=3-1\cdot 2 \quad \cdots④$

③，④より，2 を消去すると，$1=3-(17-5\cdot 3) \iff 1=6\cdot 3-17$

この式から②を用いて 3 を消去すると，$1=6(71-4\cdot 17)-17 \iff 1=6\cdot 71-25\cdot 17$

この式から①を用いて 17 を消去すると，$1=6\cdot 71-25(159-2\cdot 71) \iff 1=56\cdot 71-25\cdot 159$

この式と，$159x+71y=1$ を比べることにより，解の 1 つが $x=-25$，$y=56$ と分かる。

$159x+71y=1 \quad \cdots①$

$x=-25$，$y=56$ は方程式①の解の 1 つとなるので，$159\cdot(-25)+71\cdot 56=1 \quad \cdots②$

① − ② より，$159x-159\cdot(-25)+71y-71\cdot 56=0 \iff 159(x+25)+71(y-56)=0$

$\iff 159(x+25)=-71(y-56) \quad \cdots③$

ここで，右辺は 71 の倍数なので，左辺も 71 の倍数となる。

159，71 は互いに素なので，$x+25$ は 71 の倍数となる。

つまり，$x+25=71k \iff x=71k-25 \ (k\in\mathbb{Z})$

③に代入すると，$159\cdot 71k=-71(y-56) \iff y-56=-159k \iff y=-159k+56$

以上より，$\begin{cases} x=71k-25 \\ y=-159k+56 \end{cases} (k\in\mathbb{Z})$

○　因数分解を用いる解法

$ab=10$ を満たす整数 a，b は

$(a,\ b)=(1,\ 10)$，$(2,\ 5)$，$(5,\ 2)$，$(-10,\ -1)$，$(-1,\ -10)$，$(-2,\ -5)$，$(-5,\ -2)$，$(-10,\ -1)$

となる。このように，積の形であれば，その不定方程式を満たす整数は限定される。

ここでは，この性質を用いた解法を紹介していく。

例 15　x，y 整数のとき，方程式 $xy-2x-y=1$ を解きなさい。

ここでは，$(x-a)(y-b)=c\ \ (a,b,c\in\mathbb{Z})$　$\cdots(*)$ の形に変形することを目標とします。

$(*)$ 式の左辺を展開すると，$xy-bx-ay+ab$ となります。

このことから，x の係数 b を y の（　）に，y の係数 a を x の（　）に

入れることで，とりあえず積の形は作れそうです。

あとは少し微調整することで $(*)$ の形に変形できます。

$$(x-a)(y-\boxed{b})$$

$$xy-\boxed{b}x-ay$$

解①

$xy-2x-y=1\ \ \Leftrightarrow\ \ (x-1)(y-2)-2=1$

$\Leftrightarrow\ \ (x-1)(y-2)=3$

$x-1$，$y-2$ はともに整数なので，

$(x-1,\ y-2)=(1,\ 3)$，$(3,\ 1)$，$(-1,\ -3)$，$(-3,\ -1)$

よって，$(x,\ y)=(2,\ 5)$，$(4,\ 3)$，$(0,\ -1)$，$(-2,\ 1)$

この問題は与式を「$y=$」の形に変形しても解くことができます。

解②

$xy-2x-y=1$ は $x=1$ を解に持たないので，y について解くと，

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

ここで，左辺は整数なので，右辺も整数となる。右辺が整数となるには，

$\dfrac{3}{x-1}$ が整数となればよいので，$x-1$ は 3 の約数である。

よって，$x-1=\pm1,\ \pm3\ \ \Leftrightarrow\ \ x=-2,\ 0,\ 2,\ 4$

このとき，$y=1,\ -1,\ 5,\ 3$

以上より，$(x,\ y)=(-2,\ 1)$，$(0,\ -1)$，$(2,\ 5)$，$(4,\ 3)$

○　不等式を用いる解法

$\boxed{\textbf{例 16}}$　x，y 自然数のとき，方程式 $2xy-3x-3y=0$ を解きなさい。

$\boxed{例 15}$ と同じ問題ですが，xy の係数が 2 になっているので，少し解きづらくなっています。
まず，両辺を 2 で割って，係数を 1 にすると解きやすいでしょう。

$\boxed{\textbf{解①}}$

$$2xy-3x-3y=0 \iff xy-\frac{3}{2}x-\frac{3}{2}y=0$$

$$\iff \left(x-\frac{3}{2}\right)\left(y-\frac{3}{2}\right)=\frac{9}{4}$$

$$\iff (2x-3)(2y-3)=9$$

$x \geqq 1$，$y \geqq 1$ より，$2x-3 \geqq -1$，$2y-3 \geqq -1$
これより，$(2x-3，2y-3)=(1，9)$，$(3，3)$，$(9，1)$
よって，$(x，y)=(2，6)$，$(3，3)$，$(6，2)$

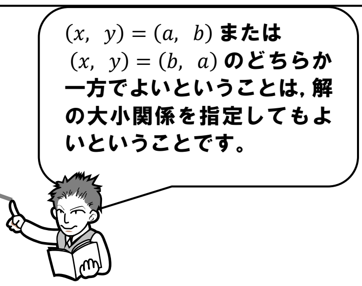
方程式 $2xy-3x-3y=0$　$\cdots(*)$ には**対称性**があります。どういうことかというと，変数 x，y を入れ替えても式が変わらないということです。
そして，対称性のある方程式には次のような性質があります。

$2\,x\,y\;-3\,x\;-3\,y\;=0$
入れ替えても変わらない

『解の１つを $(x，y)=(a，b)$ とすると,必ず $(x，y)=(b，a)$ も解になる。』

今，$(x，y)=(a，b)$ を $2xy-3x-3y=0$ の解とすると，$2ab-3a-3b=0$ が成り立ちます。
このとき，a，b を入れ替えた $2ba-3b-3a=0$ も当然成り立つわけですが，これは $(x，y)=(b，a)$ を $(*)$ に代入した式になります。つまり，$(x，y)=(b，a)$ も $(*)$ の解になるというわけです。
このことから，対称性がある方程式の場合，$(x，y)=(a，b)$ または $(x，y)=(b，a)$ のどちらか一方を見つければよいということが分かります。では，この方針で解答を作ってみましょう。

$\boxed{\textbf{解②}}$　対称性より $x \geqq y$ としてよい。



$x \neq 0$，$y \neq 0$ より，与式を xy で割ると，

$$2-\frac{3}{y}-\frac{3}{x}=0 \iff \frac{1}{x}+\frac{1}{y}=\frac{2}{3}$$

$x \geqq y$ より，$\dfrac{1}{x} \leqq \dfrac{1}{y}$ が成り立つので，$\dfrac{1}{x}+\dfrac{1}{y} \leqq \dfrac{1}{y}+\dfrac{1}{y} \iff \dfrac{2}{3} \leqq \dfrac{2}{y}$

よって，$1 \leqq y \leqq 3$

$y=3$ のとき，$\dfrac{1}{x}+\dfrac{1}{3}=\dfrac{2}{3} \iff \dfrac{1}{x}=\dfrac{1}{3} \iff x=3$

$y=2$ のとき，$\dfrac{1}{x}+\dfrac{1}{2}=\dfrac{2}{3} \iff \dfrac{1}{x}=\dfrac{1}{6} \iff x=6$

$y=1$ のとき，$\dfrac{1}{x}+1=\dfrac{2}{3} \iff \dfrac{1}{x}=-\dfrac{1}{3}$　x は自然数より不適

よって，$(x，y)=(3，3)$，$(6，2)$
対称性より，$(x，y)=(2，6)$ も解となるので，$(x，y)=(3，3)$，$(6，2)$，$(2，6)$

例 17　x，y 整数のとき，方程式 $x^2+4xy+5y^2=5$ を解きなさい。

1 つの文字に注目して解いていきます。x に注目すると与式は「x の 2 次方程式」となり，「2 次方程式が整数解を持つ」という問題に変わります。

$x^2+4xy+5y^2=5 \iff x^2+4yx+5y^2-5=0 \quad \cdots(*)$

これを x の 2 次方程式と見る。判別式を D とすると，解を持つ条件は,

$$D/4 \geqq 0 \iff 4y^2-(5y^2-5) \geqq 0$$
$$\iff -y^2+5 \geqq 0$$
$$\iff -\sqrt{5} \leqq y \leqq \sqrt{5}$$

y は整数なので，$y=0,\ \pm 1,\ \pm 2$

$y=0$ のとき，$(*) \iff x^2-5=0$　　これを満たす整数は存在しない。

$y=1$ のとき，$(*) \iff x^2+4x=0 \iff x(x+4)=0 \iff x=-4,\ 0$

$y=-1$ のとき，$(*) \iff x^2-4x=0 \iff x(x-4)=0 \iff x=0,\ 4$

$y=2$ のとき，$(*) \iff x^2+8x+15=0 \iff (x+3)(x+5)=0 \iff x=-3,\ -5$

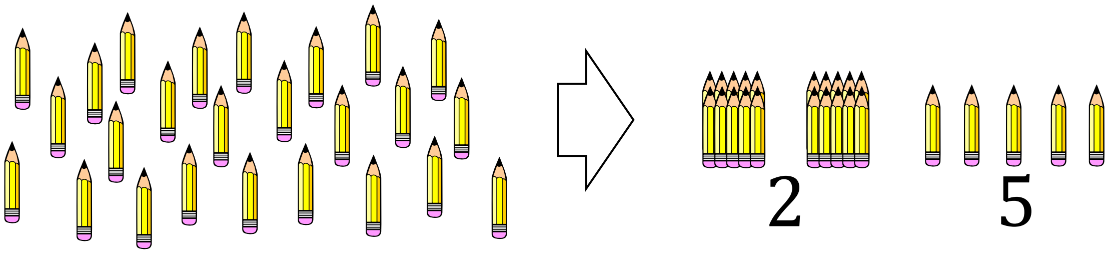
$y=-2$ のとき，$(*) \iff x^2-8x+15=0 \iff (x-3)(x-5)=0 \iff x=3,\ 5$

以上より，$(x,\ y)=(-4,\ 1),\ (0,\ 1),\ (4,\ -1),\ (0,\ -1),\ (-3,\ 2),\ (-5,\ 2),\ (3,\ -2),\ (5,\ -2)$

§6　n 進法

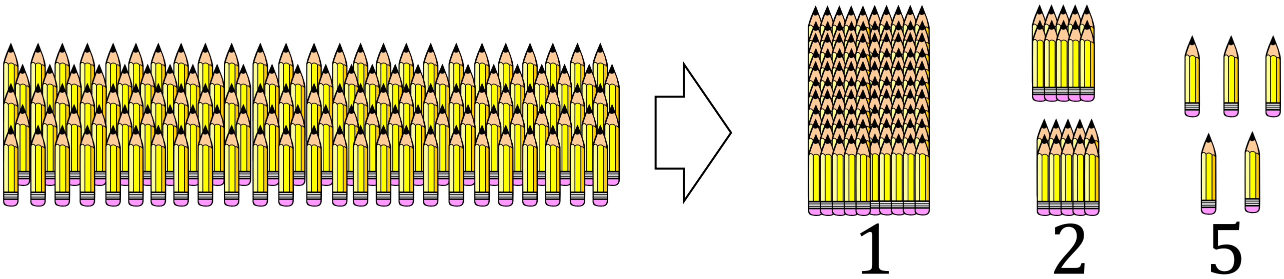
以下に 25 本の鉛筆があります。ここではまず，『25』という数字の意味を考えてみます。

この鉛筆の本数を数えるときに，1 本ずつ「1，2，3，4，…」と数えていってもいいのですが，本数が多い場合は**10 本ずつの束を作って数えた方が**正確に数えることができます。

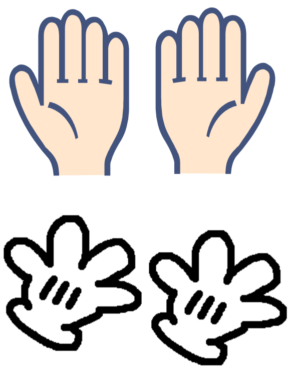


そうすると結局，10 本の束が **2** つとバラの鉛筆が **5** 本なので，25 本となるわけです。
そして，ここに実は 25 という数字の意味が隠されています。つまり，「2」が 10 本の束の数を，「5」がバラの鉛筆の数を表しているのです。

ここで，さらに本数が増やして 125 本の鉛筆を数える場合を考えます。このときも同様に 10 本の束を作っていくと，10 本の束が 12 個とバラの鉛筆が 5 本でいます。そしてこの場合は，10 本の束をさらに 10 個にまとめて，100 本(10^2 本)の束を 1 つ作ります。そうすると結局，100 本(10^2 本)の束が ***1*** つと 10 本の束が **2** つとバラの鉛筆が **5** 本なので，125 本となるわけです。つまり，125 という数字の「1」が 100 本(10^2 本)の束の数を，「2」が 10 本の束の数を，「5」がバラの鉛筆の数を表しています。



以上のように，私たちが普段使っている数字の各位の数というのは，
実は束の数を表したものなのです。



ではここで，少し数の表し方を拡張してみましょう。
私たちが数を数えるときに自然と 10 本の束を作るのは，私たちの手の指が 10 本あるからと言われています。
ではミッキーマウスは 25 本の鉛筆をどのように数えるでしょうか？
ミッキーマウスの指は 8 本です。つまり，私たちのように 10 本の束を作らずに，きっと 8 本の束を作っていくはずです。
このとき 25 本の鉛筆は，8 本の束が **3** つとバラの鉛筆が ***1*** 本に分けることができるので，
私たちが「25」と言っている鉛筆の本数を，ミッキーマウスは「**31**」と表すはずです。

また，125 本の鉛筆をミッキーマウスが数えた場合，まず 8 本の束が 15 個とバラの鉛筆が 5 本を作ります。そして，8 本の束をさらに 8 個にまとめて，64 本(8^2 本)の束を 1 個作ります。そうすると結局，125 本の鉛筆が，64 本(8^2 本)の束 **1** つ，8 本の束 **7** つ，バラの鉛筆 **5** 本に分かれるので，125 本の鉛筆はミッキーマウスにとっては「**175**」と表されるわけです。

普段，私たちが使っている数の表し方を **10 進法**というのに対して，ミッキーマウスの数の表し方を **8 進法**と言います。8 進法で表された数を **8 進数**と言い，$175_{(8)}$ のように右下に $_{(8)}$ をつけて表します。なお，10 進数の場合は普通 $_{(10)}$ を省略します。つまり，$125 = 175_{(8)}$ となるわけです。

以下で，8 進法の数の扱い方について学んでいきますが，基本的な考え方は何進法であっても同じになります。

○　10 進数から 8 進数へ

ここで，10 進数を 8 進数に直す方法を見ていきます。
これは，今見てきたように 8 本の束を作っていくことで，直すことができます。
例えば，300 を 8 進数に直す場合は，まず 300 を 8 で割ると，

$300 \div 8 = 37$ 余り 4

となるので，8 の束が 37 個とバラが **4** 個できることが分かります。そして，次に 37 を 8 で割ると，

$37 \div 8 = 4$ 余り 5

となるので，8^2 の束が **4** 個でき，8 の束が **5** 個残ります。
以上のことから，$300 = 454_{(8)}$ となります。

このように，与えられた数を 8 で次々と割っていくことで 10 進法から 8 進法に直すことができます。なお，実際の計算は右のように表記すると分かりやすくなります。

$$
\begin{array}{r|l l}
8 & 300 & \textbf{余り} \\ \hline
8 & 37 & \cdots 4 \\ \hline
 & 4 & \cdots 5
\end{array}
$$

○　8 進数から 10 進数へ

$175_{(8)}$ は先ほど見たとおり，8^2 の束が 1 つ，8 の束が 7 つ，バラが 5 つを表しているので，

$$175_{(8)} = 1 \times 8^2 + 7 \times 8 + 5 \times 1 = 125$$

と計算することができます。同様に $454_{(8)}$ は，

$$454_{(8)} = 4 \times 8^2 + 5 \times 8 + 4 \times 1 = 300$$

となります。

○　8 進法の小数

まず 10 進法における小数を確認しておきましょう。
例えば，0.234 という小数は次のように表すことができます。

$$0.234 = 2 \times \frac{1}{10} + 3 \times \frac{1}{10^2} + 4 \times \frac{1}{10^3}$$

つまり，0.234 という小数は，$\frac{1}{10}$ が 2 つ，$\frac{1}{10^2}$ が 3 つ，$\frac{1}{10^3}$ が 4 つあることを表している数であることが分かります。8 進法における小数も同様に表すことができます。例えば，$0.234_{(8)}$ は，

$$0.234_{(8)} = 2 \times \frac{1}{8} + 3 \times \frac{1}{8^2} + 4 \times \frac{1}{8^3}$$

となるわけです。この右辺を計算すると，

$$2\times\frac{1}{8}+3\times\frac{1}{8^2}+4\times\frac{1}{8^3}=\frac{39}{128}=0.3046875$$

となるので，$0.234_{(8)}=0.3046875$ が成り立ちます。

逆に，10 進数 0.3046875 を 8 進数に直すには，まずこの数を 8 倍します。

$0.3046875\times 8=2.4375\quad\cdots①$

これの整数部分 2 が 8 進数の小数第 1 位になります。

さらに，①の小数部分を 8 倍します。　$0.4375\times 8=3.5\quad\cdots②$

これの整数部分 3 が 8 進数の小数第 2 位になります。

さらに，②の小数部分を 8 倍します。　$0.5\times 8=4\quad\cdots②$

これが小数第 3 位になるので，結局 $0.3046875=0.234_{(8)}$ となるわけです。

なお，この計算は右のように表記すると分かりやすいでしょう。

$$\begin{array}{r}
0.3046875\\
\times\qquad\quad 8\\ \hline
\boxed{2}.4375\\
\times\quad 8\\ \hline
\boxed{3}.5\\
\times\ 8\\ \hline
\boxed{4}
\end{array}$$

例 18　次の 10 進数を [　] 内の表し方で表しなさい。

(1)　25 [2 進法]　　(2)　0.824 [5 進法]

(1)　25 を 2 で割ると商が 12 で余りが 1

12 を 2 で割ると商が 6 で余りが 0

6 を 2 で割ると商が 3 で余りが 0

3 を 2 で割ると商が 1 で余りが 1

これより，$25=11001_{(2)}$

$$\begin{array}{r|rl}
2 & 25 & \textbf{余り}\\
2 & 12 & \cdots 1\\
2 & 6 & \cdots 0\\
2 & 3 & \cdots 0\\
 & 1 & \cdots 1
\end{array}$$

$$\begin{array}{r}
0.824\\
\times\qquad 5\\ \hline
\boxed{4}.12\\
\times\quad 5\\ \hline
\boxed{0}.6\\
\times\ 5\\ \hline
\boxed{3}
\end{array}$$

(2)　$0.824\times 5=4.12$

$0.12\times 5=0.6$

$0.6\times 5=3$

これより，$0.824=0.403_{(5)}$

例 19　次の数を 10 進数で表しなさい。

(1)　$101011_{(2)}$　　(2)　$2012_{(3)}$　　(3)　$0.124_{(5)}$

(1)　$101011_{(2)}=1\times 2^5+0\times 2^4+1\times 2^3+0\times 2^2+1\times 2+1=32+8+2+1=43$

(2)　$2054_{(3)}=2\times 3^3+0\times 3^2+1\times 3+2=54+3+2=59$

(3)　$0.124_{(5)}=1\times\dfrac{1}{5}+2\times\dfrac{1}{5^2}+4\times\dfrac{1}{5^3}=\dfrac{39}{125}=0.312$

○　8 進法の四則計算

ここでは, 8 進法の四則計算について学んでいく。ここでの考え方は当然, 何進法になっても同じである。

足し算

$1_{(8)}+2_{(8)}=3_{(8)}$，$2_{(8)}+3_{(8)}=5_{(8)}$，$3_{(8)}+4_{(8)}=7_{(8)}$ のように，足した結果が 8 を超えなければ計算方法は 10 進法と同じになるが，8 を超えると 8 の束が 1 つできるので，1 桁繰り上がる。
例えば，$4_{(8)}+6_{(8)}$ は，10 進法で計算すると 10 となるが，$10=12_{(8)}$ なので，$4_{(8)}+6_{(8)}=12_{(8)}$ となる。

例 20　次の計算をしなさい。$324_{(8)}+57_{(8)}$

筆算は右のようになる。
まず①列は，$4_{(8)}+7_{(8)}=13_{(8)}$ となるので，1 が②列に繰り上がる。
よって②列は，$1_{(8)}+2_{(8)}+5_{(8)}=10_{(8)}$ となるので，1 が③列に繰り上がる。
これより③列は，$1_{(8)}+3_{(8)}=4_{(8)}$ となる。
よって，$324_{(8)}+57_{(8)}=403_{(8)}$

$$\begin{array}{cccc} & ③ & ② & ① \\ & 3 & 2 & 4 \\ + & & 5 & 7 \\ \hline & 4 & 0 & 3 \end{array}$$

なお，n 進法の計算は 1 度 10 進法に直してから計算するという方法もある。
$324_{(8)}=3\times8^2+2\times8+4=212$，$57_{(8)}=5\times8+7=47$ より，
$324_{(8)}+57_{(8)}=212+47=259=403_{(8)}$
としてもよい。ただ，10 進法に直してから計算し，また元に戻すので，少し時間はかかってしまう。
なるべく n 進法のまま計算するようにしましょう。

引き算

例えば，$24_{(8)}$ から $7_{(8)}$ を引く場合，まず 1 の位の計算をするが，$4_{(8)}$ から $7_{(8)}$ は引けないので，隣から 1 を借りてくることになる。隣から借りてきた 1 は，8 進法なので 8 を意味する。つまり，1 の位の計算を 10 進法で表すと，$8+4-7=5$ となるので，1 の位の計算結果は $5_{(8)}$ となる。よって，$24_{(8)}-7_{(8)}=15_{(8)}$ となる。

例 21　次の計算をしなさい。$324_{(8)}-57_{(8)}$

筆算は右のようになる。
まず①列は隣から 1 を借りてきて，$14_{(8)}-7_{(8)}=5_{(8)}$ となる。
このとき②列は，$1_{(8)}$ から $5_{(8)}$ を引けないので，隣から 1 を借りてきて，
$11_{(8)}-5_{(8)}=4_{(8)}$ となる。
③列は，②列に 1 を貸したので，$2_{(8)}$ となる。
よって，$324_{(8)}-57_{(8)}=245_{(8)}$

$$\begin{array}{cccc} & ③ & ② & ① \\ & 3 & 2 & 4 \\ - & & 5 & 7 \\ \hline & 2 & 4 & 5 \end{array}$$

掛け算

基本的には足し算と同じように計算していく。まずは各位を 10 進法と同じように計算をし，その結果が 8 を超えていれば 8 の束ができるので繰り上がる。

例えば，$4_{(8)} \times 5_{(8)}$ は，10 進法で計算すると 20 となるが，$20 = 24_{(8)}$ なので，$4_{(8)} \times 5_{(8)} = 24_{(8)}$ となる。

例 22　次の計算をしなさい。$37_{(8)} \times 25_{(8)}$

筆算は右のようになる。

まず，$37_{(8)} \times 5_{(8)}$ を計算する。

①列の $5_{(8)} \times 7_{(8)}$ は 10 進法で表すと 35 となり，$35 = 43_{(8)}$ なので，1 の位には 3 が残り，4 が繰り上がる。これより，②，③の計算は，10 進法で表すと $3 \times 5 + 4 = 19$ となり，$19 = 23_{(8)}$ なので，結局 $37_{(8)} \times 5_{(8)} = 233_{(8)}$ となる。

次に，$37_{(8)} \times 2_{(8)}$ を上と同様に計算すると，$37_{(8)} \times 2_{(8)} = 76_{(8)}$

最後に，$233_{(8)} + 760_{(8)}$ を計算すればよい。

よって，$37_{(8)} \times 25_{(8)} = 1213_{(8)}$

$$\begin{array}{rr} & 37 \\ \times & 2 \\ \hline & 76 \end{array} \qquad \begin{array}{rccc} & ③ & ② & ① \\ & & 3 & 7 \\ \times & & & 5 \\ \hline & 2 & 3 & 3 \end{array}$$

$$\begin{array}{rr} & 37 \\ \times & 25 \\ \hline & 233 \\ & 76 \\ \hline & 1213 \end{array}$$

割り算

割り算は 10 進法のときと同様に, 掛け算と引き算を組み合わせることで計算できるが, 少々大変になる。私たちが 10 進法において素早く割り算ができるのは「掛け算九九」を暗記しているからである。n 進法における「掛け算九九」を暗記していない私たちにとっては割り算のハードルはかなり高い。つまり，割り算に関しては，1 度 10 進法に直してから計算した方がよい。

MEMO