整数

要点の整理補充

数の分類

数（複素数）$a+bi$
- 実数$(b=0)$
  - 有理数
    - 整数
      - 正の整数（自然数）
        - 1
        - 素数
        - 合成数
      - 0
      - 負の整数
    - 分数
  - 無理数
- 虚数$(b\neq 0)$（$a=0$ の虚数を純虚数という）

自然数の世界：加・乗が常に可能
整数の世界：加・減・乗が常に可能
有理数の世界：加・減・乗・除（0 で割ることを除く）が常に可能
　任意の 2 つの有理数の差を限りなく小さくとっても，その間に無数の有理数がある。
　これを有理数の稠密性という。
無理数の世界：有理数ならば分数で表せる。よって，分数で表せないなら有理数ではない。
　　分数で表せない数を無理数という。
実数の世界：有理数と無理数をあわせて実数という。
　　有理数と無理数により，数直線上の数の隙間がなくなる。
　　これを実数の連続性という。
虚数の世界：実数ならば，負の実数の平方根は存在しないが，
　　虚数の世界では，負の実数の平方根が存在する。
数（複素数）の世界：実数と虚数をまとめて数（複素数）という。

素数・合成数の判別法

1 より大きい自然数 n は素数と合成数に分類できる。

n が素数でないとき，すなわち合成数のとき，

n の最小の素数を p とし，その商を q とすると，

$n = pq$　・・・①

ここで，$p > q$ とすると，q は p より小さい素数をもつことになり，

p を n の最小の素数とするという仮定に反する。

よって，$p < q$　・・・②（背理法）

①かつ②より，

$p^2 < pq = n$

$\therefore 2 \le p < \sqrt{n}$

以上より，

1 より大きい自然数 n が $\sqrt{n}$ より小さい素数をもつとき，n は合成数である。

ユークリッドの互除法

2 つの整数 a，$b\ (a \ge b)$ の最大公約数を G_1 とすると，

$a = a'G_1$，$b = b'G_1$（a' と b' は互いに素）　・・・①

a を b で割った商を q_1，余りを r_1 とすると，$a = bq_1 + r_1$　・・・②

①，②より，

$a'G_1 = b'G_1q_1 + r_1$　$\therefore r_1 = G_1(a' - b'q_1)$

よって，G_1 は a と b の最大公約数かつ b と r_1 の公約数である。

次に，

b と r_1 の最大公約数を G_2 とすると，

$G_1 \le G_2$（$\because G_1$ は b と r_1 の公約数，G_2 は b と r_1 の最大公約数）　・・・③

$b = b''G_2$，$r_1 = r_1'G_2$（b'' と r_1' は互いに素）　・・・④

②，④より，$a = b''G_2q_1 + r_1'G_2$　$\therefore a = G_2(b''q_1 + r_1')$

これより，G_2 は b と r_1 の最大公約数かつ a と b の公約数であるから，

$G_1 \ge G_2$　・・・⑤

③かつ⑤より，$G_1 = G_2$

同様に，b を r_1 で割ったときの余りを r_2 とし，r_1 と r_2 の最大公約数を G_3 とすると，

$G_2 = G_3$

よって，$G_1 = G_2 = G_3$

この作業を繰り返していき，$r_n = r_{n+1}q_{n+2}$ と余りが 0 になったとき，

r_{n+1} は r_n と r_{n+1} の最大公約数だから，$G_1 = G_2 = G_3 \cdots = r_{n+1}$

ゆえに，r_{n+1} は整数 a，$b\ (a \ge b)$ の最大公約数である。

このようにして，最大公約数を求める方法をユークリッドの互除法という。

整数 a，b が互いに素であるとき，$ax+by=1$ を満たす整数 x，y が存在する。

証明 1

$ax+by$ をその最小値 p で割ったときの余りの最大値が p より小さいことを利用

$ax+by$ の最小の正の整数を p とすると，

$ax_0+by_0=p$ を満たす整数 x_0，y_0 が存在する。

ここで，任意の $ax+by$ を p で割った商を q，余りを r とすると，

$ax+by=pq+r$ より，

$ax+by=(ax_0+by_0)q+r \quad (0\le r\le p-1)$

$\therefore a(x-qx_0)+b(y-qy_0)=r \quad (0\le r\le p-1)$

よって，r は $ax+by$ の形で表される。

ここで，

r を正の整数とすると，$r\le p-1<p$ より，

p が $ax+by$ の最小の正の整数であることに反するので，$r=0$（背理法）

よって，

任意の $ax+by$ について，$ax+by=pq$ が成り立つ。

つまり，任意の $ax+by$ は，p の倍数である。

続いて，p の値を求める。

$ax+by$ について，

$x=1$，$y=0$ のとき

$ax+by=a$

これと $ax+by$ が p の倍数であることから，a は p の倍数である。

$x=0$，$y=1$ のとき

$ax+by=b$

これと $ax+by$ が p の倍数であることから，b は p の倍数である。

したがって，p は a と b の公約数である。

ところが，a と b は互いに素であるから，公約数は 1 しかない。

ゆえに，$p=1$

以上より，

a と b が互いに素であるとき，$ax+by=1$ を満たす整数 x，y が存在する。

証明 2

余りの個数が有限であることを利用

$ax+by=1$ を満たす整数 x，y が存在することを示せばよいから，

あらかじめ，x と y に制約をつけても構わない。

そこで，任意の ax を b で割った商を $-y$，余りを r $(0\le r\le b-1)$ とし，

$1\le x_1\le x_2\le b$ について，

$ax_1=b(-y_1)+r_1$　・・・①

$ax_2=b(-y_2)+r_2$　・・・②

のとき，

$r_1=r_2$ とすると，

②－①より，$a(x_2-x_1)=b(-y_2+y_1)$

a と b は互いに素だから，$x_2-x_1=bk$，$-y_1+y_2=ak$

ところが，$1\le x_1\le x_2\le b$ より，$0\le x_2-x_1\le b-1<b$

よって，$k=0$，すなわち $x_1=x_2$

したがって，　$r_1=r_2\Rightarrow x_1=x_2$ が成り立つ。

この対偶は，$x_1\ne x_2\Rightarrow r_1\ne r_2$ であり，

これは，$ax=b(-y)+r$　$(1\le x\le b)$ において，x が異なれば r も異なることを示している。

一方，

x の要素の数は，$1\le x\le b$ より b 個

r は ax を b で割った余りだから，$0\le b\le b-1$ より，その要素の数も b 個

したがって，$r=1$ は必ず存在する。

ゆえに，$ax=b(-y)+1$，すなわち $ax+by=1$ を満たす整数 x，y が存在する。

となり，b の倍数にはなれない。

整数 a，b の最大公約数が G のとき，$ax+by=G$ を満たす整数 x，y が存在する。

証明

$a=a'G$，$b=b'G$ とすると，$ax+by=G(a'x+b'y)$

a' と b' は互いに素だから，$a'x+b'y=1$ を満たす整数 x，y が存在し，

このとき，$ax+by=G$ が成り立つ。

よって，整数 a，b の最大公約数が G のとき，$ax+by=G$ を満たす整数 x，y が存在する。

整数 a，b が互いに素であるとき

b 個の数 a，$2a$，$3a$，・・・，ba を b で割った余りはすべて異なる。

証明

$1\le i\le j\le b$ のとき，

$ia=q_ib+r_i \quad (0\le r_i\le b-1)$　・・・①

$ja=q_jb+r_j \quad (0\le r_j\le b-1)$　・・・②

とすると，

②－①より，

$(j-i)a=(q_j-q_i)b+r_j-r_i$

$r_i=r_j$ のとき

$(j-i)a=(q_j-q_i)b$

a と b は互いに素だから，

$j-i$，q_j-q_i は，それぞれ整数 k を用いて $j-i=kb$，$q_j-q_i=ka$ と表せる。

ここで，$j-i=kb$ について，

$1\le i\le j\le b$ より，$0\le j-i\le b-1<b$

よって，$k=0$

以上より，

$r_i=r_j\Rightarrow i=j$ が成り立つから，その対偶 $i\ne j\Rightarrow r_i\ne r_j$ も成り立つ。

例題 4　k^n を割った余り

(イ)

$15=3\cdot5$ より，2^n+1 が 15 で割り切れるための必要十分条件は，

2^n+1 が 3 でも 5 でも割り切れることである。

2^n+1 が 3 で割り切れるための条件

$$2^n+1=(3-1)^n+1={}_n\mathrm{C}_0 3^0\cdot(-1)^n+{}_n\mathrm{C}_1 3^1\cdot(-1)^{n-1}+{}_n\mathrm{C}_2 3^2\cdot(-1)^{n-2}+\cdots+{}_n\mathrm{C}_n 3^n\cdot(-1)^0+1$$
$$=3\left\{{}_n\mathrm{C}_1(-1)^{n-1}+{}_n\mathrm{C}_2 3\cdot(-1)^{n-2}+\cdots+{}_n\mathrm{C}_n 3^{n-1}\cdot(-1)^0\right\}+(-1)^n+1$$

より，

$(-1)^n+1=0$，すなわち n が奇数であればよい。

ここで，$n=2k+1\ (k=0,1,2,\cdots)$ とおくと，

$$2^n+1=2^{2k+1}+1$$
$$=2\cdot4^k+1$$
$$=2(5-1)^k+1$$
$$=2\cdot5\left\{{}_k\mathrm{C}_1(-1)^{k-1}+{}_k\mathrm{C}_2 5\cdot(-1)^{k-2}+\cdots+{}_k\mathrm{C}_k 5^{k-1}(-1)^0\right\}+2(-1)^k+1$$

より，

n が奇数のとき，2^n+1 を 5 で割った余りは 3 および -1，すなわち 3 および 4

よって，

2^n+1 が 3 でも 5 でも割り切れるような正整数 n は存在しない。

ゆえに，

2^n+1 は 15 で割り切れない。

（ロ）

$$2000^{2000}=(167\cdot 12-4)^{2000}={}_{2000}\mathrm{C}_0(-4)^{2000}+\sum_{k=1}^{2000}{}_{2000}\mathrm{C}_k\left\{(167\cdot 12)^k(-4)^{2000-k}\right\}$$

$$=4^{2000}+\sum_{k=1}^{2000}{}_{2000}\mathrm{C}_k\left\{(167\cdot 12)^k(-4)^{2000-k}\right\}$$

$\sum_{k=1}^{2000}{}_{2000}\mathrm{C}_k\left\{(167\cdot 12)^k(-4)^{2000-k}\right\}$は 12 で割り切れるから，

2000^{2000} を 12 で割った余りと 4^{2000} を 12 で割った余りは等しい。

ここで，

$$4^{2000}=4\cdot 4^{1999}$$

$$=4\cdot(3+1)^{1999}$$

$$=4\left\{1^{1999}+\sum_{k=1}^{1999}\left(3^k\cdot 1^{1999-k}\right)\right\}$$

$$=4+4\sum_{k=1}^{1999}3^k$$

$$=4+4\cdot 3\sum_{k=1}^{1999}3^{k-1}$$

$$=4+12\sum_{k=1}^{1999}3^{k-1}$$

より，

4^{2000} を 12 で割った余りは 4

ゆえに，

2000^{2000} を 12 で割った余りは 4 である。

例題 6　最大公約数と互除法

（イ）

(2)

(1)の結果を無視した解法

$m=m'g$，$n=n'g$（m' と n' は互いに素）　・・・①

m を n で割った商を q，余りを r とすると，$m=qn+r$　・・・②

①，②より，

$m'g=qn'g+r$

$\therefore r=(m'-qn')g$

よって，g は n と r の公約数であり，

n と r の最大公約数を g' とすると，$g\leq g'$　・・・③

また，

$n=n''g'$，$r=r'g'$（n'' と r' は互いに素）　・・・④

②，④より，

$m=qn''g'+r'g'$

$\therefore m=(qn''+r')g'$

よって，g' は m と n の公約数である。

$\therefore g\geq g'$　・・・⑤

③かつ⑤より，

$g=g'$

よって，

m を n で割った余りと n との最大公約数も g である。

例題 7　$ax+by$ の形で表現する

(1)

自然数 t に対して，t を b で割った商を $Q(t)$ とすると，

$ja=Q(ja)\cdot b+R(ja)$　・・・①

$ka=Q(ka)\cdot b+R(ka)$　・・・②

①－②より，

$a(j-k)=b(Q(ja)-Q(ka))$

a と b は互いに素だから，s を整数とすると，$j-k=sb$

一方，

$j\in N$，$k\in N$ より，$1\le j\le b$，$1\le k\le b$　$\therefore 1\le j\le b$，$-b\le -k\le -1$

$\therefore -b<-(b-1)\le j-k\le b-1<b$

よって，$j-k=sb$ をみたす s は 0 のみである。

ゆえに，$j=k$

(2)

$R(ja)=R(ka)$ ならば $j=k$ の対偶も成り立つから，

$j\neq k$ ならば $R(ja)\neq R(ka)$ である。　・・・③

$ia=Q(ia)\cdot b+R(ia)$ について

$1\le i\le b$ より，i は $1,2,3,\cdots,b$ の b 個の異なる値をとれる。　・・・④

$0\le R(ia)\le b-1$ より，$R(ia)$ は $0,1,2,\cdots,b-1$ の b 個の異なる値をとれる。　・・・⑤

③，④，⑤より，

$i=1,2,3,\cdots,b$ のとき，

$R(ia)$ は，$,0,1,2,3,\cdots,b$ のすべての値をとることになる。

よって，

$i\in N$，$R(ia)=1$ をみたす i が存在する。

例題 8　つねに整数値をとる整式／その 1

命題：任意の整数値 n に対して $f(n)$ が整数値をとる $\Rightarrow$ $2a$，$a+b$，c は整数である

証明

条件より，

$f(0)=c$，$f(1)=a+b+c$，$f(-1)=a-b+c$ は整数である。

したがって，

$f(1)-f(0)=a+b+c-c=a+b$，$f(1)+f(-1)-2f(0)=2a$ も整数である。

よって，

命題は真である。

命題：$2a$，$a+b$，c は整数である $\Rightarrow$ 任意の整数値 n に対して $f(n)$ が整数値をとる

証明

$2a=\alpha$，$a+b=\beta$，$c=\gamma$ （α,β,γ は整数）とおくと，

$a=\dfrac{\alpha}{2}$，$b=\beta-\dfrac{\alpha}{2}$ より，

$$f(n)=\frac{\alpha}{2}n^2+\left(\beta-\frac{\alpha}{2}\right)n+\gamma=\frac{\alpha}{2}\cdot n(n-1)+\beta\cdot n+\gamma$$

$n(n-1)$ は 2 の倍数だから，$\dfrac{\alpha}{2}\cdot n(n-1)$ は整数である。

また，$\beta\cdot n$，γ も整数である。

したがって，$f(n)=\dfrac{\alpha}{2}n^2+\left(\beta-\dfrac{\alpha}{2}\right)n+\gamma=\dfrac{\alpha}{2}\cdot n(n-1)+\beta\cdot n+\gamma$ は整数である。

よって，命題は真である。

以上より，

任意の整数値 n に対して $f(n)$ が整数値をとる $\Leftrightarrow$ $2a$，$a+b$，c は整数である

が成り立つ。

ゆえに，題意が示された。

例題 9　つねに整数値をとる整式／その 2

(1)

$f(x)=Ax(x+1)(x+2)+Bx(x+1)+Cx$ と $f(x)=ax^3+bx^2+(b-a)x$ は恒等式の関係にあるから，

$Ax(x+1)(x+2)+Bx(x+1)+Cx\equiv ax^3+bx^2+(b-a)x$

$x=-1$ を代入すると，

$-C=0 \quad \therefore C=0$

$\therefore Ax(x+1)(x+2)+Bx(x+1)\equiv ax^3+bx^2+(b-a)x$

$x=-2$ を代入すると，

$2B=-6a+2b \quad \therefore B=-3a+b$

$x=1$ を代入すると，

$6A+2B=2b \quad \therefore A=\frac{1}{3}(b-B)=\frac{1}{3}\{b-(-3a+b)\}=a$

以上より，

$A=a$，　$B=-3a+b$，　$C=0$

(2)

(1)より，

$f(x)=Ax(x+1)(x+2)+Bx(x+1)$

$\therefore f(1)=6A+2B$，　$f(-2)=2B$

条件より，任意の整数 n に対して $f(n)$ は整数だから，

$6A+2B$ と $2B$ は整数であり，その差 $6A+2B-2B=6A$ も整数である。

(3)

命題：$6a$ と $2b$ が整数 $\Rightarrow f(x)$ が条件（＊）を満たす

証明

$6a=k$，　$2b=l$ （k，　l は整数）とおくと，

$A=a$，　$B=-3a+b$，　$C=0$ より，

$A=a=\frac{k}{6}$，　$B=-3\cdot\frac{k}{6}+\frac{l}{2}=\frac{-k+l}{2}$，　$f(x)=Ax(x+1)(x+2)+Bx(x+1)$

よって，

$f(x)=\frac{k}{6}x(x+1)(x+2)+\frac{-k+l}{2}x(x+1)$

x が整数のとき，　$x(x+1)(x+2)$ は 6 の倍数，　$x(x+1)$ は 2 の倍数だから，

$f(x)=\frac{k}{6}x(x+1)(x+2)+\frac{-k+l}{2}x(x+1)$ は整数である。

命題：$f(x)$が条件（＊）を満たす⇒　$6a$ と $2b$ が整数

証明

(2)より，$6A$ は整数である。

(1)より，$A=a$

よって，$6a$ は整数である。

(2)より，$2B$ は整数である。

(1)より $2B=-6a+2b$　　$\therefore 2b=2B+6a$

$2B$ と $6a$ は整数だから，$2b$ は整数である。

以上より，

$6a$ と $2b$ が整数⇔ $f(x)$が条件（＊）を満たす

が成り立つ。

よって，題意が示された。

例題 11　不定方程式／2 次の型

（ロ）

$(x-2)(y-4)=7$

$x>y$ より，$x-2>y-2>y-4$

よって，

$(x-2,\ y-4)=(7,1),(-1,-7)$

これらのうち，$(x-2,\ y-4)=(-1,-7)$ は，$y=-3<0$ となり不適

よって，$(x-2,\ y-4)=(7,1)\ \therefore (x,\ y)=(9,5)$

$\therefore x=9$

例題 12　不定方程式／分数形

解 2 について補足

$\dfrac{1}{x}+\dfrac{1}{y}=\dfrac{1}{4}$ より，$\dfrac{1}{y}=\dfrac{1}{4}-\dfrac{1}{x}=\dfrac{x-4}{4x}>0\ (\because y>0)$

$\therefore 4x(x-4)>0$

$x>0$ より，$x-4>0$　$\therefore x\geq 5$

例題 15　格子点

(1)

線分 OA 上の点を(p,q)とすると，

点(p,q)は$y=\frac{b}{a}x$を満たす点だから，$q=\frac{b}{a}p$が成り立つ。

よって，$aq=bp$

aとbは互いに素だから，点(p,q)が格子点であるための必要条件は，

$p=ka$，$q=kb$を満たす自然数kが存在することである。

ところが，$0<q<b$，$0<p<a$

よって，$q=kb$，$p=ka$を満たす自然数kは存在しない。

ゆえに，線分 OA 上に（端点を除く）に格子点は存在しない。

(2)

点$(a,0)$を点 D，点$(0,b)$を点 E，線分 OA の中点$\left(\frac{a}{2},\frac{b}{2}\right)$を点 M とすると，

OA は，点 O$(0,0)$，点 D$(a,0)$，点 E$(0,b)$，点 A(a,b)を頂点とする長方形の対角線だから，

OA によって 2 分される合同な直角三角形 OAE と直角三角形 AOD は，

点 M に関して点対称である。

図形は無数の点の集まりだから，

直角三角形 OAE と直角三角形 AOD を点の集合と見なすと，

直角三角形 OAE の周を含む内部の任意の点と点 M に関して点対称な直角三角形 AOD の周を含む内部の点は 1 対 1 に対応する。

ここで，直角三角形 OAE の周を含む内部の任意の格子点を(p,q)とし，

それと点 M に関して対称な直角三角形 AOD の周を含む内部の点を(p',q')とすると，

$\left(\frac{p+p'}{2},\frac{q+q'}{2}\right)=\left(\frac{a}{2},\frac{b}{2}\right)$より $p+p'=a$ ，$q+q'=b$　$\therefore p'=a-p$，$q'=b-q$

p,q,a,bは整数だから，p',q'は整数である。すなわち，(p',q')は格子点である。

よって，点 M に関して格子点どうしが 1 対 1 に対応することになる。

このことと線分 OA 上に（端点を除く）に格子点が存在しないことから，

線分 OA は，長方形 ODAE の周を含まない内部の格子点の数を 2 分することになる。

よって，その数は，$\frac{(a-1)(b-1)}{2}$である。

また，他の格子点は，

$(1,b)$，$(a-1,b)$，$(1,b+2)$，$(a-1,b+2)$を頂点とする長方形の周を含む内部の格子点より，

その数は，$3(a-1)$

よって，求める格子点の数は，

$$\frac{(a-1)(b-1)}{2}+3(a-1)=\frac{ab-a-b+1+6a-6}{2}$$

$$=\frac{ab+5a-b-5}{2}$$

$$=\frac{(a-1)(b+5)}{2}$$

補足

直角三角形の点の 1 対 1 の対応についてわかりにくければ，
次のように理解すればよい。
点 M を通る任意の直線が直角三角形 OAE を切る線分の長さと
直角三角形 AOD を切る線分の長さは等しいから，
一方の線分上の任意の点と点 M に関して対称なもう一方の線分上の点とが
1 対 1 に対応する。