12　数の理論

85

(1)

解法 1

$4a+3b\equiv 3 \pmod 7$　・・・①

$3a+2b\equiv 5 \pmod 7$　・・・②

②×3－①×2 より，$a\equiv 9\equiv 2 \pmod 7$

①×3－②×4 より，$b\equiv -11\equiv 3 \pmod 7$

よって，a, b を 7 で割った余りはそれぞれ 2, 3

解法 2

k, l を整数とすると，条件より，

$4a+3b=7k+3$　・・・①

$3a+2b=7l+5$　・・・②

②×3－①×2 より，$a=7(3l-2k+1)+2$

①×3－②×4 より，$b=7(3k-4l-2)+3$

よって，a, b を 7 で割った余りはそれぞれ 2, 3

(2)

解法 1

m^3-n^3 を 3 で割った余りも k ならば $n^3-n^3-(m-n)$ を 3 で割った余りは 0,

$$\begin{aligned} m^3-n^3-(m-n)&=m^3-m-(n^3-n)\\ &=(m-1)m(m+1)-(n-1)n(n+1)\end{aligned}$$

$(m-1)m(m+1)$，$(n-1)n(n+1)$ は連続する 3 つの整数の積だから 3 の倍数である。

よって，$m^3-n^3-(m-n)$ は 3 の倍数である。

ゆえに，$m-n$ を 3 で割った余りが k ならば m^3-n^3 を 3 で割った余りも k である。

解法 2

$$\begin{aligned} m^3-n^3&=(m-n)(m^2+mn+n^2)\\ &=(m-n)\{(m-n)^2+3mn\}\\ &=(m-n)^3+3mn(m-n)\end{aligned}$$

これと，$(m-m)^3\equiv k^3 \pmod 3$，$3mn(m-n)\equiv 0 \pmod 3$ より，

$m^3-n^3\equiv k^3 \pmod 3$

$k=0$ のとき $k^3\equiv 0 \pmod 3$

$k=1$ のとき $k^3\equiv 1^3\equiv 1 \pmod 3$

$k=2$ のとき $k^3\equiv 2^3\equiv 8\equiv 2 \pmod 3$

よって，$m-n$ を 3 で割った余りが k ならば m^3-n^3 を 3 で割った余りも k である。

86

$a=a'g,\ b=b'g$ （a' と b' は互いに素な自然数）とおくと，

$(a'+b')g=8075=5^2\cdot17\cdot19$

$l=a'b'g$ より，$a'b'=84=2^2\cdot3\cdot7$

$a'<b'$ だから，

a'	b'	$a'+b'$	g	$(a,\ b)$
1	84	85	$5\cdot19(=95)$	$(95,\ 7980)$
2	42	44	/	/
3	28	31	/	/
4	21	25	$17\cdot19(=323)$	$(1292,\ 6783)$
6	14	20	/	/
7	12	19	$5^2\cdot17(=425)$	$(2975,\ 5100)$

補足：*n* が合成数か素数かの判定法

n を合成数，その素因数の最小値を p，n を p で割った商を q すると，$n=pq$　・・・①

また，$p>q$ とすると，q は p より小さい素因数をもつことになるから不適。

よって，$p\leq q$　・・・②

①，②より，$n=pq\geq p^2$　$\therefore p\leq\sqrt{n}$

ゆえに，n が合成数ならば $\sqrt{n}$ 以下の素因数をもつ。

したがって，$8075=5^2\cdot323$ において，323 が合成数か素数かは，

$\sqrt{323}<18$ より，323 が 17 以下の素数で割り切れるかどうかで判断できる。

87

k を自然数とすると，任意の自然数は $6k-2,\ 6k-1,\ 6k,\ 6k+1,\ 6k+2,\ 6k+3$ のいずれかで表せる。これらのうち，2 でも 3 でも割り切れない自然数，すなわち P は $6k-1$ または $6k+1$ で表せる。

$P=6k-1$ のとき

$$\begin{aligned}P^2-1&=(6k-1)^2-1\\&=36k^2-12k\\&=12k(3k-1)\\&=12k\{2k+(k-1)\}\\&=24k^2+12(k-1)k\end{aligned}$$

ここで，$(k-1)k$ は連続する 2 つの自然数の積だから 2 の倍数である。

よって，$12(k-1)k$ も 24 の倍数である。

ゆえに，P^2-1 は 24 の倍数である。すなわち 24 で割り切れる。

$P=6k+1$ のとき

$$\begin{aligned}P^2-1&=(6k+1)^2-1\\&=36k^2+12k\\&=12k(3k+1)\\&=12k\{2k+(k+1)\}\\&=24k^2+12k(k+1)\end{aligned}$$

ここで，$k(k+1)$は連続する 2 つの自然数の積だから 2 の倍数である。

よって，$12k(k+1)$も 24 の倍数である。

ゆえに，P^2-1は 24 の倍数である。すなわち 24 で割り切れる。

以上より，題意が成り立つ。

88

(1)

解法 1

$y\equiv 0\pmod 5$のとき：$y^2+2\equiv 2\pmod 5$

$y\equiv \pm 1\pmod 5$のとき：$y^2+2\equiv 3\pmod 5$

$y\equiv \pm 2\pmod 5$のとき：$y^2+2\equiv 6\equiv 1\pmod 5$

よって，題意が成り立つ。

解法 2

$y=5k,\ 5k\pm 1,\ 5k\pm 2$（kは整数）をy^2+2に代入し，y^2+2が 5 の倍数でないことを示す。

(2)

与式を変形し，$5x^2=2(y^2+2)$とし，この等式が成り立つと仮定する。

(1)より，y^2+2は 5 で割り切れないから，5 は右辺の素因数ではない。

ところが，左辺は 5 を素因数にもつ。（矛盾）

よって，等式は成り立たない。

ゆえに，与式を満たす整数$x,\ y$の組は存在しない。

89

任意の正の整数nは$n=3k-2,\ 3k-1,\ 3k$（kは自然数）で表せる。

$n=3k-2$のとき

$n\equiv 1\pmod 3$より，$n^5+5\equiv 1^5+2\equiv 3\equiv 0\pmod 3$

これと$n^5+5>3$より，n^5+5は 3 より大きい 3 の倍数だから，素数ではない。

$n=3k-1$のとき

$n\equiv 2\pmod 3$より，$n^7+7\equiv n\left(n^2\right)^3+1\equiv 2\cdot 1^3+1\equiv 3\equiv 0\pmod 3$

これと$n^7+7>3$より，n^7+7は 3 より大きい 3 の倍数だから，素数ではない。

$n=3k$のとき

$n\equiv 0\pmod 3$より，$n^3+3\equiv 0+0\equiv 0\pmod 3$

これと$n^3+3>0$より，n^3+3は 3 より大きい 3 の倍数だから，素数ではない。

90

(1)

解法 1　ユークリッドの互除法

$3n^3+n=(n^3+1)\cdot 3+n-3$ より，

$3n^3+n$ と n^3+1 の最大公約数は n^3+1 と $n-3$ の最大公約数と等しい。

$n^3+1=(n-3)(n^2+3n+9)+28$ より，

n^3+1 と $n-3$ の最大公約数は $n-3$ と 28 の最大公約数と等しい。

よって，$3n^3+n$ と n^3+1 の最大公約数は $n-3$ と 28 の最大公約数と等しい。

また，28 は 5 を約数にもたないから，$n-3$ と 28 は 5 を公約数にもたない。

よって，$3n^3+n$ と n^3+1 の最大公約数に 5 は含まれない。すなわち $g\neq 5$

解法 2

$3n^3+n$ と n^3+1 が 5 を公約数にもつと仮定すると，

適当な整数 k，l を用いることにより，

$3n^3+n=5k$　・・・①

$n^3+1=5l$　・・・②

①$-3\times$②より，$n-3=5(k-3l)$　$\therefore n=5(k-3l)+3$

これより，$n\equiv 3 \pmod 5$

このとき，$3n^3+n\equiv 84\equiv 4 \pmod 5$，$n^3+1\equiv 28\equiv 3 \pmod 5$ となり，

$3n^3+n$ および n^3+1 は 5 の倍数でない。

これは①，②と矛盾する。

よって，$3n^3+n$ と n^3+1 は 5 を公約数にもたない。

ゆえに，$3n^3+n$ と n^3+1 の最大公約数に 5 は含まれない。すなわち $g\neq 5$

解法 3

$3n^3+n$ と n^3+1 の公約数について

$n\equiv 0 \pmod 5$ のとき

$3n^3+n\equiv 0 \pmod 5$，$n^3+1\equiv 1 \pmod 5$ より，5 は公約数でない。

$n\equiv -1 \pmod 5$ のとき

$3n^3+n\equiv -4\equiv 1 \pmod 5$，$n^3+1\equiv 0 \pmod 5$ より，5 は公約数でない。

$n\equiv 1 \pmod 5$ のとき

$3n^3+n\equiv 4 \pmod 5$，$n^3+1\equiv 2 \pmod 5$ より，5 は公約数でない。

$n\equiv -2 \pmod 5$ のとき

$3n^3+n\equiv -26\equiv -1\equiv 4 \pmod 5$，$n^3+1\equiv -7\equiv -2\equiv 3 \pmod 5$ より，5 は公約数でない。

$n\equiv 2 \pmod 5$ のとき

$3n^3+n\equiv 26\equiv 1 \pmod 5$，$n^3+1\equiv 9\equiv 4 \pmod 5$ より，5 は公約数でない。

以上より，5 は $3n^3+n$ と n^3+1 の公約数ではない。

ゆえに，$3n^3+n$ と n^3+1 の最大公約数に 5 は含まれない。すなわち $g\neq 5$

(2)

解法 1

(1)の解法 1 から

$n^3+1=(n-3)(n^2+3n+9)+28=(n-3)(n^2+3n+9)+14\cdot 2$ より，

$n-3=14$ のとき，$n^3+1=(n-3)(n^2+3n+11)+0$ となり，$g=14$　$\therefore n=17$

解法 2

$3n^3+n=14k$　・・・①

$n^3+1=14l$　・・・②

とおくと，

①$-3\times$②より，$n-3=14(k-3l)$　$\therefore n=14(k-3l)+3$

これより，$n\equiv 3 \pmod{14}$

このとき，$3n^3+n\equiv 84\equiv 0 \pmod{14}$，$n^3+1\equiv 28\equiv 0 \pmod{14}$ より，

$3n^3+n$ と n^3+1 は 14 を公約数にもつ。

そこで，$n=14m+3$（$m=0, 1, 2, \cdots$）とおくと，

$m=0$ のとき

$n=3$ より，$3n^3+n=84=28\cdot 3$，$n^3+1=28$

よって，$g=28$ となり，不適

$m=1$ のとき

$n=17$ より，

$3n^3+n=3\cdot 17^3+17=17(3\cdot 17^2+1)=17\cdot 868=17\cdot 62\cdot 14=14\cdot 2\cdot 17\cdot 31$

$n^3+1=17^3+1=4914=14\cdot 351$

2，17，31 は 351 の素因数ではない。

よって，$g=14$

以上より，$g=14$ となる n の最小値は 17

91

(1)

$a \equiv 0 \pmod 3$ のとき

$a^2 \equiv 0 \pmod 3$

$a \equiv 1 \pmod 3$ のとき

$a^2 \equiv 1 \pmod 3$

$a \equiv 2 \pmod 3$ のとき

$a^2 \equiv 4 \equiv 1 \pmod 3$

よって，a^2 を 3 で割った余りは 0 か 1 である。

別解

$a = 3k-2,\ 3k-1,\ 3k$ （k は自然数）を使って示す。

(2)

$3c^2 \equiv 0 \pmod 3$ より，$a^2+b^2 = 3c^2$ のとき，$a^2+b^2 \equiv 0$

これと(1)より，$a^2 \equiv b^2 \equiv 0 \pmod 3$

ゆえに，(1)より，$a \equiv b \equiv 0 \pmod 3$　・・・①

①より，$a = 3k,\ b = 3l$ （$k,\ l$ は自然数）とおくと，$a^2+b^2 = 9\left(k^2+l^2\right)$

よって，$9\left(k^2+l^2\right) = 3c^2$　$\therefore c^2 = 3\left(k^2+l^2\right) \equiv 0 \pmod 3$

ゆえに，(1)より，$c \equiv 0 \pmod 3$

以上より，題意が成り立つ。

(3)

ある自然数 $a_0,\ b_0,\ c_0$ が存在し，${a_0}^2+{b_0}^2 = 3{c_0}^2$ を満たすと仮定する。

(2)より，$a_0,\ b_0,\ c_0$ は 3 の倍数だから，

$a_0 = 3a_1,\ b_0 = 3b_1,\ c_0 = 3c_1$ となる自然数 $a_1,\ b_1,\ c_1$ が存在し，

$9{a_1}^2+9{b_1}^2 = 3\cdot 9{c_1}^2$ より，${a_1}^2+{b_1}^2 = 3{c_1}^2$

${a_n}^2+{b_n}^2 = 3{c_n}^2$ （$n = 0,\ 1,\ 2,\ \cdots$）が成り立つとき，

(2)より，$a_n,\ b_n,\ c_n$ は 3 の倍数であるから，

$a_n = 3a_{n+1},\ b_n = 3b_{n+1},\ c_n = 3c_{n+1}$ となる自然数 $a_{n+1},\ b_{n+1},\ c_{n+1}$ が存在する。

よって，帰納的に，

$a^2+b^2 = 3c^2$ を満たす自然数 $a_n,\ b_n,\ c_n$ （$n = 0,\ 1,\ 2,\ \cdots$）は無数存在する。

ところが，$a_n = 3a_{n+1},\ b_n = 3b_{n+1},\ c_n = 3c_{n+1}$ （$n = 0,\ 1,\ 2,\ \cdots$）より，

$a_0 > a_1 > a_2 > \cdots > a_n > a_{n+1} > \cdots > 0$，$b_0 > b_1 > b_2 > \cdots > b_n > b_{n+1} > \cdots > 0$，

$c_0 > c_1 > c_2 > \cdots > c_n > c_{n+1} > \cdots > 0$ となるから，

$a_n,\ b_n,\ c_n$ （$n = 0,\ 1,\ 2,\ \cdots$）の数は有限である。（矛盾）

ゆえに，${a_0}^2+{b_0}^2 = 3{c_0}^2$ を満たすある自然数 $a_0,\ b_0,\ c_0$ は存在しない。

すなわち $a^2+b^2 = 3c^2$ を満たす自然数 $a,\ b,\ c$ は存在しない。

92

(1)

$a^b-1=p$ （p は素数）とすると，$a^b-1=(a-1)(a^{b-1}+a^{b-2}+\cdots+1)$ より，

$(a-1)(a^{b-1}+a^{b-2}+\cdots+1)=p$

a, b は 2 以上の整数だから，$1\le a-1\le a^{b-1}+a^{b-2}+\cdots+1$

よって，$a-1=1$ すなわち $a=2$

このとき，$2^b-1=p$

b が合成数のとき

b は 2 以上の 2 つの整数の積で表せるから，$b=mn$（m, n は 2 以上の整数）とおくと，

$$\begin{aligned}2^b-1&=2^{mn}-1\\&=(2^m)^n-1\\&=(2^m-1)\{(2^m)^{n-1}+(2^m)^{n-2}+\cdots+1\}\end{aligned}$$

$$3\le 2^m-1<(2^m)^{n-1}+(2^m)^{n-2}+\cdots+1$$

よって，2^b-1 は 3 以上の 2 つの整数の積で表せることから素数ではない。

b が素数のとき

2^b-1 は $(2-1)(2^{b-1}+2^{b-2}+\cdots+1)$

すなわち 1 と $2^{b-1}+2^{b-2}+\cdots+1$ の積でしか表せないから，2^b-1 は素数である。

以上より，a^b-1 が素数ならば，$a=2$ であり，かつ b は素数である。

(2)

命題の対偶「$b=2^c$ と表せないならば a^b+1 は素数でない」が真であることを示す。

$b=2^c$ と表せないことと b が 3 以上の奇数を因数にもつことは同値だから，

2^c と表せない b を $b=2^c\cdot k$ （c は 0 以上の整数，k は 3 以上の奇数）とおくと，

$$\begin{aligned}a^b+1&=a^{2^c\cdot k}+1\\&=(a^{2^c})^k+1\end{aligned}$$

ここで，式を簡単にするため，$a^{2^c}=A$ とおくと，k は奇数だから，

$$\begin{aligned}a^b+1&=A^k+1\\&=(A+1)(A^{k-1}-A^{k-2}+\cdots-A+1)\end{aligned}$$

これと

$A=a^{2^c}\ge 2^{2^0}=2$ より，

$A+1\ge 3$

$$\begin{aligned}A^{k-1}-A^{k-2}+\cdots-A+1&=(A^2-A+1)(A^{k-3}+A^{k-6}+\cdots+1)\\&\ge A^2-A+1\end{aligned}$$

$$=\left(A-\frac{1}{2}\right)^2+\frac{3}{4}$$
$$\geq\left(2-\frac{1}{2}\right)^2+\frac{3}{4}$$
$$=3$$

より，

a^b+1は 3 以上の 2 つの整数の積で表されるから，a^b+1は素数でない。

よって，命題の対偶が真である。

ゆえに，命題は真である。

補足

初項 1，公比$-A$，項数nの等比数列の和は$1+(-A)^1+(-A)^2+\cdots+(-A)^{n-1}=\dfrac{1-(-A)^n}{1-(-A)}$

nが奇数ならば，$1-A+A^2-\cdots-A^{n-2}+A^{n-1}=\dfrac{1+A^n}{1+A}$より，

$A^n+1=(A+1)\left(A^{n-1}-A^{n-2}+\cdots-A+1\right)$