

「はじめての数論」の回答例

yassu

平成 29 年 1 月 5 日

1 第 1 章の回答例

1.1 以下のプログラムによって, 3, 4 番目の三角数は $1225 = 35^2$, $416 = 204^2$.

有効な方法は分らない.

こんな数はたぶん無限にある.

1.2

$$\begin{aligned}1 &= 1^2, \\1 + 3 &= 4 = 2^2, \\4 + 5 &= 9 = 3^2, \\9 + 7 &= 16 = 4^2, \\16 + 9 &= 25 = 5^2\end{aligned}$$

などとなるから

$$\sum_{j=1}^n (2j-1) = n^2$$

が予想される.

1.3

三つ子素数は $(3, 5, 7)$ に限ることを示す.

任意の自然数は $3l, 3l+1, 3l+2 (l \in \mathbf{N})$ と表すことができる.

$(p, p+2, p+4)$ を三つ子素数とする. このとき, ある自然数 l があって, $p = 3l, 3l+1, 3l+2$ のいずれかで表される.

$l = 1$ のとき, $(p, p+2, p+4) = (3, 5, 7)$ である.

$l \neq 1$ のとき, $3l$ は素数ではないから, $p = 3l+1$ もしくは $3l+2$ と表される.

$p = 3l+1$ とすると, $p+2 = 3l+3 = 3(l+1)$ となって, これは素数ではないから不敵.

$p = 3l+2$ とすると, $p+2 = 3l+4, p+4 = 3l+6 = 3(l+2)$ となるから, $p+4$ は素数ではない.

以上によって、三つ子素数は (3, 5, 7) に限る.

1.4 (a) $N^2 - 1$ が十数であるのは $N = 2$ のときに限る. なぜなら,

$$N^2 - 1 = (N - 1)(N + 1)$$

であり, $N^2 - 1$ が十数であるためには $N - 1 = 1$ となる必要があるからである.

(b) おそらく無数に存在する. N によってそれぞれ調べてみると

$$N = 2 \Rightarrow N^2 - 2 = 2; \text{素数},$$

$$N = 3 \Rightarrow N^2 - 2 = 7; \text{素数},$$

$$N = 4 \Rightarrow N^2 - 2 = 14 = 2 \times 7,$$

$$N = 5 \Rightarrow N^2 - 2 = 23; \text{素数},$$

$$N = 6 \Rightarrow N^2 - 2 = 34 = 2 \times 17,$$

$$N = 7 \Rightarrow N^2 - 2 = 47; \text{素数},$$

$$N = 8 \Rightarrow N^2 - 2 = 62 = 2 \times 31,$$

$$N = 9 \Rightarrow N^2 - 2 = 79; \text{素数},$$

$$N = 10 \Rightarrow N^2 - 2 = 98 = 2 \times 7^2,$$

$$N = 11 \Rightarrow N^2 - 2 = 119,$$

$$N = 12 \Rightarrow N^2 - 2 = 142 = 2 \times 71,$$

$$N = 13 \Rightarrow N^2 - 2 = 167,$$

$$N = 14 \Rightarrow N^2 - 2 = 194 = 2 \times 97,$$

$$N = 15 \Rightarrow N^2 - 2 = 253.$$

(c) $N^2 - 3$ の形の素数は多分無数に存在する.

最初の方から正の数を列挙してみると

$$N = 2 \Rightarrow 2^2 - 3 = 1,$$

$$N = 3 \Rightarrow 3^2 - 3 = 6 = 2 \times 3,$$

$$N = 4 \Rightarrow 4^2 - 3 = 13; \text{素数},$$

$$N = 5 \Rightarrow 5^2 - 3 = 22 = 2 \times 11,$$

$$N = 6 \Rightarrow 6^2 - 3 = 33 = 3 \times 11,$$

$$N = 7 \Rightarrow 7^2 - 3 = 46 = 2 \times 23,$$

$$N = 8 \Rightarrow 8^2 - 3 = 61; \text{prime},$$

$$N = 9 \Rightarrow 9^2 - 3 = 78 = 2 \times 39,$$

$$N = 10 \Rightarrow 10^2 - 3 = 97; \text{prime}$$

$N^2 - 4$ の形の素数は 5 に限る. なぜなら

$$N^2 - 4 = (N - 2)(N + 2)$$

となるからである.

(d) 少なくとも平方数ではない.

1.5

n が偶数のとき:

$n = 2m$ とおくと

$$\begin{aligned}1 + 2 + \cdots + 2m &= (2m + 1) + ((2m - 1) + 2) + ((2m - 2) + 3) + \cdots + ((m + 1) + m) \\&= m \cdot (2m + 1) \\&= \frac{n}{2}(n + 1).\end{aligned}$$

n が奇数のとき:

$n = 2m - 1$ とおくと

$$\begin{aligned}1 + 2 + \cdots + (2m - 1) &= (1 + (2m - 1)) + (2 + (2m - 2)) + \cdots + ((m - 1) + (m + 1)) + m \\&= \underbrace{2m + 2m + \cdots + 2m}_{m-1} + m \\&= 2m(m - 1) + m \\&= (n + 1)\left(\frac{n + 1}{2} - 1\right) + \frac{n + 1}{2} \\&= (n + 1)\left(\frac{n + 1}{2} - 1 + \frac{1}{2}\right) \\&= (n + 1) \cdot \frac{n + 1 - 2 + 1}{2} = \frac{n}{2}(n + 1).\end{aligned}$$

2 第2章の回答例

2.1 (a) 組み合わせとして考えるのは

$$\begin{aligned}(a, b) &= (3m, 3n), (3m + 1, 3n), (3m + 2, 3n), \\&\quad (3m, 3n + 1), (3m + 1, 3n + 1), (3m + 2, 3n + 1), \\&\quad (3m, 3n + 2), (3m + 1, 3n + 2), (3m + 2, 3n + 2)\end{aligned}$$

のように書かれる場合である. 必要なら a と b を入れ替えることによって, この表の右上半分だけを考える. すなわち,

$$(a, b) = (3m + 1, 3n + 1), (3m + 2, 3n + 1), (3m + 2, 3n + 2)$$

の場合 対応する既約ピタゴラス数 (a, b, c) が存在しないことを示したい.

まず, $c = 3l$ とかけているとき, c^2 は 3 の倍数であり, $c = 3l + 1$ とかけているとき, c^2 は 3 で割ると 1 余り, $c = 3l + 2$ とかけているとき, c^2 は 3 で割ると 1 余る.

$(a, b) = (3m + 1, 3n + 1)$ のとき,

$$\begin{aligned}a^2 + b^2 &= (3m + 1)^2 + (3n + 1)^2 \\&= 9(m^2 + n^2) + 6(m + n) + 2\end{aligned}$$

となるが, c^2 は 3 で割ると 2 余る組がないから不適.

$(a, b) = (3m + 2, 3n + 1)$ のとき,

$$a^2 + b^2 = 9(m^2 + n^2) + 6(2m + n) + 5.$$

よって, この場合も $a^2 + b^2$ を 3 で割ると 2 余るので不適.

$(a, b) = (3m + 2, 3n + 2)$ のとき

$$(3m + 2)^2 + (3n + 2)^2 = 9(m^2 + n^2) + 12(m + n) + 8.$$

よってこの場合も $a^2 + b^2$ を 3 で割ると 2 余るので不適.

(b) 分らない.

2.2 仮定より, ある整数 k_1, k_2 があって

$$m = dk_1,$$

$$n = dk_2$$

が成り立つ. このとき,

$$m + n = d(k_1 + k_2),$$

$$m - n = d(k_1 - k_2)$$

となるから, 主張を得る.

2.3 (a) 任意の 1 より大きな奇数が現れる. 実際, 定理 2.1 で $t = 1$ とおけば $a = s$.

(b) 少なくとも 4 の倍数が現れる. 8 で割って 4 余る数はかならず現れる.

b は 4 の倍数であることを示す.

s, t はともに奇数であるから, ある自然数 s_1, t_1 があって, $s = 2s_1 - 1$, $t = 2t_1 - 1$ が成り立つ. このとき

$$\begin{aligned} b &= \frac{1}{2}(s - t)(s + t) \\ &= \frac{1}{2}(2s_1 - t_1)(2s_1 + 2t_1 - 2) \\ &= 2(s_1 - t_1)(s_1 + t_1 - 1) \end{aligned}$$

となる. ここで, $s_1 - t_1$ と $s_1 + t_1 - 1$ は 2 を法として異なるので, b は 4 の倍数である.

次に, 8 で割って 4 余る数は必ず現れることを示す.

b を 4 で割って 8 余る自然数とする. ある互いに素な奇数 $s, t (s > t)$ があって

$$b = \frac{s^2 - t^2}{2}$$

を満たすことを示したい. $b = 4k (k \text{ は奇数})$ と置くと

$$4k = \frac{s^2 - t^2}{2}.$$

分母を払って

$$8k = s^2 - t^2.$$

ここで

$$\begin{aligned} s^2 &= t^2 + 8k \\ &= t^2 + 8(k-2) + 16 \end{aligned}$$

であるから, $t = (k-2)^2$ と置くと

$$\begin{aligned} s^2 &= (k-2)^2 + 8(k-2) + 16 \\ &= (k+2)^2. \end{aligned}$$

よって, $s = k+2$ と置けばよい. 最後に, k は奇数であったから, $k-2$ と $k+2$ は互いに素である.

(c) 4 で割ると 1 余る数.

$s = 2s_1 - 1, t = 2s_2 - 1$ と置くと

$$\begin{aligned} c &= \frac{s^2 + t^2}{2} \\ &= \frac{1}{2}((2s_1 - 1)^2 + (2s_2 - 1)^2) \\ &= \frac{1}{2}(8(s_1^2 + s_2^2) - 8s_1s_2 + 2) \\ &= 4(s_1^2 + s_2^2) - 4s_1s_2 + 1 \\ &= 4(s_1^2 - s_1s_2 + s_2^2) + 1 \end{aligned}$$

となるから, c は 4 で割ると 1 余る.

2.4 見つけられない.

2.5 a) $n \leq 4$ における a, b, c の値を表にすると

$T_1 = 1$	$b_1 = 4 \cdot 1 = 4$	$3^2 + 4^2 = 5^2,$
$T_2 = 1 + 2 = 3$	$b_2 = 4 \cdot 3 = 12$	$5^2 + 12^2 = 13^2,$
$T_3 = 3 + 3 = 6$	$b_3 = 4 \cdot 6 = 24$	$7^2 + 24^2 = 25^2,$
$T_4 = 6 + 4 = 10$	$b_4 = 4 \cdot 10 = 40$	$9^2 + 40^2 = 41^2.$

ここで, b_n を T_n に対応する既約ピタゴラス数の b とおいた.

T_5) $T_5 = 10 + 5 = 15$. また, $b_5 = 4 \cdot 15 = 60$.

これより, $11^2 + 60^2 = 61^2$ が予想できる. 実際計算してみると

$$11^2 + 60^2 = 121 + 3600 = 3721 = 61^2.$$

T_6) $T_6 = 15 + 6 = 21, b_6 = 4 \cdot 21 = 84$ より

$$13^2 + 84^2 = 85^2$$

が予想できる. 計算してみると

$$\begin{aligned}13^2 + 84^2 &= 169 + 7059 \\ &= 7225, \\ 85^2 &= 7225\end{aligned}$$

であるから, 確かに成り立っている.

T_7) $T_7 = 21 + 7 = 28$, $b_7 = 4 \cdot 28 = 112$ であるから

$$15^2 + 112^2 = 113^2$$

が予想される. 実際

$$\begin{aligned}15^2 + 112^2 &= 225 + 12544 \\ &= 12769, \\ 113^2 &= 12769\end{aligned}$$

なので, 確かに成り立っている.

b) 存在する.

$$(a, b, c) = (2n + 1, 4T_n, 4T_n + 1)$$

が既約ピタゴラス数の組であることを示す. 実際, 定理 2.1 において $t = 1$, $s = 2n + 1$ とおけば t と s は互いに素で

$$\begin{aligned}a &= 2n + 1, \\ b &= \frac{(2n + 1)^2 - 1}{2} \\ &= \frac{4n^2 + 4n}{2} \\ &= 2n(n + 1) \\ &= 4 \cdot \frac{n}{2}(n + 1) = 4T_n, \\ c &= \frac{1^2 + (2n + 1)^2}{2} \\ &= \frac{4n^2 + 4n + 2}{2} \\ &= 2n^2 + 2n + 1 \\ &= 4 \cdot \frac{n}{2}(n + 1) + 1 = 4T_n + 1.\end{aligned}$$

2.6

定理 2.1 において $c - a = 2$ とおけば

$$c - a = \frac{s^2 + t^2}{2} - st = 2$$

より

$$s = t + 2$$

を得る.

(a)

$t = 1, s = 3$ とおけば

$$a = 3, \quad b = \frac{9-1}{2} = 4, \quad c = \frac{3^2+1^2}{2} = 5.$$

また, $t = 3, s = 5$ とおけば

$$a = 15, b = \frac{5^2-3^2}{2} = \frac{16}{2} = 8, c = \frac{3^2+5^2}{2} = 17.$$

(b)

差が 2 である自然数の組が共通因数を持つには, その 2 つの自然数が偶数であり, 共通因数は 2 である場合にかぎる.

例えば, $s = 999, t = 997$ とおくと

$$a = 999 \cdot 997, b = \frac{999^2 - 997^2}{2}, c = \frac{999^2 + 997^2}{2}$$

を得て, $c - a = 2$ である.

(c) $s = t + 2$ を定理 2.1 に代入すればよい. すなわち

$$\begin{aligned} a &= t \cdot (t + 2), \\ b &= \frac{(t + 2)^2 - t^2}{2} \\ &= \frac{4t + 4}{2} \\ &= 2(t + 1), \\ c &= \frac{t^2 + (t + 2)^2}{2} \\ &= \frac{2t^2 + 4t + 4}{2} \\ &= t^2 + 2t + 2. \end{aligned}$$

ここで, t は奇数.

2.7 定理 2.1 の下の表に $2c - 2a = 2(c - a)$ の値を追記すると以下のようになる.

s	t	a	b	c	$2(c-a)$
3	1	3	4	5	4
5	1	5	12	13	8
7	1	7	24	25	36
9	1	9	40	41	64
5	3	15	8	17	4
7	3	21	20	29	16
7	5	35	12	37	4
9	5	45	28	53	16
9	7	63	15	65	4

この表によって $2(c-a) = (s-t)^2$ が予想される. 実際

$$\begin{aligned}
 2 \cdot (c-a) &= 2 \cdot \left(\frac{s^2+t^2}{2} - st \right) \\
 &= s^2 + t^2 - 2st \\
 &= s^2 - 2st + t^2 \\
 &= (s-t)^2
 \end{aligned}$$

であるから, 主張は正しい.

3 第3章の回答例

3.1

(a) u と v が共通因数 $k > 1$ をもつとする. このとき, $u = ku', v = kv'$ とおくと

$$a = k^2(u'^2 - v'^2), \quad b = 2k^2u'v', \quad c = k^2(u'^2 + v'^2)$$

となるから, a, b, c は共に k^2 で割り切れる.

(b) u, v が共に奇数であれば, $u^2 - v^2, u^2 + v^2$ は偶数であるから, (a, b, c) は既約ピタゴラス数の組でない.

$u = 3, v = 1$ とおくと

$$(a, b, c) = (8, 6, 10)$$

となるが, これは既約ピタゴラス数の組ではない.

(c) (d) の問題のために, s と t が共通因数を持つ場合は右に ✓ を, s と t が共通因数を持たないが (a, b, c) が既約ピタゴラス数の組ではない場合は ✓✓ をつける.

u	v	a	b	c	
2	1	3	4	5	
3	1	8	6	10	✓✓
3	2	5	12	13	

4	1	15	8	17	
4	2	12	16	20	✓
4	3	7	24	25	
5	1	24	10	26	✓✓
5	2	21	20	29	
5	3	16	30	34	✓✓
5	4	9	40	41	
6	1	35	12	37	
6	2	32	24	40	✓
6	3	27	36	45	✓
6	4	20	48	50	✓
6	5	11	60	61	
7	1	48	14	50	✓✓
7	2	45	28	53	
7	3	40	42	58	✓✓
7	4	33	56	65	
7	5	24	70	74	✓✓
7	6	13	84	85	
8	1	63	16	65	
8	2	60	32	68	✓
8	3	55	48	73	
8	4	48	64	80	✓
8	5	39	80	89	
8	6	28	96	90	✓
8	7	15	112	113	
9	1	80	18	82	✓✓
9	2	77	36	85	
9	3	72	54	90	✓
9	4	65	72	97	
9	5	56	90	106	✓✓
9	6	45	108	117	✓
9	7	32	126	130	✓✓
9	8	17	144	145	
10	1	99	20	101	
10	2	96	40	104	✓
10	3	91	60	109	
10	4	84	80	116	✓
10	5	75	100	125	✓
10	6	64	120	136	✓

10	7	51	140	149	
10	8	36	160	164	✓
10	9	19	180	181	

(d) 「 u と v が共通因数を持たない」 かつ 「 u と v の偶奇が異なる」.

(e) u と v が共通因数を持つ場合, (a, b, c) は既約ではないことは 3.1 で示した. u と v が奇数であるとき, $u^2 - v^2$ は偶数であり, $2uv$ も偶数であるから, (a, b, c) は既約でない.

u と v が共通因数を持たず, u と v の偶奇が異なるとき $u^2 - v^2$ と $2uv$ が互いに素であることを示そう.

$u^2 - v^2$ と $2uv$ が素数 p を共通因数として持ったとして, $2uv = pu'$, $u^2 - v^2 = pv'$ とおく.

$u^2 - v^2$ は奇数であるから, p は奇素数である. また, $2uv = pu'$ より, u か v は p の倍数である.

よって, u も v も p の倍数であり, これは u と v が共通因数を持たないことに反する.

3.2

(a) 円の方程式 $x^2 + y^2 = 2$ に傾き $m \in \mathbf{Q}$ で $(1, 1)$ を通る直線の方程式 $y = m(x - 1) + 1 = mx - m + 1$ を代入すると

$$x^2 + (m(x - 1) + 1)^2 = 2$$

$$x^2 + (mx - m + 1)^2 = 2$$

$$(1 + m^2)x^2 + 2mx(1 - m) + m^2 - 2m - 1 = 0$$

$$(x - 1)((1 + m^2)x - (m^2 - 2m - 1)) = 0.$$

よって, $x \neq 1$ とすると

$$x = \frac{m^2 - 2m - 1}{1 + m^2}.$$

これを $y = mx - m + 1$ に代入して

$$\begin{aligned} y &= m \cdot \frac{m^2 - 2m - 1}{1 + m^2} - m + 1 \\ &= \frac{m(m^2 - 2m - 1) - m(1 + m^2) + 1 + m^2}{1 + m^2} \\ &= \frac{-m^2 - 2m + 1}{1 + m^2} \\ &= -\frac{m^2 + 2m - 1}{1 + m^2}. \end{aligned}$$

最後に $m = \frac{v}{u}$ とおくと

$$\begin{aligned}x &= \frac{v^2 - 2uv - u^2}{u^2 + v^2}, \\y &= -\frac{v^2 + 2uv - u^2}{u^2 + v^2} \\&= \frac{u^2 - 2uv - v^2}{u^2 + v^2}.\end{aligned}$$

3.3

$x^2 + y^2 = 1$ に $(-1, 0)$ を通り $m \in \mathbf{Q}$ を傾きとする直線の方程式 $y = m(x+1)$ を連立させると

$$\begin{aligned}x^2 - m^2(x+1)^2 &= 1. \\(1 - m^2)x^2 - 2m^2x - 1 - m^2 &= 0. \\(x+1)((1 - m^2)x - (1 + m^2)) &= 0.\end{aligned}$$

$x \neq -1$ とすると

$$x = \frac{1 + m^2}{1 - m^2}.$$

これを $y = m(x+1)$ に代入すると

$$\begin{aligned}y &= m(x+1) \\&= m \cdot \left(\frac{1 + m^2}{1 - m^2} + 1 \right) \\&= m \cdot \frac{1 + m^2 + 1 - m^2}{1 - m^2} \\&= \frac{2m}{1 - m^2}.\end{aligned}$$

また, $m = \frac{v}{u}$ とおくと

$$x = \frac{u^2 + v^2}{u^2 - v^2}, \quad y = \frac{2uv}{u^2 - v^2}.$$