11/14 更新

Q.046

Step 1. $a^2 \leqq a$ のとき。
このとき $0 \leqq a \leqq 1$ である。x が $(x-a)(x-a^2) < 0$ を満たすことと, 区間 (a^2, a) に属することは同値である。しかし, a の範囲から $(a^2, a) \subset (0, 1)$ なので, 5 つの整数を含めることは出来ない。よってこの場合解なし。

Step 2. $a^2 > a$ のとき。
$a < 0$ または $a > 1$ である。x は区間 (a, a^2) に属する。この区間に整数が 5 個入っていれば良い。つまり, ある整数 N が存在して

$$N \leqq a < N+1 < N+2 < N+3 < N+4 < N+5 < a^2 \leqq N+6$$

であればよいが, 整数 N が $N \leqq a < N+1$ を満たすことは $N = \lfloor a \rfloor$ であること, それと同様に $N+5 < a^2 \leqq N+6$ は $N+6 = \lceil a^2 \rceil$ と同じであることに注意すると,

$$\lfloor a \rfloor + 6 = \lceil a^2 \rceil$$

を a が満たすことと, (a, a^2) が整数を 5 個含むことは同値である。そこで, 上を満たす a を求めることとしよう。

$\lfloor x \rfloor \lceil x^2 \rceil \geqq x^2$ を使うと,

$$a + 6 \geqq a^2 \quad \Leftrightarrow \quad (a-3)(a+2)$$

を満たすことが必要条件となる。よって $-2 \leqq a \leqq 3$ が必要条件である。以下, $\lfloor a \rfloor = k$ の値で場合分け $(k = -2, -1, 0, 1, 2, 3)$ をする。

(i) $k = -2$ のとき
$-2 \leqq a < -1$ かつ, $4 = \lceil a^2 \rceil$ となる。

$$\lceil a^2 \rceil = 4 \Leftrightarrow 3 < a^2 \leqq 4$$

であるから, $-2 \leqq a < -\sqrt{3}$ である。

(ii) $k = -1$ のとき
$-1 \leqq a < 0$ かつ,

$$\lceil a^2 \rceil = 5 \Leftrightarrow 4 < a^2 \leqq 5$$

なので解なし。

(iii) $k = 0$ のとき
$0 \leqq a < 1$ かつ $5 < a^2 \leqq 6$ なので解なし。

(iv) $k = 1$ のとき
$1 \leqq a < 2$ かつ $6 < a^2 \leqq 7$ なので解なし。

(v) $k = 2$ のとき
$2 \leqq a < 3$ かつ $7 < a^2 \leqq 8$ である。これは $\sqrt{7} < a < 2\sqrt{2}$ のときである。

(vi) $k = 3$ のとき
$-2 \leqq a \leqq 3$ かつ $k = 3$ なので $a = 3$ のときである。これは $\lceil 9 \rceil = 9$ を満たすので解である。

以上より

$$\boldsymbol{-2 \leqq a < -\sqrt{3}, \quad \sqrt{7} < a < 2\sqrt{2}, \quad a = 3}$$

Q.065

(1) $X = 5 \cdot 2^7$ とする。注意より $X + 1 = 641$ であるが,

$$\begin{aligned} 5^4 \cdot 2^{28} + 2^{32} &= 2^{28}(5^4 + 2^4) = 2^{28} \cdot 641 \\ 5^4 \cdot 2^{28} - 1 &= X^4 - 1 \\ &= (X+1)(X-1)(X^2+1) \\ &= 641(X-1)(X^2+1) \end{aligned}$$

となるので, いずれも 641 の倍数である。 □

(2) $(5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1$ で, 左辺が 641 の倍数同士の和なのでこれも 641 の倍数である。

Q.090

(1) n の 10 進法表示は

$$n = \sum_{k=0}^{N} a_k 10^k \quad (N \geqq 0, a_k \in \{0, 1, \cdots, 9\}$$

であるが, これの mod9 が

$$n \equiv \sum_{k=0}^{N} a_k (10-9)^k = \sum_{k=0}^{N} a_k \pmod 9$$

となり, 右辺はまさしく桁の数字の総和を表す。 □

(2) 入っていない桁を a とする。a は $\{0, 1, \cdots, 9\}$ の元である。このとき, 2^{29} の桁の総和は

$$0 + 1 + 2 + \cdots + 8 + 9 - a = 45 - a$$

である。一方で, $2^{29} \equiv 5 \pmod 9$ であるから, $5 \equiv 45 - a$ でなければならない。これを解くと $a \equiv 4 \pmod 9$ となり,a は $\{0, 1, \cdots, 9\}$ の元であるから, $a = 4$ である。

Q.74

(1) $u=1+\sqrt{2}$ であることを示す。$G \ni u > 1$ はよい。$1 < w \leqq u$ なる $w \in G$ を考え, $w = a+b\sqrt{2}$ とおく。$|a^2-2b^2| = w|a-b\sqrt{2}| = 1$ であるから,

$$|a-b\sqrt{2}| = \frac{1}{w} < 1 \quad (\because w > 1)$$

より, $-1 < a-b\sqrt{2} < 1$ となる。これと $1 < w = a+b\sqrt{2}$ が成り立つから,

$$-1+1 < (a-b\sqrt{2}) + (a+b\sqrt{2})$$

$$1+(a-b\sqrt{2}) < 1+(a+b\sqrt{2})$$

が成り立つ。整理して $0<a$, $0<b$ を得るので, $1 \leqq a, 1 \leqq b$ でなければならず, 結局

$$1+\sqrt{2} = u \leqq w$$

となる。$1 < w \leqq u$ としたから, $w=u$ となる。すなわち u は最小である。

(2) 次を示す。

$$w_1, w_2 \in G \quad \Rightarrow \quad w_1 w_2 \in G$$

$w_i = a_i + b_i\sqrt{2} \quad (a_i^2 - 2b_i^2 = \pm 1, w_i > 0)$ とおく。$w_1 w_2 > 0$ であることは明らか。積を計算すると

$$w_1 w_2 = (a_1 a_2 + 2b_1 b_2) + \sqrt{2}(a_2 b_1 + a_1 b_2)$$

であるが,

$$\begin{aligned} & (a_1 a_2 + 2b_1 b_2)^2 - 2(a_2 b_1 + a_1 b_2)^2 \\ = \ & (a_1 a_2)^2 + 4(b_1 b_2)^2 - 2(a_2 b_1)^2 - 2(a_1 b_2)^2 \\ = \ & (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) \\ = \ & \pm 1 \quad (a_i^2 - 2b_i^2 \in \{-1, 1\}) \end{aligned}$$

となる。よって, $w_1 w_2 \in G$ が示された。つまり「G は積で閉じている」ことが示された。

次に整数 n に対して $u^n \in G$ を示す。$n=0$ のときは $u^0 = 1$ で, 明らかに G に含まれる。n が正なら, $u \in G$ から, 先の積で閉じていることを用いると $u^n \in G$ となる。n が負なら, $(u^{-1})^{-n}$ を考え, $u^{-1} = \sqrt{2}-1 \in G$ なので, この場合も G が積で閉じていることから, u^n は G に属する。よって, すべての $n \in \mathbb{Z}$ で $u^n \in G$ である。

最後に, $w_1 = g$, $w_2 = u^n$ として適用すれば $gu^n \in G$ が導かれ, 題意は示された。 □

(3) G の元 g をひとつ取る。このとき, ある整数 $n(g)$ が存在して

$$u^{n(g)-1} < g \leqq u^{n(g)}$$

を満たす。両辺を $u^{n(g)-1}$ で割ると

$$1 < gu^{-n(g)+1} \leqq u$$

であり, (2) で示したことから $gu^{-n(g)+1}$ は G の元であって, さらに 1 より大きい。(1) で u の最小性を示したので, $gu^{-n(g)+1} = u$ でなければならない。よって $g = u^{n(g)}$ を得るから, 題意は示された。 □

Q.162(12/2 更新)

体積を求める領域を K とし, その体積を V とする。曲線 $y = \log x \ (1 \leqq x \leqq e)$ を x 軸で回転させたときの曲面は

$$\begin{cases} y^2 + z^2 = (\log x)^2 \\ 1 \leqq x \leqq e \end{cases}$$

として表せる。この曲面は xz 平面対称であるから K もそうであり, K のうちの $y \geqq 0$ の部分の体積は $\frac{1}{2}V$ である。

K は $-1 \leqq y \leqq 1$ の範囲に存在するので, $y = k \ (0 \leqq k \leqq 1)$ で K を切断したときの断面積を考える。上の y 軸で回す前の曲面の定式化から, その曲面を $y=k$ で切断した部分を xz 平面へ射影すると

$$\begin{cases} z^2 = (\log x)^2 - k^2 \\ e^k \leqq x \leqq e \end{cases}$$

という曲線になるので, これを C_k と呼ぶこととする。C_k 上の点 P は $(t, \pm\sqrt{(\log t)^2 - k^2})$ と書くことができ $(e^k \leqq t \leqq e)$, 符号がいずれであっても $(0,0)$ との距離は $t^2 + (\log t^2) - k^2 =: D(t)$ となる。$D(t)$ は明らかに $[e^k, e]$ 上増加するから, $e^{2k} \leqq D(t) \leqq e^2 + 1 - k^2$ であることが分かる。これは, C_k 上で最も原点に近い点が $(e^{2k}, 0)$ であり, 最も遠い点が $(e, \sqrt{1-k^2})$ であることから来る。よって, C_k を原点中心に回転させると, 極座標で表現して **円環領域 $\boldsymbol{e^k \leqq r \leqq \sqrt{e^2+1-k^2}}$** になることが分かるので, これが K の平面 $y=k$ による断面である。つまり, その断面積を $S(k)$ とおけば

$$S(k) = \pi(e^2 + 1 - k^2 - e^{2k})$$

となる。よって,

$$\begin{aligned} \frac{1}{2}V &= \int_0^1 S(y)\,dy \\ &= \pi \int_0^1 (e^2 + 1 - y^2 - e^{2y})\,dy \\ &= (e^2+1)\pi - \pi \int_0^1 (y^2 + e^{2y})\,dy \\ &= (e^2+1)\pi - \pi \left[\frac{y^3}{3} + \frac{1}{2}e^{2y} \right]_0^1 \\ &= (e^2+1)\pi - \left\{ \left(\frac{1}{3} - 0 \right)\pi - \frac{1}{2}\left(e^2 - 1\right)\pi \right\} \\ &= \left(\frac{1}{2}e^2 + \frac{7}{6} \right)\pi \end{aligned}$$

以上より, $\boldsymbol{V = \left(e^2 + \frac{7}{3} \right)\pi}$

Q.126(12/3 更新)

まず, $\dfrac{d}{dx}(864n^2 f(x)) = 3x(36n - x)$ であることに注意すると, $f(x)$ は区間 $[0, 36n]$ 上増加しているため, i を $0 \leqq i < 36n$ を満たす整数であるとして, $[f(i)] \leqq [f(i+1)]$ が常に成り立つことが分かる。したがって, このような i のうち, この不等式の等号を生じさせないものが k 種類あるとすれば, 求める個数は $k+1$ である。

$f(i+1) - f(i) - 1$ を計算してみる。

$$\begin{aligned} & \frac{1}{864n^2}\left\{54n((i+1)^2 - i^2) - ((i+1)^3 - i^3)\right\} - 1 \\ = \ & \frac{1}{864n^2}\left\{-3i^2 + (108n-3)i + (54n-1) - 864n^2\right\} \end{aligned}$$

{ } の中身の i の二次式について, 判別式 D を計算する:

$$D = (108n-3)^2 + 12(-864n^2 + 54n - 1) = 1296n^2 - 3$$

よって, 2 次方程式 $-3X^2 + (108n-3)X + (-864n^2 + 54n - 1) = 0$ の解は $X = 18n - \dfrac{1}{2} \pm \dfrac{\sqrt{D}}{6}$ と求まるので,

$$f(i+1) - f(i) - 1 \geqq 0 \Leftrightarrow 18n - \frac{1}{2} - \frac{\sqrt{D}}{6} \leqq i \leqq 18n - \frac{1}{2} + \frac{\sqrt{D}}{6}$$

であることが分かる。i は整数で考えているが, それでもこの不等式を満たす整数というのは精密に考えることが出来る。つまり, 右の範囲を満たす i とは, i が整数であることを考慮すれば, 天井関数と床関数により

$$\left\lceil 18n - \frac{1}{2} - \frac{\sqrt{D}}{6} \right\rceil \leqq i \leqq \left\lfloor 18n - \frac{1}{2} + \frac{\sqrt{D}}{6} \right\rfloor$$

を満たす整数 i ということができるが, この最左辺と最右辺については, $6n - \dfrac{1}{2} < \dfrac{\sqrt{D}}{6} = \sqrt{36n^2 - \dfrac{1}{12}} < 6n$ に注意すれば

$$\begin{aligned} \left\lceil 18n - \frac{1}{2} - \frac{\sqrt{D}}{6} \right\rceil &= 12n \\ \left\lfloor 18n - \frac{1}{2} + \frac{\sqrt{D}}{6} \right\rfloor &= 24n - 1 \end{aligned}$$

が従うので, 結局

$$f(i+1) - f(i) - 1 \geqq 0 \Leftrightarrow 12n \leqq i < 24n$$

となる。つまり, この i の範囲においては $f(i) + 1 \leqq f(i+1) \Rightarrow [f(i)] < [f(i+1)]$ が成り立つ。これは,

$$7n = [f(12n)] < [f(12n+1)] < \cdots < [f(24n)] = 20n$$

という増加列 $\{[f(i)]\}$ が, どの 2 つも違う整数を登場させるので, この部分には $7n$ から $20n$ の間に飛び飛びで $12n+1$ 個の整数が登場していることが分かる。

逆に, $0 \leqq i < 12n$ あるいは $24n \leqq i < 36n$ の場合は $f(i) \leqq f(i+1) < f(i)+1$ となるので, $[f(i)] \leqq [f(i+1)]$ の等号は成り立つ場合も成り立たない場合もあるけれども, 等号が成り立たない場合であるとしても, **$[f(i)]$ と $[f(i+1)]$ の差は 1 にしかならない。** つまり,

$$0 = [f(0)] \leqq [f(1)] \leqq \cdots \leqq [f(12n)] = 7n$$

という整数の広義増加列は, 0 から $6n$ までの $7n+1$ 個の整数がスキップされることなく登場している。同様にして

$$20n = [f(24n)] \leqq [f(24n+1)] \leqq \cdots \leqq [f(36n)] = 27n$$

の間の $7n+1$ 個の整数もすべて登場する。

以上のことから, 単に $(12n+1) + (7n+1) + (7n+1)$ とすると, これは $7n$ と $20n$ を 2 つずつカウントすることになるので, 求める個数はそこから 2 を引いた

$$\boldsymbol{26n + 1}$$

である。

1/20 更新

(1) 二項定理を使う。以下の合同式は mod100 である。

$$(10+1)^{11} = \sum_{k=0}^{11} 10^k {}_{11}\mathrm{C}_k \equiv 10 \cdot {}_{11}\mathrm{C}_1 + 1 \equiv \mathbf{11}$$

(2) 次の因数分解を利用する。

$$\begin{aligned} & 3^{2^n} - 1 \\ = \ & (3^{2^{n-1}}+1)(3^{2^{n-2}}+1)\cdots(3^{2^1}+1)(3^{2^0}+1)(3^{2^0}-1) \end{aligned}$$

ここで, $3^{2^k}+1$ $(k=1,2,\cdots,n-1)$ は $3^{2^k}+1 \equiv 2 \pmod 4$ によって 2 で 1 回しか割れない。また, $3^{2^0}+1=4$, $3^{2^0}-1=2$ に注意すると, 上の式から $3^{2^n}-1$ は 2 で $n+2$ 回割れる。よって $3^{2^n}-1 \equiv 0 \pmod{2^{n+2}}$ である。よって,

$$3^{2^n} \equiv \mathbf{1} \pmod{2^{n+2}}$$

となる。(数学的帰納法を使って証明する方法もある。)

(3) $4444 \equiv -2 \pmod 9$ により $(-2)^{4444} \bmod 9$ を見ればよい。$(-2)^6 \equiv 64 \equiv 1 \pmod 9$ なので

$$\begin{aligned} (-2)^{4444} &\equiv (-2)^{6\times 740+4} = 64^{740}\cdot(-2)^4 \\ &\equiv 1^{640}\cdot 16 \equiv \mathbf{7} \pmod 9 \end{aligned}$$

(4) $\prod_{k=1}^{999}(10^k-1)$ という数である ($\prod$ は総積の記号)。よって,

$$\begin{aligned} \prod_{k=1}^{999}(10^k-1) &= 9\times 99 \times \prod_{k=1}^{997}(10^{k+2}-1) \\ &\equiv 891\prod_{k=1}^{997}(-1) \\ &= 891(-1)^{997} \\ &\equiv \mathbf{109} \end{aligned}$$

(5) この場合, mod100 を考えるよりは mod4 と mod25 に分けてそれぞれを調べるとよい。これは, 100 を互いに素な 2 つの数の積 4×25 と考えて mod4, mod25 を調べれば, mod100 の値が復元できるということ (中国剰余定理) を利用している。

$6^{2017} \equiv 0 \pmod 4$ である。よって, $6^{2017} = 4k_1$ $(k_1 \in \mathbb{Z})$ と書ける。

二項定理より

$$6^{2017} = (5+1)^{2017} \equiv {}_{2017}\mathrm{C}_1 \cdot 5 + 1 \equiv 11 \pmod{25}$$

なので, $6^{2017} = 25k_2 + 11$ $(k_2 \in \mathbb{Z})$ と書ける。いま, $4k_1 = 25k_2+11$ が成り立っているが, mod 4 を取ると $k_2 \equiv 1 \pmod 4$ が従う。よって, $k_2 = 4k_3+1$ $(k_3 \in \mathbb{Z})$ と書くことができる。したがって,

$$6^{2017} = 25k_2 + 11 = 25(4k_3+1)+11 = 100k_3 + 36$$

となるので, mod 100 の値が復元でき, $6^{2017} \equiv 36 \pmod{100}$ となる。

(6) 10 の (mod 13) による位数を考える。つまり, $10^d \equiv 1 \pmod{13}$ となるような最小の自然数 d を求める。一般に剰余類の数 a と mod を取る数 b が互いに素ならそのような位数は存在し, その位数は「$\phi(b)$ の約数」の中で取れる。この場合なら, $\phi(13)=12$ なので 12 の約数から見てあげるとよい。

実際, $10^6 \equiv (-3)^6 \equiv (-27)^2 \equiv (-1)^2 \equiv 1 \pmod{13}$ である。大切なのは, そのように 6 が位数とわかったとき, 10^m を 6 で割ることを考えて $10^m = 6k+r$ $(k\in\mathbb{Z}, 0 \leqq r < 6)$ と表したとき,

$$10^{10^m} = 10^{6k}\cdot 10^r \equiv (10^6)^k \cdot 10^r \cdot 1^k \cdot 10^r \equiv 10^r \pmod{13}$$

となることである。そこで, r, つまり $10^m \bmod 6$ を求めればよいことになる。調べればわかるように, $10^m \equiv 4 \pmod 6$ がすべての自然数 m で成り立つので $r=4$ としてとれる。よって,

$$10^{10^m} \equiv 10^4 \equiv (-3)^4 = 81 \equiv \mathbf{3} \pmod{13}$$

(7) 階乗のある素因数の指数を決定する方法はルジャンドルの定理による。この場合, 2017! に 5 が何回かけられているかは,

$$\lfloor \frac{2014}{5} \rfloor = 402, \lfloor \frac{2014}{25} \rfloor = 80, \lfloor \frac{2014}{125} \rfloor = 16,$$
$$\lfloor \frac{2014}{625} \rfloor = 3, \lfloor \frac{2014}{5^k} \rfloor = 0 \ (\text{for } k \geqq 5)$$

に出てきたすべての数を足し合わせればよい。つまり, $402+80+16+3 = 501$ であり, $2014! = 5^{501}m$ のように書ける。$m = 25k+r$ $(0 \leqq r < 25)$ と書いたとき, $2014! = 5^{503}k + 5^{501}r$ となるので, r が分かると $2014! \bmod 5^{503}$ もわかる。r は $\frac{2014!}{5^{501}}$ の 25 で割ったあまりとして求まるので, この $\frac{2014!}{5^{501}}$ を調べたい。

$f(n) = (5n+1)(5n+2)(5n+3)(5n+4)$ とする。まず, すべての n に対して

$$f(n) \equiv -1 \pmod{25}$$

であることに注意せよ。これは展開からただちに従う。

方針としては, $i=0,1,2,3$ に対して, 2014! の中から「5^i の倍数だが 5^{i+1} の倍数でないもの」だけを取り出した積 P_i を調べることである。それらを, $f(n)$ を利用して表現する。

まず P_0 は次のようになる。

$$P_0 = f(0)f(1)\cdots f(402)$$

, P_1 は, 2005, 2010 が微妙に余るが, 次のように書ける。

$$P_1 = (5^4 f(0))(5^4 f(1))\cdots(5^4 f(79)) \times 2005 \times 2010$$

同様に,

$$P_2 = (25^4 f(0))(25^4 f(1))\cdots(25^4 f(15))$$
$$P_3 = (125^4 f(0))(125^4 f(1))(125^4 f(2)) \times 2000$$
$$P_4 = 625^3(1\times 2\times 3)$$

したがって, $2014! = P_0P_1P_2P_3P_4$ である。$\dfrac{2014!}{5^{501}}$ は, P_i から 5 の部分を消せばよい。きりの悪い部分をかき集めて $C = 2005 \times 2010 \times 2000 \times P_4$ とし, 5 の成分のみ取り出して $C = 5^{17}D$ とする (D は 5 で割れない整数である)。いま,

$$2014! = C\prod_{k=0}^{402} f(k)\prod_{l=0}^{79} 5^4 f(l)\prod_{m=0}^{15} 25^4 f(m)\prod_{n=0}^{2} 125^4 f(n)$$

であるから, 5^{501} で割ると, 5 の成分は消失して

$$\begin{aligned}\frac{2014!}{5^{501}} &= D\prod_{k=0}^{402} f(k)\prod_{l=0}^{79} f(l)\prod_{m=0}^{15} f(m)\prod_{n=0}^{2} f(n)\\ &\equiv D(-1)^{403}(-1)^{80}(-1)^{16}(-1)^3 \quad (\because f(n) \bmod 25 = 1)\\ &\equiv D \pmod{25}\end{aligned}$$

となる。$D = 401 \times 402 \times 16(1 \times 2 \times 3)$ であったから,

$$D \equiv 1 \times 2 \times 16 \times 1 \times 2 \times 3 \equiv 17 \pmod{25}$$

より, $r = 17$ としてとれるから,

$$\boldsymbol{2014! \equiv 17 \cdot 5^{501} \pmod{5^{503}}}$$

(8) 問題文に不備がある。本問では $p \geqq 3$ である。
${}_{p-1}\mathrm{C}_{\frac{p-1}{2}} \equiv k \pmod p$ とする。以下の modulo は mod$p$ とする。このとき, 左辺の階乗を払うことで

$$(p-1)! \equiv k\left(\frac{p-1}{2}!\right)^2$$

となる。ここで, 右辺の $\left(\dfrac{p-1}{2}\right)^2$ は片方の $\left(\dfrac{p-1}{2}\right)!$ を

$$\left(\frac{p-1}{2}\right)! \equiv \left(-\frac{p+1}{2}\right)\cdot\left(-\frac{p+3}{2}\right)\cdot\cdots\cdot\{-(p-1)\}$$

とすることで, $\left\{\left(\dfrac{p-1}{2}\right)!\right\}^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)!$ であることが分かる。よって,

$$(p-1)! \equiv k(p-1)!(-1)^{\frac{p-1}{2}}$$

より, $k \equiv (-1)^{\frac{p-1}{2}}$ を得る。したがって,

$$\boldsymbol{k \equiv \begin{cases}1 & (p \equiv 1 \pmod 4)\\ p-1 & (p \equiv 3 \pmod 4)\end{cases} \pmod p}$$

(9) $n = 114514^{1919}$ とする。(5) でも見たように, $810 = 2\times5\times81$ と見て, mod$2, 5, 81$ の情報から mod810 の情報を復元する方法で計算する。まず, $n \equiv 0 \pmod 2$ は容易。mod5 では, $n \equiv (-1)^{1919} \equiv 4$ である。$114514 \bmod 81 = 61$ であり, 61^{1919} を考えればよい。これはまずオイラーの定理によって指数を減らすことができる。$\phi(81) = 54$ なので, $61^{54} \equiv 1 \pmod{81}$ である。$1919 \equiv 29 \pmod{54}$ なので, $61^{1919} \equiv 61^{29} \pmod{81}$ である。さらに, $61^{27} \equiv 1 \pmod{81}$ である。実際, $61^{54} - 1 = (61^{27} - 1)(61^{27} + 1) \equiv 0 \pmod{81}$ であって, $61^{27}+1$ が 3 の倍数でないことに注意すると, $61^{27} - 1 \equiv 0 \pmod{81}$ となる。よって,

$$61^{29} \equiv 61^2 \equiv (-20)^2 = 400 \equiv 76 \pmod{81}$$

である。これらの情報から mod810 の情報を復元しよう。まず, これまでの情報から

$$n = 81k_1 + 76 = 2k_2 = 5k_3 + 4$$

となる (以降 k_i はすべて整数を表す)。$2k_2 = 5k_3 + 4$ より k_3 は偶数なので $k_3 = 2k_4 + 1$ とかけて, $5k_3 + 4 = 10k_4 + 4$ となって n の mod10 の情報を得る。$81k_1 + 76 = 10k_4 + 4$ に mod10 をして $k_1 \equiv 8$ となるので $k_1 = 10k_5 + 8$ となり, $n = 810k_5 + 724$ となる ($648 + 76 = 724$)。よって,

$$\boldsymbol{n \equiv 724 \pmod{810}}$$

(10) まず, (6) のことをおさらいすると, $10^{10^m} \bmod 13$ を求めるのに, 指数にある 10^m の mod6 を見た。これは, $10^d \bmod 13$ で d を動かしたときの周期が 6 であることを利用した上での解法である。本問はその発想を繰り返し利用する。まず,
次のように文字を置く。

$$a = 4^{4^{4^{4^{4^m}}}}, b = 4^{4^{4^{4^m}}}, c = 4^{4^{4^m}}$$
$$d = 4^{4^{4^m}}, e = 4^{4^m}, f = 4^m$$

すなわち,

$$a = 2^{2b}, b = 2^{2c}, c = 2^{2d}, d = 2^{2e}, e = 2^{2f}$$

である。
まず, 47 は素数である。Fermat の小定理より, $2^n \bmod 47$ は少なくとも周期 46 になっている。そこで, $2^{2b} \bmod 47$ を求めるには, $2b \bmod 46$, つまり $b \bmod 23$ が分かるとよい。

$2^{2c} \bmod 23$ を知るには同様にして $c \bmod 11$ を知ればよく, 再び同じ理由で $2^{2d} \bmod 11$ は $d \bmod 5$ を調べればよい。$d = 4^e$ は偶数なので, $d \bmod 5 = 1$ である。これが分かったのであとは流れを逆にたどっていけばよい。(実は e が偶数とわかればあとは気にしなくてよい。というより, 本当は肩に並んだ 4 の個数が 1 つだけ余分である。)

さて, 逆算をしていくと, いま $d = 5k_1 + 1$ と書けることが分かった。 11 は素数なので Fermat の小定理が使えることに注意し, mod11 で,

$$c = 4^{5k_1+1} \equiv 2^{10k_1+2} \equiv 2^2 \equiv 4$$

よって $c = 11k_2 + 4$ と書ける。 23 は素数であり,mod23 で,

$$b = 4^{11k_2+4} \equiv 2^{22k_2+8} \equiv 2^8 \equiv 3$$

よって $b = 23k_3 + 3$ と書ける。 47 は素数であり, mod47 で,

$$a = 4^{23k_3+3} = 2^{46k_3+6} \equiv 2^6 \equiv \mathbf{17}$$

である。この結果は,m によらない。(もっというと, f の部分を m と置いても結果は変わらない。)

Q.30 (2/8 更新)

(1) まず, $(x,y,z) \neq (0,0,0)$ なる解が得られたとする。このとき, x,y,z の最大公約数 g が定義できる。そのとき,

$$x^n + 2y^n = 4z^n \Rightarrow \left(\frac{x}{g}\right)^n + 2\left(\frac{y}{g}\right)^n = 4\left(\frac{z}{g}\right)^n$$

であるから, (x,y,z) が解ならば $(\frac{x}{g}, \frac{y}{g}, \frac{z}{g})$ も解であることが従う。よって, 初めから x,y,z の最大公約数は 1 であると仮定してよい。

$x^n = 4z^n - 2y^n$ より x は偶数でなければならない。$n \geqq 3$ であるから x^n は 8 の倍数である。とくに 4 の倍数であって, mod4 を考えると

$$0 \equiv 2y^n \pmod 4$$

となる。このことから y は偶数でなければない。続いて mod8 を考えると, x^n, y^n は 8 の倍数だから

$$0 \equiv 4z^n \pmod 8$$

となる。よって z も偶数でなければならない。x,y,z がすべて偶数なので, このことは最大公約数を 1 としたことに反する。よって $(x,y,z) = (0,0,0)$ であることが必要で, これは明らかに解である。[*1] □

(2) $(x,y,z,w) \neq (0,0,0,0)$ なる解があったとする。このとき, 十分大きい自然数 N によって $(N!x, N!y, N!z, N!w)$ を考えることで, $(0,0,0,0)$ ではない整数解を得ることが出来る。そこで, 初めから x,y,z,w が整数であるとして良い。そして, 今回の場合も前問と同様にして x,y,z,w の最大公約数が 1 であるとしてよい。

mod5 を考えることにより

$$x^2 \equiv 2y^2 \pmod 5$$

を得る。$y \not\equiv 0 \pmod 5$ であるなら, $yk \equiv 1 \pmod 5$ なる整数 k が取れるので

$$(kx)^2 \equiv 2 \pmod 5$$

となる。[*2]しかし 2 は mod5 における平方剰余ではないので不適である。よって $y \equiv 0 \pmod 5$ である. $x^2 \equiv 0 \pmod 5$ なので x も 5 の倍数である。

よって x^2, y^2 は 25 の倍数である。つづいて $bmod25$ を考えると,

$$5(z^2 - 3w^2) \equiv 0 \pmod{25}$$

より, $x^2 \equiv 3w^2 \pmod 5$ でなければならない。$w \not\equiv 0 \pmod 5$ なら $wl \equiv 1 \pmod 5$ なる整数 l を取って $(lx)^2 \equiv 3 \pmod 5$ となるが, 3 は mod5 の平方剰余ではないので不適である。よって $w \equiv 0 \pmod 5$ であり, $z \equiv 0 \pmod 5$ も従う。

以上より x,y,z,w はすべて 5 の倍数となり, 最大公約数を 1 としたことに反する。よって最初に取ったような $(0,0,0,0)$ ではない有理数解は存在し得ない。$(0,0,0,0)$ は明らかに解である。 □

[*1] 無限降下法的な議論でもよい。無限降下法はどの項の次数も同じであるようなときに使えることが多い。(個人的にはこのように最大公約数を取る方が好きである)

[*2] もちろん, $2y^2 \equiv 0, 2, 3 \pmod 5$ であることを見て「0 以外非平方剰余なので」と言っても良い

Q.188 (2/8)

(注意: 本問では x,y は実数とする)

(1) まず $x = y = 0$ の場合はどちらの方向も明らかによい。そうでない場合を考えると, $x + y > 0$ となるので

$$\begin{aligned} x - y \geqq 0 &\Leftrightarrow (x-y)(x+y) \geqq 0 \quad (\because x + y \geqq 0) \\ &\Leftrightarrow x^2 - y^2 \geqq 0 \end{aligned}$$

である。

(2)

まず, $y = 0$ の場合は $x^2 \geqq 0$ なので明らかにどちらの方向もよい。$y \neq 0$ にして同値を示せばよい。たとえば, 次のようにして示せる。

$$\begin{aligned} x^2 \geqq y^2 &\Leftrightarrow \left(\frac{x}{y}\right)^2 \geqq 1 \\ &\Leftrightarrow \left|\frac{x}{y}\right|^2 \geqq 1 \\ &\Leftrightarrow |x|^2 \geqq |y|^2 \\ &\Leftrightarrow |x| \geqq |y| \qquad (\because \text{前問}) \end{aligned}$$

(3) $x^2 - 4 \geqq 0$ の必要がある。また, 左辺はそのときに常にプラスなので, $x - 3 \geqq 0$ である必要がある。よって, $x \geqq 3$ に限定して解けばよい。このとき, (1) より両辺を 2 乗しても同値なので $x^2 - 4 \leqq (x-3)^2$ を解くことと同値である。これは $x \geqq \dfrac{13}{6}$ となるから, 解は存在しない。

(4) 同様のことから, $x^2 \geqq 4$ でかつ $x \geqq 1$ である。そこで, $x \geqq 2$ に限定して解けばよい。この制限のもとで (1) より両辺を 2 乗しても同値であり,

$$x^2 - 4 \leqq (x-1)^2 \Leftrightarrow x \leqq \frac{5}{2}$$

となる。よって, $2 \leqq x \leqq \dfrac{5}{2}$ である。

Q.222

$f(t) = \dfrac{(x^2 + \sqrt{\pi}t)e^{t^2}}{t^2 \log t}$ とおく。$x \neq \sqrt{\pi}$ のとき, 平均値の定理より, $c \in [\sqrt{\pi}, x] \cup [x, \sqrt{\pi}]$ が存在して,

$$\begin{aligned} &\int_{\sqrt{\pi}}^{x} \frac{(x^2 + \sqrt{\pi}x)}{(x^3 - \sqrt{\pi}x^2 + \pi x - \pi\sqrt{\pi})x^2 \log x} \\ = &\frac{1}{x^2 + \pi} \cdot \frac{1}{x - \sqrt{\pi}} \int_{\sqrt{\pi}}^{x} f(t)\,dt \\ = &\frac{1}{x^2 + \pi} \cdot f(c) \end{aligned}$$

$x \to \sqrt{\pi}$ のとき, $c \to \sqrt{\pi}$ であるから,

$$\to \frac{1}{2\pi} \cdot \frac{2\pi}{\pi \log \sqrt{\pi}} = \frac{2e^{\pi}}{\pi \log \pi}$$

Q,241(6/21 更新)

$\mathrm{P}=(\sqrt{2},\sqrt{3},\sqrt{5})$ とする[*3]。P と格子点 (l,m,n) の距離は

$$\sqrt{(l-\sqrt{2})^2+(m-\sqrt{3})^2+(n-\sqrt{5})^2}$$

である。この距離の **2 乗**を $f(l,m,n)$ とおく。二つの格子点 (l_1,m_1,n_1), (l_2,m_2,n_2) に対して, $f(l_1,m_1,n_1)=f(l_2,m_2,n_2)$ が成り立っていたとする。このとき, $f(l_1,m_1,n_1)-f(l_2,m_2,n_2)=0$ の左辺を計算すれば

$$\begin{aligned}&(l_1^2+m_1^2+n_1^2-l_2^2-m_2^2-n_2^2)\\&\quad+2(l_2-l_1)\sqrt{2}+2(m_2-m_1)\sqrt{3}+2(n_2-n_1)\sqrt{5}=0\end{aligned}$$

となる。

本問の核心的なアイデアではあるが, 次の補題は認めることとする (証明はさほど難しくない)。

補題 1. $\sqrt{2},\sqrt{3},\sqrt{5}$ は無理数である。また, a,b,c,d を有理数とし, $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}=0$ が成り立つとする。このとき, $a=b=c=d=0$ である。

この補題によって,

$$2(l_2-l_1)=0,\quad 2(m_2-m_1)=0,\quad 2(n_2-n_1)=0$$

が従うので, $(l_1,m_1,n_1)=(l_2,m_2,n_2)$ である。すなわち,

$$f(l_1,m_1,n_1)=f(l_2,m_2,n_2)\Rightarrow(l_1,m_1,n_1)=(l_2,m_2,n_2)$$

だから, 対偶を取れば

$$(l_1,n_1,m_1)\neq(l_2,m_2,n_2)\Rightarrow f(l_1,m_1,n_1)\neq f(l_2,m_2,n_2)$$

である。すなわち, $f(l,m,n)$ は格子点全体の集合で定義された実数値関数であって, 異なる二つの格子点に対して異なる値を返すような関数である。よって, **座標空間内の格子点全体を, $f(l,m,n)$ の値が小さい順番に $(l_1,m_1,n_1),(l_2,m_2,n_2),\cdots$ と並べることができる。**つまり, i 番目の格子点 (l_i,m_i,n_i) とは「f の値が i 番目に小さいような格子点」として定義するのである。

このように並べたとき, $f(l_i,m_i,n_i)<f(l_{i+1},m_{i+1},n_{i+1})$ が成り立っている (等号は成り立たない!)。そこで, 正の実数 R_N を $f(l_N,m_N,n_N)<R_N^2<f(l_{N+1},m_{N+1},n_{N+1})$ が成り立つように取る。このとき, 球

$$(x-\sqrt{2})^2+(y-\sqrt{3})^2+(z-\sqrt{5})^2<R_N^2$$

は, その内部に (l_i,m_i,n_i) $(i=1,2,\cdots,N)$ という N 個の格子点だけを含む球となっている。 □

Q.242(6/21 更新)

まず $\sin 1,\sin 2,\sin 3,\cos 1$ の大小を決定する。
そのためにこの 5 つの数をすべて $\sin x$ $(0\leqq x\leqq\frac{\pi}{2})$ の形で表したい。$\sin 1$ に関してはすでにその表示になっている。その他の数については, 三角関数の公式から

$$\sin 2=\sin(\pi-2),\sin 3=\sin(\pi-3),\cos 1=\sin(\frac{\pi}{2}-1)$$

である。したがって, $\sin 1,\sin 2,\sin 3,cos1$ の大小を見るには, $1,\pi-2,\pi-3,\frac{\pi}{2}-1$ の大小を見ればよい ($\sin x$ が $0\leqq x\leqq\frac{\pi}{2}$ で単調増加だから)。そして, 実際に計算すれば

$$\pi-3<\frac{\pi}{2}-1<1<\pi-2<$$

であるから,

$$\sin 3<\cos 1<\sin 1<\sin 2$$

となる。
$\pi<4<2\pi$ より $\sin 4<0$ である。これ以外の数はすべて正である。
$\tan 1>\tan\frac{\pi}{4}=1$ である。これ以外の数はすべて 1 未満である。よって, $\pi-3$ 以外の数について

$$\sin 4<\sin 3<\cos 1<\sin 1<\sin 2<\tan 1$$

まで分かる。

$0\leqq x$ のとき $\sin x\leqq x$ であることを思い出そう。これに $x=\pi-3$ を代入すれば $\sin(\pi-3)=\sin 3<\pi-3$ となる。

$\pi-3<0.15$ である[*4]。一方で, $\cos 1>\cos\frac{\pi}{3}=\frac{1}{2}>0.15$ なので $\pi-3<\cos 1$ である。

以上より,

$$\boldsymbol{\sin 4<\sin 3<\pi-3<\cos 1<\sin 1<\sin 2<\tan 1}$$

[*3] これが球の中心となるが, これ以外にも様々な取り方がある。後述の補題が成り立つような座標を取ると良い。

[*4] $\pi=3.14\cdots$ と問題文に書いたので, $3.14<\pi<3.15$ は認めてよいものとして出題している。

0.1 Q.143

(1) 階差型である。$A_{n+1}-A_n=2^n$ より

$$A_{n+1}-A_1=\sum_{k=1}^{n}(A_{k+1}-A_k)=\sum_{k=1}^{n}2^k=2^{n+1}-2$$

より $A_{n+1}=2^{n+1}$ なので $A_n=2^n-1$ $(n\geqq 2)$. $n=1$ もよい。
(2) まず $B_2=1+B_1=0$ である。式を見ると $B_{n+1}+(n+1)B_{n+1}=B_{n+2}$ $(n\geqq 1)$ である。よって $B_{n+2}=(n+2)B_{n+1}$ $(n\geqq 1)$ である[*5]が, $B_2=0$ なので $B_3=0$, $B_4=0$, $\cdots$ となる。よって

$$\boldsymbol{B_1=-1,\quad B_n=0(n\geqq 2)}$$

(3) $C_{n+1}-f(n+1)=3(C_n-f(n))$ となるような n の関数 $f(n)$ を見つければ, $\{C_n-f(n)\}$ が等比数列で

$$C_n-f(n)=3^{n-1}(C_1-f(1))\quad(n\geqq 1)$$

が分かる。$f(n)$ を求めよう。

$$C_{n+1}=3C_n+\{f(n+1)-3f(n)\}$$

であるから, すべての $n\geqq 1$ で $f(n+1)-3f(n)=2n-1$ が成り立つものを選べばよい。$f(n)=an+b$ と書けると思って a,b を求めれば $f(n)=-n$ であると分かる。よって

$$C_n-(-n)=3^{n-1}(1-(-1))$$

だから整理して $C_n=2\cdot 3^{n-1}-n$ $(n\geqq 1)$ を得る。
(8) $H_{n+3}+H_{n+2}+H_{n+1}=H_{n+2}+H_{n+1}+H_n=2$ より $H_n=H_{n+3}$ なので周期数列である。$H_3=2-H_1-H_2=-4$ であるから

$$\boldsymbol{\{H_n\}=3,3,-4,3,3,-4,3,3,-4,\cdots}$$

(19) $S_n+n=a_n$ とおく。$a_1=1$ である。

$$S_{n+1}-S_n=a_{n+1}-a_n-1=2\sqrt{a_n}$$

より $a_{n+1}=a_n+2\sqrt{a_n}+1=(\sqrt{a_n}+1)^2$ を得る。$b_n=\sqrt{a_n}$ とおくと, $b_1=1$ であって

$$b_{n+1}^2=(b_n+1)^2$$

であり, $b_{n+1}=\pm(b_n+1)$ である。だが, $\sqrt{a_n}\geqq 0$ なので $b_n+1>0$ かつ $b_{n+1}\geqq 0$ より $b_{n+1}=b_n+1$ でなければならない。これは $n\geqq 1$ で成り立つので $b_n=n$ である。よって $a_n=n^2$ であり, $S_n=n^2-n$ を得る。

0.2 Q.045

(1) x^2,y^2 は正である。$41-y^2\leqq 40$ より $1\leqq x^2\leqq 40$ を満たすことが必要。よって $x=1,2,3,4,5,6$ の中から調べれば十分。これらの中から探せば

$$(x,y)=(4,5),(5,4)$$

のみと分かる。
(2)

$$\begin{aligned}&(ac-bd)^2+(ad+bc)^2\\ =\ &(ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2\\ =\ &a^2c^2+a^2d^2+b^2c^2+b^2d^2\\ =\ &(a^2+b^2)(c^2+d^2)\end{aligned}$$

なお, これは「整数 x,y を用いて x^2+y^2 の形で表せるような整数全体の集合は積について閉じている」ということを主張している。
(3) $2009=41\times 49=(4^2+5^2)(0^2+7^2)$ に注意すると, (2) で $a=4,b=5,c=0,d=7$ として

$$(-35)^2+28^2=35^2+28^2=2009$$

を得る。よって $n=1$ の場合はよい。$n=k$ $(k\geqq 1)$ において $a_k^2+b_k^2=2009^k$ となるような自然数 a_k,b_k が存在したと仮定する。このとき,

$$\begin{aligned}2009^{k+1}&=(35^2+28^2)(a_k^2+b_k^2)\\ &=(35a_k-28b_k)^2+(35b_k+28a_k)^2\\ &=(28a_k-35b_k)^2+(28b_k+35a_k)^2\end{aligned}$$

であるから, $35a_k-28b_k\neq 0$ であるなら

$$a_{k+1}=|35a_k-28b_k|,\quad b_k=35a_k+28b_k$$

とし, $35a_k-28b_k=0$ であるなら $28a_k-35b_k=0$ とはならないことが分かるので

$$a_{k+1}=|28a_k-35b_k|,\quad b_{k+1}=28b_k+35a_k$$

とおくことによって, $2009^{k+1}=a_{k+1}^2+b_{k+1}^2$ とすることができる。よって数学的帰納法により, すべての n で $a_n^2+b_n^2=2009^n$ となるように自然数 a_n,b_n を構成することが出来る。 □

7/26

Q.25(修正)

$F(a,b,c)=\dfrac{2a+b}{c}+\dfrac{2b+c}{a}$ とおく。a,c を固定すると、F は b に関して増加する関数である。よって、a,c を固定した上では b は $a\geq b\geq c$ を動くから、$b=c$ とすると小さくできる。すなわち、

$$F(a,b,c)\geq F(a,c,c)=1+\frac{2a}{c}+\frac{3c}{a}$$

である。$a,c>0$ だから、相加相乗平均の不等式より、

$$F(a,c,c)\geq 1+2\sqrt{\frac{2a}{c}\cdot\frac{3c}{a}}=1+2\sqrt{6}$$

が成立する。等号の成立は $2a^2=3c^2$ のときなので、たとえば $b=c=2$, $a=\sqrt{6}$ とすると、最小値

$$F(2,2,\sqrt{6})=1+2\sqrt{6}$$

が実現する。よって求める最小値は $1+2\sqrt{6}$。 l

[*5] これが $n=0$ で成り立っていると勘違いすると $B_n=-n!$ となり誤りである。

7/30

Q.171

a, b, n, x から作られる等差数列を S と呼ぶことにする。ただし, S の階差は非負であるように並べておく。たとえば a, b, n, x のうちの a が S の中に選ばれていないという状況を, $a \notin S$ で表すことにする。方程式

$$a + b^n = nx \tag{1}$$

について考える。

Step.1($b < x$, $n < x$) $n \leqq (1+1)^{n-1} = 2^{n-1} \leqq b^{n-1}$ より $bn \leqq b^n$ が従うので $bn < a + b^n = nx$ より $b < x$ である。

$n^2 \leqq 1 + 2^n$ が成り立つことに注意すると

$$n^2 \leqq 1 + 2^n \leqq 1 + b^n < a + b^n = nx$$

となるので $n < x$ である。

また, このことから特に $x \neq 2$ が分かる。

Step.2(S の階差が 0 であるとき)

このとき S は (p, p, p) (p は素数) となる。b, n のいずれかは S に選ばれているので Step1. より $x \notin S$ が従う。よって $a = b = n = p$ とすると $p + p^p = px$ より $1 + p^{p-1} = x$ である。$p > 2$ であると左辺は 2 より大きい偶数で x は素数でないから $p = 2$ となり $x = 3$ となる。よって $(a, b, n, x) = (2, 2, 2, 3)$ は一つの解である。

以降 S の階差 d は正であるとする。まず a, b, n, x がすべて奇数であると左辺は偶数, 右辺は奇数なので不適。よって a, b, n, x のいずれかが 2 である。このとき, $2 \notin S$ である。なぜなら,$2 \in S$ であるとそれは S のうち最小の元であって, 最大の元は $2 + 2d$ と書ける。これが a, b, n, x のいずれかに等しいので $2 + 2d$ は素数でなければならない。しかし, $d > 0$ であるからこれは 2 より大きい偶数であり, 素数ではない。よって $2 \notin S$ である。同じ理由によって a, b, n, x の中に「2」は一つしか存在しない。

$2 \notin S$ と Step1. を考慮した上で, a, b, n, x や S としてありえる状況は次のいずれかである。

$$\begin{aligned}
&a = 2 \text{ で}, \quad S = (b, n, x) \quad \text{or} \quad (n, b, x) \\
&n = 2 \text{ で}, \quad S = (a, b, x) \quad \text{or} \quad (b, a, x) \quad \text{or} \quad (b, x, a) \\
&b = 2 \text{ で}, \quad S = (a, n, x) \quad \text{or} \quad (n, a, x) \quad \text{or} \quad (n, x, a)
\end{aligned}$$

Step.3($a = 2$ の場合 (易))

考えるべき方程式は

$$2 + b^n = nx$$

である。$S = (s_1, s_2, s_3)$ とするとき, 等差数列だから $s_1 + s_3 = 2s_2$ が成り立つ。このとき $s_3 < 2s_2$ が自動的に成り立っていることに注意する。

Step.3.1($S = (b, n, x)$ の場合)

このとき $3 \leqq b < n$ より $5 \leqq n$ でなければならず, $x < 2n$ だから

$$2 + 2^n \leqq 2 + b^n = nx < 2n^2$$

だが $n \geqq 7$ では $2 + 2^n > 2n^2$ なので不適。よって $n = 5$ で, $b < n$ だから $b = 3$ でなければならない。よって階差 2 だから $x = 7$ である。しかしこれらは実際の解ではない。

Step.3.2($S = (n, b, x)$ の場合)

$n \geqq 3$ かつ $b \geqq 5$ であり, $x < 2b$ が成り立つ。よって

$$b^n < 2 + b^n = nx < 2bn$$

より $b^{n-1} < 2n$ だから $5^{n-1} < 2n$ となる。これは $n \geqq 3$ で成り立たないので不適。

Step.4($n = 2$ の場合)

考えるべき方程式は

$$a + b^2 = 2x \tag{2}$$

である。

Step.4.1($S = (a, b, x)$ の場合 (易))

このとき $b \geqq 5$ である。$2x = 4b - 2a$ であるから $a + b^2 = 4b - 2a$ より $3a = b(4 - b) < 0$ で解なし。

Step.4.2($S = (b, a, x)$ の場合 (易))

$2x = 4a - 2b$ であり, $a + b^2 = 4a - 2b$ より $b(b + 2) = 3a$ である。右辺は素因数分解であるから $b + 2$ は素数でなければならない。素因数分解として同じであるという観点でこの式を見ると $b = 3, b + 2 = a$ となる。よって $a = 5$ で, $x = 7$ である。そして

$$5 + 3^2 = 2 \cdot 7$$

は確かに正しい。よって $(a, b, n, x) = (5, 3, 2, 7)$ は一つの解である。

Step.4.3($S = (b, x, a)$ の場合 (易))

$2x = a + b$ だから $a + b^2 = a + b$ で $b^2 = b$ だがこれは成り立たない。

Step.5($b = 2$ の場合)

考えるべき方程式は

$$a + 2^n = nx \tag{3}$$

である。このケースにおいては mod 6, mod 9 の考察が威力を発揮する。まず, n はこの場合奇素数だから, $n > 3$ であるなら $n \equiv \pm 1 \pmod 6$ である。すると $n = 6k \pm 1$ と書けるが, $n = 6k + 1$ なら $2^n \equiv 64^k \cdot 2 \equiv 2 \pmod 9$ で, $n = 6k - 1$ なら $2^n \equiv 5 \pmod 9$ となることが分かる。

また, $S = (s_1, s_2, s_3)$ の階差 d は, $s_1 > 3$ である限りは 3 の倍数でなければならない。なぜなら, 3 の倍数でないなら $d \equiv \pm 1 \pmod 3$ であるが, s_1 も $s_1 \equiv \pm 1 \pmod 3$ であり, いかなる場合においても $s_1 + d$, $s_1 + 2d$ のいずれかは mod3 で 0 となる。$s_1 + d, s_1 + 2d$ は 3 より大きいが, 素数であったからこのようなことは起こりえない。よって $s_1 > 3$ ならば d は 3 の倍数である。とくにそのとき, $S = (s_1, s_2, s_3)$ は $s_1 \equiv s_2 \equiv s_3 \pmod 3$ を満たすことに注意せよ。

Step.5.1($S = (a, n, x)$ の場合 (易))

$3 \leqq a,x < 2n$ だから $3 + 2^n < 2n^2$ である。これは $n \geqq 7$ で成り立たない。$5 \leqq n$ なので $n = 5$ に決まる。よって $a = 3, x = 7$ で,

$$3 + 2^5 = 5 \cdot 7$$

は確かに正しい。よって $(a, b, n, x) = (3, 2, 5, 7)$ は一つの解である。

Step.5.2($S = (n, a, x)$ の場合 (難))
まず $n = 3$ とすると $19 + x = 6x$ となるがこのような x はない。よって $n > 3$ であり, d は 3 の倍数であり, $n = 6k \pm 1$ となる。$n = 6k+1$ であるとき, $2^n \equiv 2 \pmod 9$, $a = n+d \equiv 1 \pmod 3$, $nx = (a+d)(a-d)$ を用いて (3) の mod9 を考えると

$$a + 2 \equiv a^2 - d^2 \equiv a^2 \pmod 9$$

より $a^2 - a - 2 \equiv 0 \pmod 9$ である。$a^2 - a - 2 \equiv (a+4)^2 \equiv 0 \pmod 9$ なので, この解は $a+4$ が 3 の倍数であるとき, すなわち $a \equiv 2 \pmod 3$ であるときに限る。これは $a \equiv 1 \pmod 3$ に反する。

$n = 6k - 1$ のとき, $2^n \equiv 5 \pmod 9$, $a = n + d \equiv 2 \pmod 3$ である。同様に考えると

$$a + 5 \equiv a^2 \pmod 9$$

となる。$a \equiv 2 \pmod 3$ であるから $a \equiv 2, 5, 8 \pmod 9$ であるが, この中に上を満足するものはない。

Step.5.3($S = (n, x, a)$ の場合 (難))
$a = 2x - n$ より (3) は

$$2x - n + 2^n = nx$$

となる。まず $n = 3$ とすると $2x + 5 = 3x$ より $x = 5$ で, 階差は 2 だから $a = 7$ となる。これらは素数で

$$7 + 2^3 = 3 \cdot 5$$

は確かに満たされる。よって $(a, b, n, x) = (7, 2, 3, 5)$ は一つの解である。

$n > 3$ とする。d は 3 の倍数であるから, $n \equiv x \equiv a \pmod 3$ でなければならない。

$n = 6k + 1$ のとき[*6],

$$2x - n + 2 \equiv nx \pmod 9$$

で, 変形すると

$$(n-2)(x+1) \equiv 0 \pmod 9$$

である。$n-2$ は今の場合 3 の倍数ではないから $x+1$ は 3 で割り切れる。よって $x \equiv 2 \pmod 3$ だが, $n \equiv 1 \pmod 3$ なので矛盾。

$n = 6k - 1$ のとき,

$$2x - n + 5 \equiv nx \pmod 9$$

で, 変形すると

$$(n-2)(x+1) \equiv 3 \pmod 9$$

である。今の場合 $n \equiv x \equiv 2 \pmod 3$ であるから, $n-2, x+1$ はともに 3 の倍数になる。すると上の左辺は 0 であるから矛盾である。

以上より, 求める (a, b, n, x) は

$$\boldsymbol{(a, b, n, x) = (2, 2, 2, 3), (5, 3, 2, 7), (3, 2, 5, 7), (7, 2, 3, 5)}$$

Q.56

0.2.1 (1)

単位円 (周長 2π) を考え, それに外接する正方形 (周長 8) を取ることで $2\pi < 8$ が従う。また, 単位円の周を 6 等分する点を取って正六角形 (周長 6) を取ることで $6 < 2\pi$ が従う。[*7]

(2)

e の定義は

$$\lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$$

である。[*8]n は十分大きい自然数とする。まず, 二項定理によって

$$1 + \frac{{}_n\mathrm{C}_1}{n} = 2 < \left(1 + \frac{1}{n}\right)^n$$

が成り立つので $2 < e$ である。次に, $\left(1 + \frac{1}{n}\right)^n$ を展開したときに現れる $a_k = \frac{{}_n\mathrm{C}_k}{n^k}$ を上から評価する。$n^k \geqq n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1)$ であることに注意すれば, $n^k (n-k)! \geqq n!$ であるから

$$a_k = \frac{{}_n\mathrm{C}_k}{n^k} = \frac{n!}{k!(n-k)!n^k} \leqq \frac{n!}{k!n!} = \frac{1}{k!}$$

が従う (もちろん $k > 1$ なら等号は成り立たない)。よって

$$\left(1 + \frac{1}{n}\right)^n < 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} = 1 + \sum_{k=1}^{n} \frac{1}{k!}$$

となる。最後に, $2^{k-1} \leqq k!$ が $1 \leqq k$ で常に成り立つから

$$1 + \sum_{k=1}^{n} \frac{1}{k!} < 1 + \sum_{k=1}^{n} \frac{1}{2^{k-1}} = 1 + 2\left\{1 - \frac{1}{2^n}\right\} < 3$$

が分かる。よって $e < 3$ が示された。

[*6] この場合は mod3 までででも分かる。ただし $n = 6k - 1$ の場合は mod9 を見ないと分からない。

[*7] 本当は「周長に関する大小」が正六角形 < 単位円 < 正方形になることは調べないといけないけれども, 見るからに明らかではあり, 高校数学ならこの方法で十分であると思われる。

[*8] $e = \sum_{k=0}^{\infty} \frac{1}{k!}$ という事実はあるけれども, 高校数学の範囲で認めて良いか怪しい部分があると思われる。定義に立ち返るのが安全である。

0.3 Q.240

補題 2.

有理数 a に対し, $(a,0)\in A$

$(a,0),(b,0)\in A \implies (a\pm b,0)\in A$

$(a,0)\in A \implies (\sqrt{|a|},0)\in A$

(1) 題意より $(0,0),(1,0)\in A$ である。針を原点においてコンパスを使うことで $(a,0)\in A$ なら $(-a,0)\in A$ でもあるから $a>0$ の場合を考えれば良い。自然数 m,n によって $a=\dfrac{m}{n}$ と表す。コンパスによって適当な自然数倍の長さを持った線分を構成することができるので, $(\frac{1}{n},0)\in A$ を示せば $(a,0)\in A$ も従う。

たとえば次のようにして $(\frac{1}{m},0)\in A$ を言うことが出来る:

原点から $(1,1)$ に向かう半直線を考え, 原点と $(1,1)$ にコンパスを合わせ, それを使うことで点 (k,k) $(k=1,2,\cdots,n)$ を作図することができる。(n,n) と $(1,0)$ を結ぶ直線を l_n とし, l_n に平行な直線で $(1,1)$ を通るものがコンパスと定規で作図できる。l_1 と x 軸の交点が $(\frac{1}{m},0)$ である。よって $(\frac{1}{m},0)\in A$ である。

(2) $a,b>0$ としてよい。

(3) $a>0$ としてよい。(1),(2) より, 十分大きい自然数 n を取って $a-\dfrac{1}{4n^2}>0$ かつ $(a\pm\dfrac{1}{4n^2},0)\in A$ である。$a+\dfrac{1}{4n^2}$ を斜辺に, $a-\dfrac{1}{4n^2}$ を高さにもつ直角三角形が作図でき, その直角三角形の辺の長さは $\dfrac{1}{n}\sqrt{a}$ であるから n 倍することで $\sqrt{a}$ の長さの線分が作図できるからよい。

0.4 11/30

0.4.1 Q.244

(1): 偽である。たとえば $P(x)=\dfrac{x(x-1)}{2}$ とせよ。x が整数のとき, $x(x+1)$ は必ず偶数であるが, 明らかに整数係数多項式ではない。よってこれが反例である。ちなみに, このような整数の上で常に整数値となる多項式 $P(x)$ は**整数値多項式**と呼ばれており, 一般に次のような形で表示できることと同値であることが知られている。

$$P(x)=\sum_{k=0}^{N}a_kp_k(x)$$

ただし, $a_k\in\mathbb{Z}, N\geqq 0, p_k(x)=\dfrac{x(x-1)\cdots(x-k+1)}{k!}$. 先の解答で挙げた $P(x)$ は $p_2(x)$ にあたる。

(2): **偽である！**(本問は中々の引っかけ問題である.[*9] 間違えても気にしなくてよい)

たとえば次のような関数はもれなく $f'(x)=\dfrac{1}{x}$ を満たすけれども, すべての実数で $f(x)=\log|x|+C$ となるわけではない:

$$f(x)=\begin{cases}\log x+A & (x>0)\\ \log(-x)+B & (x<0)\end{cases},\quad A,B\text{ は任意の実定数}$$

つまり, 積分定数にあたるものを 2 カ所に与えても問題ないということである。

(**余談**) この現象は高度な話で de Rham Cohomology(ド・ラームコホモロジー) という概念に関連があり, $f(x)$ が $x\neq 0$ でしか定義されてないことに起因する問題である。さて, 上の f を天下りに与えはしたが, 次のように考えれば自然と現れるものであることが理解できる。$g(x):=f(x)-\log|x|$ は $\mathbb{R}-\{0\}$ 上の無限回微分可能な関数で, $g'(x)=0$ を満たしている。結果論的には,

$$g(x)=\begin{cases}A & (x>0)\\ B & (x<0)\end{cases}$$

であるから, このようなものに限ることを示せばいいわけだが, $g'(x)=0$ ということは $g(x)$ は $\mathbb{R}-\{0\}$ の各点 x の十分近くでは定数関数である。しかし $g(x)$ は $\mathbb{R}-\{0\}$ 全体の定数関数にはならない。なぜなら, この $\mathbb{R}-\{0\}$ という領域が, 原点で断絶を起こしているから。より数学的には「$\mathbb{R}-\{0\}$ は二つの連結成分 $\mathbb{R}_{>0}$ と $\mathbb{R}_{<0}$ に分割される」から。一方で原点を埋めた $\mathbb{R}$ 全体で $F'(x)=0$ ならば $F(x)$ は定数であることは紛れもなく真であって, 局所定数関数 g が二つの半直線 $\mathbb{R}_{>0}$ と $\mathbb{R}_{<0}$ の上では定数であることも平均値の定理から容易に分かることである。だから, $g(x)$ は「二つの連結成分 (半直線) に実数 A,B を割り当てるしかない」のだから, このように決まってしまうのである。

ようは「微分方程式は, "何処"で解くかで様子が変わることがある」と言えるのだ。

一般に C^∞ 多様体 M(なめらかで図形みたいなもの) に関する"不変量"として de Rham Cohomology $H^*(M)$ というものが定義される。物としては $\mathbb{R}$ ベクトル空間なので $0,\mathbb{R},\mathbb{R}^2,\mathbb{R}^3,\cdots$ といった"値"をとるものであり[*10], 不変量なので, これを用いて多様体という図形を分類できたりできなかったりするという代物だ。$H^*(M)$ は $H^0(M),H^1(M),H^2(M),\cdots$ というものたちに分解され, それらが"微分操作で繋がっている"ようなものである。とくにこの中の $H^0(M)$ は「M 上の無限回微分可能な関数であって, 微分して 0 であるようなもの全体の集合」と同じである。だから, 先と同様に「M 上の局所定数関数全体」の集合である。$M=\mathbb{R}$ なら, 局所定数関数は本当の定数関数しかないから $H^0(\mathbb{R})=\mathbb{R}$. 一方で本問のように $H^0(\mathbb{R}-\{0\})=\mathbb{R}^2$ である。右辺の $\mathbb{R}$ の指数が, M **の連結成分の個数に等しい**のだろうと想像できると思う (厳密に示すにはやはり少し言葉が必要なのだが)。

さて, このことをふまえた上で再び次の問題に挑戦してみたいという人はいるかな？

(**問題**): $M=\mathbb{R}-\{0,1,2,\cdots,100\}$ で定義された関数 $f(x)$ であって

$$f'(x)=\frac{1}{x^2}+\frac{1}{(x-1)^2}+\frac{1}{(x-2)^2}+\cdots+\frac{1}{(x-100)^2}$$

を満たすものをすべて求めよ。(**Hint:** $H^0(M)=\mathbb{R}^{102}$)

de Rham Cohomology は代数的位相幾何学という分野で登場する。京大数学科では 3 回生で習う程度のものである。参考書としては Raoul Bott , Loring W.Tu の Differential Forms in Algebraic Topology という本が有名である (前提知識としては多様体論, 加群論の初歩, 線形代数程度, であろうか)。

(3): **真である。** 任意の無理数 p を取る。このとき p を近似する有理数列 $q_1,q_2,\cdots,$ が存在する。具体的には, p の 10 進展開を小数第 n 位で切り捨てるなどとすればよい。連続性から

$$f(p)=f(\lim_{n\to\infty}q_n)=\lim_{n\to\infty}f(q_n)=\lim_{n\to\infty}0=0$$

なので示された。

0.4.2 Q.245

(1): **偽である。** $x=0,y=\sqrt{2},z=-\sqrt{2}$ とすればよい。実際

$$x+y+z=0,xy+yz+zx=-2,xyz=0.$$

別のアプローチも述べておこう。$x+y+z\in\mathbb{Q},\cdots$ などという条件から, 解と係数の関係をふまえれば

$$(T-x)(T-y)(T-z)$$

という T の多項式は実解を 3 つ持つ有理数多項式にになるわけである。だから, そのような多項式の根は果たして有理数なのか?という視点で解く事もできる。センスがあるのかないのかわからない反例だが,

$$T(T-\cos\frac{2\pi}{3})(T-\cos\frac{4\pi}{3})=T^3+\frac{3}{4}T+\frac{1}{4}$$

[*9] アンケート機能使ったら偽と答えた方が半分未満だった。

[*10] 少しややこしいが, この"値"としての $\mathbb{R}$ はどちらかというと「代数構造の入った $\mathbb{R}$」であり, 多様体としての $\mathbb{R},\mathbb{R}-\{0\}$ とは少し性格が違うものではある。もちろん, $\mathbb{R}$ は $\mathbb{R}$ でしかないが, 群 (対称的な構造を持った集合) とも思えたり多様体とも思えたりするということだ。

などもよいだろう。これは

$$\cos 3\theta = -4\cos^3\theta + 3\cos\theta$$

の $\cos 3\theta = 1$ となる場合, すなわち $\theta = 0, \frac{2\pi}{3}, \frac{4\pi}{3}$ から現れる三次方程式である。

(2): **真である。** n 乗根は何も実数に限る話ではない。単に n 乗して x になったら x の n 乗根というのである。実際に 8 乗して 16 になることは容易である:

$$(1+\sqrt{-1})^8 = (2\sqrt{-1})^4 = (-4)^2 = 16$$

(3): **偽である。** 本問の中ではこれが最もトリッキーである。数学界の反例探しというのを甘く見てはいけない。ただ, 正直なところ具体的な"$f(x)$ の数式"を与えるのは面倒だしそれだけ見てもわからないので, どういうグラフであるかの説明をするだけで想像をしてほしい。

まず $-\pi/2 \leqq x \leqq 0$ では $f(x) = \cos x - 1$ とする。$x = -\frac{\pi}{2}$ での傾きが 1 だから, そこから微分可能になるように別の単調増加グラフをつなげればいい。たとえば $y = e^x$ の $x \leqq 0$ の部分を, $(0,1) \to (-\frac{\pi}{2}, -1)$ という平行移動で繋げれば良い。これで $f(x)$ の $x \leqq 0$ の部分は完成した。

次に $0 \leqq x \leqq \pi$ では $\sin x$ の $-\pi/2 \leqq x \leqq \pi/2$ のグラフ (これは単調増加) を平行移動して $f(0) = 0$ のところで繋げる (この繋げ方は微分可能である)。次に $\pi \leqq x \leqq 2\pi$ においては, $\frac{1}{2^2}\sin x$ の $-\pi/2 \leqq x \leqq \pi/2$ の部分を繋げればよい。以下このように繋げていく。すなわち, この次には $y = \frac{1}{3^2}\sin 3^2 x$ $(-\pi/18 \leqq x \leqq \pi/18)$ を繋げてから $y = \frac{1}{4^4}\sin x$ $(-\pi/2 \leqq \pi/2)$ を繋げていき, 以下 $n = 3, 4, 5, 6, \cdots$ に対しても

$$y = \frac{1}{(2n-1)^2}\sin(2n-1)^2 x$$

の $(-\pi/\{2(2n-1)^2\} \leqq x \leqq \pi/\{2(2n-1)^2\}$ の部分を繋げてから

$$y = \frac{1}{(2n)^2}\sin x$$

の $-\pi/2 \leqq \pi/2$ の部分を繋げる。

よくみると $-\pi/2 \leqq x \leqq \pi/2$ の部分にあるサインカーブを (縦に縮めて) 何度も繋げているから, 横方向にいくらでも $f(x)$ が伸びていくことが分かる。これで $f(x)$ が帰納的な構成を通して実数全体で定義されたことになる。繋げていった物としてはサインカーブの増加部分しか使っていないわけだから, (狭義) 単調増加性は明らか。微分可能性もつながりの部分で傾きが 0 になっていることから分かるであろう。

さて, この $f(x)$ はいわば階段状であるが, 天にまで登っていくわけではない。なぜなら, 用いたサインカーブは $\frac{1}{k^2}\sin Ax$ という形であって, 一つ上昇するときに上昇値は $\frac{2}{k^2}$ しかないので, $\sum_{k=1}^{\infty}\frac{2}{k^2} < \infty$ というよく知られた話によって $f(x) < M$ が常に満たされるように定数 M を取ることが出来る。しかしながら $\lim_{x\to\infty} f'(x) = 0$ は満たされない。なぜなら, 繋げたサインカーブのうち $\frac{1}{(2k-1)^2}\sin(2k-1)^2 x$ というものを微分すると $\cos(2k-1)^2 x$ であって, この導関数の値が 1 になるような点をこのサインカーブは含んでしまっていて, $f'(x)$ が無限回 1 という値を取ることがわかるからである。

よってこのような $f(x)$ を与えると良い。

(4): **真である。**有名問題ではあるが, 対偶, あるいは背理法を使わないと難しいというのはなぜか不思議な感じがする。さて, $\sqrt{x}$ が有理数だと仮定して x が有理数であることを示せばよいが, 有理数の積は有理数なのであたりまえである。