

$n^p - (2p + 1)n + 3p$  が素数となるような  
整数  $n$ , 素数  $p$  の組  $(n, p)$  をすべて求めよ。

[解答] フェルマーの小定理より任意の整数  $n$  について  $n^p \equiv n \pmod{p}$  である。

よって与式は

$$n^p - (2p + 1)n + 3p \equiv n - n \equiv 0 \pmod{p}$$

となる。つまり与式が素数となるときは、 $n^p - (2p + 1)n + 3p = p$  のときと同一値である。故に方程式  $n^p - (2p + 1)n + 2p = 0$  を解けばよい。式を変形すると  $n[n^{p-1} - (2p + 1)] = -2p$  となり、 $p$  は素数なので、 $n = \pm 1, \pm 2, \pm p, \pm 2p$  に絞られる。 $n = 1$  のとき、 $1 - (2p + 1) + 2p = 0$  よって  $n = 1$  のときは任意の素数  $p$  について条件を満たすので、解として  $(n, p) = (1, q)$  ( $q$  は任意の素数) が得られる。 $n = -1$  のとき、方程式は  $4p + 1 + (-1)^p = 0$  となるので、明らかに不適。

[1]  $n = p$  のとき 方程式は  $p^p = p(2p - 1)$  と変形でき、 $2p - 1$  は  $p$  の倍数ではないことから、両辺の素因数  $p$  の数に矛盾が生じる。よって解なし。

[2]  $n = -p$  のとき 方程式は  $p^p = p(2p + 3)$  と変形でき、 $p \neq 3$  のとき  $2p + 3$  は  $p$  の倍数ではないことから、両辺の素因数  $p$  の数に矛盾が生じる。よって  $p = 3$  でなければならず、これは確かに方程式を満たすので、解  $(n, p) = (-3, 3)$  が得られる。

[3]  $n = 2p$  のとき 方程式は  $(2p)^p = (2p)^2$  と変形でき、素因数  $p$  の個数を考えて、これを満たす  $p$  は  $p = 2$  のみ。よって解  $(n, p) = (4, 2)$  が得られる。

[4]  $n = -2p$  のとき 方程式は  $(-2p)^p = -2p(2p + 2)$  と変形でき、 $p \neq 2$  のとき  $2p + 2$  は  $p$  の倍数ではないことから、両辺の素因数  $p$  の数に矛盾が生じる。よって  $p = 2$  でなければならないが、これは方程式を満たさないの解なし。

[5]  $n = 2$  のとき 方程式は  $2^{p-1} = (p - 1) + 2$  と変形できる。微分を用いることで  $2^x > x + 2$  ( $x \geq 3$ ) となることがわかるので、 $p - 1 < 3$  となる必要があり  $p = 2, 3$  と絞られる。それぞれ条件を満たすのか確認すると、解とし

て  $(n, p) = (2, 3)$  のみが得られることが分かる。

[6]  $n = -2$  のとき  $p = 2$  のときの解が  $n = 1, 4$  と既に 2 つ得られており、 $p = 2$  のとき方程式は  $n$  についての 2 次方程式となるので、もう解を持つことはない。よって  $p \neq 2$ 、すなわち  $p$  は奇素数としてよい。すると  $n = -2$  より方程式は  $2^p = 6p + 2$  と変形できる。微分を用いることで  $2^x > 6x + 2$  ( $x \geq 6$ ) となることがわかるので、 $p < 6$  となり  $p = 2, 3, 5$  と絞られる。 $p = 3$  の場合も既に 3 つの解が  $n = 1, 2, -3$  が得られているので、 $p = 5$  の場合のみ調べればよく、解として  $(n, p) = (-2, 5)$  が得られることが分かる。

[1] ~ [6] より求める解は

$(n, p) = (1, q), (4, 2), (2, 3), (-3, 3), (-2, 5)$  ( $q$  は任意の素数) である。  $\square$

[別解]  $n = \pm 1, \pm 2, \pm p, \pm 2p$  と絞り込んだ後に、複雑だがもう少し解析的に解く方法もある。

$n = \pm 1$  のときを同様に調べた後、 $n = 1$  で解を持つことから方程式の左辺を  $n - 1$  で割り算して、方程式を  $n^{p-1} + n^{p-2} + \dots + n - 2p = 0$  と変形することができることを利用する。

[1]  $n > 0$  のとき

$$n^{p-1} + n^{p-2} + \dots + n - 2p \geq n^{p-1} - 2p$$

より、 $0 \geq n^{p-1} - 2p$  である必要がある。そこで関数  $f(x) = n^{x-1} - 2x$  を考える。 $p \geq 2$  より  $x \geq 2$  のときを考えればよい。 $f(2) = n - 4$  より、 $n > 4$  のときは  $f(2) > 0$  となることに注意しておく。 $x \geq 2$  に注意して、 $n > 4$  のとき

$$\begin{aligned} f'(x) &= n^{x-1} \log n - 2 \\ &> 4^{x-1} \log 4 - 2 \\ &\geq 4 \log 4 - 2 \\ &= 2(2 \log 4 - 1) \\ &> 0 \end{aligned}$$

ゆえに  $n > 4$  のときは  $x \geq 2$  で  $f'(x) > 0$ 、そして  $f(2) > 0$  であるので、 $f(x) > 0$  ( $x \geq 2$ ) である。つまり  $n > 4$  においては  $0 \geq n^{p-1} - 2p$  は成り立たないので不適。これより  $2 \leq n \leq 4$  とわかり、解が  $n = \pm 1, \pm 2, \pm p, \pm 2p$  に絞られていることを思い出すと、 $n = 3, 4$  のときはそれぞれ  $p = 3, 2$  となる必要があることがわかる。それぞれ代入して実際に条件を満たすことを確かめると、解として  $(n, p) = (4, 2)$  のみを得られることが分かる。 $n = 2$  のときは、もとの解法と同様にして、解として  $(n, p) = (2, 3)$  のみを得られることが分かる。以上より解として  $(n, p) = (4, 2), (2, 3)$  が得られた。

[2]  $n < 0$  のとき

$p = 2$  のときは、もとの方程式が  $n$  についての 2 次方程式となり、既に 2 つの解  $n = 1, 4$  が得られている。よって  $p = 2$  のときはこれ以上解が存在しないので  $p \neq 2$  としてもよく、このとき  $p$  は奇数になることに注意する。 $N = -n$

とおくと  $N > 0$  で、方程式は  $p$  が奇数より  $N^{p-1} - N^{p-2} + \dots - N - 2p = 0$  と書き換えられる。ここで  $N = 1$  すなわち  $n = -1$  のとき解なしなので、 $N \geq 2$  としてもよい。このとき  $N^{k+1} - N^k = N^k(N - 1) > 0$  ( $k$  は自然数) であることを利用すると、方程式の左辺は

$$\begin{aligned} & N^{p-1} - N^{p-2} + \dots - N - 2p \\ &= (N^{p-1} - N^{p-2}) + (N^{p-3} - N^{p-4}) + \dots + (N^2 - N) - 2p \\ &> N^{p-1} - N^{p-2} - 2p \end{aligned}$$

となるので、 $0 > N^{p-1} - N^{p-2} - 2p$  が成り立つ必要がある。そこで関数  $g(x) = N^{x-1} - N^{x-2} - 2x$  ( $x \geq 3$ ) を考える。 $g(3) = N(N - 1) - 6$  より、 $N > 3$  のときは  $g(3) > 0$  であることに注意しておく。 $x \geq 3$  に注意して、 $N > 3$  のとき

$$\begin{aligned} g'(x) &= N^{x-1} \log N - N^{x-2} \log N - 2 \\ &= N^{x-2}(N - 1) \log N - 2 \\ &> 3(3 - 1) \log 3 - 2 \\ &= 2(3 \log 3 - 2) \\ &> 0 \end{aligned}$$

ゆえに  $N > 3$  のときは  $x \geq 3$  で  $g'(x) > 0$ 、そして  $g(3) > 0$  であるので、 $g(x) > 0$  ( $x \geq 3$ ) である。つまり  $N > 3$  のときは、 $0 > N^{p-1} - N^{p-2} - 2p$  は成り立たないので不適。これより  $2 \leq N \leq 3$  とわかり、解が  $n = \pm 1, \pm 2, \pm p, \pm 2p$  に絞られていることを思い出すと、 $N = 3$  のときは  $p = 3$  となる必要があることがわかる。代入して条件を満たすのかを確かめると、実際満たすことが確かめられるので、解として  $(n, p) = (-3, 3)$  が得られる。残りは  $N = 2$  すなわち  $n = -2$  のときである。もとの解法と同様にして解として  $(n, p) = (-2, 5)$  が得られる。以上より  $n < 0$  の場合を調べ終え、解として  $(n, p) = (-3, 3), (-2, 5)$  が得られた。

[1][2] より求める解は

$(n, p) = (1, q), (4, 2), (2, 3), (-3, 3), (-2, 5)$  ( $q$  は任意の素数) である。  $\square$