

[解答例]

b_1, b_2, \dots, b_n は異なる素数であるとして考えてよい. また, 問題の仮定を満たすような 2 つの組 $(x, y_1, y_2, \dots, y_n)$ と $(x', y_1', y_2', \dots, y_n')$ があるとき, x と x' は互いに素であるとしてよい. $S = \{b_1, b_2, \dots, b_n\}$ とすると, $\text{GCD}(a^x - 1, a^{x'} - 1) = a - 1$ であるから, $a - 1$ の素因数の集合は S である. そして $a \geq 3$ である. $z > 1$ である整数 z に対し, $a^z - 1$ の素因数の集合が S であるとき, z の任意の素因数 p に対し, $y = \text{GCD}(a - 1, a^{p-1} + a^{p-2} + \dots + 1)$ とおくと, $a \equiv 1 \pmod{y}$, $a^{p-1} + a^{p-2} + \dots + 1 \equiv p \pmod{y}$ であるから $y = 1$ or p であるが, $y \neq 1$ なので, $y = p$ となる. すると, $p \in S$ であり, ゆえに, $a^{p-1} + a^{p-2} + \dots + 1$ は p の中である. ここで p が奇数であると仮定すると, $a \equiv 1 \pmod{p}$ であることから, $p^2 \nmid a^{p-1} + a^{p-2} + \dots + 1$ となるが, $a^{p-1} + a^{p-2} + \dots + 1 = p$ は $a \geq 3$ だから成立しない. ゆえに $p = 2$ であって, z は 2 の中である. ゆえに $0 < x < x'$ とすると, $\text{GCD}(x, x') = 1$ だから, $x = 1, x' = 2^l$ ($l \geq 1$) とおける. また, $a + 1 = 2^t$ ($t \geq 2$) とおける. このとき $a^x - 1 = a - 1 = 2(2^{t-1} - 1)$ である. また, $l \geq 2$ であると仮定すると, $a^2 + 1 = (2^t - 1)^2 + 1$ は $a^{x'} - 1$ の因数である. すると, $2^{t-1} - 1$ の任意の素因数 q に対して, $a^2 + 1 \equiv 2 \pmod{q}$ となるが, $q \neq 2$ であるから, 仮定に矛盾する. ゆえに $l = 1$ であって, このとき $t = 2$ となる. したがって, $a = 3$, かつ $n = 1$ であって, $b_1 = 2$ である.