p を素数，n を自然数，$a,\ b,\ c$ を整数とする．$a-b$ が n で割り切れるとき，$a \equiv b \pmod{n}$ と書くことにする．このとき，次の問いに答えよ．ただし，素数の性質「ab が p で割り切れるならば，a は p で割り切れるかまたは b は p で割り切れる」は用いてもよい．

(1) $x^2 \equiv a^2 \pmod{p}$ を満たす整数 x をすべて求めよ．

(2) $x^2+2bx+c \equiv 0 \pmod{p}$ を満たす整数 x で $0 \leqq x \leqq p-1$ であるものは 2 個以下であることを示せ．

(3) $x^2-4x+2 \equiv 0 \pmod{79}$ を満たす整数 x で $0 \leqq x \leqq 78$ であるものをすべて求めよ．

(4) $x^2-6x+9 \equiv 0 \pmod{49}$ を満たす整数 x で $0 \leqq x \leqq 48$ であるものをすべて求めよ．

(19 静岡大 後 理)

【答】

(1) $x = kp \pm a$ (k は整数)

(2) 略

(3) $x = 11,\ 72$

(4) $x = 3,\ 10,\ 17,\ 24,\ 31,\ 38,\ 45$

【解答】

(1) $x^2 \equiv a^2 \pmod{p}$ より

$$x^2-a^2 \equiv 0 \pmod{p}$$
$$\therefore\ (x+a)(x-a) \equiv 0 \pmod{p}$$

すなわち，「$(x+a)(x-a)$ は素数 p で割り切れる」．与えられた「素数の性質」より

「$x+a$ は素数 p で割り切れるかまたは $x-a$ は素数 p で割り切れる」

すなわち

$$x+a \equiv 0 \pmod{p} \quad \text{または} \quad x-a \equiv 0 \pmod{p}$$
$$\therefore\ x \equiv \pm a \pmod{p}$$

よって，求める x は

$$\boldsymbol{x = kp \pm a\ (k \text{ は整数})} \qquad \cdots\cdots(\text{答})$$

(2) $x^2+2bx+c \equiv 0 \pmod{p}$

を満たす整数 x が存在するとき，その 1 つを n とすると

$$n^2+2bn+c \equiv 0 \pmod{p}$$

辺々引いて

$$x^2-n^2+2b(x-n) \equiv 0 \pmod{p}$$
$$(x-n)(x+n+2b) \equiv 0 \pmod{p}$$

「素数の性質」より

$$x-n \equiv 0 \pmod{p} \quad \text{または} \quad x+n+2b \equiv 0 \pmod{p}$$
$$\therefore\ x = kp+n,\ kp-n-2b \quad (k \text{ は整数})$$

このうち，$0 \leqq x \leqq p-1$ であるものは 2 個以下である． $\cdots\cdots$ (証明終わり)

(3) $x^2 - 4x + 2 \equiv 0 \pmod{79}$

を変形すると

$$x^2 - 4x + 2 \equiv 79 \pmod{79}$$
$$x^2 - 4x - 77 \equiv 0 \pmod{79}$$
$$(x+7)(x-11) \equiv 0 \pmod{79}$$

「素数の性質」より

$$x + 7 \equiv 0 \pmod{79} \quad \text{または} \quad x - 11 \equiv 0 \pmod{79}$$
$$\therefore \quad x = 79k - 7,\ 79k + 11 \ (k \text{ は整数})$$

このうち，$0 \leqq x \leqq 78$ であるものは

$$x = 72,\ 11$$ ……(答)

(4) $x^2 - 6x + 9 \equiv 0 \pmod{49}$

を変形すると

$$(x-3)^2 \equiv 0 \pmod{7^2}$$
$$\therefore \quad (x-3)^2 \equiv 0 \pmod{7}$$

7 は素数であるから,「素数の性質」より

$$x - 3 \equiv 0 \pmod{7}$$
$$\therefore \quad x = 7k + 3 \quad (k \text{ は整数})$$

である．このうち $0 \leqq x \leqq 48$ であるものは

$$\boldsymbol{x = 3,\ 10,\ 17,\ 24,\ 31,\ 38,\ 45}$$ ……(答)