Q6.10 $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong$ { Cyclic (p: 奇素数 or $e=1$) / $\mathbb{Z}/2\mathbb{Z} \times$ Cyclic ($p=2$, $e\geq 2$) }

- $\#(\mathbb{Z}/p^e\mathbb{Z})^\times = p^{e-1}(p-1)$

(☺ $\overline{n} \in (\mathbb{Z}/p^e\mathbb{Z})^\times \Longleftrightarrow \gcd(n, p^e)=1 \Longleftrightarrow p \nmid n$

pの倍数は $p \cdot 2p \cdot 3p, \cdots, p^{e-1}\cdot p$ の p^{e-1} 個

ここは0と合同.

$\therefore \#(\mathbb{Z}/p^e\mathbb{Z})^\times = p^e - p^{e-1} = p^{e-1}(p-1)$)

$e=1$ のとき - $X^{p-1}-1 \equiv 0 \pmod p$ の解の個数は $p-1$ 個ちょうど.

(☺ p: 素数 $\Rightarrow$ $X^p \equiv X \pmod p$ が全ての X について成立

$\Rightarrow$ $X(X^{p-1}-1) \equiv 0 \pmod p$ が

$X = 0, 1, 2, \cdots, p-1$ に対して成立.

$\Rightarrow$ $X^{p-1}-1 \equiv 0 \pmod p$ が

$X = \underbrace{1, 2, \cdots, p-1}_{p-1\text{個}}$ に対して成立)

ここで. テキスト p46 (44) を思い出す:

($(\mathbb{Z}/p\mathbb{Z})^\times$ が有限アーベル群であることは明らか)

$(\mathbb{Z}/p\mathbb{Z})^\times$: Cyclic $\Longleftrightarrow \forall g \mid \#(\mathbb{Z}/p\mathbb{Z})^\times$: prime.

$\#\{ n \in (\mathbb{Z}/p\mathbb{Z})^\times \mid n^g \equiv 1 \pmod p \} \leq g$ (*)

$n^g - 1 \equiv 0 \pmod p$ となる n の個数は. $n^g - 1$ が g 次式なので 高々 g 個. つまり. (*) が成立している.

よって. $(\mathbb{Z}/p\mathbb{Z})^\times$ は Cyclic //

$p \neq 2$ のとき　（e は何でもOK）

$\#(\mathbb{Z}/p^e\mathbb{Z})^\times = p^{e-1}(p-1)$ だったので、$(\mathbb{Z}/p^e\mathbb{Z})^\times$ には mod p で位数 $p-1$ の元が存在する。これを a とおく。

ここで、$a^{p^{e-1}}$ という元を考えると、$(a^{p^{e-1}})^{p-1} \equiv 1 \pmod{p^e}$

（$\because \#(\mathbb{Z}/p^e\mathbb{Z})^\times = p^{e-1}(p-1)$ ゆえ）

つまり、$a^{p^{e-1}}$ の位数は $p-1$ を割る。実はこの位数は $p-1$ ちょうどであることを示す。　㊛（下でいう $r \mid p-1$）

そこで今、$(a^{p^{e-1}})^r \equiv 1 \pmod{p^e}$ であるとすると、

$$1 \equiv (a^{p^{e-1}})^r \equiv a^r \pmod{p}$$

（$(a^{p^{e-1}})^r \equiv 1 \pmod{p^e}$ なのだから、mod p でもちろん成立）

（$(a^{p^{e-1}})^r = (a^r)^{p^{e-1}} = (a^r)^{p \cdot p^{e-2}}$
$\equiv (a^r)^{p^{e-2}} = (a^r)^{p \cdot p^{e-3}}$
$\equiv (a^r)^{p^{e-3}} \cdots \equiv a^r \pmod{p}$）

a は mod p で位数 $p-1$ の元だったから、$p-1 \mid r$

これと㊛より　$p-1 = r$ が示された。

（$\therefore$ $a^{p^{e-1}}$ の mod p^e での位数は $p-1$ である）

ここで、次の式が成り立つことを使う：

$$(1+p)^{p^i} \equiv 1 + p^{i+1} \pmod{p^{i+2}}$$

（☺）帰納法により示す。（i についての induction）

$i=1$ のときは

$$(1+p)^p = 1 + {}_pC_1 p + {}_pC_2 p^2 + \underbrace{{}_pC_3 p^3 + \cdots}_{\text{これらは全て mod } p^3 \text{ で } 0}$$

$$\equiv 1 + p \cdot p + \underbrace{\frac{p(p-1)}{2}}_{\text{これも mod } p^3 \text{ で } 0} p^2$$

$$\equiv 1 + p^2 \pmod{p^3}$$　OK.

iのとき成立を仮定して、$i+1$で成立を示す：

$$(1+p)^{p^{i+1}} = \{(1+p)^{p^i}\}^p$$

$$\equiv \{1+p^{i+1}\}^p \pmod{p^{i+3}}$$

(**)

$$= 1 + {}_pC_1\, p^{i+1} + {}_pC_2 (p^{i+1})^2 + \cdots$$

$$= 1 + p^{i+2} + \underbrace{\left(\frac{p(p-1)}{2} p^{i-1}\right)}_{\left(\text{これは } \frac{p-1}{2} \in \mathbb{Z} \ (p:\text{奇素数}) \text{ より。} \mathbb{Z} \text{のえ} \quad (\text{注}) \ p=2 \text{でも OK}\right)} \cdot p^{i+3} + \cdots$$

$$\equiv 1 + p^{i+2} \pmod{p^{i+3}}$$

(Remark. (**)の部分は $(1+p)^{p^i} \equiv 1 + p^{i+1} \pmod{p^{i+2}}$ なので、これの辺を p 個の積を考えると $\bmod p^{i+3}$ で合同がわかる。)

ということで、これを使えば次が分かる：

- $(1+p)^{p^{e-2}} \equiv 1 + p^{e-1} \pmod{p^e}$

  $\not\equiv 1$ (☺ p^{e-1} は $\bmod p^e$ で 1 にはならない)

- $(1+p)^{p^{e-1}} = \{(1+p)^{p^{e-2}}\}^p$

  $\equiv (1+p^{e-1})^p \pmod{p^e}$

  $= 1 + {}_pC_1\, p^{e-1} + \underbrace{{}_pC_2 (p^{e-1})^2 + \cdots}_{\text{これらは全て } p^e \times \triangle \text{ の形ゆえ } 0}$

  $\equiv 1 + p^e \pmod{p^e}$

  $\equiv 1 \pmod{p^e}$

$\Rightarrow$ 上の2つから、$1+p$ の位数は $\underbrace{p^{e-1}}_{(\bmod p^e \text{での})}$ である。

(☺ $1+p$ の位数を r とすると、$r \mid p^{e-1}$ であるから $r = p^m$ の形
これと、$(1+p)^{p^m} \equiv 1 \pmod{p^e} \Rightarrow (1+p)^{p^{m+1}} = \{(1+p)^{p^m}\}^p \equiv 1 \pmod{p^e}$
から、$m \leq e-2$ だと上の条件に矛盾。 $\therefore m = e-1$)

以上より、($\mathrm{mod}\ p^e$ で $a^{p^{e-1}}$ の位数は $p-1$. $1+p$ の位数は p^{e-1})

$(a^{p^{e-1}}(1+p)$ の位数$) = \mathrm{lcm}(p-1, p^{e-1}) = (p-1)p^{e-1}$

互いに素　　$\#(\mathbb{Z}/p^e\mathbb{Z})^\times$ に等しい!!

つまり. $a^{p^{e-1}}(1+p)$ を使って.

$(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle a^{p^{e-1}}(1+p) \rangle$ と書ける (=Cyclic) //

$p=2$, $e\geq 2$ のとき

$e=2$ の時は $(\mathbb{Z}/2^2\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ (ちなみに $\langle \overline{3} \rangle$ とかける)

でOK ($\mathbb{Z}/2\mathbb{Z}$ と自明な巡回群 $\langle \overline{1} \rangle$ との積)

以降 $e\geq 3$ とする　先と同じ方法で. 次を帰納法で示せる:

$$(1+2^2)^{2^{i-1}} \equiv 1+2^{i+1} \pmod{2^{i+2}}$$

(:) 先とほとんど同じ　$i=1$ はOK. i のときOKと仮定.

$$\begin{aligned}(1+2^2)^{2^i} &= \{(1+2^2)^{2^{i-1}}\}^2 \\ &\equiv (1+2^{i+1})^2 \pmod{2^{i+3}} \\ &= 1+2^{i+2}+2^{i-1}\cdot 2^{i+3} \\ &\equiv 1+2^{i+2} \pmod{2^{i+3}} \quad \text{OK.}\end{aligned}$$

これより.

- $(1+2^2)^{2^{e-3}} \equiv 1+2^{e-1} \pmod{2^e}$
  $\not\equiv 1 \pmod{2^e}$
- $(1+2^2)^{2^{e-2}} = \{(1+2^2)^{2^{e-3}}\}^2 \equiv (1+2^{e-1})^2 \pmod{2^e}$
  $= 1+2^e+2^{e-2}\cdot 2^e \equiv 1 \pmod{2^e}$.

∴ $1+2^2$ の $\mathrm{mod}\ 2^e$ での位数は 2^{e-2} となる.

これにより. $H = \{ a \in (\mathbb{Z}/2^e\mathbb{Z})^\times \mid a \equiv 1 \pmod 4 \}$ と

おくと. H は 5 で生成される Cyclic gp.

(:) $5 = 1 + 2^2$ の $\bmod 2^e$ での位数は 2^{e-2}

$$\#(\mathbb{Z}/2^e\mathbb{Z})^\times = 2^e - \underbrace{2^{e-1}}_{(2^e\text{以下の偶数の個数})} = 2^{e-1} \quad (2^e \text{以下の奇数の個数})$$

2^e 以下の奇数は 2^{e-1} 個で. それらは

- 4 で割って 1 余るもの が 2^{e-2} 個
- 4 で割って 3 余るもの が 2^{e-2} 個.

ずつある. しかも. 5 は 4 で割って 1 余る.

H は 4 で割って 1 余るものの集まりであるから. $H = \langle 5 \rangle$.

となる。($\#H$ と 5 の位数が等しいから)

一方. 残る "4 で割って 3 余る" 数たちは $(-1)H$ とかける.

(:) $a \in H$ とすると $a = 4n+1$ の形,

$$(-1)a = -4n-1 \equiv 4n-1 \pmod 4$$
$$\equiv 4n+3 \pmod 4$$

となって. 4 で割って 3 余る数になる.

これで $(\mathbb{Z}/2^e\mathbb{Z})^\times$ の元を出しつくしたことになるから.

$$(\mathbb{Z}/2^e\mathbb{Z})^\times = H \underset{\text{disjoint 和}}{\sqcup} (-1)H$$

$$\cong \langle -1 \rangle \times H.$$

$$\cong \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{位数2の Cyclic gp.}} \times \underbrace{\langle 5 \rangle}_{H \text{ は Cyclic}}$$

となり 示された //

めでたし