

2.10.6

中国剰余定理 1)

$$G \cong (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \\ \times (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \dots \textcircled{1}$$

$H \leq G$ の指数 2 の部分群 H とする。

問題 2.10.4)

$H \supset 2G$ であり。

定理 2.10.2 と 第三同型定理から

H は $G/2G$ の指数 2 の部分群と 1対1に対応する。

よって ①より

$(\mathbb{Z}/8\mathbb{Z})/(\mathbb{Z}/4\mathbb{Z})$ 1)

$$G/2G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

後は 問題 2.10.2 と同じ論法で

求める数 173

今見返して
173-2*85=3
173 mod 8 = 5

* 「 $0, 1, 2, \dots, (p^k-1)q$ は p^k で割った余りは

p と q が互いに素なとき、互いに異なり、という命題を利用する

簡易
[証明]

仮に $i \cdot q, j \cdot q$ の余りが同じであると (一般性から $i \geq j$ と仮定)

$$(i-j)q \equiv 0 \pmod{p^k}$$

よって $0 \leq i \leq p^{k-1}, 0 \leq j \leq p^{k-1}, j \leq i$ より

$0 \leq i-j \leq p^{k-1}-1$ かつ $i-j$ は p^k で割り切れるから

かつ q は p と互いに素なため $(i-j)q \equiv 0 \pmod{p^k}$ と矛盾する。