

数学アラカルト第2回レポート

学校名

学科名

学籍番号

氏名

レポート課題1. \mathbb{Z}_6 の要素同士の加法の結果を表にせよ. また, \mathbb{Z}_6^* の要素同士の乗法の結果を表にせよ.

\mathbb{Z}_6	+	0	1	2	3	4	5
	0						
	1						
	2						
	3						
	4						
	5						

\mathbb{Z}_6^*	×	1	5
	1		
	5		

レポート課題2. ある人が暗証番号 a (2桁の数) を公開数 $N = 437$, 公開鍵 $e = 85$ で暗号化したら, $b = 96$ を得た. この人の暗証番号 a を求めよ.

$$N = 437 = 19 \cdot 23,$$

$$p = 19, q = 23 \text{ とおくと } L = \text{lcm}(p-1, q-1) = \text{lcm}(18, 22) = 198,$$

$$nL + 1 = 198n + 1 = ed \text{ (} e < 198, 1 < d < 198 \text{) である.}$$

$$e = 85 \text{ より, } 198n - 85d = -1 \text{ である.}$$

$$\frac{198}{85} = \quad + \frac{1}{\quad}$$

$$+ \frac{1}{\quad} = \quad$$

よって, $n = \quad$, $d = \quad$

故に $a \equiv \quad \equiv \quad \pmod{437}$,

暗証番号は $a = \quad$

アンケートにお答えください

1. 今回の講義は面白かったですか

面白かった 少し面白かった 少しつまらなかった つまらなかった

2. 今回の講義は難しかったですか

難しかった 少し難しかった 少し簡単だった 簡単だった

3. 今回の講義を受けた感想、意見などをお書きください

記入できたら送信ボタンを押してください。初めから、書き直すときはクリアボタンを押してください。

送信 クリア