アルゴリズム論特論　(塩田)

2015 年 5 月 25 日

定理 法 n の剰余類 $\bar{a}$ に対し、

$$\bar{a} \text{ の逆数が存在 } \Leftrightarrow \gcd(a, n) = 1$$

アルゴリズム

入力：法 n と剰余類 $\bar{a}$

出力：$\bar{x} =$ (法 n での $\bar{a}$ の逆数) となる整数 x

1° a, n を引数とする拡張ユークリッドアルゴリズムを実行し、

$$\gcd(a, n) = ax + ny$$

を満たす x, y を求める。

2° $\gcd(a, n) \neq 1$ ならば「存在しません」と出力し終了。

3° x を出力。

宿題 引数 a, n に対し、

$$\bar{x} = \text{(法 } n \text{ での } \bar{a} \text{ の逆数)}$$

となる整数 x ($0 \leqq x < n$) を返り値とする関数 `modinv` を定義し、動作確認をせよ。

提出期限：6 月 1 日　(メールでも紙媒体でも可)