アルゴリズム論特論 （塩田）

2015年5月18日

フェルマの小定理 素数 p と、p で割り切れない整数 a に対して

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ。

宿題 下記の素数 p たちについて、$a = 2$ の場合のフェルマの小定理

$$2^{p-1} \equiv 1 \pmod{p}$$

を計算によって確かめてみよ（無理な場合は潔く諦めよ。）

(1) $p = 607$（10-bit）
(2) $p = 552259$（20-bit）
(3) $p = 900949267$（30-bit）
(4) $p = 660768960311$（40-bit）
(5) $p = 661425977735249$（50-bit）

（数字はホームページからコピペした方が確かかも。）

提出期限：5月25日 （メールでも紙媒体でも可）