# 1-26

tamakoron

平成 28 年 5 月 22 日

## 1　練習問題 1.26

1.24 での問題が遅い理由を考える．expmod が square に部分を明示的に掛け算にしているため, 1 回につき同じ計算を 2 回おこなっている．そのため, 指数関数的に expmod が行われる．よって $\Theta(logn)$ で 計算できる問題を $\Theta(n)$ で説いてしまっている．

コードを表すと以下となる

```
(defun expmod (base exp m)
  (cond ((= exp 0) 1)
        ((even? exp)
         (rem
          ;; ↓ (square (expmod base (/ exp 2) m))
          (* (expmod base (/ exp 2) m)
             (expmod base (/ exp 2) m))
          m))
        (t
         (rem (* base
                 ( expmod base (- exp 1) m))
              m))))
```