練習問題（第 3 回）

問 1．

次の (1) ~ (4) の多項式は，それぞれ（問題の大きさを n として）アルゴリズムの計算時間を表現したものである．これらのオーダを示しなさい．

(1) $3n + 2\log n$ (2) $n^3 - n^2 + 5n + 3$

(3) $10n\log n + 5n^2$ (4) $2^n + n^2 + 2$

（ヒント）

$$\frac{\log_2 n}{n} \leqq \frac{\log_2 e}{e} = 0.5307\ldots \text{（定数）}$$

問 2．

ユーザ認証に利用されるパスワードの安全性について考える．通常，パスワードに使用可能な文字は全部で 95 種類である．したがって，「総当たりによってパスワードを見破ろうとする」アルゴリズムを考えると，パスワードの長さを n として，その時間複雑度は $O(95^n)$ になるが，ここでは計算を簡単にするため $O(100^n)$ として考えよう．

いま，このアルゴリズムをある計算機環境で実装して実行したところ，$n = 2$ の場合に 2 秒以下で計算が完了した．パスワードを長くして $n = 3, 4, 5$ とした場合，それぞれどれだけの時間があればパスワードを見破られてしまうか答えなさい．（答えは 2×10^k [秒] のかたちで構わない．）

（ヒント）$O(2^n)$ と $O(n^2)$ の違いについて：これから $O(100^n)$ の場合についても類推して下さい．

- 2^n の場合：n を +1 したとき $2^{n+1} = 2 \times 2^n$ なので，もと（2^n）の 2 倍となる．しかし，n を 2 倍にした場合は $2^{2n} = 2^n \times 2^n$ となり，もと（2^n）の 2^n 倍ということになるがこれは n によって値が変わるため，単純に「〜倍になる」とはいえない．
- n^2 の場合：n を +1 すると $(n+1)^2 = n^2 + 2n + 1$ となり，もと（n^2）より $2n + 1$ だけ大きくなるがこれは n によって値が変わるため，単純に「〜倍になる」とはいえない．しかし，n を 2 倍にした場合は $(2n)^2 = 2^2 \times n^2$ となって話が単純になり，もと（n^2）の 2^2 倍といえる．