アルゴリズム論特論 （塩田）

2014年6月16日　前回までの復習

問1　法と呼ばれる自然数 n をひとつ固定したとき、法 n の合同式

$$a \equiv b \pmod{n}$$

の定義は次のように色々な言い換えがある：

(1) $a-b$ は n の [　　] である

(2) n は $a-b$ の [　　] である

(3) a と b は、n で割った [　　] が等しい

法 n の合同式のもとでは加法・減法・乗法を無条件に行うことができ、除算は除数が法 n と [　　] であるときに限り行うことができる。

問2　「フェルマの小定理」とは、素数 p と全ての整数 a に対して合同式

$$a^{\square} \equiv a \pmod{p}$$

が成り立つという定理である。

問3　2つの整数 a, b が互いに素であるとき、[　　] を満たす整数 x, y が存在する。この x の値は RSA 暗号の [　　] に用いられる。最大公約数やこの x の値は [　　] のアルゴリズムを用いれば高速に求めることができる。

問4　自然数 n と同程度の大きさの整数は、おおよそ [　　] 個にひとつが素数である。

問5　下記の選択肢から当てはまるものを選べ。

自然数 n のビット長	
n 以下の2数の加法・減法演算の計算量	
n 以下の2数の乗法・除法演算の計算量	
n 以下の2数を入力とするユークリッドのアルゴリズム	
$\bmod n$ の逆数計算	
n 程度の数 b, e に対して $b^e \,\%\, n$ を求める反復2乗法	
フェルマテストによる n 程度の数の素数判定	
フェルマテストによる n 程度の素数の生成	

$O(n)$,　$O(n^2)$,　$O(\log n)$,　$O(\log^2 n)$,　$O(\log^3 n)$,　$O(\log^4 n)$,　$O(n \log n)$