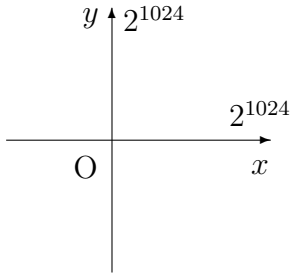
アルゴリズム論特論 （塩田）

2014 年 5 月 26 日　前回までの復習

問 1　$y = \log x$ のグラフの真の姿を描け。



問 2　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、$a - b$ が n の [　　] であることである。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る。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。例えば mod 7 では $\frac{1}{2} \equiv$ [　　] , $\frac{1}{3} \equiv$ [　　] である。

問 3　2 つの整数 a, b が [　　] であるとき、$ax + by = 1$ を満たす整数 x, y が存在する。この x の値は RSA 暗号の [　　] に用いられたり、合同式における [　　] の計算に用いられる。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 (拡張版)	
mod n の逆数計算	

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