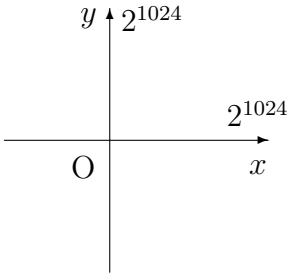
アルゴリズム論特論　(塩田)

2014 年 6 月 2 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

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

の定義は次のように色々な言い換えがある：

(1) $a - b$ は n の $\boxed{}$ である

(2) n は $a - b$ の $\boxed{}$ である

(3) a と b は、n で割った $\boxed{}$ 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 $\boxed{}$ であるときに限り行うことができる。

問 3　「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

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

が成り立つという定理である。

問 4　2 つの整数 a, b が互いに素であるとき、$\boxed{}$ を満たす整数 x, y が存在する。この x の値は RSA 暗号の $\boxed{}$ に用いられる。最大公約数やこの x の値は $\boxed{}$ 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 5　自然数 n と同程度の大きさの整数は、おおよそ $\boxed{}$ 個にひとつが素数である。

問 6　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	
mod n の逆数計算	

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