アルゴリズム論特論 （塩田）

2014 年 6 月 23 日　前回までの復習

問 1　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、法 b における a の [　　] であり、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 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　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 4　素数 p と、$\gcd(e, p-1) = 1$, $ed \equiv 1 \pmod{p-1}$ を満たすべき指数 e, d があるとする。このとき、平文の集合 P, 暗号文の集合 C, 暗号化関数 E, 復号化関数 D を次のように定めて暗号を設計することができる：

$$P \xrightarrow{E} C \xrightarrow{D} P$$

$$P = C = \{0, 1, \cdots, p-1\}, \quad E(x) = x^e \,\%\, p, \quad D(y) = y^d \,\%\, p$$

p, e, d がおおよそ n 程度の数であるとき、以下の計算量を O-記法を用いて述べよ。

フェルマテストによる p の生成	
e, d の生成	
$E(x)$ の計算	
$D(y)$ の計算	

また、この暗号は公開鍵暗号であるか否か、理由と共に述べよ。
