# Homework #4

Due date: 2016.04.13.Wed

1. symbol의 집합 $S = \{s_0, s_1, ..., s_{n-1}\}$ 에 대해 Affine Cipher $A : S \to S$는 두 정수 $K_1, K_2$를 사용하여 다음과 같이 정의할 수 있다.

$$A(s_i) = s_j,\ j = (K_1 i + K_2)\ mod\ n\ (K_1, K_2 \in Z,\ gcd(K_1, n) = 1)$$

이 때, Affine Ciper $A$는 bijection임을 보이시오. (6점)

2. 0이 아닌 세 자연수 $a, b, c$에 대해 $(a, b, c \in N_1)$

$$gcd(a^b - 1, a^c - 1) = a^{gcd(b,c)} - 1$$

가 성립함을 보이시오. (5점)

3. Fibonacci number $f$는 다음과 같이 정의할 수 있다.

$$f_0 = 0, f_1 = 1$$
$$f_n = f_{n-1} + f_{n-2}\ (n \geq 2)$$

이 때, 모든 자연수 $n \in N_1$ 에 대해 다음이 성립함을 Induction을 사용하여 보이시오. (6점)

$$f_{2n} = f_n(f_{n+1} + f_{n-1})$$
$$f_{2n-1} = f_n^2 + f_{n-1}^2$$

4. alphabet $\Sigma = \{T, F, p, q, r, s, \neg, \wedge, \vee, \to, \leftrightarrow, (, )\}$ 로 만들어지는(over) language $WFF \subseteq \Sigma^*$의 syntax grammar는 다음과 같다.

$$E ::= T|F|p|q|r|s|\neg E|E \wedge E|E \vee E|E \to E|E \leftrightarrow E|(E)$$

이 때, string $\neg(p \wedge \neg r) \to q \vee s$가 $WFF$의 원소임을 보이시오. (3점)