Homework #4

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_2를 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 A는 bijection임을 보이시오. (6점)

Affine Cipher A가 one-to-one이고 onto임을 보이자.
1)one-to-one
A가 one-to-one이 아니라고 가정하자.
즉, $(K_1 i + K_2)\ mod\ n = (K_1 j + K_2)\ mod\ n$를 만족하게 하는 서로 다른 두 자연수 $i, j < n$가 존재한다고 하자.
그렇다면 $n | (K_1 i + K_2) - (K_1 j + K_2)$, 즉 $n | K_1(i - j)$을 만족해야 한다.
$0 < i - j < n$ 이므로 $i - j$는 n과 서로소이고 $gcd(K_1, n) = 1$ 이므로 K_1 역시 n과 서로소이다.
따라서 $K_1(i - j)$는 n으로 나누어 떨어지지 않고 이는 가정과 모순이다.
따라서 A는 one-to-one이다.
2)onto
A는 정의역과 공역이 같고, one-to-one이므로 자명하게 A는 onto이다.
따라서 Affine Ciper A는 bijection이다.

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

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

가 성립함을 보이시오. (5점)

1) b와 c가 같을 경우
자명하게 저 식이 성립함을 알 수 있다.
2) b와 c가 다를 경우
편의를 위해, b>c라고 가정하자. b+c의 값을 사용하여, strong induction으로 증명한다.
basis) b+c = 3 (b = 2, c = 1)
$gcd(a^2 - 1, a - 1) = ((a - 1)(a + 1), a - 1) = a - 1$ 이므로
$gcd(a^2 - 1, a - 1) = a^{gcd(2,1)} - 1$ 이 성립한다.
induction) b+c<k라면$(k > 3)$ $gcd(a^b - 1, a^c - 1) = a^{gcd(b,c)} - 1$ 을 만족한다고 할 때
b+c=k인 두 자연수 b,c도 위의 식을 만족함을 보이자.
b>c이므로 $a^b - 1 = (a^c - 1)a^{b-c} + a^{b-c} - 1$ 이다.
유클리드 호제법에 의해 $gcd(a^b - 1, a^c - 1) = gcd(a^c - 1, a^{b-c} - 1)$ 이고
c+(b-c) = b < k이므로 $gcd(a^c - 1, a^{b-c} - 1) = a^{gcd(b-c,c)} - 1$ 이고
$gcd(b - c, c) = gcd(b, c)$ 이므로 $a^{gcd(b-c,c)} - 1 = a^{gcd(b,c)} - 1$ 이므로
b+c=k인 두 자연수 b,c에 대해 $gcd(a^b - 1, a^c - 1) = a^{gcd(b,c)} - 1$을 만족한다.
따라서 0이 아닌 세 자연수 a, b, c에 대해 $gcd(a^b - 1, a^c - 1) = a^{gcd(b,c)} - 1$ 가 성립한다.

3. Fibonacci number f는 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)

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

모든 자연수 $n \in N_1$ 에 대해 $f_{2n} = f_n(f_{n+1} + f_{n-1})\ f_{2n-1} = f_n^2 + f_{n-1}^2$ 임을 보이자.

basis) n = 1일 때

$f_2 = 2 = f_1(f_2 + f_0)$, $f_1 = 1 = f_1^2 + f_0^2$

induction) 어떤 자연수 n이 $f_{2n} = f_n(f_{n+1} + f_{n-1})\ f_{2n-1} = f_n^2 + f_{n-1}^2$ 을 만족한다고 할 때

$f_{2n+2} = f_{n+1}(f_{n+2} + f_n)$,$f_{2n+1} = f_{n+1}^2 + f_n^2$ 임을 보이자.

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

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

$= f_{n+1}^2 + f_n^2$

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

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

따라서 모든 자연수 $n \in N_1$ 에 대해 $f_{2n} = f_n(f_{n+1} + f_{n-1})\ f_{2n-1} = f_n^2 + f_{n-1}^2$ 은 성립한다.

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

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

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

1) $p \in WFF$ [$E ::= p$]
2) $r \in WFF$ [$E ::= q$]
3) $\neg r \in WFF$ [2), $E ::= \neg E$]
4) $p \wedge \neg r \in WFF$ [1),2), $E ::= E \wedge E$]
5) $(p \wedge \neg r) \in WFF$ [$E ::= (E)$]
6) $\neg(p \wedge \neg r) \in WFF$ [4), $E ::= \neg E$]
7) $q \in WFF$ [$E ::= q$]
8) $s \in WFF$ [$E ::= s$]
9) $q \vee s \in WFF$ [6),7), $E ::= E \vee E$]
10) $\neg(p \wedge \neg r) \rightarrow q \vee s \in WFF$ [5),8), $E ::= E \rightarrow E$]