ДОМАШНЯ РОБОТА №7
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

1. R - комутативне кільце з одиницею.

   реф. Оскільки R є комутативним кільцем з одиницею, нехай $a, b \in R$. Тоді $a = b$ та $b = a$. Отже, для деякої одиниці $\varepsilon \in R$. $b = a\varepsilon$, а отже і $a = b\varepsilon$

   сим. Якщо $b = a\varepsilon$ для деякої одиниці $\varepsilon \in R$, то $a = b\varepsilon^{-1}$ та ε^{-1} - одиниця.

   транз. Якщо $b = a\varepsilon_1$ та $c = b\varepsilon_2$ для деяких одиниць $\varepsilon_1, \varepsilon_2 \in R$, то $c = b\varepsilon_2 = a\varepsilon_1\varepsilon_2 = aw$, де $w = \varepsilon_1\varepsilon_2$ - одиниця.

2. - $[0] = \{0\}$
   - $[1] = \{1, 5, 7, 11\}$
   - $[2] = \{2, 10\}$
   - $[3] = \{3, 9\}$
   - $[4] = \{4, 8\}$
   - $[6] = \{6\}$

3. Нехай $\varphi : G \to H$ - гомоморфізм, $K = \ker\varphi$ - ядро гомоморфізму. $\forall g \in G, \forall h \in \ker\varphi$, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)(\varphi(g))^{-1} = \varphi(g)e_K(\varphi(g))^{-1} = \varphi(g)(\varphi(g))^{-1} = e_K$. Отже $\ker\varphi$ - нормальна підгрупа G.

4. $(3) = \{0, -3, 3, -6, 6, \dots\}$. В підкільця (3) нема ідеалів, окрім самого ж (3), а отже він головний. $(6) = \{0, -6, 6, -12, 12, \dots\}$. В підкільця (6) є елементи кратні 2 і 3, тобто воно не є головним. Отже (6) - не максимальний в $\mathbb{Z}$. А от в (3) максимальним ідеалом буде (6), так як більше (6) є лише (3) а воно і є самим кільцем.

5. Якщо n буде простим ($n = p$) необоротним буде елмент 0, а він утворює ідеал $\{0\}$. Якщо n буде складеним ($n = kp^\alpha$), необоротними будуть елементи, які не взаємно прості з n і вони не будуть обовєязково утворювати ідеал. Якщо n буде степінню просто числа ($n = p^\alpha$) необоротними будуть 0 та усі $p^{\alpha-i}$, $i = \overline{0, \alpha - 1}$, і вони будуть утворювати ідеал. Отже $n = p^\alpha, \alpha > 0$.