Matematyka dyskretna I
Zestaw 7

1. Wypisać unormowane wielomiany nierozkładalne stopnia nie większego niż 4 nad $\mathbb{F}_2$ i $\mathbb{F}_3$.

2. Przedstawić wielomian f w postaci iloczynu wielomianów nierozkładalnych nad ciałem $\mathbb{F}_p$.
(a) $f = X^{16} - X$, $p = 2$.
(b) $f = X^9 - X$, $p = 3$.
(c) $f = X^{27} - X$, $p = 3$.

3. Wyznaczyć liczbę unormowanych wielomianów nierozkładalnych stopnia nie większego niż 8 nad $\mathbb{F}_2$, $\mathbb{F}_3$ i $\mathbb{F}_5$.

4. Przedstawić wielomian f w postaci iloczynu wielomianów nierozkładalnych nad ciałem $\mathbb{F}_p$.
(a) $f = X^7 + X^4 + X^2 + X + 1$, $p = 2$.
(b) $f = X^8 + X^7 + 2X^6 + X^2 + X + 2$, $p = 3$.
(c) $f = X^9 + 2X^7 + X^6 + 3X^5 + X^4 + 2X^2 + 3X + 3$, $p = 5$.

5. Czy w przedstawieniu wielomianu f w postaci iloczynu wielomianów nierozkładalnych nad $\mathbb{F}_p$ każdy czynnik występuje w potędze 1?
(a) $f = X^6 + X^3 + X^2 + X$, $p = 2$.
(b) $f = X^6 + X^4 + X^2 + X$, $p = 3$.
(c) $f = X^6 + 2X^5 + 3X^4 + 2X^3 + 4X^2 + X + 4$, $p = 5$.

6. W ciele $\mathbb{F}_q$ rozwiązać równanie $f(x) = 0$.
(a) $f = X^2 + 1$, $q = 9$.
(b) $f = X^2 + X + 2$, $q = 9$.
(c) $f = X^2 + 2X + 3$, $q = 25$.

7. Niech p będzie liczbą pierwszą i $\alpha \in \mathbb{F}_{p^2}$ będzie pierwiastkiem wielomianu $X^2 + aX + b$, gdzie $a, b \in \mathbb{F}_p$. Udowodnić, że jeśli $\alpha \notin \mathbb{F}_p$, to $(c\alpha + d)^{p+1} = d^2 - acd + bc^2$. Wykorzystując ten fakt policzyć $(2 + 3i)^{101}$, gdzie i jest pierwiastkiem z -1 w $\mathbb{F}_{19^2}$.

8. Udowodnić, że jeśli $f \in \mathbb{F}_p[X]$, to $f' = 0$ wtedy i tylko wtedy, gdy istnieje wielomian $g \in \mathbb{F}_p[X]$ takie, że $f = g^p$.