

1. Sia $f = a_n X^n + \dots + a_1 X + a_0$ un polinomio in $\mathbf{Z}[X]$. Sia $\alpha = p/q$ (dove $p, q \in \mathbf{Z}$ con $q \neq 0$ e $\text{mcd}(p, q) = 1$) uno zero di f . Dimostrare che p divide a_0 e q divide a_n .
2. Decidere se il polinomio $X^5 + X^3 + 1$ è irriducibile o meno negli anelli $\mathbf{Z}_2[X]$, $\mathbf{Z}_3[X]$, $\mathbf{Z}[X]$, $\mathbf{Q}[X]$ e $\mathbf{R}[X]$.
3. (a) Dimostrare che i polinomi $X^6 + X^3 + 1$ e $X^5 - 8$ sono irriducibili in $\mathbf{Q}[X]$. (Sugg. usare il criterio di Eisenstein.)
(b) Dimostrare che $X^4 - X^2 + 1$ è un polinomio irriducibile in $\mathbf{Q}[X]$.
4. Dimostrare che $X^3 + Y^3 + XY^2 + X^2 + Y^2$ è irriducibile in $\mathbf{Z}[X, Y]$.
5. (a) Fattorizzare il polinomio $X^4 + 1$ in $\mathbf{R}[X]$.
(b) Fattorizzare il polinomio $X^4 + 1$ in $\mathbf{Z}[i][X]$.
(c) Dimostrare che $X^4 + 1$ è riducibile in $\mathbf{Z}_p[X]$ per ogni primo p , ma è irriducibile in $\mathbf{Z}[X]$. (Sugg. almeno uno fra $-1, 2, -2$ è quadrato in $\mathbf{Z}_p^*$.)
6. Dimostrare che il numero 16 è ottava potenza in $\mathbf{Z}_p^*$ per ogni primo p (ma non è ottava potenza in $\mathbf{Z} \dots$) (Sugg. almeno uno fra $-1, 2, -2$ è quadrato in $\mathbf{Z}_p^*$.)
7. (a) Siano $f(X), g(X)$ due polinomi in $\mathbf{Z}[X]$; Fattorizzare $f(X)^2 - g(X)^2$;
(b) Fattorizzare $X^4 - 4X^3 + 4X^2 - 25$ in fattori irriducibili di $\mathbf{Z}[X]$ (Sugg: usare (a));
(c) Fattorizzare $X^6 - X^2 + 20X - 100$ in fattori irriducibili di $\mathbf{Z}[X]$;
(d) Fattorizzare 999919 in fattori irriducibili di $\mathbf{Z}$.
8. Fattorizzare in fattori irriducibili in $\mathbf{Q}[X, Y]$:
(a) $Y^5 - X^2 - 2$;
(b) $X^{12} + Y^3 + Y$;
(c) $X^4 + 4Y^4$;
(d) $Y^3 - (X + 2)Y^2 + Y + X(X + 1)$.
9. (a) Determinare i polinomi irriducibili di grado 2 in $\mathbf{Z}_2[X]$ e $\mathbf{Z}_3[X]$;
(b) Fattorizzare $X^5 - X + 1$ in fattori irriducibili in $\mathbf{Z}_2[X]$ e $\mathbf{Z}_3[X]$;
(c) Fattorizzare $X^5 - X + 1$ in fattori irriducibili in $\mathbf{Z}[X]$.
10. Definiamo l' n -esimo *polinomio ciclotomico* $\Phi_n(X)$ induttivamente:

$$\prod_{d|n} \Phi_d(X) = X^n - 1.$$

- (a) Verificare che $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\dots$ e dimostrare che $\Phi_n(X)$ è irriducibile per $n \leq 4$.
- (b) Dimostrare che per ogni $n \geq 1$ il polinomio $\Phi_n(X)$ appartiene a $\mathbf{Z}[X]$.
- (c) Dimostrare che il grado di $\Phi_n(X)$ è uguale a $\varphi(n)$, dove φ indica la funzione di Eulero.
- (d) Sia p primo, $k \geq 1$ e sia $n = p^k$. Dimostrare che $\Phi_n(X) = \Phi_p(X^{n/p})$.
- (e) Sia p primo, $k \geq 1$ e sia $n = p^k$. Dimostrare che $\Phi_n(X)$ è irriducibile in $\mathbf{Z}[X]$.
- (f) Dimostrare che $\Phi_{12}(X)$ è irriducibile.
11. Dimostrare l'identità di Eulero per la funzione ζ di Riemann: per $s \in \mathbf{R}_{>1}$ abbiamo che

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - \frac{1}{p^s}}.$$

- (b) Sia p un primo. Dimostrare le seguenti uguaglianze fra serie di potenze in $\mathbf{Z}[[X]]$

$$\prod_{g \in \mathbf{Z}_p[X] \text{ monico, irr.}} \frac{1}{1 - X^{\deg(g)}} = \sum_{f \in \mathbf{Z}_p[X] \text{ monico}} X^{\deg(f)} = \frac{1}{1 - pX}.$$