Teoria de Galois

Lista 4

- 1) Mostre que $x^d - 1$ é um divisor de $x^n - 1$ se, e somente se, $d|n$. (Sugestão escreva $n = qd + r$ e $x^n - 1 = (x^n - x^r) + (x^r - 1)$).
- 2) Mostre que, se $m|n$ e a é um número inteiro positivo, então $a^m - 1$ é um divisor de $a^n - 1$. Conclua que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ se, e somente se $m|n$.
- 3) Prove que

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha).$$

Conclua com isto que

$$\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}.$$

então o produto dos elementos não nulos de um corpo finito é igual a 1 se $p = 2$ e -1 se p é ímpar. Para p ímpar e $n = 1$ deduza o teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}.$$

- 4) Mostre que $f(x)^p = f(x^p)$ para qualquer polinômio $f(x) \in \mathbb{F}_p[x]$.
- 5) Sejam m e n dois inteiros tais que $\text{mdc}(m, n) = 1$. Se ζ é uma raiz n -ésima primitiva da unidade e ξ é uma raiz m -ésima primitiva da unidade, mostre que $\zeta\xi$ é uma raiz mn -ésima primitiva da unidade.
- 6) Mostre que, se ζ é uma raiz n -ésima primitiva da unidade e $d|n$ então ζ^d é uma raiz $\frac{n}{d}$ -ésima primitiva da unidade.
- 7) Seja $n > 1$ um inteiro ímpar, mostre que $\Phi_{2n}(x) = \Phi_n(-x)$.

Os próximos exercícios darão um roteiro para a demonstração de um caso especial do teorema de Dirichlet sobre primos em progressões aritméticas que diz que existem infinitos números primos da forma $p \equiv a \pmod{m}$ com $\text{mdc}(a, m) = 1$.

- 8) Dado um polinômio $P(x) \in \mathbb{Z}[x]$ de grau maior ou igual a 1, existem infinitos divisores primos da coleção de números inteiros $P(1), P(2), P(3)$, etc. (Sugestão: Suponha que os únicos primos que são divisores daquela lista de números são $p_1, \dots, p_k$. Seja N um inteiro tal que $P(N) = a \neq 0$. Considere o polinômio $Q(x) = a^{-1}P(N + p_1 \dots p_k x) \in \mathbb{Q}[x]$ mostre que $Q(x) \in \mathbb{Z}[x]$ e que $Q(n) \equiv 1 \pmod{p_1 \dots p_k}$ Conclua que existe $M \in \mathbb{N}^*$ tal que $Q(M)$ tem um divisor diferente de qualquer um dos primos $p_1, \dots, p_k$)
- 9) Seja p um primo ímpar não divisor de m e seja $a \in \mathbb{Z}$ tal que $\Phi_m(a) \equiv 0 \pmod{p}$ (Φ_m é o m -ésimo polinômio ciclotômico). Mostre que $\text{mdc}(a, p) = 1$ e que a ordem de $\bar{a}$ em $\mathbb{Z}_p^\times$ é exatamente igual a m .
- 10) Seja $a \in \mathbb{Z}$. mostre que, se p é um primo ímpar divisor de $\Phi_m(a)$ então ou $p|m$ ou $p \equiv 1 \pmod{m}$.
- 11) Conclua que existem infinitos primos $p \equiv 1 \pmod{m}$.