

FINITE FIELDS PROBLEM SET

MATHCAMP 2003

1. This problem explains an important application of group theory to field theory.
 - (a) Suppose that G is a commutative group, and $x, y \in G$ are elements of order m and n respectively. Show that there is an element in G of order $\text{LCM}(m, n)$. (Hint: consider $x^a y^b$ for an intelligent choice of a and b .)
 - (b) If G is a finite group and N is the maximum of the orders of the elements of G , prove that x^N is the identity for all $x \in G$.
 - (c) Let K be a field, and suppose that $G \subset K^\times$ is a finite (multiplicative) subgroup. Use the previous problem, together with the fact that a polynomial of degree d has at most d distinct roots, to prove that G is a cyclic group.
 - (d) Conclude that if K is a finite field of size p^n , the group K^\times is cyclic of size $p^n - 1$, and in particular contains elements of order $p^n - 1$.
2. Let K be a field, and $K[x]$ the ring of polynomials in the variable x over K . If $f(x) = a_n x^n + \cdots + a_0$, we define the *derivative* of $f(x)$ to be

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

- (a) Show that $(f + g)' = f' + g'$ and $(fg)' = f'g + fg'$.
 - (b) Suppose that $g(x)^2$ divides $f(x)$. Prove that $g(x)$ divides $f'(x)$. Conclude that any repeated factor of $f(x)$ divides the GCD of $f(x)$ and $f'(x)$.
 - (c) Show that $x^{p^n} - x \in \mathbb{F}_p[x]$ has no repeated factor.
3. In this problem, we will count the number of irreducible polynomials of degree n over \mathbb{F}_p .

- (a) Here is one method. We've seen that $x^{p^n} - x$ is the product of all irreducible polynomials of degree dividing n , hence p^n is the sum of the degrees of the irreducible polynomials of degree dividing n . Use the inclusion-exclusion principle to show that the number of irreducible polynomials of degree dividing n is

$$\frac{1}{n} \left(p^n - \sum_i p^{n/l_i} - \sum_{i \neq j} p^{n/l_i l_j} + \cdots \right)$$

- where the l_i are the *distinct* primes dividing n .
- (b) Alternately, if N_d is the number of irreducible polynomials of degree d over \mathbb{F}_p , note that $p^n = \sum_{d|n} dN_d$, and use Möbius inversion to find the above formula for N_n .
 - (c) Check this result explicitly for $n = 1, 2, 3$.