Mathematics 3159B **Bradley Assaly-Nesrallah**
Introduction to Cryptography
Assignment 3, Problem 1 Due Date: October 20, 2020

Solution

1. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ where each $a_i \in \mathbb{Z}$. Let p be prime such that $p|a_i$ for all i and $p^2 \nmid a_0$

We want to show that $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial.

Proof. We proceed by contradiction, suppose that f(x) is reducible, that f(x)=g(x)h(x) for some $g(x), h(x) \in \mathbb{Z}[x]$ where 0<deg(g(x)),deg(h(x))<deg(f(x)) with $g(x) = b_dx^d + b_{d-1}x^{d-1} + ... + b_0$, and $h(x) = c_dx^e + c_{e-1}x^{e-1} + ... + c_0$ with d,e>1.
Thus by $p^2 \nmid a_0$ and $a_0 = b_0c_0$ we know that that either $p \nmid b_0$ or $p \nmid c_0$.
Suppose $p \nmid b_0$, we know the leading coefficient of x^n for f(x) is 1, thus $1 = b_dc_e \implies b_d = c_e = 1$ where clearly $p \nmid 1$, so $p \nmid b_d$ and $p \nmid c_e$.
Let c_k with $k \in \mathbb{Z}$ be the smallest term in h(x) such that $p \nmid c_k$, thus $a_k = b_0c_k + b_1c_{k-1} + b_2c_{m-2} + ...,$
Thus all terms are divisible by p except b_0c_k, as we know $b_0 = 1$ is not divisible by p nor is c_k by assumption.
Thus the whole term is not divisible by p, so $p \nmid a_k$, we know the only terms in f(x) not divisible by p is the leading coefficient and the constant term so k=0 or k=n, but the degree of c is greater that zero thus k=n, so h(x) is a polynomial of degree n, contradicting our assumption that deg(h(x))<deg(f(x)).
Hence, f(x) is irreducible so we are done.

□

2. Let p be a prime. We want to show that $f(x) = x^{p-1} + x^{p-2} + ... + x + 1 = \frac{x^p - 1}{x-1} \in \mathbb{Z}[x]$ is irreducible.

Proof. We consider the map $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $\phi : f(x) \to f(x+1)$ which is an evaluation homomorphism of f(x) at x+1, thus it is a ring homomorphism. We know the mapping is an isomorphism, as the inverse map ϕ^{-1} is clearly an evaluation function of f(x) at x-1.

Let g(x)=f(x+1) $= \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + ... + \binom{p}{p-1} = x^{p-1} + px^{p-2} + ... + p,$
Clearly $\binom{p}{k}$ is divisible by p for $1 \leq k < p$,
So $p^2 \nmid p = a_0$, $p \nmid 1 = a_n$ and $p|a_j$ for $1 \leq j < p-1$ thus we can use the result from question 1 to conclude that g(x) is irreducible $\in \mathbb{Z}[x]$.

Now suppose f(x) is reducible, that f(x)=h(x)i(x) with $h(x), i(x) \in \mathbb{Z}[x]$,
With 0<deg(h(x)),deg(i(x))<deg(f(x)), then g(x)=f(x+1)=h(x+1)k(x+1) but we know that g(x) is irreducible, contradicting our assumption that f(x) is reducible.
So f(x) is irreducible in $\mathbb{Z}[x]$ and we are done. $\square$

3. Let $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ with p a prime. We want disprove the claim that f is irreducible over any finite field by giving a counterexample.

Proof. Consider the polynomial f with p=7, $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ in $\mathbb{F}_2$.
We want to show that f(x) is reducible, that f(x)=g(x)h(x) for some $g(x), h(x) \in \mathbb{F}_2$ where 0<deg(g(x)),deg(h(x))<deg(f(x))
Observe that $(x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^3 + x^4 + x^3 + x + x^3 + x^2 + 1 = x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \pmod 2$ thus clearly f is reducible over $\mathbb{F}_2$, a finite field, disproving the claim so we are done.

$\square$