Problems Finite Fields, July 25, 2023

Problem 1. *Show that for every $n \geq 1$ the equation*

$$\phi(x) = n!$$

has a positive integer solution x.

Problem 2. *Show that for every prime p and integer n the equation*

$$n \equiv x^2 + y^2 \pmod{p}$$

has an integer solution x, y.

Problem 3. *Find the minimal polynomial $f(X)$ of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Z}$. Show that there is no prime p such that $f(X)$ is irreducible modulo p.*

Problem 4. *(a) Let $n \geq 2$ be an integer. Denote by R the radical (maximal square free factor) of n, namely the product of the prime factors of n. Check*

$$\phi_n(X) = \phi_R(X^{n/R}). \tag{1}$$

(b) Let p be a prime number and let m_1 a positive integer prime to p. Set $m = pm_1$. Prove

$$\Phi_{m_1}(X^p) = \Phi_m(X)\Phi_{m_1}(X).$$

(c) Let p be a prime number and m a positive integer multiple of p. Write $m = p^r m_1$ with $\gcd(p, m_1) = 1$ and $r \geq 1$. Deduce from (a) and (b)

$$\Phi_{m_1}(X^{p^r}) = \Phi_m(X)\Phi_{m_1}(X^{p^{r-1}}).$$

(d) For $r \geq 0$, p prime and m a multiple of p, check

$$\Phi_{p^r m}(X) = \Phi_m(X^{p^r}) \text{ and } \varphi(p^r m) = p^r \varphi(m).$$

Deduce

$$\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \Phi_p(X^{p^{r-1}})$$

when p is a prime and $r \geq 1$.
(e) Let n be a positive integer. Prove

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd,} \\ 2\varphi(n) & \text{if } n \text{ is even,} \end{cases}$$

$$\Phi_{2n}(X) = \begin{cases} -\Phi_1(-X) & \text{if } n = 1, \\ \Phi_n(-X) & \text{if } n \text{ is odd and } \geq 3, \\ \Phi_n(X^2) & \text{if } n \text{ is even.} \end{cases}$$

Deduce, for $\ell \geq 1$ and for m odd ≥ 3,

$$\begin{aligned} &\Phi_{2^\ell}(X) = X^{2^{\ell-1}} + 1 \\ &\Phi_{2^\ell m}(X) = \Phi_m(-X^{2^{\ell-1}}), \\ &\Phi_m(X)\Phi_m(-X) = \Phi_m(X^2). \end{aligned}$$

(f) Check, for $n \geq 1$,

$$\Phi_n(1) = \begin{cases} 0 & \text{for } n = 1, \\ p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise.} \end{cases}$$

(g) Check, for $n \geq 1$,

$$\Phi_n(-1) = \begin{cases} -2 & \text{for } n = 1, \\ 1 & \text{if } n \text{ is odd} \geq 3; \\ \Phi_{n/2}(1) & \text{if } n \text{ is even.} \end{cases}$$

In other terms, for $n \geq 3$,

$$\Phi_n(-1) = \begin{cases} p & \text{if } n = 2p^r \text{ with } p \text{ a prime and } r \geq 1; \\ 1 & \text{if } n \text{ is odd or if } n = 2m \text{ where } m \text{ has at least two distinct prime divisors.} \end{cases}$$