Problem 1. (5 points.) Let $p$ be an odd prime number and let $a, b \in \mathbb{Z}$ be integers not divisible by $p$. Show that if the congruence equation
\[ ax^p \equiv b \pmod{p^2} \]
is solvable, then for any positive integer $n$, the congruence equation
\[ ax^p \equiv b \pmod{p^n} \]
is solvable.

Solution. We let $x^2 \in \mathbb{Z}$ be a solution to the congruence equation $ax^p \equiv b \pmod{p^2}$; clearly, $p \nmid x^2$ since $p \nmid b$. We construct inductively $x^m \in \mathbb{Z}$ solving the congruence equation $ax^p \equiv b \pmod{p^m}$ for all $m > 2$. So, we suppose that already
\[ ax^p_m \equiv b \pmod{p^m} \]
and find $x_{m+1} := x_m + \ell p^{m-1}$ for some suitable $\ell \in \{0, 1, \ldots, p-1\}$ such that
\[ ax^p_{m+1} \equiv b \pmod{p^{m+1}}. \]
We compute
\[ ax^p_{m+1} - b = (ax^p_m - b) + ax^{p-1}_m p^m \cdot \ell + \sum_{i=2}^{p} ax^{p-1}_m \binom{p}{i} p^{(m-1)i} \ell^i. \]
For each $i = 2, \ldots, p-1$, we have that the above term in the summation: $ax^{p-1}_m \binom{p}{i} p^{(m-1)i} \ell^i$ is divisible by $p^{i + m - i}$ and that exponent of $p$ is at least $m + 1$ (knowing that $i \geq 2$ and also $m \geq 2$). On the other hand, the term of the above summation: $ap^{(m-1)i} \ell^i$ is also clearly divisible by $p^{m+1}$ simply because $m \geq 2$ and also $p \geq 3$. Therefore,
\[ ax^p_{m+1} - b \equiv p^m \cdot (k_m + ax^{p-1}_m \ell) \pmod{p^{m+1}}, \]
where $k_m \in \mathbb{Z}$ satisfies $ax^p_m - b = p^m \cdot k_m$. Now, because $p \nmid a$ and also $p \nmid x_m$ (note that $p \nmid x_2$ and then for each $m > 2$, we have that $x_m \equiv x_2 \pmod{p^i}$), we conclude that we can find $\ell \in \{0, \ldots, p-1\}$ such that $p \mid (k_m + ax^{p-1}_m \ell)$, thus proving the existence of $x_{m+1}$ with the desired property.

Problem 2. (5 points.) Find a polynomial $f \in \mathbb{Z}[x]$ with the property that there exists no integer $a$ such that $f(a) = 0$, but on the other hand, for each positive integer $m$, the congruence equation
\[ f(x) \equiv 0 \pmod{m} \]
is solvable.

Solution. We consider $f(x) := (x^2 + 17)(x^2 + 1)(x^2 - 17)$, which clearly has no integer roots; however, we will prove that for each positive integer $m$, the congruence
equation \( f(x) \equiv 0 \pmod{m} \) is solvable. For this it suffices (according to Chinese Remainder Theorem) to prove that the congruence equation \( f(x) \equiv 0 \pmod{p^a} \) is solvable for each prime power \( p^a \). We split our analysis into several cases.

**Case 1.** \( p \neq 2, 17 \)

In this case, we first note that not all three Legendre symbols \( \left( \frac{-17}{p} \right), \left( \frac{-1}{p} \right) \) and \( \left( \frac{17}{p} \right) \) may equal \(-1\) since
\[
\left( \frac{-17}{p} \right) = \left( \frac{-1}{p} \right) \cdot \left( \frac{17}{p} \right).
\]
So, there exists \( a \in \{-17, 17, -1\} \) such that \( \left( \frac{a}{p} \right) = 1 \). This means the congruence equation
\[
x^2 \equiv a \pmod{p}
\]
is solvable and moreover, letting \( x_0 \in \mathbb{Z} \) a solution of this congruence equation, then clearly \( 2x_0 \not\equiv 0 \pmod{p} \) since \( p \neq 2 \) and also, \( p \nmid x_0 \) (because \( p \nmid a \), again because \( p \neq 17 \)). Therefore, Hensel’s Lemma applies to this solution \( x_0 \) and to the polynomial \( g(x) := x^2 - a \), thus proving that for each \( \alpha \in \mathbb{N} \), the congruence equation \( g(x) \equiv 0 \pmod{p^a} \) is solvable; in particular, the congruence equation \( f(x) \equiv 0 \pmod{p^4} \) is solvable in this case.

**Case 2.** \( p = 17 \)

In this case, the congruence equation \( x^2 + 1 \equiv 0 \pmod{17} \) has the solution \( x_0 = 4 \), which clearly satisfies the Hensel’s Lemma and then for each \( \alpha \in \mathbb{N} \), there exists a solution to the congruence equation \( x^2 + 1 \equiv 0 \pmod{17^\alpha} \).

**Case 3.** \( p = 2 \)

In this last case, we note that for \( x_4 := 1 \), we have that \( x_4^2 - 17 \equiv 0 \pmod{2^4} \). We claim that if for some \( m \geq 4 \), we have that \( x_m \in \mathbb{Z} \) satisfies \( x_m^2 - 17 \equiv 0 \pmod{2^m} \), then we can find \( \ell \in \{0, 1\} \) such that \( x_{m+1} := x_m + 2^{m-1} \ell \) satisfies \( x_{m+1}^2 - 17 \equiv 0 \pmod{2^{m+1}} \). Indeed, we let \( k_m \in \mathbb{Z} \) such that \( x_m^2 - 17 = 2^m \cdot k_m \) and then compute
\[
x_{m+1}^2 - 17 = (x_m^2 - 17) + 2^m x_m \ell + 2^{2m-2} \ell^2
\]
and since \( 2m - 2 \geq m + 1 \) (because \( m \geq 4 \)), then
\[
x_{m+1}^2 - 17 \equiv 2^m \cdot (k_m + x_m \ell) \pmod{2^{m+1}},
\]
which means that (since \( x_m \) is odd because \( x_4 = 1 \) is odd and for all \( m \geq 4 \), we have that \( x_m \equiv x_4 \pmod{8} \)), we conclude that we can choose a suitable \( \ell \in \{0, 1\} \) such that \( k_m + x_m \ell \) is even and therefore \( x_{m+1}^2 - 17 \equiv 0 \pmod{2^{m+1}} \). In conclusion, each congruence equation \( f(x) \equiv 0 \pmod{2^a} \) (for \( \alpha \in \mathbb{N} \)) is solvable, as claimed.

**Problem 3.** (4 points.) Let \( p \) be a prime number with the property that there exists an integer \( m \) such that
\[
p \mid (m^4 - m^2 + 1).
\]
Prove that \( p \equiv 1 \pmod{12} \).

**Solution.** It suffices to prove that \( p \equiv 1 \pmod{3} \) and also, \( p \equiv 1 \pmod{4} \).

Now, the fact that \( p \mid (m^4 - m^2 + 1) \) means that \( p \) must be odd, since \( m^4 - m^2 + 1 = m^2(m^2 - 1) + 1 \) is odd. Furthermore, since \( m^4 - m^2 = m \cdot (m - 1)m(m + 1) \) contains a product of three consecutive integers, then \( m^4 - m^2 + 1 \) cannot be divisible by 3 and therefore, \( p > 3 \).
We have that $p$ divides $4m^4 - 4m^2 + 4 = (2m^2 - 1)^2 + 3$, which means that $-3$ is a quadratic residue modulo $p$. We compute
\[
\left(\frac{-3}{p}\right) = \left(\frac{1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p+1}{2}} = \left(\frac{p}{3}\right),
\]
where in the last computation we employed also the Gauss Quadratic Reciprocity Law. So, we need $1 = \left(\frac{p}{3}\right)$, which yields $p \equiv 1 \pmod{3}$.

On the other hand, $p \mid (m^2 + 1) \cdot (m^4 - m^2 + 1) = m^6 + 1$. However, $p$ does not divide $m^6 - 1$ (since $p$ cannot divide the difference, which is 2). So, we get that $p$ must divide $(m^6 - 1)(m^6 + 1) = m^{12} - 1$ but it does not divide $m^6 - 1$. So, the order of $m$ modulo $p$ divides 12 but it does not divide 6, which means that the order $\text{ord}_p(m)$ must be divisible by 4. Since this order always divides $p - 1$, we get that $p \equiv 1 \pmod{4}$.

Since $p \equiv 1 \pmod{3}$ and $p \equiv 1 \pmod{4}$, we conclude that $p \equiv 1 \pmod{12}$.

**Problem 4.** (5 points.) Let $p$ be a prime number and let $F \in \mathbb{Z}[x]$ be a polynomial of degree less than $p - 1$. Prove that $p$ divides the sum
\[
F(0) + F(1) + \cdots + F(p-1).
\]

**Solution.** We let $F(x) = \sum_{i=0}^{d} c_i x^i$, where $d = \deg(F) < p - 1$ (and the coefficients $c_i$ are all integers). Clearly, it suffices to prove that $p$ divides $\sum_{j=1}^{p-1} j^i$ for each $i = 1, \ldots, p - 2$.

We know that there exists a primitive root $g$ modulo the prime $p$ and so, the nonzero residue classes modulo $p$ are expressed as \{$g, g^2, \ldots, g^{p-1}$\} (modulo $p$). So, it suffices to prove that for each $i = 1, \ldots, p - 2$, we have that $p$ divides
\[
\sum_{j=1}^{p-1} (g^j)^i = g^i \cdot \frac{(g^{(p-1)} - 1)}{g^i - 1},
\]
which it does since the denominator is not divisible by $p$ (note that $1 \leq i < p - 1$ and $g$ has order $p - 1$ modulo $p$), while $p \mid (g^{p-1})^i - 1$. (Also, the above sum is clearly an integer.)

**Problem 5.** (5 points.) Let $p$ be a prime number, let $n \in \mathbb{N}$ and let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial of degree less than $n$. Prove that the number of solutions to the congruence equation
\[
f(x_1, \ldots, x_n) \equiv 0 \pmod{p}
\]
is divisible by $p$.

**Solution.** The fundamental observation is that for any integer $a$, we have that $p \mid 1 - a^{p-1}$ if $a \not\equiv 0 \pmod{p}$ and $1 - a^{p-1} \equiv 1 \pmod{p}$ if $p \mid a$. So, the number
\[
S := \sum_{0 \leq a_1, \ldots, a_n \leq p-1} (1 - f(a_1, \ldots, a_n)^{p-1})
\]
is a number congruent modulo $p$ with the number $N$ of solutions to the congruence equation $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$. We consider any monomial appearing in the expansion of $f(x_1, \ldots, x_n)^{p-1}$; such a monomial $M_j$ is of the form
\[
x_1^{d_1} \cdots x_n^{d_n},
\]
for some nonnegative integers $d_i$ with the property that
\[ \sum_{i=1}^{n} d_i \leq d \cdot (p - 1) < n \cdot (p - 1). \]

So, in the monomial $M_j$, there is at least one index $i \in \{1, \ldots, n\}$ such that the exponent $d_i$ of $x_i$ in $M$ is less than $p - 1$. But then
\[ S \equiv - \sum_j \sum_{0 \leq a_1, \ldots, a_n \leq p-1} c_j M_j(a_1, \ldots, a_n) \pmod{p} \]
for some integer coefficients $c_j$ (since we have $p^n$ terms in the above inner summation). On the other hand,
\[ \sum_{0 \leq a_1, \ldots, a_n \leq p-1} M_j(a_1, \ldots, a_n) = \prod_{i=1}^{n} \left( \sum_{\ell=0}^{p-1} \ell d_i \right). \]

By the result of Problem 4, for the particular index $i$ for which $d_i < p - 1$, we have that $p$ divides the sum $\sum_{\ell=0}^{p-1} \ell d_i$ and therefore, $p$ divides the sum $\sum_{0 \leq a_1, \ldots, a_n \leq p-1} M_j(a_1, \ldots, a_n)$. In conclusion, $p \mid S$ and therefore, also $p \mid N$. 