Putnam Exam #72 (2011), Problem B-6. Let $p$ be an odd prime. Show that for at least $(p + 1)/2$ values of $n$ in \{0, 1, 2, \ldots, p - 1\),
$$\sum_{k=0}^{p-1} k! \cdot n^k$$
is not divisible by $p$.

Solution (Noam D. Elkies) For $n = 0$ the $k = 0$ term in the sum is $0! \cdot 0$; we assume that $0^0$ is to be interpreted as 1, so that the problem asks to prove that the polynomial
$$F(x) = \sum_{k=0}^{p-1} k! X^k \in \mathbb{F}_p[X]$$
has at most $t$ distinct roots in $\mathbb{F}_p$, where $p = 2t + 1$.

Define a linear functional $I : \mathbb{F}_p[X] \to \mathbb{F}_p$ by
$$I(P) = P(0) - \sum_{x \in \mathbb{F}_p^*} F(x^{-1}) P(x).$$

Then
$$I(1) = P(0) - \sum_{x \in \mathbb{F}_p^*} F(x) = 1 - \sum_{k=0}^{p-1} \left( k! \sum_{x \in \mathbb{F}_p^*} x^k \right).$$

Each inner sum vanishes except for $k = 0$ and $k = p - 1$, for which $\sum_{x \in \mathbb{F}_p^*} x^k = \sum_{x \in \mathbb{F}_p^*} 1 = -1$. Since the coefficients 1 and $(p - 1)!$ sum to zero by Wilson’s theorem, we conclude that $I(1) = 1$. Also for $0 < m < p - 1$
$$I(X^m) = - \sum_{x \in \mathbb{F}_p^*} x^{-m} F(x) = - \sum_{k=0}^{p-1} \left( k! \sum_{x \in \mathbb{F}_p^*} x^{-m+k} \right),$$
and the inner sum vanishes except for $k = m$ when it equals $-1$, so
$$I(X^m) = m!$$
for all $m < p - 1$ (including $m = 0$).

It follows that if $P$ is the reduction mod $p$ of some $\tilde{P} \in \mathbb{Z}[X]$ of degree less than $p - 1$ then
$$I(P) \equiv \int_0^\infty \tilde{P}(x) e^{-x} \, dx \mod p$$
(note that the integral is indeed an integer and so can be reduced mod $p$).

Now suppose that $F$ has more than $t$ roots in $\mathbb{F}_p$, and thus takes at most $t$ nonzero values. These nonzero values include $F(0) = 1$. Then there is a monic polynomial $Q \in \mathbb{F}_p[X]$ of degree at most $t$ such that $Q(0) = 0$ and $F(x^{-1})Q(x) = 0$ for all $x \in \mathbb{F}_p^*$. This polynomial satisfies $I(X^mQ) = 0$ for each $m = 0, 1, 2, \ldots, t - 1$. That is, $Q$ is orthogonal to $\{R \in \mathbb{F}_p[X] : \deg R < t\}$ with respect to the inner product $\langle Q, R \rangle := I(QR)$. Therefore $F(X) = (-1)^t L_t(X)$, where $L_t$ is the
degree-\( t \) Laguerre polynomial, which is known to have leading coefficient \((-1)^{t}/t!\) and constant coefficient 1. This contradicts \( Q(0) = 0 \), QED.

Remark: The key facts about Laguerre polynomials that we need, besides their constant and leading coefficients, are that \( m! L_m(X) \in \mathbb{Z}[X] \) and \( \int_{0}^{\infty} (L_m(x))^2 e^{-x} \, dx = 1 \) for all \( m \); this lets us reduce mod \( p \) the orthogonal expansion \( Q = \sum_{m} I(L_m Q) \cdot L_m \). This ultimately comes down to the nonvanishing mod \( p \) of determinants such as \( \det((i + j)!_{i,j=0}^{m}) = \prod_{k=1}^{m} k!^2 \), but evaluating such determinants directly is not all that easy either.