OC604. Find all monic polynomials f with integer coefficients satisfying the following condition: there exists a positive integer N such that p divides $2(f(p))!+1$ for every prime $p > N$ for which $f(p)$ is a positive integer.

Originally from the 2016 Balkan Mathematical Olympiad, Problem 3.

We received 5 solutions, of which 4 were correct and complete. We present the solution by Missouri State University Problem Solving Group.

If $\deg(f) > 1$, then for all sufficiently large p, $f(p) > p$. Hence, $2(f(p))! + 1 \equiv 0 + 1 \not\equiv 0 \pmod p$ and f cannot have the required property. Also, f cannot be constant, for then p must divide the constant $2(f(p))! + 1$, and there are only finitely many such p. A linear polynomial $f(p) = p+k$ for $k \geq 0$ does not have the required property. This is because $f(p) \geq p$ and $2(f(p))!+1 \equiv 0+1 \not\equiv 0 \pmod p$.

Therefore, the remaining candidates are linear polynomials $f(p) = p - k$ with $k > 0$. Notice that $(p-1)(p-2) = p(p-3) + 2 \equiv 2 \pmod p$.

Let $k = 3$. We have

$$\begin{aligned} 2(p-3)! + 1 &\equiv (p-1)(p-2)(p-3)! + 1 \\ &\equiv (p-1)! + 1 \\ &\equiv -1 + 1 \text{ (by Wilson's theorem)} \\ &\equiv 0 \pmod p . \end{aligned}$$

Therefore, $f(p) = p - 3$ satisfies the condition of the problem.

Let $k = 1$. Then

$$\begin{aligned} 2(p-1)! + 1 &\equiv 2(-1) + 1 \text{(by Wilson's theorem)} \\ &\equiv -1 \pmod p . \end{aligned}$$

Therefore, $f(p) = p - 1$ does not satisfy the condition of the problem.

Let $k = 2$. We have

$$\begin{aligned} 2(p-2)! + 1 &\equiv (p-1)(p-2)(p-2)! + 1 \\ &\equiv (p-2)(p-1)! + 1 \\ &\equiv (-2)(-1) + 1 \text{ (by Wilson's theorem)} \\ &\equiv 3 \pmod p . \end{aligned}$$

Only $p = 3$ satisfies this condition. Therefore, $f(p) = p - 2$ does not satisfy the condition of the problem.

Assume there exists $k > 3$ that satisfies the condition of the problem. Then

Assume there exists $k > 3$ that satisfies the condition of the problem. Then

$$2(p-k)! + 1 \equiv 0 \pmod{p}.$$

Multiply the above by $(p-3)(p-4)\cdots(p-(k-1))$ to get

$$2(p-3)! + (p-3)(p-4)\cdots(p-(k-1)) \equiv 0 \pmod{p},$$

or

$$-1 + (-3)(-4)\cdots(-(k-1)) \equiv 0 \pmod{p}.$$

The last congruence implies that infinitely many primes, p, divide the constant on the left-hand side of the congruence, which is impossible.

We conclude that the only polynomial satisfying the condition of the problem is $f(p) = p - 3$.