We are interested in the Bell numbers (OEIS A000110) which can be defined by the recurrence

$$B(n+1) = \sum_{i=0}^{n} \binom{n}{i} B(i), \quad \forall n \in \mathbb{N}.$$

Theorem 6.2 of [1] shows that for any odd prime p, the sequence $\{B(n) \bmod p^s\}$ is purely periodic of period

$$p^{s-1} \times \left(\text{some divisor of } \frac{p^p - 1}{p-1}\right).$$

We introduce the following notation: for

$$f = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{Z}[X],$$

we will write $f \equiv 0 \pmod{m}$ for the statement

$$a_0 B(n) + a_1 B(n+1) + \cdots + a_d B(n+d) \equiv 0 \pmod{m}, \quad \forall n \in \mathbb{N}. \tag{1}$$

Of course, $f \equiv g \pmod{m}$ will mean that $f - g \equiv 0 \pmod{m}$. A first observation is that if $f \equiv g \pmod{m}$, then $fh \equiv gh \pmod{m}$ for any $h \in \mathbb{Z}[X]$. This is obvious since it is true when we take h to be the monomials. In fact, the Bell numbers have nothing to do here, and such a relation still holds true if we replace the Bell numbers by any integer sequences. What makes the Bell numbers peculiar is the following propositions. We begin with

Proposition 1 ([1], Lemma 4.11)**.** If $f \in \mathbb{Z}[X]$ satisfies $f(X) \equiv 0 \pmod{m}$, then $f(X+k) \equiv 0 \pmod{m}$ for any $k \in \mathbb{N}$.

Proof. By induction, we only need to show that the Proposition is true for $k = 1$. Let's first prove that

$$\sum_{i=0}^{\ell} \binom{\ell}{i} B(n+i) \stackrel{?}{=} \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} B(\ell + j + 1), \quad \forall n, \ell \in \mathbb{N}.$$

The RHS is

$$\sum_{j=0}^{n} (-1)^{j} \binom{n}{j} B(\ell + j + 1) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} \sum_{i=0}^{\ell+j} \binom{\ell+j}{i} B(i).$$

Now we only need to show that the generating functions are equal, namely

$$\sum_{i=0}^{\ell} \binom{\ell}{i} X^{n+i} \stackrel{?}{=} \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} \sum_{i=0}^{\ell+j} \binom{\ell+j}{i} X^i \in \mathbb{Z}[X],$$

and both sides are obviously equal to $X^n (X+1)^\ell$.

Let $f(X) = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{Z}[X]$, then

$$f(X+1) = \sum_{i=0}^{d} \left(\sum_{\ell=0}^{d} a_\ell \binom{\ell}{i} \right) X^i,$$

and so we need to prove

$$\sum_{i=0}^{d} \left(\sum_{\ell=0}^{d} a_\ell \binom{\ell}{i} \right) B(n+i) \stackrel{?}{\equiv} 0 \pmod{m}, \quad \forall n \in \mathbb{N}.$$

But the LHS is

$$\begin{aligned}
\sum_{\ell=0}^{d} a_\ell \sum_{i=0}^{\ell} \binom{\ell}{i} B(n+i) &= \sum_{\ell=0}^{d} a_\ell \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} B(\ell + j + 1) \\
&= \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} \underbrace{\sum_{\ell=0}^{d} a_\ell B(\ell + j + 1)}_{\equiv 0 \pmod{m}} \equiv 0 \pmod{m}.
\end{aligned}$$

□

The next proposition allows us to pass from a congruence modulo p^{s-1} to modulo p^s.

Proposition 2 ([1], Lemma 5.3)**.** Let p be a prime. If $f \equiv 0 \pmod{p^{s-1}}$, then

$$(X^p - X)f(X) \equiv f(X+p) \pmod{p^s}.$$

Proof. We expand

$$X(X-1)\cdots(X-(k-1)) = \sum_{j=0}^{k} \lambda_{k,j} X^j, \quad \forall k \in \mathbb{N}.$$

We will use without proof the identity

$$\sum_{j=0}^{k} \lambda_{k,j} B(n+j) = \sum_{i=0}^{n} k^{n-i} \binom{n}{i} B(i), \quad \forall k, n \in \mathbb{N}.$$

Note that $X(X-1)\cdots(X-(p-1)) \in X^p - X + p\mathbb{Z}[X]$. Since $f \equiv 0 \pmod{p^{s-1}}$, what we need to prove becomes

$$X(X-1)\cdots(X-(p-1))f(X) \overset{?}{\equiv} f(X+p) \pmod{p^s}.$$

Write $f(X) = a_0 + a_1 X + \cdots + a_d X^d$, then

$$\begin{aligned} X(X-1)\cdots(X-(p-1))f(X) &= (\lambda_{p,0} + \lambda_{p,1}X + \cdots + \lambda_{p,p}X^p)(a_0 + a_1 X + \cdots + a_d X^d) \\ &= \sum_{j=0}^{p+d} \left(\sum_{j_1+j_2=j} \lambda_{p,j_1} a_{j_2} \right) X^j; \\ f(X+p) &= \sum_{i=0}^{d} \left(\sum_{\ell=0}^{d} p^{\ell-i} a_\ell \binom{\ell}{i} \right) X^i, \end{aligned}$$

and so our goal is to prove

$$\sum_{j=0}^{p+d} \left(\sum_{j_1+j_2=j} \lambda_{p,j_1} a_{j_2} \right) B(n+j) \overset{?}{\equiv} \sum_{i=0}^{d} \left(\sum_{\ell=0}^{d} p^{\ell-i} a_\ell \binom{\ell}{i} \right) B(n+i) \pmod{p^s}, \quad \forall n \in \mathbb{N}. \tag{2}$$

We pose

$$R_n := \sum_{i=0}^{d} \left(\sum_{\ell=0}^{d} p^{\ell-i} a_\ell \binom{\ell}{i} \right) B(n+i)$$

to be the RHS of (2). We have $f(X+p) \equiv 0 \pmod{p^{s-1}}$ by Proposition 1, which is to say

$$R_n \equiv 0 \pmod{p^{s-1}}, \quad \forall n \in \mathbb{N}.$$

The LHS of (2) is, of course, equal to

$$\sum_{j_2=0}^{d} a_{j_2} \sum_{j_1=0}^{p} \lambda_{p,j_1} B(n+j_1+j_2) = \sum_{j_2=0}^{d} a_{j_2} \sum_{i=0}^{n+j_2} p^{n+j_2-i} \binom{n+j_2}{i} B(i).$$

Note that

$$\sum_{i=0}^{n+j_2} p^{n+j_2-i} \binom{n+j_2}{i} B(i) = \sum_{j=0}^{n} p^{n-j} \binom{n}{j} \left(\sum_{i=0}^{j_2} p^{j_2-i} \binom{j_2}{i} B(j+i) \right);$$

this is because

$$\sum_{i=0}^{n+j_2} p^{n+j_2-i} \binom{n+j_2}{i} X^i = \sum_{j=0}^{n} p^{n-j} \binom{n}{j} \left(\sum_{i=0}^{j_2} p^{j_2-i} \binom{j_2}{i} X^{j+i} \right)$$

(the generating functions of both sides are equal to $(X+p)^{n+j_2}$), hence the LHS of (2) is equal to

$$\sum_{j_2=0}^{d} a_{j_2} \sum_{j=0}^{n} p^{n-j}\binom{n}{j}\left(\sum_{i=0}^{j_2} p^{j_2-i}\binom{j_2}{i}B(j+i)\right) = \sum_{j=0}^{n} p^{n-j}\binom{n}{j}\left(\sum_{j_2=0}^{d} a_{j_2}\sum_{i=0}^{j_2} p^{j_2-i}\binom{j_2}{i}B(j+i)\right)$$
$$= \sum_{j=0}^{n} p^{n-j}\binom{n}{j}R_j \equiv R_n \pmod{p^s}.$$

□

In particular, if we take $s=1$ and $f=1$, then

$$X^p - X - 1 \equiv 0 \pmod{p}.$$

Corollary 1 ([1], Theorem 5.9)**.** Let p be a prime. Then

$$(X^p - X - 1)^{2s-1} \equiv 1 \pmod{p^s}.$$

Proof. Induction on s. The $s=1$ case has already been proved. Write

$$C(X) = X^p - X - 1, \quad Q(X) = (C(X+p) - C(X))/p \in \mathbb{Z}[X].$$

Suppose that $C^{2i-1} \equiv 1 \pmod{p^i}$ for all $i = 1, \cdots, s-1$, then $C^{2s-2} \equiv 1 \pmod{p^{s-1}}$. By Proposition 2, we have

$$C^{2s-1} = (X^p - X)C^{2s-2} - C^{2s-2} \equiv C(X+p)^{2s-2} - C(X)^{2s-2} = (C+pQ)^{2s-2} - C^{2s-2} \pmod{p^s}.$$

By induction hypothesis, we have

$$p^{2s-2-i}C^i \equiv 0 \pmod{p^{2s-2-i+\lceil i/2\rceil}}, \quad i = 0, 1, \cdots, 2s-3,$$

and so it suffice to show that $2s-2-i+\lceil i/2\rceil = 2s-2-\lfloor i/2\rfloor \geq s$ for $i = 0, 1, \cdots, 2s-3$, which is obvious. □

The following result is a key relation satisfied by the Bell numbers.

Proposition 3 ([1], Theorem 5.10)**.** Let p be an *odd* prime, then

$$(X+1)^{p^{s-1}} \equiv X^{p^s} \pmod{p^s}, \quad (X+1)^{p^{s-1}} \not\equiv X^{p^s} \pmod{p^{s+1}}.$$

The latter expresses that the corresponding congruence (1) is not true for some n.

Theorem ([1], Theorem 6.2)**.** Let p be an *odd* prime, then

$$X^{p^{s-1}(p^p-1)/(p-1)} \equiv 1 \pmod{p^s}, \quad X^{p^{s-2}(p^p-1)/(p-1)} \not\equiv 1 \pmod{p^s}\ (s \geq 2).$$

Proof. We first prove that

$$(X^p - X)^{p^{s-1}} \equiv 1 \pmod{p^s}.$$

Write $C = X^p - X - 1$, then the LHS is $(C+1)^{p^{s-1}} = \sum_{i=0}^{p^{s-1}} \binom{p^{s-1}}{i} C^i$. By Corollary 1, we have

$$\binom{p^{s-1}}{i} C^i \equiv 0 \pmod{p^{v_p\left(\binom{p^{s-1}}{i}\right)+\lceil i/2\rceil}},$$

and so it suffice to show that

$$v_p\left(\binom{p^{s-1}}{i}\right) + \lceil i/2\rceil \geq s, \quad \forall i = 1, \cdots, p^{s-1}.$$

Kummer's theorem tells us that $v_p\left(\binom{p^{s-1}}{i}\right) = s-1-v_p(i)$ for $i = 1, \cdots, p^{s-1}$, then we need to show $v_p(i) \le \lceil i/2 \rceil - 1$, which is quite obvious by $p \ge 3$ and $i \ge p^{v_p(i)}$.

We note that, for $i \in \mathbb{N}$,

$$\begin{aligned}(X+i)^{p^{s-1}} &\equiv (X+(i-1))^{p^s} \text{ (by Proposition 1)}\\ &\equiv (X+(i-2))^{p^{s+1}} \text{ (again by Proposition 1; note that } f-g \text{ divides } f^p-g^p)\\ &\equiv \cdots \equiv X^{p^{s-1+i}} \pmod{p^s}.\end{aligned}$$

Multiplying these congruences for $i = 0, \cdots, k-1$ yields

$$X^{p^{s-1}(p^k-1)/(p-1)} = X^{p^{s-1}+p^s+\cdots+p^{s-1+(k-1)}} \equiv X^{p^{s-1}}(X+1)^{p^{s-1}}\cdots(X+(k-1))^{p^{s-1}} \pmod{p^s}. \tag{3}$$

Take $k = p$ in (3). Note that $X(X+1)\cdots(X+(p-1)) \in X^p - X + p\mathbb{Z}[X]$, hence

$$X^{p^{s-1}}(X+1)^{p^{s-1}}\cdots(X+(p-1))^{p^{s-1}} \in (X^p-X)^{p^{s-1}} + p^s\mathbb{Z}[X].$$ [1]

We conclude that

$$X^{p^{s-1}(p^p-1)/(p-1)} \equiv (X^p-X)^{p^{s-1}} \equiv 1 \pmod{p^s}.$$

For $s \ge 2$, suppose on the contrary that

$$X^{p^{s-2}+p^{s-1}(p^{p-1}-1)/(p-1)} = X^{p^{s-2}(p^p-1)/(p-1)} \equiv 1 \pmod{p^s}.$$

Taking $k = p-1$ in (3) yields

$$1 \equiv X^{p^{s-2}} \equiv X^{p^{s-1}}(X+1)^{p^{s-1}}\cdots(X+(p-2))^{p^{s-1}} \pmod{p^s}.$$

Multiply both sides by $(X-1)^{p^{s-1}}$. We have $(X-1)X(X+1)\cdots(X+(p-2)) \in X^p - X + p\mathbb{Z}[X]$, hence

$$(X-1)^{p^{s-1}} \equiv X^{p^{s-2}} \pmod{p^s}.$$

By Proposition 1, we then have

$$X^{p^{s-2}} \equiv (X+1)^{p^{s-1}} \pmod{p^s},$$

contradicting the second half of Proposition 3! $\square$

In conclusion: the sequence $\{B(n) \bmod p^s\}$ (viewed as a sequence of integers) satisfies a linear recurrence whose characteristic polynomial divides $X^{p^{s-1}(p^p-1)/(p-1)}-1$, but does not divide $X^{p^{s-2}(p^p-1)/(p-1)}-1$.

References

[1] W. F. Lunnon et al., "Arithmetic properties of Bell numbers to a composite modulus I", Acta Arithmetica 35 (1979), pp. 1-16.

[1] By induction on r, if $f-g \in p^r\mathbb{Z}[X]$, then $f^p - g^p \in p^{r+1}\mathbb{Z}[X]$.