AN ELEMENTARY (NUMBER THEORY) PROOF OF TOUCHARD’S CONGRUENCE

GREG HURST AND ANDREW SCHULTZ

Abstract. Let $B_n$ denote the $n$th Bell number. We use well-known recursive expressions for $B_n$ to give a generalizing recursion that can be used to prove Touchard’s congruence.

1. Introduction

For a positive integer $n$, the Bell number $B_n$ is the number of ways a set of $n$ elements can be partitioned into nonempty subsets. Computations of Bell numbers rely on well-known recursive formulae. For example, one can compute $B_{n+1}$ by enumerating partitions according to the size of the subset $S$ which contains the $n+1$st element; if $|S| = n + 1 - d$ then there are \( \binom{n}{n-d} \) choices for the other elements of $S$ and $B_d$ ways to partition the elements not in $S$. Hence we have

\[
B_{n+1} = \sum_{d=0}^{n} B_d \binom{n}{n-d}.
\]

Alternatively, one can compute $B_n$ by keeping track of the number of subsets in a given partition; the Stirling number of the second kind $\{n\}_k$ counts the number of partitions of $n$ elements into precisely $k$ subsets, and so one has the well-known formula

\[
B_n = \sum_{k=1}^{n} \{n\}_k.
\]

Calculations for $\{n\}_k$ rely on the binomial-like recurrence relation

\[
\{n+1\}_k = \{n\}_{k-1} + k \{n\}_k.
\]

Using the identities above, we derive an expression for $B_{n+j}$ which generalizes both (1.1) and (1.2):
Theorem 1.4. For positive integers \( n \) and \( j \),

\[
B_{n+j} = \sum_{k=1}^{n} P_j(k) \binom{n}{k},
\]

where \( P_j(x) \) is the degree \( j \) polynomial \( \sum_{r=0}^{j} B_{j-r} \binom{j}{r} x^r \).

It appears that this formulation wasn’t discovered until recently when a combinatorial proof of this result was given in [1]. We arrived at this result independently through algebraic manipulations of (1.1-1.3); since this result comes directly from these well-known identities, it is surprising that Theorem 1.4 wasn’t recognized much sooner.

This project began when the first author was a student in the second author’s elementary number theory class. Before knowing the general form of the polynomials \( P_j(k) \) from Theorem 1.4, the authors could find specific identities such as

\[
B_{n+5} = \sum_{k=1}^{n} (k^5 + 5k^4 + 20k^3 + 50k^2 + 75k + 52) \binom{n}{k}.
\]

These computations were being carried out just as modular arithmetic was being introduced in the concurrent course, and it was clear that when \( j \) was prime the polynomials \( P_j(k) \) were ripe for simplification modulo \( j \). Flushing this observation out not only provided a great tour of some of the most familiar identities and techniques for computations modulo \( p \), but ultimately led to a rediscovery of

Corollary 1.5 (Touchard’s Congruence). For positive integers \( n \) and \( m \) and \( p \) a prime number,

\[
B_{n+p^m} \equiv mB_n + B_{n+1} \mod p.
\]

2. A Proof of Theorem 1.4

We prove the result by induction, with \( j = 0 \) our (trivial) base case. By induction we have

\[
B_{n+j+1} = \sum_{k=1}^{n+1} P_j(k) \binom{n+1}{k} = \sum_{k=1}^{n+1} \sum_{r=0}^{j} B_{j-r} \binom{j}{r} k^r \binom{n+1}{k}.
\]
Applying identity (1.3) to \( \binom{n+1}{k} \), and using \( \binom{n}{0} = \binom{n}{n+1} = 0 \), we have

\[
\sum_{k=1}^{n+1} \sum_{r=0}^{j} B_{j-r} \binom{j}{r} k^r \left( \binom{n}{k-1} + k \binom{n}{k} \right) = \sum_{k=2}^{n+1} \sum_{r=0}^{j} B_{j-r} \binom{j}{r} k^r \binom{n}{k-1} + \sum_{k=1}^{n} \sum_{r=0}^{j} B_{j-r} \binom{j}{r} k^{r+1} \binom{n}{k}.
\]

The coefficient of \( k^{\ell} \binom{n}{k} \) in this sum is then

\[
\sum_{r=\ell}^{j} B_{j-r} \binom{j}{r} \binom{\ell}{r} \ell + B_{j-(\ell-1)} \binom{j}{\ell-1} = \sum_{r=\ell}^{j} B_{j-r} \binom{j}{r} \binom{\ell}{r-\ell} + B_{j-\ell+1} \binom{j}{\ell-1}.
\]

We now make the change of variable \( d = j - r \) in the first sum and apply identity (1.1), leaving us with:

\[
\left( \sum_{d=0}^{j-\ell} B_d \binom{j-\ell}{j-\ell-d} \right) \binom{j}{\ell} + B_{j-\ell+1} \binom{j}{\ell-1} = B_{j-\ell+1} \binom{j}{\ell} + B_{j-\ell+1} \binom{j}{\ell-1} = B_{j-\ell+1} \binom{j+1}{\ell}.
\]

Thus we have \( B_{n+j+1} = \sum_{k=1}^{n} \sum_{r=0}^{j+1} B_{j+1-r} \binom{j+1}{r} k^r \binom{n}{k} = \sum_{k=1}^{n} P_{j+1}(k) \binom{n}{k} \).

### 3. Computations modulo \( p \)

If \( p \) is an odd prime, it is well known that \( \binom{p^m}{r} \equiv 0 \mod p \) whenever \( 0 < r < p^m \), and so all but two of the terms of \( P_{p^m}(x) \) are congruent to zero modulo \( p \). Applying Theorem (1.4) and Fermat’s Little Theorem, we therefore have

\[
B_{n+p^m} \equiv \sum_{k=1}^{n} (B_{p^m} + k^{p^m} B_0) \binom{n}{k} \equiv \sum_{k=1}^{n} (B_{p^m} + k) \binom{n}{k} \mod p.
\]
Since \( P_1(k) = 1 + k \), Theorem 1.4 gives \( B_{n+1} = \sum (1 + k) \binom{n}{k} \), and so rearranging the previous congruence gives

\[
B_{n+p^m} \equiv (B_{p^m} - 1) \sum_{k=1}^{n} \binom{n}{k} + \sum_{k=1}^{n} (1 + k) \binom{n}{k} \equiv (B_{p^m} - 1)B_n + B_{n+1} \mod p.
\]

The same congruence holds for \( p = 2 \) as well: if \( m > 2 \) then \( \binom{2m}{r} \equiv 0 \mod 2 \) for \( 0 < r < 2^m \) and our previous argument holds, and if \( m = 2 \) the only additional term is \( 3k^2B_2 = 6 \equiv 0 \mod 2 \).

To verify Corollary 1.5 then, we only need to prove the following

**Lemma 3.1.** For every positive integer \( m \) and prime number \( p \), \( B_{p^m} \equiv m + 1 \mod p \).

**Proof.** \( B_{p^m} \) enumerates the partitions of \( \mathbb{Z}/p^m\mathbb{Z} \). Our strategy will be to let \( \mathbb{Z}/p^m\mathbb{Z} \) act on these partitions in the natural way: for elements \( x \) and \( y \) of \( \mathbb{Z}/p^m\mathbb{Z} \) we define \( f_y(x) = x + y \mod p^m \), and \( f_y(P) \) is the partition we get by applying \( f_y \) element-wise to \( P \). Any partition not fixed under this action will belong to an orbit of size a power of \( p \), and so the number of fixed partitions is equivalent to \( B_{p^m} \) modulo \( p \).

So suppose you have some fixed partition \( P \) with elements \( a \) and \( b \) inside subsets \( \mathcal{A} \) and \( \mathcal{B} \) (respectively). Then clearly \( f_{b-a}(a) = b \), and since \( P \) is fixed this means \( f_{b-a}(\mathcal{A}) = \mathcal{B} \). Hence for a fixed partition \( P \), all subsets of \( P \) must be the same size, and therefore some power of \( p \). We claim that the only fixed partition whose subsets are size \( p^j \) is the partition whose subsets contain elements which are congruent to each other modulo \( p^{m-j} \). This would leave us with \( m + 1 \) many fixed partitions, as desired.

To prove the claim, suppose to the contrary that we have a fixed partition \( P \) with elements \( a, b \) in the same \( p^j \)-element subset \( \mathcal{A} \) which satisfy \( a \not\equiv b \mod p^{m-j} \). Now \( f_{b-a}(a) = b \), and so \( \mathcal{A} \) is permuted by the action of \( f_{b-a} \). Hence for any integer \( r \), the \( r \)-fold composition of the map \( f_{b-a} \) — namely, the map \( f^{(r)}_{b-a} \) — again takes \( a \) to some element of \( \mathcal{A} \). Now clearly \( f^{(r)}_{b-a}(a) \equiv f^{(s)}_{b-a}(a) \mod p^m \) if and only if

\[
a + r(b - a) \equiv a + s(b - a) \mod p^m.
\]

Since \( a \not\equiv b \mod p^{m-j} \), however, this congruence forces \( r - s \equiv 0 \mod p^j+1 \). Hence for \( r \) between 1 and \( p^j+1 \), the elements \( f^{(r)}_{b-a}(a) \) are distinct constituents of \( \mathcal{A} \). It follows that \( |\mathcal{A}| > p^j \), a contradiction. \( \square \)
4. Acknowledgement

Both authors would like to thank Bruce Reznick for his advice, guidance, and constant cheer.

References

[1] M. Spivey. A Generalized Recurrence for Bell Numbers. *J. Int. Seq.* **11** (2008), no. 2, Article 08.2.5.

808 Coventry Point, Springfield IL, 62702 USA

*E-mail address*: ChipH588@aol.com

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street, Urbana, IL 61801 USA

*E-mail address*: acs@math.uiuc.edu