0.1 Binomial Sum Divisible by Primes

1 *(MM, Problem 1392, George Andrews)* Prove that for any prime p in the interval $\left]n, \frac{4n}{3}\right]$, p divides

PEN E16

$$\sum_{j=0}^{n} \binom{n}{j}^4.$$

Solution by Darij Grinberg.

The problem can be vastly generalized:

Theorem 1. Let ℓ be a positive integer. If n_1, n_2, ..., n_ℓ are positive integers and p is a prime such that $(\ell - 1)(p - 1) < \sum\limits_{i=1}^{\ell} n_i$ and $n_i < p$ for every $i \in \{1, 2, ..., \ell\}$, then $p \mid \sum\limits_{j=0}^{p-1} (-1)^{\ell j} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$.

Before we prove this, we first show some basic facts about binomial coefficients and remainders modulo primes. We recall how we define binomial coefficients:

Definition. The binomial coefficient $\binom{x}{u}$ is defined for all reals x and for all integers u as follows: $\binom{x}{u} = \dfrac{x \cdot (x-1) \cdot ... \cdot (x-u+1)}{u!}$ if $u \geq 0$, and $\binom{x}{u} = 0$ if $u < 0$.

Note that the empty product evaluates to 1, and $0! = 1$, so this yields $\binom{x}{0} = \dfrac{x \cdot (x-1) \cdot ... \cdot (x-0+1)}{0!} = \dfrac{\text{empty product}}{0!} = \dfrac{1}{1} = 1$ for every $x \in \mathbb{Z}$.

Theorem 2, the upper negation identity. If n is a real, and r is an integer, then $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$.

Proof of Theorem 2. We distinguish two cases: the case $r < 0$ and the case $r \geq 0$.
If $r < 0$, then $\binom{-n}{r} = 0$ and $\binom{n+r-1}{r} = 0$, so that $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$ ensues.
If $r \geq 0$, then, using the definition of binomial coefficients, we have

$$\binom{-n}{r} = \frac{(-n) \cdot (-n-1) \cdot ... \cdot (-n-r+1)}{r!} = (-1)^r \cdot \frac{n \cdot (n+1) \cdot ... \cdot (n+r-1)}{r!}$$
$$= (-1)^r \cdot \frac{(n+r-1) \cdot ... \cdot (n+1) \cdot n}{r!} = (-1)^r \cdot \binom{n+r-1}{r}.$$

Hence, in both cases $r < 0$ and $r \geq 0$, we have established $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$. Thus, $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$ always holds. This proves Theorem 2.

Theorem 3. If p is a prime, if u and v are two integers such that $u \equiv v \mod p$, and if k is an integer such that $k < p$, then $\binom{u}{k} \equiv \binom{v}{k} \mod p$.

Proof of Theorem 3. If $k < 0$, then $\binom{u}{k} = \binom{v}{k}$ (because $\binom{u}{k} = 0$ and $\binom{v}{k} = 0$), so that Theorem 3 is trivial. Thus, it remains to consider the case $k \geq 0$ only. In this case, $k!$ is coprime with p (since $k! = 1 \cdot 2 \cdot ... \cdot k$, and all numbers 1, 2, ..., k are coprime with p, since p is a prime and $k < p$).

Now, $u \equiv v \mod p$ yields

$$\begin{aligned} k! \cdot \binom{u}{k} &= k! \cdot \frac{u \cdot (u-1) \cdot ... \cdot (u-k+1)}{k!} = u \cdot (u-1) \cdot ... \cdot (u-k+1) \\ &\equiv v \cdot (v-1) \cdot ... \cdot (v-k+1) = k! \cdot \frac{v \cdot (v-1) \cdot ... \cdot (v-k+1)}{k!} = k! \cdot \binom{v}{k} \mod p. \end{aligned}$$

Since $k!$ is coprime with p, we can divide this congruence by $k!$, and thus we get $\binom{u}{k} \equiv \binom{v}{k} \mod p$. Hence, Theorem 3 is proven.

Finally, a basic property of binomial coefficients:

Theorem 4. For every nonnegative integer n and any integer k, we have $\binom{n}{k} = \binom{n}{n-k}$.

This is known, but it is important not to forget the condition that n is nonnegative (Theorem 4 would not hold without it!).

Now we will reprove an important fact:

Theorem 5. If p is a prime, and $f \in \mathbb{Q}[X]$ is a polynomial of degree $< p-1$ such that $f(j) \in \mathbb{Z}$ for all $j \in \{0, 1, ..., p-1\}$, then $\sum_{j=0}^{p-1} f(j) \equiv 0 \mod p$.

Before we prove Theorem 5, we recall two lemmata:

Theorem 6. If p is a prime and i is an integer satisfying $0 \leq i \leq p-1$, then $\binom{p-1}{i} \equiv (-1)^i \mod p$.

Theorem 7. If N is a positive integer, and f is a polynomial of degree $< N$, then $\sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = 0$.

Theorem 6 appeared as Lemma 1 in [2], post #2. Theorem 7 is a standard result from finite differences theory.

Proof of Theorem 5. Let $N = p-1$. Then, f is a polynomial of degree $< N$ (since f is a polynomial of degree $< p-1$). Thus, Theorem 7 yields $\sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = 0$. Hence,

$$0 = \sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = \sum_{j=0}^{p-1} (-1)^j \underbrace{\binom{p-1}{j}}_{\substack{\equiv (-1)^j \mod p \\ \text{by Theorem 6}}} f(j) \equiv \sum_{j=0}^{p-1} \underbrace{(-1)^j (-1)^j}_{\substack{= ((-1)^j)^2 = ((-1)^2)^j \\ = 1^j = 1}} f(j) = \sum_{j=0}^{p-1} f(j) \mod p.$$

This proves Theorem 5.

Proof of Theorem 1. The condition $(\ell-1)(p-1) < \sum_{i=1}^{\ell} n_i$ rewrites as $\ell(p-1)-(p-1) < \sum_{i=1}^{\ell} n_i$. Equivalently, $\ell(p-1) - \sum_{i=1}^{\ell} n_i < p-1$.

For every $i \in \{1,2,...,\ell\}$, we have $p - n_i - 1 \geq 0$, since $n_i < p$ yields $n_i + 1 \leq p$.

For every $i \in \{1,2,...,\ell\}$ and every integer j with $0 \leq j < p$, we have

$$\begin{aligned}
\binom{n_i}{j} &= \binom{-(-n_i)}{j} = (-1)^j \binom{(-n_i)+j-1}{j} \qquad \text{(after Theorem 2)} \\
&\equiv (-1)^j \binom{p-n_i+j-1}{j} \qquad \text{(by Theorem 3, since } (-n_i)+j-1 \equiv p-n_i+j-1 \mod p \text{ and } j<p) \\
&= (-1)^j \binom{p-n_i+j-1}{(p-n_i+j-1)-j} \\
&\qquad \text{(by Theorem 4, since } p-n_i+j-1 \text{ is nonnegative, since } p-n_i-1 \geq 0 \text{ and } j \geq 0) \\
&= (-1)^j \binom{p-n_i+j-1}{p-n_i-1} = (-1)^j \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{(p-n_i-1)!} \mod p.
\end{aligned}$$

Hence, for every integer j with $0 \leq j < p$, we have

$$\begin{aligned}
\prod_{i=1}^{\ell} \binom{n_i}{j} &\equiv \prod_{i=1}^{\ell} (-1)^j \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{(p-n_i-1)!} = \left((-1)^j\right)^{\ell} \prod_{i=1}^{\ell} \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{(p-n_i-1)!} \\
&= \left((-1)^j\right)^{\ell} \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{\prod_{i=1}^{\ell} (p-n_i-1)!} \mod p,
\end{aligned}$$

so that

$$\begin{aligned}
&\prod_{i=1}^{\ell} (p-n_i-1)! \cdot (-1)^{\ell j} \prod_{i=1}^{\ell} \binom{n_i}{j} \\
&\equiv \prod_{i=1}^{\ell} (p-n_i-1)! \cdot \underbrace{(-1)^{\ell j} \cdot \left((-1)^j\right)^{\ell}}_{\substack{=(-1)^{\ell j} \cdot (-1)^{\ell j} \\ =(-1)^{2\ell j}=1, \text{ since} \\ 2\ell j \text{ is even}}} \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{\prod_{i=1}^{\ell} (p-n_i-1)!} \\
&= \prod_{i=1}^{\ell} (p-n_i-1)! \cdot \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u)}{\prod_{i=1}^{\ell} (p-n_i-1)!} \\
&= \prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+j-1)-u) \mod p. \qquad (1)
\end{aligned}$$

Now, define a polynomial f in one variable X by

$$f(X) = \prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p-n_i+X-1)-u). \qquad (2)$$

Then,

$$\deg f = \deg\left(\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+X-1)-u)\right) = \sum_{i=1}^{\ell}\sum_{u=0}^{(p-n_i-1)-1}\underbrace{\deg((p-n_i+X-1)-u)}_{=1}$$

(since the degree of a product of some polynomials is the sum of the degrees of these polynomials)

$$= \sum_{i=1}^{\ell}\underbrace{\sum_{u=0}^{(p-n_i-1)-1} 1}_{\substack{=(p-n_i-1)\cdot 1\\ =p-n_i-1\\ =p-1-n_i}} = \sum_{i=1}^{\ell}(p-1-n_i) = \underbrace{\sum_{i=1}^{\ell}(p-1)}_{=\ell(p-1)} - \sum_{i=1}^{\ell} n_i = \ell(p-1) - \sum_{i=1}^{\ell} n_i < p-1.$$

In other words, f is a polynomial of degree $< p-1$. Besides, obviously, $f \in \mathbb{Q}[X]$, and we have $f(j) \in \mathbb{Z}$ for all $j \in \{0,1,...,p-1\}$ (since $f \in \mathbb{Z}[X]$). Thus, Theorem 5 yields $\sum_{j=0}^{p-1} f(j) \equiv 0 \mod p$. Thus,

$$0 \equiv \sum_{j=0}^{p-1} f(j) = \sum_{j=0}^{p-1}\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+j-1)-u) \qquad \text{(by (2))}$$

$$= \sum_{j=0}^{p-1}\prod_{i=1}^{\ell}(p-n_i-1)! \cdot (-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}$$

$$\left(\text{since } \prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+j-1)-u) = \prod_{i=1}^{\ell}(p-n_i-1)! \cdot (-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j} \text{ by (1)}\right)$$

$$= \prod_{i=1}^{\ell}(p-n_i-1)! \cdot \sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j} \mod p.$$

In other words,

$$p \mid \prod_{i=1}^{\ell}(p-n_i-1)! \cdot \sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}. \tag{3}$$

For every $i \in \{1,2,...,\ell\}$, the integer $(p-n_i-1)!$ is coprime with p (since $(p-n_i-1)! = 1\cdot 2\cdot ...\cdot(p-n_i-1)$, and all numbers 1, 2, ..., $p-n_i-1$ are coprime with p because p is a prime and $p-n_i-1<p$). Hence, the product $\prod_{i=1}^{\ell}(p-n_i-1)!$ is also coprime with p. Thus, (3) yields

$$p \mid \sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}.$$

Thus, Theorem 1 is proven.

Theorem 1 is a rather general result; we can repeatedly specialize it and still get substantial assertions. Here is a quite strong particular case of Theorem 1:

Theorem 8. Let ℓ be an even positive integer. If n_1, n_2, ..., n_ℓ are positive integers and p is a prime such that $(\ell-1)(p-1) < \sum_{i=1}^{\ell} n_i$ and $n_i < p$ for every $i \in \{1,2,...,\ell\}$, then $p \mid \sum_{j=0}^{p-1}\prod_{i=1}^{\ell}\binom{n_i}{j}$.

Proof of Theorem 8. Theorem 1 yields $p \mid \sum\limits_{j=0}^{p-1} (-1)^{\ell j} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. But ℓ is even, so that ℓj is even for any $j \in \mathbb{Z}$, and thus

$$\sum_{j=0}^{p-1} \underbrace{(-1)^{\ell j}}_{\substack{=1, \text{ since} \\ \ell j \text{ is even}}} \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} 1 \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} \prod_{i=1}^{\ell} \binom{n_i}{j}.$$

Hence, $p \mid \sum\limits_{j=0}^{p-1} (-1)^{\ell j} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$ becomes $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. Therefore, Theorem 8 is proven.

Specializing further, we arrive at the following result (which I proved in [1], post #2):

Theorem 9. If n and k are positive integers and p is a prime such that $\frac{2k-1}{2k}(p-1) < n < p$, then $p \mid \sum\limits_{j=0}^{n} \binom{n}{j}^{2k}$.

Proof of Theorem 9. Let $\ell = 2k$. Define positive integers $n_1, n_2, ..., n_\ell$ by $n_i = n$ for every $i \in \{1, 2, ..., \ell\}$. Then, $n_i < p$ for every $i \in \{1, 2, ..., \ell\}$ (since $n_i = n < p$) and

$$(\ell - 1)(p-1) = (2k-1)(p-1) = 2k \cdot \underbrace{\frac{2k-1}{2k}(p-1)}_{<n} < 2kn = \ell n = \sum_{i=1}^{\ell} n = \sum_{i=1}^{\ell} n_i.$$

Hence, Theorem 8 yields $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. But $\prod\limits_{i=1}^{\ell} \binom{n_i}{j} = \prod\limits_{i=1}^{\ell} \binom{n}{j} = \binom{n}{j}^{\ell} = \binom{n}{j}^{2k}$, and thus

$$\sum_{j=0}^{p-1} \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} \binom{n}{j}^{2k} = \sum_{j=0}^{n} \binom{n}{j}^{2k} + \sum_{j=n+1}^{p-1} \underbrace{\binom{n}{j}^{2k}}_{\substack{=0, \text{ since } n \geq 0 \text{ and} \\ j>n \text{ yield } \binom{n}{j}=0}} \qquad (\text{since } n < p)$$

$$= \sum_{j=0}^{n} \binom{n}{j}^{2k} + \underbrace{\sum_{j=n+1}^{p-1} 0}_{=0} = \sum_{j=0}^{n} \binom{n}{j}^{2k}.$$

Therefore, $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$ becomes $p \mid \sum\limits_{j=0}^{n} \binom{n}{j}^{2k}$. Hence, Theorem 9 is proven.

The problem quickly follows from Theorem 9 in the particular case $k = 2$.

References

1 *PEN Problem E16*, http://www.mathlinks.ro/viewtopic.php?t=150539

2 *PEN Problem A24*, http://www.mathlinks.ro/viewtopic.php?t=150392