A BINOMIAL IDENTITY ON THE LEAST PRIME FACTOR OF AN INTEGER

SAMUEL A. HAMBLETON

ABSTRACT. An identity for binomial symbols modulo an odd positive integer \( n \) relating to the least prime factor of \( n \) is proved. The identity is discussed within the context of Pell conics.

1. INTRODUCTION

Many results exist on identities relating to binomial coefficients \( \binom{m}{r} \) modulo \( n \) where \( n \) is an odd positive integer \( \geq 2 \). Granville \( [2] \) has given new results concerning \( \binom{m}{r} \pmod{p^q} \) where \( p \) is prime, with a nice account of known results. Perhaps the most well known identity on factorials modulo \( n \) is Wilson’s theorem, which states that a positive integer \( n \) is prime if and only if \((n-1)！ \equiv -1 \pmod{n}\). Granville \( [3] \) writes that Fleck \( [2] \) has generalized Wilson’s theorem to the statement that for all positive integers \( r \) less than or equal to the least prime divisor of \( n \), \( n \) is prime if and only if

\[
\prod_{j=0}^{n-1-r} \binom{r+j}{r} \equiv (-1)^{r+1} \prod_{j=1}^{r-1} \binom{r}{j} \pmod{n}.
\]

Similarly, we will consider the residue modulo an odd positive integer \( n \) of a symbol \( \beta(n, r) \) defined in terms of binomial coefficients where, likewise, \( r \) is less than or equal to the least prime divisor \( p \) of \( n \). We will briefly discuss the case \( r > p \). Let \( [a] \) and \( \lceil a \rceil \) respectively denote the greatest integer \( A \leq a \), and the least integer \( A \geq a \).

Theorem 1.1. Let \( n \) be an odd positive integer, let \( r \geq 2 \) be an integer, and let \( p \) be the least prime divisor of \( n \). Define \( \alpha(n, r) \) to be the non-negative residue modulo \( n \) of

\[
\beta(n, r) = (-1)^{\lceil \frac{r}{2} \rceil} \left( \frac{n-1}{2} \right) \left( \frac{\lceil \frac{n-1}{2} \rceil}{\lceil \frac{r}{2} \rceil} \right) - \left( \frac{\lceil \frac{n-1}{2} \rceil}{\frac{r}{2}} \right) \left( \frac{n-1}{r} \right) (-2)^r.
\]

Then \( \alpha(n, r) \) satisfies \( \alpha(n, r) = \begin{cases} 0 \pmod{n} & \text{if } r < p \\ n/p \pmod{n} & \text{if } r = p \end{cases} \).

Eqn. \( \Box \) occurs as the leading coefficient of the difference modulo \( n \) of two polynomials which are important in the study of the affine genus zero curves known as Pell conics examined in detail by Lemmermeyer \( [7, 8] \) and other authors \( [1, 3] \) in relation to the analogy between these curves and elliptic curves. Let \( \Delta \) be the

\ Daytona: July 28, 2011.
2010 Mathematics Subject Classification. Primary 11A51, 11B65; Secondary 11B39, 11G20.
Key words and phrases. Binomial symbols, factorization, Pell Conics, Dickson polynomials.
fundamental discriminant of a quadratic number field $K = \mathbb{Q}(\sqrt{\Delta})$. Pell conics are the curves

$$C : X^2 - \Delta Y^2 = 4,$$

with group law

$$(2) \quad \mathcal{P}_1 + \mathcal{P}_2 = \left( \frac{X_1 X_2 + \Delta Y_1 Y_2}{2}, \frac{X_1 Y_2 + X_2 Y_1}{2} \right)$$

defined for points $\mathcal{P}_1 = (X_1, Y_1)$ and $\mathcal{P}_2 = (X_2, Y_2)$ over $(\mathbb{Z}/n), \mathbb{Z}, \mathbb{Q}$, and algebraic numbers $\overline{\mathbb{Q}}$ among various other rings $R$ for which the binary operation $+$ of Eqn. (2) forms a group $\mathcal{C}(R)$ with identity $(2, 0)$. See [2] for more on these curves.

We define the polynomials $\mathcal{F}_n(X)$ by

$$\mathcal{F}_1 = 1, \mathcal{F}_3 = X + 1, \mathcal{F}_{2j+3} = X\mathcal{F}_{2j+1} - \mathcal{F}_{2j-1},$$

The origin of the polynomials $\mathcal{F}_n(X)$ can be traced to D. H. Lehmer [6] who has compared a Lucas function to Sylvester polynomials $\Psi_n(x, y)$ appearing in Bachmann’s [1] book. The polynomials $\Psi_n(x, y)$ correspond to the $G_n(x)$ used by Williams [10].

$$\mathcal{F}_n(X) = G_{(n-1)/2}(X) \text{of Williams} = \Psi_n(x, 1) \text{of Sylvester according to Lehmer}.$$

It has been shown [4, 5] that the zeros of the polynomials $\mathcal{F}_n(X)$ are in one to one correspondence with the X-coordinates of the non-trivial points $\mathcal{P} \neq (2, 0)$ of order dividing $n$ in the group $\mathcal{C}(\overline{\mathbb{Q}})$, non-trivial points of the $n$-torsion subgroup $\mathcal{C}(\overline{\mathbb{Q}})[n]$. One simply expresses the X-coordinate of $n(X, Y)$, meaning $n-1$ additions $(X, Y) + (X, Y) + \ldots + (X, Y)$, as $(X - 2)\mathcal{F}_n(X) + 2$. In order to give a proof of quadratic reciprocity [3] using $p$-torsion on Pell conics where $p$ is an odd prime, it was demonstrated that

$$\mathcal{F}_p(X) \equiv (X - 2)^{\frac{n-1}{2}} \pmod{p}.$$

The leading coefficient of the polynomial $\mathcal{F}_n(X) - (X - 2)\sum_{j=0}^{n/2} (-a)^j x^{n-2j}$. In particular, the identity, p.32 of [3],

$$\mathcal{F}_{2n+1}(X) = E_n(X, 1) + E_{n-1}(X, 1),$$

allows writing, for odd $n$,

$$\mathcal{F}_n(X) = \sum_{r=0}^{\frac{n-1}{2}} (-1)^r \binom{\frac{n-1}{2} - \left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{2} \right\rfloor}{r} X^{\frac{n-2}{4} - r}.$$

This completes the discussion of the context of the identity for $\beta(n, r)$.

2. Proof of the main result

We require the following equality which holds for all positive integers $a$.

$$(3) \quad \prod_{j=1}^{a} (a + j) = 2^a \prod_{j=0}^{a-1} (2j + 1).$$

Eqn. (4) may be proved by reordering the products in the numerator and denominator of $\prod_{j=1}^{a} \frac{a + j}{2j - 2}$, showing that this is equal to 1. The proof of Theorem [14] is as follows.
\[ \alpha(n, r) = (\alpha)^s \left( \frac{n-1}{r} - t \right) \times (\alpha)^s \left( \frac{n-1}{r} \right) (-2)^s, \]
\[ = \left( \frac{(-1)^s}{s!} \right)^2 \alpha \left( \frac{n-1}{s} \right) \prod_{j=1}^{t-1} \left( \frac{n-1}{r} - s - j \right), \]
\[ = \left( \frac{(-1)^s}{s!} \right)^2 \prod_{j=1}^{t-1} (s+j) \prod_{j=1}^{t-1} \left( \frac{n-1}{r} - s - j \right), \]
\[ = \left( \frac{(-1)^s}{s!} \right)^2 \prod_{j=1}^{t-1} (s+j) \prod_{j=1}^{t-1} \left( \frac{n-1}{r} - s - j \right), \]
\[ = \left( \prod_{j=1}^{t-1} (s+j) \right) 2^{-t} \prod_{j=1}^{t-1} (1 + 2s + 2j - n), \]
\[ \alpha(n, p) \equiv \left( \prod_{j=1}^{t-1} (s+j) \right) 2^{-t} \prod_{j=1}^{t-1} (1 + 2s + 2j) \pmod{n}. \]

Since \( r \) is strictly less than \( p \), the integers \( r! \) and \( n \) are relatively prime. By Eqn. \( \[3] \), \( \alpha(n, r) = 0 \). Now let \( r = p = 2s + 1 \). Then

\[ \beta(n, p) = (-1)^s \left( \frac{n-1}{s} - 1 \right) \times (\alpha)^s \left( \frac{n-1}{p} \right) 2^s, \]
\[ = \left( \frac{(-1)^s}{s!} \right)^2 \prod_{j=1}^{s} \left( \frac{n-1}{s} - 2j \right) \prod_{j=1}^{s} \left( \frac{n-1}{2} - s - j \right), \]
\[ = \left( \frac{(-1)^s}{s!} \right)^2 \prod_{j=1}^{s} \left( \frac{n-1}{s} - 2j \right) \prod_{j=1}^{s} \left( \frac{n-1}{2} - s - j \right), \]
\[ = \frac{\prod_{j=0}^{s} (s+j) + 2^s \left( \frac{n}{p} - 1 \right) \prod_{j=1}^{s} \left( n-1 - 2j \right) \prod_{j=1}^{s} \left( n-1 + 1 + 2j \right)}{(p-1)!2^s} \prod_{j=1}^{s} \left( -n + p + 2j \right), \]
\[ \alpha(n, p) \equiv \left( \prod_{j=0}^{s} (s+j) + 2^s \left( \frac{n}{p} - 1 \right) \prod_{j=1}^{s} (s+j) \right) \prod_{j=1}^{s} (p-1)!2^{-s} \prod_{j=1}^{s} (p+2j) \pmod{n}, \]
\[ = \frac{n}{p} \prod_{j=1}^{s} (p-1)!2^{-s} \prod_{j=1}^{s} (s+j) \pmod{n}, \]
\[ = \frac{n}{p} \prod_{j=1}^{s} (p+2j) \pmod{n}, \]
\[ = \frac{n}{p} \prod_{j=1}^{s-1} (2j) \pmod{n}. \]

Fermat's theorem shows that \( \prod_{j=1}^{p-1} (2j) \pmod{n} \equiv 1 \pmod{p} \). It follows that \( \alpha(n, p) = \frac{n}{p} \pmod{p} \). \( \square \)

We conclude by speculating as to the value of \( \alpha(n, r) \) when \( r \) exceeds the least prime divisor of \( n \), within some bounds. The author has only tested the following conjecture for \( n < 10^6 \).
Conjecture 2.1. Let $p$ be the least prime divisor of an odd integer $n$ and assume that $2\sqrt{n} < 3p$. If $r$ is an integer bounded by $p < r < \sqrt{n}$ then $\alpha(n, r) > 0$.

If Conjecture 2.1 holds and the least prime divisor $p$ of $n$ satisfies $2\sqrt{n} < 3p$ then the follow exponential algorithm will terminate.

Algorithm 2.2. Let $A = (a_1, a_2)$ and assume we wish to factor $n$. Set $A = (2, \lfloor \sqrt{n} \rfloor)$. If $\alpha\left(n, \left\lfloor \frac{a_1 + a_2}{2} \right\rfloor \right) = 0$, Set $A = \left(\left\lfloor \frac{a_1 + a_2}{2} \right\rfloor, a_2\right)$, otherwise set $A = \left(a_1, \left\lfloor \frac{a_1 + a_2}{2} \right\rfloor\right)$, and print $A$. Repeat until $a_2 - a_1 \leq 2$.

Acknowledgments

The author would like to thank Victor Scharaschkin for doctoral supervision of which this project has been a very small part of, and supported by the University of Queensland.

References

1. P. Bachmann, Die Lehre von der Kreisteilung, Leipzig, pp. 9, 10 (1872).
5. S. Hambleton, V. Scharaschkin, Pell conics and quadratic reciprocity, RMJM, to appear.
10. H. Williams, Effective primality tests for some integers of the form $A5^n - 1$ and $A7^n - 1$, Math. Comp. 48, 177, 385–403 (1987).

School of Mathematics and Physics, University of Queensland, St. Lucia, Queensland, Australia 4072

E-mail address: maths.uq.edu.au