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 [2]. Granville [3] 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 that the least prime divisor of n, n is prime if and only if

$$\prod_{j=0}^{n-1-r} \binom{r+j}{r} \equiv (-1)^{\binom{r+1}{2}} \prod_{j=1}^{r-1} \binom{r}{j} \pmod{n}.$$

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 $\lfloor a \rfloor$ 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*

$$\beta(n,r) = (-1)^{\lfloor \frac{r}{2} \rfloor} \binom{\frac{n-1}{2} - \lceil \frac{r}{2} \rceil}{\lfloor \frac{r}{2} \rfloor} - \binom{\frac{n-1}{2}}{r} (-2)^r. \tag{1}$$

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. (1) 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 [4, 5] in relation to the analogy between these curves and elliptic curves. Let Δ be the

Date: 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

$$\mathcal{C} : \mathrm{X}^2 - \Delta \mathcal{Y}^2 = 4,$$

with group law

$$\mathcal{P}_1 + \mathcal{P}_2 = \Big(\frac{\mathrm{X}_1\mathrm{X}_2 + \Delta \mathcal{Y}_1\mathcal{Y}_2}{2}, \frac{\mathrm{X}_1\mathcal{Y}_2 + \mathrm{X}_2\mathcal{Y}_1}{2}\Big) \tag{2}$$

defined for points $\mathcal{P}_1 = (\mathrm{X}_1, \mathcal{Y}_1)$ and $\mathcal{P}_2 = (\mathrm{X}_2, \mathcal{Y}_2)$ 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 [7] for more on these curves.

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

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

The origin of the polynomials $\mathcal{F}_n(\mathrm{X})$ 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 $G_m(x)$ used by Williams [10].

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

It has been shown [4, 5] that the zeros of the polynomials $\mathcal{F}_n(\mathrm{X})$ 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 $n(\mathrm{X}, \mathcal{Y})$, meaning $n-1$ additions $(\mathrm{X}, \mathcal{Y}) + (\mathrm{X}, \mathcal{Y}) + \ldots (\mathrm{X}, \mathcal{Y})$, as $(\mathrm{X} - 2)\mathcal{F}_n(\mathrm{X})^2 + 2$. In order to give a proof of quadratic reciprocity [5] using p-torsion on Pell conics where p is an odd prime, it was demonstrated that

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

The leading coefficient of the polynomial $\mathcal{F}_n(\mathrm{X}) - (\mathrm{X} - 2)^{\frac{n-1}{2}}$ evaluated modulo n is the more general question which we address. The polynomials $\mathcal{F}_n$ are also discussed in the context of Dickson polynomials of the second kind, $E_n(x, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}$. In particular, the identity, p.32 of [9],

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

allows writing, for odd n,

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

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.

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

Eqn. (3) may be proved by reordering the products in the numerator and denominator of $\prod_{j=1}^{a} \frac{a+j}{4j-2}$, showing that this is equal to 1. The proof of Theorem 1.1 is as follows.

Proof. First assume that $r < p$. Let $s = \lfloor r/2 \rfloor$ and $t = \lceil r/2 \rceil$. Then

$$\begin{aligned}
\beta(n,r) &= (-1)^s \binom{\frac{n-1}{2} - t}{s} - \binom{\frac{n-1}{2}}{r} (-2)^r, \\
&= \Big(\frac{(-1)^s}{s!} - \frac{(-2)^r \prod_{j=0}^{t-1} \big(\frac{n-1}{2} - j\big)}{r!} \Big) \prod_{j=1}^{t-1} \big(\frac{n-1}{2} - s - j\big), \\
&= \Big(\frac{(-1)^s \prod_{j=1}^{t} (s+j) - (-2)^r \prod_{j=0}^{t-1} \big(\frac{n-1}{2} - j\big)}{r!} \Big) \prod_{j=1}^{t-1} \big(\frac{n-1}{2} - s - j\big), \\
&= \Big(\frac{(-1)^s \prod_{j=1}^{t} (s+j) - (-1)^{r+t} 2^s \prod_{j=0}^{t-1} \big(1 + 2j - n\big)}{r!(-2)^{t-1}} \Big) \prod_{j=1}^{t-1} \big(1 + 2s + 2j - n\big), \\
&= \Big(\frac{\prod_{j=1}^{t} (s+j) - 2^s \prod_{j=0}^{t-1} \big(1 + 2j - n\big)}{r!} \Big) 2^{-t+1} (-1)^{r-1} \prod_{j=1}^{t-1} \big(1 + 2s + 2j - n\big), \\
\alpha(n,p) &\equiv \Big(\frac{\prod_{j=1}^{t} (s+j) - 2^s \prod_{j=0}^{t-1} \big(1 + 2j\big)}{r!} \Big) 2^{-t+1} (-1)^{r-1} \prod_{j=1}^{t-1} \big(1 + 2s + 2j\big) \pmod{n}.
\end{aligned}$$

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

$$\begin{aligned}
\beta(n,p) &= (-1)^s \binom{\frac{n-1}{2} - s - 1}{s} + \binom{\frac{n-1}{2}}{p} 2^p, \\
&= \Big(\frac{(-1)^s}{s!} + \frac{2^s \prod_{j=0}^{s} \big(n - 1 - 2j\big)}{p!} \Big) \prod_{j=1}^{s} \big(\frac{n-1}{2} - s - j\big), \\
&= \Big(\frac{(-1)^s}{s!} + \frac{2^s (\frac{n}{p} - 1) \prod_{j=0}^{s-1} \big(n - 1 - 2j\big)}{(p-1)!} \Big) \prod_{j=1}^{s} \big(\frac{n-1}{2} - s - j\big), \\
&= \frac{\prod_{j=0}^{s-1} (s+j+1) + 2^s \left(\frac{n}{p} - 1\right) \prod_{j=0}^{s-1} \big(-n + 1 + 2j\big)}{(p-1)! 2^s} \prod_{j=1}^{s} \big(-n + p + 2j\big), \\
\alpha(n,p) &\equiv \Big(\prod_{j=0}^{s-1} (s+j+1) + \Big(\frac{n}{p} - 1\Big) \prod_{j=1}^{s} \big(s+j\big) \Big) (p-1)!^{-1} 2^{-s} \prod_{j=1}^{s} \big(p + 2j\big) \pmod{n}, \\
&\equiv \frac{n}{p} (p-1)!^{-1} 2^{-s} \prod_{j=1}^{s} \big(s+j\big) \big(p + 2j\big) \pmod{n}, \\
&\equiv \frac{n}{p} (p-1)!^{-1} 2^{-p+1} \prod_{j=1}^{p-1} \big(p + j\big) \pmod{n}, \\
&\equiv \frac{n}{p} \prod_{j=1}^{p-1} (2j)^{-1} \big(p + j\big) \pmod{n}.
\end{aligned}$$

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

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 $\alpha\Big(n, \left\lfloor\frac{a_1+a_2}{2}\right\rfloor\Big) = 0$, Set $A = \Big(\left\lfloor\frac{a_1+a_2}{2}\right\rfloor, a_2\Big)$, otherwise set $A = \Big(a_1, \left\lfloor\frac{a_1+a_2}{2}\right\rfloor\Big)$, 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 Kreistheilung*, Leipzig, pp. 9, 10 (1872).
2. L. Dickson, *History of the theory of numbers*, **I**, AMS Chelsea publishing, (1992)
3. A. Granville, *Binomial Coefficients* $\pmod{p^q}$, available at: http://www.cecm.sfu.ca/organics/papers/granville/
4. S. Hambleton, *Generalized Lucas–Lehmer tests using Pell conics*, Proc. AMS, to appear.
5. S. Hambleton, V. Scharaschkin, *Pell conics and quadratic reciprocity*, RMJM, to appear.
6. D. H., Lehmer, *An extended theory of Lucas' functions*, The Ann. Math., **31**, (3), 419–448, (1930).
7. F. Lemmermeyer, *Conics – A poor man's elliptic curves*, arXiv:math/0311306v1, preprint available at: http://www.fen.bilkent.edu.tr/franz/publ/conics.pdf
8. F. Lemmermeyer, *Modular Pell conics*, preprint available at: http://www.rzuser.uni-heidelberg.de/~hb3/publ-new.html
9. R. Lidl, G. Mullen, G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical (1993).
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: sah@maths.uq.edu.au