A PROOF OF THE MANN-SHANKS PRIMALITY CRITERION CONJECTURE FOR EXTENDED BINOMIAL COEFFICIENTS

Steffen Eger
Dept. of Computer Science, Goethe University, Frankfurt am Main, Germany
eger.steffen@gmail.com

Received: 2/18/14, Accepted: 9/18/14, Published: 10/30/14

Abstract
We show that the Mann-Shanks primality criterion holds for weighted extended binomial coefficients (which count the number of weighted integer compositions), not only for the ordinary binomial coefficients.

1. Introduction

In 1972, Mann and Shanks [4] gave the following criterion for primality of an integer:

> An integer $n > 1$ is prime if and only if m divides $\binom{m}{n-2m}$ for all integers m with $0 \leq 2m \leq n$.

Equivalently, this can be expressed as follows. Consider the left-justified form of the Pascal triangle T_2 and displace the entries in each row two places to the right from the previous row (so that the $m+1$ entries in row m occupy columns $2m$ to $3m$, inclusive); also, underline the entries in row m which are divisible by m. Then, the column number n is prime if and only if all the entries in column n are underlined. Table 1 illustrates.

Bollinger [1] showed that the same criterion holds in the extended Pascal triangles T_3, where entries in row m are sums of the overlying 3 entries, and conjectured that it holds for T_4, T_5, etc., but could not give a proof. We show that, indeed, the Mann-Shanks primality criterion holds in all extended Pascal triangles, and even in weighted ones, as we define below.

$m \backslash n$	0	1	$\underline{2}$	$\underline{3}$	4	$\underline{5}$	6	$\underline{7}$	8	9	10	$\underline{11}$	12	$\underline{13}$	14	15	16	$\underline{17}$
0	1																	
1			$\underline{1}$	$\underline{1}$														
2					1	$\underline{2}$	1											
3							1	$\underline{3}$	$\underline{3}$	1								
4									1	$\underline{4}$	6	$\underline{4}$	1					
5											1	$\underline{5}$	$\underline{10}$	$\underline{10}$	$\underline{5}$	1		
6													1	$\underline{6}$	15	20	15	$\underline{6}$
7															1	$\underline{7}$	$\underline{21}$	$\underline{35}$
8																	1	$\underline{8}$

Table 1: The displaced Pascal triangle T_2.

2. The Mann-Shanks criterion for extended binomial coefficients

The extended (and weighted) binomial coefficients [2, 3] $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$, are defined as follows,

$$\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}} = [x^n]\Big(\sum_{s\in\mathbb{N}} f(s)x^s\Big)^k, \tag{1}$$

where $f : \mathbb{N} \to \mathbb{N}$ is a weighting function and $[x^n]p(x)$ denotes the coefficient of x^n in the polynomial or power series $p(x)$. Ordinary binomial coefficients (entries in T_2) are retrieved by setting $f(0) = f(1) = 1$ and $f(s) = 0$ for all $s > 1$; moreover, trinomial coefficients (entries in T_3) are retrieved by setting $f(0) = f(1) = f(2) = 1$ and $f(s) = 0$ for all $s > 2$, etc. We now state our main theorem.

Theorem 1. *Consider the coefficients* $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$ *defined in* (1)*. Let* $f(0) = f(1) = 1$*. Then, an integer* $n > 1$ *is prime if and only if* m *divides* $\binom{m}{n-2m}_{(f(s))_{s\in\mathbb{N}}}$ *for all integers* m *with* $0 \le 2m \le n$*.*

We prove Theorem 1 with the help of four lemmas. First, we show that the coefficients $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$ have the combinatorial interpretation of denoting the number of *f-weighted integer compositions* of the integer n with k *parts* where part values $s \in \mathbb{N}$ may occur in $f(s)$ different colors, i.e., $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$ gives the number of solutions $(\pi_1, \ldots, \pi_k) \in \mathbb{N}^k$ of where each part size π_i may be colored in $f(\pi_i)$ different colors. For instance, for $f(0) = f(2) = 1$, $f(1) = 2$ and $f(s) = 0$ for all $s > 2$, we have $\binom{2}{3}_{(f(s))_{s\in\mathbb{N}}} = 4$ and, indeed, $3 = 1 + 2 = 2 + 1 = 1^* + 2 = 2 + 1^*$, where we use a star superscript $(*)$ to differentiate between the two colors of 1. Also note that integer compositions are distinguished from the more well-studied objects of *integer partitions* in that, for compositions, order of parts matters. In other words, for our above example, there are four f-weighted integer compositions of 3 with 2 parts, but only two f-weighted integer partitions, namely, $3 = 2 + 1 = 2 + 1^*$.

Lemma 1 (Eger [2]). *The coefficients* $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$ *have the combinatorial interpretation of denoting the number of* f*-weighted integer compositions of* n *with* k *parts, and allow the representation*

$$\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}} = \sum_{\substack{\sum_{s\in[n]} k_s=k,\\ \sum_{s\in[n]} sk_s=n}} \binom{k}{(k_s)_{s\in[n]}} \prod_{s\in[n]} f(s)^{k_s}, \tag{2}$$

where $\binom{k}{a,b,\ldots} = \frac{k!}{a!b!\cdots}$ *denote the ordinary multinomial coefficients,* $[n] = \{0, 1, \ldots, n\}$*, and the sum on the right-hand side of* (2) *is over all nonnegative integers* $k_0, \ldots, k_n$ *subject to the indicated constraints.*

Proof. Collecting terms, we find that $[x^n]p(x)$, for $p(x) = (\sum_{s\in\mathbb{N}} f(s)x^s)^k$, is given as

$$\sum_{\pi_1+\cdots+\pi_k=n} f(\pi_1)\cdots f(\pi_k), \tag{3}$$

where the sum is over all different solutions in nonnegative integers $\pi_1, \ldots, \pi_k$ of $\pi_1 + \cdots + \pi_k = n$. This proves the combinatorial interpretation of $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$. To prove representation (2), note that the right-hand side of (2) sums over all integer partitions of n with k parts — k_s gives the *multiplicity* of part size $s \in [n]$ — and the multinomial coefficients distribute the part size 'types' $0, \ldots, n$, occurring with multiplicities $k_0, \ldots, k_n$, among the total of k parts (making compositions out of partitions), while $\prod_s f(s)^{k_s}$ is, in this context, simply $f(\pi_1)\cdots f(\pi_k)$ written in 'partition form'. Hence, the right-hand side of (2) and (3), which is $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$, represent the same count. $\square$

Next, we show that weighted extended binomial coefficients share an important property with binomial coefficients, their particulars, namely, that if k and n are relatively prime, then $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}} \equiv 0 \pmod{k}$. We prove this via an easily verified result about multinomial coefficients, which Bollinger [1] attributes to Ricci [5] and which we will also make use of in the proof of Lemma 4 below.

Lemma 2 (Ricci [5]). *Let* $k_1, \ldots, k_\ell$ *be nonnegative integers, not all zero, with* $k_1 + \cdots + k_\ell = k$*. Then*

$$\binom{k}{k_1, \ldots, k_\ell} \equiv 0 \pmod{\frac{k}{\gcd(k_1, \ldots, k_\ell)}},$$

where $\gcd(k_1, \ldots, k_\ell)$ *denotes the greatest common divisor of* $k_1, \ldots, k_\ell$*.*

Lemma 3. *Let* $k, n \geq 0$*, not both zero, with* $\gcd(k, n) = 1$*. Then* k *divides* $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$*.*

Proof. Consider an arbitrary term $\binom{k}{k_0,\ldots,k_n}\prod_{s\in[n]} f(s)^{k_s}$ in the sum representation (2) of $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$. Assume that $d=\gcd(k_0,\ldots,k_n)>1$. Then, d divides both k — since $k=k_0+\cdots+k_n$ — and n — since $n=0\cdot k_0+\cdots+n\cdot k_n$ — a contradiction. Hence $d=1$, and, by Lemma 2, $\binom{k}{k_0,\ldots,k_n}\equiv 0 \pmod{k}$. Hence, since k divides each term, it divides the sum, and, consequently, also $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}}$. $\square$

Lemma 4. *Let p be a prime number and let $r\geq 1$ be an integer. Then,*

$$\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}\equiv f(0)^{p(r-1)}f(1)^p\binom{pr}{p} \pmod{pr},$$

whereby $\binom{pr}{p}$ denotes the ordinary binomial coefficient.

Proof. By representation (2), $\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}$ can be written as

$$\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}=\sum_{\substack{k_0+\cdots+k_p=pr,\\ 0\cdot k_0+\cdots+p\cdot k_p=p}}\binom{pr}{k_0,\ldots,k_p}\prod_{s\in[p]} f(s)^{k_s}. \tag{4}$$

For a term in the sum, either $d=\gcd(k_0,\ldots,k_p)=1$ or $d=p$, since otherwise, if $1<d<p$, then, $d\cdot(0\cdot k_0/d+\cdots p\cdot k_p/d)=p$, whence p is composite, a contradiction. Those terms on the right-hand side of (4) for which $d=1$ contribute nothing to the sum modulo pr, by Lemma 2, so they can be ignored. But, from the equation $0\cdot k_0+1\cdot k_1+\cdots p\cdot k_p=p$, the case $d=p$ precisely happens when $k_1=p$, $k_2=\cdots=k_p=0$ and when $k_0=p(r-1)$ (from the equation $k_0+\cdots+k_p=pr$), whence, as required, $\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}\equiv f(0)^{p(r-1)}f(1)^p\binom{pr}{p} \pmod{pr}$. $\square$

Now, we are ready to prove our main theorem.

Proof of Theorem 1. Let $n>1$ be prime. Let m be an integer such that $0\leq 2m\leq n$. Then, $\gcd(m,n-2m)=1$. Hence, by Lemma 3, m divides $\binom{m}{n-2m}_{(f(s))_{s\in\mathbb{N}}}$.

Conversely, let $n>1$ not be prime. If n is even, choose $m=n/2$. Then $\binom{m}{n-2m}_{(f(s))_{s\in\mathbb{N}}}=\binom{n/2}{0}_{(f(s))_{s\in\mathbb{N}}}=f(0)^{n/2}=1$. Clearly, m does not divide 1 since $m>1$. If n is odd and composite, let p be a prime divisor of n and choose $m=(n-p)/2$. Then $m=pr$ for a positive integer r (note that p divides $m=(pq-p)/2$, whereby $n=pq$) and $\binom{m}{n-2m}_{(f(s))_{s\in\mathbb{N}}}=\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}$. By Lemma 4 and our assumption on f, $\binom{pr}{p}_{(f(s))_{s\in\mathbb{N}}}\equiv\binom{pr}{p} \pmod{pr}$. Finally, it is easy to show that (see Mann and Shanks [4]), for all $r\geq 1$,

$$\binom{pr}{p}\not\equiv 0 \pmod{pr},$$

which completes the proof. $\square$

Remark 1. *Of interest remain the cases when* $\big(f(0), f(1)\big) \neq (1,1)$*. By the proof of Theorem 1, it is clear that primality of* n *implies that* m *divides* $\binom{m}{n-2m}_{(f(s))_{s\in\mathbb{N}}}$ *even in this case, because this merely relies on the fact that* m *and* $n-2m$ *are relatively prime, and not also on* f*. However, the converse need no longer be true. For example, for* $f(0) = a$*,* $f(1) = b$ *and* $f(s) = 0$ *for all* $s > 1$*, it is easy to see that* $\binom{k}{n}_{(f(s))_{s\in\mathbb{N}}} = a^{k-n}b^n\binom{k}{n}$*. Thus, for* $a = 2$*,* $b = 1$*, and* $n = 4$*, for instance, we have* $\binom{0}{4}_{(f(s))_{s\in\mathbb{N}}} = \binom{1}{2}_{(f(s))_{s\in\mathbb{N}}} = 0$ *and* $\binom{2}{0}_{(f(s))_{s\in\mathbb{N}}} = 4$*, whence* m *divides* $\binom{m}{4-2m}_{(f(s))_{s\in\mathbb{N}}}$ *for all* $0 \leq 2m \leq n$*.*

References

[1] R.C. Bollinger, The Mann-Shanks primality criterion in the Pascal-T triangle T3, *Fibonacci Quart.* **27** (1989), 272–275.

[2] S. Eger, Restricted weighted integer compositions and extended binomial coefficients, *J. Integer Seq.* **16** (2013).

[3] N.-E. Fahssi, The polynomial triangles revisited, Preprint available at http://arxiv.org/abs/1202.0228 (2012).

[4] H. B. Mann and D. Shanks, A necessary and sufficient condition for primality, and its source, *J. Combin. Theory Ser. A* **13** (1972), 131–134.

[5] G. Ricci, Sui coefficienti binomiale e polinomali, *Giornale di Matematiche (Battaglini)* **69** (1931), 9–12.