ACTA ARITHMETICA
116.3 (2005)

On the multiplicative independence of binomial coefficients

by

JIANGUO XIA and HOURONG QIN (Nanjing)

1. Introduction. Let F be a finite extension of the field $\mathbb{Q}$ of rational numbers with the ring of integers O_F. For a finite set S of primes of F containing all infinite primes, we use U_S to denote the group of S-units of F, i.e., $a \in U_S$ if and only if $\operatorname{ord}_p(a) = 0$ for all primes p of F not belonging to S. We call the elements in the set $W_S := U_S \cap (1 - U_S)$ *good S-units*. It is known that W_S is finite (see [2, Theorem 1]).

Let $S = \{\infty, 2, 3, \ldots, p\}$ be the set of the first n prime numbers together with ∞, i.e., $p = p_n$. For $1 \le k \le p/2$, put $q_k = k/(p-k)$. It is clear that every q_k is a good S-unit.

Two open problems were raised by Browkin in [1].

(a) Is it true that exactly $n-1$ numbers among q_k are multiplicatively independent?
(b) Is the index $(U_S \wedge U_S : \lambda(A(W_S)))$ finite? Equivalently, are the free ranks of both groups equal?

We remark that a positive answer to problem (a) in fact answers problem (b) affirmatively. Browkin claimed that the answer to problem (a) is positive when $p \le 47$ or $p = 101$.

Let G be the subgroup of $\mathbb{Q}^*$ generated by the binomial coefficients $\binom{p-1}{i}$, $i=1,\ldots,[p/2]$. Because $q_k = \binom{p-1}{k-1}/\binom{p-1}{k}$ and $\binom{p-1}{k} = (q_1 \cdots q_k)^{-1}$, G is equal to the subgroup of $\mathbb{Q}^*$ generated by good S-units q_k, $k = 1, \ldots, [p/2]$. We see that exactly $n-1$ numbers among q_k are multiplicatively independent if and only if the rank of G is $n-1$.

In this paper, we prove the following theorem, which means that the answers to the two problems mentioned above are positive.

2000 *Mathematics Subject Classification*: 05A10, 11B65, 11R27.

Key words and phrases: rank of subgroups, good S-units.

This work was supported by the National Natural Science Foundation of China 10471118, SRFDP, the Jiangsu Natural Science Foundation Bk2002023, the National Distinguished Youth Science Foundation of China Grant and the 973 Grant.

THEOREM. *Let $p = p_n$ be the nth prime and G the subgroup of $\mathbb{Q}^*$ generated by the binomial coefficients $\binom{p-1}{i}$, $i = 1, \ldots, [p/2]$. Then the rank of G is $n-1$.*

2. Proof of Theorem. It is evident that the rank of G does not exceed $n-1$ since every binomial coefficient $\binom{p-1}{i}$ has the form

$$\binom{p-1}{i} = p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}$$

for some integers $m_1, \ldots, m_{n-1} \in \mathbb{Z}$.

In order to prove that the rank of G is exactly $n-1$, we only need to prove the following assertion:

There exist integers $e_{k1}, \ldots, e_{kk}$ with $e_{kk} \neq 0$ such that $2^{e_{k1}} 3^{e_{k2}} \cdots p_k^{e_{kk}} \in G$ for $1 \leq k \leq n-1$.

The case $n = 1$, i.e., $p_n = 2$, is trivial.

Now suppose that $p = p_n$ is an odd prime. First let us prove that the assertion is true for $k = 1$, i.e., $2^{e_{11}} \in G$ for some $e_{11} \in \mathbb{Z}$ with $e_{11} \neq 0$.

Set $b_0 = 1$, $a_1 = b_0 \cdot 2^{m_1}$, where $m_1 \in \mathbb{Z}$ and 2^{m_1} is the highest power of 2 less than p. Then $p/2 < a_1 < p$. Set $b_1 = p - a_1$. Then $0 < b_1 < p/2$. Set $a_2 = b_1 \cdot 2^{m_2}$, where $m_2 \in \mathbb{Z}$ and 2^{m_2} is the highest power of 2 less than p/b_1. Then $p/2 < a_2 < p$. In general, we define $a_i = b_{i-1} \cdot 2^{m_i}$, $b_i = p - a_i$ by induction on i, where $m_i \in \mathbb{Z}$ and 2^{m_i} is the highest power of 2 less than p/b_{i-1}. Then $p/2 < a_i < p$. Thus $b_i < p/2$ and $m_i > 0$ for any i.

Notice that each of a_i is a positive integer less than p, so there exist i and j with $i < j$ such that $a_i = a_j$. Thus

$$\begin{aligned}
\frac{a_i}{p - a_i} \cdot \frac{a_{i+1}}{p - a_{i+1}} \cdots \frac{a_{j-1}}{p - a_{j-1}} &= \frac{a_i}{b_i} \cdot \frac{a_{i+1}}{b_{i+1}} \cdots \frac{a_{j-1}}{b_{j-1}} \\
&= \frac{a_{i+1}}{b_i} \cdot \frac{a_{i+2}}{b_{i+1}} \cdots \frac{a_j}{b_{j-1}} = 2^{m_{i+1} + \cdots + m_j}.
\end{aligned}$$

Set $e_{11} = m_{i+1} + \cdots + m_j$. Then $e_{11} > 0$ and $2^{e_{11}} \in G$. So the assertion is true for $k = 1$.

Next let us prove that the assertion is true for $k = 2$, i.e., $2^{e_{21}} 3^{e_{22}} \in G$ for some $e_{21}, e_{22} \in \mathbb{Z}$ with $e_{22} \neq 0$.

Set $b_0 = 1$, $a_1 = b_0 \cdot 3^{m_1}$, where $m_1 \in \mathbb{Z}$ and 3^{m_1} is the highest power of 3 less than p. Then $p/3 < a_1 < p$. Let $p - a_1 = 2^{n_1} b_1$ with b_1 odd. Since a_1 is odd, $n_1 \geq 1$. So $b_1 \leq (p - a_1)/2 < p/3$. Set $a_2 = b_1 \cdot 3^{m_2}$, where $m_2 \in \mathbb{Z}$ and 3^{m_2} is the highest power of 3 less than p/b_1. Then $p/3 < a_2 < p$. Since $b_1 < p/3$, $m_2 \geq 1$. Let $p - a_2 = 2^{n_2} b_2$ with b_2 odd. Then $n_2 \geq 1$. In general, we define a_i and b_i by induction on i: $a_i = b_{i-1} \cdot 3^{m_i}$, where $m_i \in \mathbb{Z}$ and 3^{m_i} is the highest power of 3 less than p/b_{i-1}. Let $p - a_i = 2^{n_i} b_i$ with b_i odd. It is easy to prove by induction on i that $b_i < p/3$. So m_i is a positive integer.

Notice that each of a_i is a positive integer less than p, so there exist i and j with $i < j$ such that $a_i = a_j$. Thus

$$\frac{a_i}{b_i} \cdot \frac{a_{i+1}}{b_{i+1}} \cdots \frac{a_{j-1}}{b_{j-1}} = \frac{a_{i+1}}{b_i} \cdot \frac{a_{i+2}}{b_{i+1}} \cdots \frac{a_j}{b_{j-1}} = 3^{m_{i+1}+\cdots+m_j}.$$

So

$$\frac{a_i}{p-a_i} \cdot \frac{a_{i+1}}{p-a_{i+1}} \cdots \frac{a_{j-1}}{p-a_{j-1}} = 2^{-(n_i+\cdots+n_{j-1})} \cdot 3^{m_{i+1}+\cdots+m_j}.$$

Set $e_{21} = -(n_i + \cdots + n_{j-1})$, $e_{22} = m_{i+1} + \cdots + m_j$. Then $e_{22} > 0$ and $2^{e_{21}}3^{e_{22}} \in G$. So the assertion is true for $k = 2$.

Finally, let us prove that the assertion is true for $3 \le k \le n-1$, i.e., there exist integers $e_{k1}, \ldots, e_{kk}$ with $e_{kk} \ne 0$ such that $2^{e_{k1}}3^{e_{k2}} \cdots p_k^{e_{kk}} \in G$ for $3 \le k \le n-1$.

Let $q = p_k$. Set $b_0 = 1$, $a_1 = b_0 q^{m_1}(2l_1 - 1)$, where $m_1 \in \mathbb{Z}$ and q^{m_1} is the highest power of q less than p, l_1 the largest integer with $b_0 q^{m_1}(2l_1 - 1)$ less than p. Then $p/q < b_0 q^{m_1} < p$ and $b_0 q^{m_1}(2l_1 - 1) < p < b_0 q^{m_1}(2l_1 + 1)$. Let $p - a_1 = 2^{n_1} b_1$ with b_1 odd. Then $n_1 \ge 1$. In general, we define a_i and b_i by induction on i: $a_i = b_{i-1} q^{m_i}(2l_i - 1)$ with $p/q < b_{i-1}q^{m_i} < p$ and $b_{i-1}q^{m_i}(2l_i - 1) < p < b_{i-1}q^{m_i}(2l_i + 1)$, $p - a_i = 2^{n_i} b_i$ with b_i odd. Clearly $2l_i - 1 < q$ for $i \ge 1$. Since q is odd, $2l_i + 1 \le q$ for $i \ge 1$.

Since each of a_i is a positive integer less than p, there exist i and j with $i < j$ such that $a_i = a_j$. Thus

$$\begin{aligned}\frac{a_i}{b_i} \cdot \frac{a_{i+1}}{b_{i+1}} \cdots \frac{a_{j-1}}{b_{j-1}} &= \frac{a_{i+1}}{b_i} \cdot \frac{a_{i+2}}{b_{i+1}} \cdots \frac{a_j}{b_{j-1}} \\ &= q^{m_{i+1}+\cdots+m_j}(2l_{i+1} - 1) \cdots (2l_j - 1)\end{aligned}$$

and

$$\begin{aligned}&\frac{a_i}{p-a_i} \cdot \frac{a_{i+1}}{p-a_{i+1}} \cdots \frac{a_{j-1}}{p-a_{j-1}} \\ &\qquad = \frac{a_i}{b_i} \cdot \frac{a_{i+1}}{b_{i+1}} \cdots \frac{a_{j-1}}{b_{j-1}} 2^{-(n_i+\cdots+n_{j-1})} \\ &\qquad = q^{m_{i+1}+\cdots+m_j}(2l_{i+1} - 1) \cdots (2l_j - 1) \cdot 2^{-(n_i+\cdots+n_{j-1})}.\end{aligned}$$

We claim that $m_{i+1} + \cdots + m_j > 0$. In fact, if $m_{i+1} + \cdots + m_j = 0$, then $m_{i+1} = \cdots = m_j = 0$. Since $a_i = a_j$, we have $b_i = b_j$ and $a_{i+1} = a_{j+1}$, which means that $l_{j+1} = l_{i+1}$. Since $m_{i+1} = m_{i+2} = 0$, $a_{i+1} = b_i(2l_{i+1} - 1)$, $a_{i+2} = b_{i+1}(2l_{i+2} - 1)$. By definition of l_{i+1} we have

$$\frac{2l_{i+1} - 1}{2l_{i+1} + 1} p < a_{i+1} < p.$$

Notice that $n_{i+1} \ge 1$, hence

$$0 < b_{i+1} = \frac{p - a_{i+1}}{2^{n_{i+1}}} \le \frac{p - a_{i+1}}{2} < \frac{1}{2l_{i+1} + 1} p.$$

So $2l_{i+2}-1 \geq 2l_{i+1}+1$, hence $l_{i+2} > l_{i+1}$. Continuing this process, we finally get $l_{j+1} > l_j > l_{j-1} > \cdots > l_{i+2} > l_{i+1}$, which is a contradiction to $l_{j+1} = l_{i+1}$. On the other hand, $m_{i+1} + \cdots + m_j \geq 0$, hence $m_{i+1} + \cdots + m_j > 0$.

Since $2l_{i+1} - 1 < q, \ldots, 2l_j - 1 < q$, $(2l_{i+1} - 1) \cdots (2l_j - 1)$ has the form $3^{e_{k2}} \cdots p_{k-1}^{e_{k,k-1}}$ for some $e_{k2}, \ldots, e_{k,k-1} \in \mathbb{Z}$. Let $e_{k1} = -(n_i + \cdots + n_{j-1})$, $e_{kk} = m_{i+1} + \cdots + m_j$. Then $2^{e_{k1}} 3^{e_{k2}} \cdots p_{k-1}^{e_{k,k-1}} p_k^{e_{kk}} \in G$ and $e_{kk} > 0$. So the assertion is true for $3 \leq k \leq n-1$.

This completes the proof.

Acknowledgements. The authors are greatly indebted to the referee for careful reading of this paper and detailed suggestions for improvement.

References

[1] J. Browkin, *K-theory, cyclotomic equations, and Clausen's function*, in: Structural Properties of Polylogarithms, L. Lewin (ed.), Math. Surveys Monogr. 37, Amer. Math. Soc., Providence, RI, 1991, 233–273.

[2] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.

Jianguo Xia
Department of Mathematics
Nanjing Normal University
Nanjing, 210097, China
E-mail: jgxia@pine.njnu.edu.cn

Hourong Qin
Department of Mathematics
Nanjing University
Nanjing, 210093, China
E-mail: hrqin@nju.edu.cn

Received on 26.4.2004
and in revised form on 23.9.2004 (4755)