MATH. SCAND. 76 (1995), 194–200

POLYNOMIALS INVOLVING THE FLOOR FUNCTION

INGER JOHANNE HÅLAND and DONALD E. KNUTH

Abstract.

Some identities are presented that generalize the formula

$$x = 3x\lfloor x\lfloor x\rfloor\rfloor - 3\lfloor x\rfloor\lfloor x\lfloor x\rfloor\rfloor + \lfloor x\rfloor^3 + 3\{x\}\{x\lfloor x\rfloor\} + \{x\}^3$$

to a representation of the product $x_0x_1\ldots x_{n-1}$.

1. Introduction.

Let $\lfloor x\rfloor$ be the greatest integer less than or equal to x, and let $\{x\} = x - \lfloor x\rfloor$ be the fractional part of x. The purpose of this note is to show how the formulas

$$xy = \lfloor x\rfloor y + x\lfloor y\rfloor - \lfloor x\rfloor\lfloor y\rfloor + \{x\}\{y\} \tag{1.1}$$

and

$$\begin{aligned} xyz = {} & x\lfloor y\lfloor z\rfloor\rfloor + y\lfloor z\lfloor x\rfloor\rfloor + z\lfloor x\lfloor y\rfloor\rfloor \\ & - \lfloor x\rfloor\lfloor y\lfloor z\rfloor\rfloor - \lfloor y\rfloor\lfloor z\lfloor x\rfloor\rfloor - z\lfloor x\lfloor y\rfloor\rfloor \\ & + \lfloor x\rfloor\lfloor y\rfloor\lfloor z\rfloor \\ & + \{x\}\{y\lfloor z\rfloor\} + \{y\}\{z\lfloor x\rfloor\} + \{z\}\{x\lfloor y\rfloor\} \\ & + \{x\}\{y\}\{z\} \end{aligned} \tag{1.2}$$

can be extended to higher-order products $x_0x_1\ldots x_{n-1}$.

These identities make it possible to answer questions about the distribution mod 1 of sequences having the form

$$\alpha_1 n\lfloor\alpha_2 n\ldots\lfloor\alpha_{k-1}n\lfloor\alpha_k n\rfloor\rfloor\ldots\rfloor, \quad n = 1, 2, \ldots. \tag{1.3}$$

Such sequences are known to be uniformly distributed mod 1 if the real numbers $1, \alpha_1, \ldots, \alpha_k$ are rationally independent [1]; we will prove that (1.3) is uniformly distributed in the special case $\alpha_1 = \alpha_2 = \ldots = \alpha_k = \alpha$ if and only if α^k is irrational,

Received January 3, 1944.

when k is prime. (It is interesting to compare this result to analogous properties of the sequence

$$\alpha_0 \lfloor \alpha_1 n \rfloor \lfloor \alpha_2 n \rfloor \ldots \lfloor \alpha_k n \rfloor, \quad n = 1, 2, \ldots, \tag{1.4}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_k$ are positive real numbers. If $k \geqq 3$, such sequences are uniformly distributed mod 1 if and only if α_0 is irrational [2].)

2. Formulas for the product $x_0 x_1 \ldots x_{n-1}$.

The general expression we will derive for $x_0 x_1 \ldots x_{n-1}$ contains $2^{n+1} - n - 2$ terms. Given a sequence $X = (x_0, x_1, \ldots, x_{n-1})$ we regard x_{n+j} as equivalent to x_j, and for integers $a \leqq b$ we define

$$X^{a:b} = \begin{cases} 1, & \text{if } a = b; \\ x_a \lfloor X^{(a+1):b} \rfloor, & \text{otherwise.} \end{cases} \tag{2.1}$$

Thus $X^{1:4} = x_1 \lfloor x_2 \lfloor x_3 \rfloor \rfloor$ and $X^{4:(n+1)} = x_4 \lfloor x_5 \lfloor \ldots \lfloor x_{n-1} \lfloor x_0 \rfloor \rfloor \ldots \rfloor \rfloor$. Using this notation, we obtain an expression for $x_0 x_1 \ldots x_{n-1}$ by taking the sum of

$$\{X^{s_1:s_2}\}\{X^{s_2:s_3}\} \ldots \{X^{s_k:(s_1+n)}\} - (-1)^k \lfloor X^{s_1:s_2} \rfloor \lfloor X^{s_2:s_3} \rfloor \ldots \lfloor X^{s_k:(s_1+n)} \rfloor \tag{2.2}$$

over all nonempty subsets $S = \{s_1, \ldots, s_k\}$ of $\{0, 1, \ldots, n-1\}$, where $s_1 < \cdots < s_k$. This rule defines $2^{n+1} - 2$ terms, but in the special case $k = 1$ the two terms of (2.2) reduce to

$$\{X^{s_1:(s_1+n)}\} + \lfloor X^{s_1:(s_1+n)} \rfloor = X^{s_1:(s_1+n)} \tag{2.3}$$

so we can combine them and make the overall formula n terms shorter. The right-hand side of (1.2) illustrates this construction when $n = 3$.

To prove that the sum of all terms (2.2) equals $x_0 x_1 \ldots x_{n-1}$, we replace $\{X^{a:b}\}$ by $X^{a:b} - \lfloor X^{a:b} \rfloor$ and expand all products. One of the terms in this expansion is $x_0 x_1 \ldots x_{n-1}$; it arises only from the set $S = \{0, 1, \ldots, n-1\}$. The other terms all contain at least one occurrence of the floor operator, and they can be written

$$x_{u_1} \ldots x_{v_1 - 1} \lfloor X^{v_1:u_2} \rfloor x_{u_2} \ldots x_{v_2 - 1} \lfloor X^{v_2:u_3} \rfloor x_{u_3} \ldots x_{v_3 - 1} \ldots \lfloor X^{v_k:(u_1+n)} \rfloor \tag{2.4}$$

where $u_1 \leqq v_1 < u_2 \leqq v_2 < u_3 \leqq \cdots \leqq v_k < n$. We want to show that all such terms cancel out. For example, some of the terms in the expansion when $n = 9$ have the form

$$x_1 \lfloor X^{2:4} \rfloor x_4 x_5 \lfloor X^{6:7} \rfloor \lfloor X^{7:10} \rfloor = x_1 \lfloor x_2 \lfloor x_3 \rfloor \rfloor x_4 x_5 \lfloor x_6 \rfloor \lfloor x_7 \lfloor x_8 \lfloor x_0 \rfloor \rfloor \rfloor,$$

which is (2.4) with $u_1 = 1, v_1 = 2, u_2 = 4, v_2 = 6, u_3 = v_3 = 7$. It is easy to see that this term arises from the expansion of (2.2) only when S is one of the sets $\{1, 2, 4, 5, 6, 7\}$, $\{1, 4, 5, 6, 7\}$, $\{1, 2, 4, 5, 7\}$, $\{1, 4, 5, 7\}$; in those cases it occurs with the respective signs $-$, $+$, $+$, $-$, so it does indeed cancel out.

In general, the only sets S leading to the term (2.4) have $S = \{s \mid u_j \leqq s < v_j\} \cup \{v_j \mid u_j = v_j\} \cup T$, where T is a subset of $U = \{v_j \mid u_j \neq v_j\}$. If U is empty, all parts of the term (2.4) appear inside floor brackets and this term is cancelled by the second term of (2.2). If U contains $m > 0$ elements, the 2^m choices for S produce 2^{m-1} terms with a coefficient of $+1$ and 2^{m-1} with a coefficient of -1. This completes the proof.

Notice that we used no special properties of the floor function in this argument. The same identity holds when $\lfloor x \rfloor$ is an arbitrary function, if we define $\{x\} = x - \lfloor x \rfloor$.

The formulas become simpler, of course, when all x_j are equal. Let

$$x^{:k} = \begin{cases} 1, & \text{if } k = 0; \\ x\lfloor x^{:(k-1)} \rfloor, & \text{if } k > 0; \end{cases} \tag{2.5}$$

and let

$$a_k = \{x^{:k}\}, \quad b_k = \lfloor x^{:k} \rfloor. \tag{2.6}$$

Then an identity for x^n can be read off from the coefficients of z^n in the formula

$$\frac{xz}{1 - xz} = \frac{a_1 z + 2a_2 z^2 + 3a_3 z^3 + \cdots}{1 - a_1 z - a_2 z^2 - a_3 z^3 - \cdots} + \frac{b_1 z + 2b_2 z^2 + 3b_3 z^3 + \cdots}{1 + b_1 z + b_2 z^2 + b_3 z^3 + \cdots}, \tag{2.7}$$

which can be derived from (2.2) or proved independently as shown below. For example,

$$x^2 = a_1^2 + 2a_2 - b_1^2 + 2b_2;$$

$$x_3 = a_1^3 + 3a_1 a_2 + 3a_3 + b_1^3 - 3b_1 b_2 + 3b_3;$$

$$x^4 = a_1^4 + 4a_1^2 a_2 + 4a_1 a_3 + 2a_2^2 + 4a_4 - b_1^4 + 4b_1^2 b_2 - 4b_1 b_3 - 2b_2^2 + 4b_4.$$

In general we have

$$x^n = p_n(a_1, a_2, \ldots, a_n) - p_n(-b_1, -b_2, \ldots, -b_n), \tag{2.8}$$

where the polynomial

$$p_n(a_1, a_2, \ldots, a_n) = \sum_{k_1 + 2k_2 + \cdots + nk_n = n} \frac{(k_1 + k_2 + \cdots + k_n - 1)!\,n}{k_1!\,k_2! \cdots k_n!} a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} \tag{2.9}$$

contains one term for each partition of n.

It is interesting to note that (2.7) can be written

$$\frac{zd}{dz}\ln\frac{1}{1-xz}=\frac{zd}{dz}\ln\frac{1}{1-a_1z-a_2z^2-\cdots}-\frac{zd}{dz}\ln\frac{1}{1+b_1z+b_2z^2+\cdots},$$

hence we obtain the equivalent identity

$$\frac{1}{1-xz}=\frac{1+b_1z+b_2z^2+b_3z^3+\cdots}{1-a_1z-a_2z^2-a_3z^3-\cdots}. \tag{2.10}$$

This identity is easily proved directly, because it says that $a_k + b_k = xb_{k-1}$ for $k \geqq 1$. Therefore it provides an alternative proof of (2.7). It also yields formulas for x^n with mixed a's and b's, and with no negative coefficients. For example,

$$x^2 = a_1^2 + a_2 + a_1b_1 + b_2;$$

$$x^3 = a_1^3 + 2a_1a_2 + a_3 + (a_1^2 + a_2)b_1 + a_1b_2 + b_3;$$

$$x^4 = a_1^4 + 3a_1^2a_2 + 2a_1a_3 + a_2^2 + a_4 + (a_1^3 + 2a_1a_2 + a_3)b_1 + (a_1^2 + a_2)b_2 + a_1b_3 + b_4.$$

3. Application to uniform distribution.

We can now apply the identities to a problem in number theory, as stated in the introduction. Let $[0\,..\,1) = \{x \mid 0 \leqq x < 1\}$.

LEMMA 1. *For all positive integers k and l, there is a function* $f_{k,l}(y_1, y_2, \ldots, y_{k-1})$ *from* $[0\,..\,1)^{k-1}$ *to* $[0\,..\,1)$ *such that*

$$\frac{x^{:k}}{l} \equiv \frac{x^k}{kl} - f_{k,l}\left(\left\{\frac{x}{k!l}\right\}, \left\{\frac{x^2}{k!l}\right\}, \ldots, \left\{\frac{x^{k-1}}{k!l}\right\}\right) \pmod 1. \tag{3.1}$$

PROOF. Let

$$\hat{p}_n(a_1, a_2, \ldots, a_{n-1}) = p_n(a_1, a_2, \ldots, a_n) - na_n \tag{3.2}$$

be the polynomial of (2.9) without its (unique) linear term. Then

$$\frac{x^{:k}}{l} = \frac{x^k}{kl} - \frac{1}{kl}\hat{p}_k(a_1, \ldots, a_{k-1}) + \frac{1}{kl}\hat{p}_k(-b_1, \ldots, -b_{k-1}). \tag{3.3}$$

We proceed by induction on k, defining the constant $f_{1,l} = 0$ for all l. Then if $y_j = \{x^j/k!l\}$ and $l_j = k!l/j!$ we have

$$a_j = \left\{l_j\frac{x^{:j}}{l_j}\right\} = \{l_j((j-1)!y_j - f_{j,l_j}(y_1, \ldots, y_{j-1}))\}$$

and

$$b_j = \left\lfloor l_j \frac{x^{:j}}{l_j} \right\rfloor = l_j \left\lfloor \frac{x^{:j}}{l_j} \right\rfloor + \sum_{i=1}^{l_j-1} \left\lfloor \left\{ \frac{x^j}{l_j} \right\} + \frac{i}{l_j} \right\rfloor$$
$$\equiv \sum_{i=1}^{l_j-1} \left\lfloor \{(j-1)! y_j - f_{j,l_j}(y_1, \ldots, y_{j-1})\} + \frac{i}{l_j} \right\rfloor \pmod{kl},$$

because of the well-known identities

$$\{lx\} = \{l\{x\}\}, \quad \lfloor lx \rfloor = \sum_{i=0}^{l-1} \lfloor x + i/l \rfloor, \tag{3.4}$$

when l is a positive integer. Therefore (3.1) holds with

$$f_{k,l}(y_1, \ldots, y_{k-1}) \tag{3.5}$$
$$= \left\{ \frac{1}{kl} \hat{p}_k(\bar{a}_{1,k,l}, \ldots, \bar{a}_{k-1,k,l}) - \frac{1}{kl} \hat{p}_k(-\bar{b}_{1,k,l}, \ldots, -\bar{b}_{k-1,k,l}) \right\},$$

where

$$\bar{a}_{j,k,l} = \{((j-1)! y_j - f_{j,k!l/j!}(y_1, \ldots, y_{j-1}))k!l/j!\}, \tag{3.6}$$

$$\bar{b}_{j,k,l} = \sum_{i=1}^{k!l/j!-1} \left\lfloor \{(j-1)! y_j - f_{j,k!l/j!}(y_1, \ldots, y_{j-1})\} + \frac{j! i}{k! l} \right\rfloor. \tag{3.7}$$

For example,

$$f_{2,3}(y) = \{(\alpha_1^2 - \beta_1^2)/6\},$$
$$f_{3,1}(y, z) = \{(3\alpha_1\alpha_2 + \alpha_1^3 - 3\beta_1\beta_2 + \beta_1^3)/3\},$$

where $\alpha_1 = \{6y\}$, $\alpha_2 = \{3z - 3f_{2,3}(y)\}$, $\beta_1 = \lfloor y + \frac{1}{6} \rfloor + \lfloor y + \frac{2}{6} \rfloor + \ldots + \lfloor y + \frac{5}{6} \rfloor$, and $\beta_2 = \lfloor \{z - f_{2,3}(y)\} + \frac{1}{3} \rfloor + \lfloor \{z - f_{2,3}(y)\} + \frac{2}{3} \rfloor$.

LEMMA 2. *The function $f_{k,l}$ of Lemma 1 does not preserve Lebesgue measure, and neither does $\{klmf_{k,l}\}$ for any positive integer m.*

PROOF. It suffices to prove the second statement, for if $f_{k,l}$ were measure-preserving the functions $\{mf_{k,l}\}$ would preserve Lebesgue measure for all positive integers m. Notice that $\{klmf_{k,l}\} = \{m\hat{p}_k(\bar{a}_{1,k,l}, \ldots, \bar{a}_{k-1,k,l})\}$, because $\hat{p}_k(-\bar{b}_{1,k,l}, \ldots, -\bar{b}_{k-1,k,l})$ is an integer. The triangular construction of (3.6) makes it clear that $\bar{a}_{1,k,l}, \ldots, \bar{a}_{k-1,k,l}$ are independent random variables defined on the probability space $[0\,..\,1)^{k-1}$, each uniformly distributed in $[0\,..\,1)$. Therefore it suffices to prove that $\{m\hat{p}_k(a_1, \ldots, a_{k-1})\}$ is not uniformly distributed when $a_1, \ldots, a_{k-1}$ are independent uniform deviates.

We can express $\hat{p}_k(a_1, \ldots, a_{k-1})$ in the form

$$ka_1a_{k-1} + a_1q_1(a_1, \ldots, a_{k-2}) + ka_2a_{k-2} + a_2q_2(a_2, \ldots, a_{k-3}) + \cdots + \tfrac{1}{2}ka_{k/2}^2,$$

for some polynomials $q_1, \ldots, q_{\lfloor (k-1)/2 \rfloor}$, where the final term $\frac{1}{2}ka_{k/2}^2$ is absent when k is odd. Then we can let $y_j = a_j$ for $j \leq \frac{1}{2}k$ and $y_j = a_j - q_{k-j}(a_{k-j}, \ldots, a_{j-1})/k$ for $j > \frac{1}{2}k$, obtaining independent uniform deviates $y_1, \ldots, y_{k-2}$ for which $m\hat{p}_k(a_1, \ldots, a_{k-1})$ equals

$$(3.8) \qquad g_k(y_1, \ldots, y_{k-1}) = mky_1y_{k-1} + mky_2y_{k-2} + \cdots + (\tfrac{m}{2}ky_{k/2}^2[k \text{ even}]).$$

For example, $g_4(y_1, y_2, y_3) = 4y_1y_3 + 2y_2^2$ and $g_5(y_1, y_2, y_3, y_4) = 5y_1y_4 + 5y_2y_3$ when $m = 1$.

The individual terms of (3.8) are independent, and they have monotone decreasing density functions mod. 1. (The density function for the probability that $\{kxy\} \in [t \,..\, t + dt]$ is $\sum_{j=0}^{k-1} \frac{1}{k} \ln \frac{k}{j+t}\, dt$.) Therefore they cannot possibly yield a uniform distribution. For if $f(x)$ is the density function for a random variable on $[0 \,..\, 1)$, we have $E(e^{2\pi i X}) = \int_0^1 e^{2\pi i x} f(x)\, dx \neq 0$ when $f(x)$ is monotone; for example, if $f(x)$ is decreasing, the imaginary part is

$$\int_0^{1/2} \sin(2\pi x)(f(x) - f(1-x))\, dx > 0.$$

If Y is an independent random variable with monotone density, we have $E(e^{2\pi i\{X+Y\}}) = E(e^{2\pi i(X+Y)}) = E(e^{2\pi i X})E(e^{2\pi i Y}) \neq 0$. But $E(e^{2\pi i U}) = 0$ when U is a uniform deviate. Therefore (3.8) cannot be uniform mod 1.

Now we can deduce properties of sequences like

$$(\alpha n)^{:k} = \alpha n \lfloor \alpha n \lfloor \ldots \lfloor \alpha n \rfloor \ldots \rfloor \rfloor$$

as n runs through integer values.

THEOREM. *If the powers $\alpha^2, \ldots, \alpha^{k-1}$ are irrational, the sequence $\{m(\alpha n)^k - km(\alpha n)^{:k}\}$, for $n = 1, 2, \ldots$, is not uniformly distributed in $[0 \,..\, 1)$ for any integer m.*

PROOF. This result is trivial when $k = 1$ and obvious when $k = 2$, since $\{(\alpha n)^2 - 2(\alpha n)^{:2}\} = \{\alpha n\}^2$. But for large values of k it seems to require a careful analysis. By Lemma 1 we have

$$(3.9) \qquad \{m(\alpha n)^k - km(\alpha n)^{:k}\} = \left\{kmf_{k,1}\left(\left\{\frac{\alpha n}{k!}\right\}, \ldots, \left\{\frac{\alpha^{k-1}n^{k-1}}{k!}\right\}\right)\right\},$$

and Lemma 2 tells that $\{kmf_{k,1}\}$ is not measure preserving.

Let S be an interval of $[0 \,..\, 1)$, and T its inverse image in $[0 \,..\, 1)^{k-1}$ under $\{kf_{k,1}\}$, where $\mu(T) \neq \mu(S)$. It is easy to see that if $(y_1, \ldots, y_{k-1}) \in T$ and $y_1, \ldots, y_{k-1}$ are irrational, there are values $\varepsilon_1, \ldots, \varepsilon_{k-1}$ such that $[y_1 \,..\, y_1 + \varepsilon_1) \times \cdots \times [y_{k-1} \,..\, y_{k-1} + \varepsilon_{k-1}) \subseteq T$. Therefore the irrational points of T can be covered by disjoint half-open hyperrectangles. We will show that (3.9) is not uniform by using Theorem 6.4 of [3], which implies that the sequence $(\{\alpha_1 n^{e_1}\}, \ldots, \{\alpha_s n^{e_s}\})$ is uniformly distributed in $[0\,..\,1)^s$ whenever $\alpha_1, \ldots, \alpha_s$ are irrational numbers and the integer exponents $e_1, \ldots, e_s$ are distinct. Thus the probability that $\{(\alpha n)^k - k(\alpha n)^{:k}\} \in S$ approaches $\mu(T)$ as $n \to \infty$; the distribution is nonuniform.

COROLLARY. *If the powers $\alpha^2, \ldots, \alpha^{k-1}$ are irrational, the sequence $\{(\alpha n)^{:k}\}$, for $n = 1, 2, \ldots$, is uniformly distributed in $[0\,..\,1)$ if and only if α^k is irrational.*

PROOF. If α^k is irrational, $\{\alpha^k n^k / k\}$ is uniformly distributed in $[0\,..\,1)$ and independent of $(\{\alpha n/k!\}, \ldots, \{\alpha^{k-1} n^{k-1}/k!\})$, by the theorem quoted above from [3]. Therefore the right-hand side of (3.1) is uniform.

If α^k is rational, say $\alpha^k = p/q$, assume that $\{(\alpha n)^{:k}\}$ is uniform. Then $\{q(\alpha^k n^k - k(\alpha n)^{:k}\} = \{-qk(\alpha n)^{:k}\}$ is also uniform, contradicting what we proved.

We conjecture that the theorem and its corollary remain true for all real α, without the hypothesis that $\alpha^2, \ldots, \alpha^{k-1}$ are irrational.

REFERENCES

1. I. J. Håland, *Uniform distribution of generalized polynomials.* J. Number Theory 45 (1993), 327–366.
2. I. J. Håland, *Uniform distribution of generalized polynomials of the product type*, Acta Arith. 67 (1994), 13–27.
3. L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, New York, Wiley, 1974.

AGDER COLLEGE OF ENGINEERING
N-4890 GRIMSTAD
NORWAY

COMPUTER SCIENCE DEPARTMENT
STANFORD UNIVERSITY
STANFORD CA 94305
U.S.A.