Discrete Mathematics 27 (1979) 245–259
© North-Holland Publishing Company

CYCLOTOMIC POLYNOMIALS AND NONSTANDARD DICE

Joseph A. GALLIAN
Department of Mathematical Sciences, University of Minnesota-Duluth, Duluth, MN 55812, U.S.A.

and

David J. RUSIN
Department of Mathematics, University of Chicago, Chicago, IL 60637, U.S.A.

Received 5 October 1978
Revised 14 March 1979

In this paper, we consider a broad generalization of a problem which first appeared in *Scientific American*. The original problem was to find all possible ways to label n cubes with positive integers so that the n cubes, when thrown simultaneously, will yield the same sum totals with the same frequency as n ordinary dice labelled 1 through 6. We investigate the analogous problem for n dice, each with m labels. A simple, purely algebraic characterization of solutions to this problem is given, and the problem is solved for certain infinite families of the parameter m. Several results on the general problem are included, and a number of avenues for further research are suggested.

1. Introduction

In a recent issue of *Scientific American* [1], Martin Gardner discusses the possibility of labelling a pair of cubes with positive integers in such a way that the frequency of the sum of the upward faces of the two cubes is the same as that of an ordinary pair of dice labelled 1 through 6. He mentions that besides the standard dice, there is exactly one more pair which produces the same result. This problem was first posed and solved by George Sicherman. In this paper, we consider an analogous problem for n dice, each with m labels. Throughout the paper, we assume $n > 1$, $m > 1$, and the probability that any one of m positive integer labels (counting repetitions) on a die has the probability $1/m$ of occurring. A spinner labelled 1 through m (like those used in games of chance) is a physical example of such a die. The cover of the *Mathematics Magazine*, Vol. 49, No. 3, shows how one could construct a solid with m labels, each one having probability $1/m$ of occurring.

2. Definitions

A die labelled 1 through m is called a standard one. A die with a total of m labels (counting repetitions) is said to have size m. A game with n dice is called an

n-dice game. The general problem of interest may be stated as follows: Given n and m, determine all possible sets of n dice, each of size m, so that the probability of obtaining any particular sum is the same as that obtained by using the set of n standard dice of size m. Any labelling that appears on one of n such dice is called a solution of an n-dice game with dice-size m. For example, Sicherman discovered that the labellings 1, 2, 2, 3, 3, 4 and 1, 3, 4, 5, 6, 8 are solutions to a 2-dice game with dice-size 6. Thus, a pair of cubes with these labels would yield the same probabilities as an ordinary pair of dice. If a sequence P of labels is a solution of an n-dice game, then P is obviously a solution of a k-dice game for any $k > n$, for one could simply combine the original set of n solution dice, of which P was one, with $k-n$ standard dice. Thus, for any nonstandard solution P of some n-dice game, it is of interest to find the smallest positive integer n for which this is true. Such an n is called the game-size of P. Define the game-size of the standard die to be 1.

3. The method

The general problem can be approached in the following way. Suppose, for $i = 1$ to n, the set of dice with labels $a_{i1}, a_{i2}, \ldots, a_{im}$ yields the same probabilities as n standard dice of size m. Let P_i denote the polynomial $x^{a_{i1}} + x^{a_{i2}} + \cdots + x^{a_{im}}$. In this way, we establish a 1–1 correspondence between solutions and polynomials. For convenience, we often refer to the polynomial corresponding to a solution of a game as a solution itself. Now, it is easy to see that our conditions require that

$$P_1 P_2 \cdots P_n = (x^m + x^{m-1} + \cdots + x^2 + x)^n = x^n \left(\frac{x^m - 1}{x - 1} \right)^n$$

and $P_i(1) = m$ for $i = 1$ to n. Since monic polynomials with integer coefficients can be factored over the integers in only one way as a product of irreducibles, the only possible irreducible factors for P_i are simply those of

$$x^m + \cdots + x = x(x^{m-1} + \cdots + 1) = \frac{x(x^m - 1)}{x - 1}.$$

Thus, the possible irreducible factors for P_i are x and the cyclotomic polynomials for divisors of m greater than 1.

Let's illustrate the technique for $m = 8$. If P is a polynomial obtained from a sequence of labels as described above, $P(x)$ must have the form

$$x^q (x+1)^r (x^2+1)^s (x^4+1)^t,$$

since $x + x^2 + \cdots + x^8$ factors as $x(x+1)(x^2+1)(x^4+1)$. Since the labels are positive integers, $P(x)$ is divisible by x, and, therefore, $q \geq 1$. If 1 occurred as a label on some solution die more than once, there would be more than one way to obtain a sum of n, using the n solution dice. But there is only one way to obtain a sum of n, using n standard dice, so $q=1$. This, together with the fact that $P(1)=2^3$, gives

$$P(x)=x(x+1)^r(x^2+1)^s(x^4+1)^t$$

where $r+s+t=3$. Trying all possible combinations for r, s, t, we obtain the following labels as possible solutions to an n-dice game with octahedrons:

(a) 1, 2, 3, 4, 5, 6, 7, 8 (standard),
(b) 1, 3, 5, 5, 7, 7, 9, 11,
(c) 1, 2, 2, 3, 3, 4, 4, 5,
(d) 1, 2, 5, 5, 6, 6, 9, 10,
(e) 1, 2, 3, 3, 4, 4, 5, 6,
(f) 1, 3, 3, 5, 5, 7, 7, 9,
(g) 1, 2, 2, 3, 5, 6, 6, 7,
(h) 1, 5, 5, 5, 9, 9, 9, 13,
(i) 1, 2, 2, 2, 3, 3, 3, 4,
(j) 1, 3, 3, 3, 5, 5, 5, 7.

A pair of dice with labels b and c yields a 2-dice game. The same is true of d and e, and f and g. Thus, the sequences b through g have game-size 2. Although h, i, and j are not solutions to a 2-dice game, {h, e, c}, {i, b, f}, and {j, d, g} each form 3-dice games.[1]

4. General results on solution dice

In this section, we present the solutions for certain infinite families of dice and give some general properties that solutions must have.

Throughout the remainder of the paper, p and q denote primes. We use $\lambda_k(x)$ to denote the kth cyclotomic polynomial. Properties of these polynomials can be found in [2, pp. 263–267].

Our first result gives a convenient way to determine whether or not a polynomial is the solution to some dice game.

Theorem 1. *A polynomial $P(x)$ is a solution to some game with dice of size m if and only if*:

(1) *$P(x)$ has nonnegative, integral coefficients*;
(2) *$P(x)$ is monic*;
(3) *$P(1)=m$*;
(4) *$P(x)/x$ is a polynomial, all of whose roots are mth roots of unity.*

[1]Incidentally, standard dice in the shape of an octahedron, as well as the other four Platonic solids, are commercially available from Creative Publications, 3977 East Bayshore Road, P. O. Box 10328, Palo Alto, California 94303.

Proof. Necessity is easy. We need (1), since the coefficient of x^k is the number of sides labelled "k." For (2), recall that

$$P \cdot P_2 \cdot \cdots \cdot P_n = x^n\left(\frac{x^m - 1}{x - 1}\right)^n$$

where $P_2, P_3, \ldots, P_n$ correspond to the other dice in the game; using (1) on each P_i, and comparing the leading coefficients, we see that each P_i is monic. Condition (3) ensures that the number of labels assigned (= $P(1)$, the sum of the coefficients) is the same as the number of sides (= m). And (4) follows, since $P(x)/x$ divides $(x^m - 1)^n/(x - 1)^n$ as in Section 3.

For the proof of sufficiency, we must show how to construct dice, given a polynomial $P(x)$ satisfying (1) through (4). Conditions (1) and (4) together yield

$$P(x) = c \cdot x \prod \lambda_{d_i}(x)$$

for some (not necessarily distinct) divisors d_i of m. Since the λ_d are known to be monic, (2) implies that $c = 1$.

Now recall that each λ_d may be written

$$\lambda_d(x) = \frac{\prod_{i=1}^{n}(x^{k_i} - 1)}{\prod_{i=1}^{n}(x^{l_i} - 1)}$$

for some n, where each k_i divides d. This means that $P(x)$ may be written

$$P(x) = \frac{x \prod_{i=1}^{n} (x^{k_i} - 1)}{\prod_{i=1}^{n} (x^{l_i} - 1)}$$

for some n and for some k_i dividing m.

Let $Q(x)$ be the polynomial

$$Q(x) = x^n\left(\frac{x^m - 1}{x - 1}\right)^n \Big/ P(x)$$
$$= x^{n-1} \prod_{i=1}^{n} \left(\frac{x^m - 1}{x^{k_i} - 1}\right) \cdot \prod_{i=1}^{n} \left(\frac{x^{l_i} - 1}{x - 1}\right).$$

Next, we use the fact that $k_i \mid m$ and the identity

$$\frac{x^{rst} - 1}{x^r - 1} = \frac{x^{rst} - 1}{x^{rs} - 1} \cdot \frac{x^{rs} - 1}{x^r - 1}$$

repeatedly to factor each of the terms

$$\left(\frac{x^m - 1}{x^{k_i} - 1}\right) \quad \text{and} \quad \left(\frac{x^{l_i} - 1}{x - 1}\right)$$

into the product of terms with the form $(x^{ap}-1)/(x^a-1)$ with p prime. This gives

$$(*) \qquad Q(x)=x^{n-1}\prod\left(\frac{x^{a_ip_i}-1}{x^{a_i}-1}\right).$$

Now,

$$Q(1)=\left[x^n\left(\frac{x^m-1}{x-1}\right)^n \text{ at } x=1\right]\Big/P(1)$$
$$=m^n/m=m^{n-1}, \quad \text{by (3).}$$

On the other hand, when we evaluate

$$\left(\frac{x^{a_ip_i}-1}{x^{a_i}-1}\right) \quad \text{at } x=1,$$

we get p_i. Thus, (*) gives $m^{n-1}=\prod p_i$. So, for each fixed prime p, the number of times $p_i=p$ in the expression (*) is

$$(n-1)\cdot(\text{number of times } p \text{ divides } m).$$

Therefore, we may partition the set of subscripts i into $n-1$ subsets $S_1, S_2, \ldots, S_{n-1}$ such that $\prod_{i\in S_j} p_i=m$ for each j.

If we let

$$Q_j(x)=x\prod_{i\in S_j}\left(\frac{x^{a_ip_i}-1}{x^{a_i}-1}\right),$$

then $Q=Q_1\cdot Q_2\cdot\;\cdots\;\cdot Q_{n-1}$. Now, each Q_j is the product of x and expressions of the form

$$\left(\frac{x^{ap}-1}{x^a-1}\right)=1+x^a+x^{2a}+\cdots+x^{(p-1)a}.$$

So, each Q_j certainly has nonnegative, integral coefficients whose sum is

$$Q_j(1)=\prod_{i\in S_j} x\left(\frac{x^{a_ip_i}-1}{x^{a_i}-1}\right)_{x=1}=\prod_{i\in S_j} p_i=m.$$

$P(x)$ likewise has nonnegative integral coefficients with sum m (only here do we really use condition (3)!).

Therefore, for each of the n polynomials $Q_1, Q_2, \ldots, Q_{n-1}$ and P, we label the sides of an m-sided die by letting the number of sides labelled "k" be the coefficient of x^k in that polynomial. When these n dice are thrown together, the frequencies of the possible face-sums may be read off from the coefficients of

$$Q_1 \cdot Q_2 \cdot \cdots \cdot Q_{n-1} \cdot P = Q \cdot P = x^n\left(\frac{x^m - 1}{x - 1}\right)^n;$$

that is, this set of n dice is equivalent to n standard (m-sided) dice. This makes P (as well as each Q_i) a "solution," as desired.

Theorem 2. *There are exactly 3 distinct solution dice in an n-dice game with dice-size pq, where p and q are not necessarily distinct primes. Moreover, the 3 solutions are the same for all n.*

Proof. Suppose $P(x)$ is a solution to an n-dice game with dice-size pq. We consider the case that $p \neq q$ first. The analysis in Section 3 shows that $P(x)$ has the form

$$x(\lambda_p(x))^r(\lambda_q(x))^s(\lambda_{pq}(x))^t.$$

Since $P(1) = pq$, it follows that $r = s = 1$. We next establish a bound for t. To this end, denote the degree of $\lambda_{pq}(x)$ by u, and the degree of $P(x)$ by v. Then the coefficient of x^{u-1} in $\lambda_{pq}(x)$ is -1 and, therefore, the coefficient of x^{v-1} in $P(x)$ is $2-t$. Thus, we need only consider the cases where $t = 0$, $t = 1$, $t = 2$. (Note that $t = 1$ corresponds to the standard die.) It is straightforward to check that these three cases yield polynomials that satisfy Theorem 1 and have game-size at most 2, so we are finished with the case that $p \neq q$.

Now, consider the case when $p = q$. Then, $P(x)$ has the form

$$x(\lambda_p(x))^r(\lambda_{p^2}(x))^s.$$

Since all the coefficients of $\lambda_{p^2}(x)$ are nonnegative and $P(1) = p^2$, we must have $r + s = 2$. This gives rise to three cases also, and, as before, each of the three resulting polynomials satisfies Theorem 1 and has game-size at most 2.

Since the above polynomials are independent of n (recall, we assume throughout the paper that $n > 1$) and have game-size at most 2, the "moreover" part of the theorem is true.

The actual solutions for two special cases of Theorem 2 are worth singling out.

Corollary 1. *The totality of solutions for an n-dice game with dice-size $2p$ ($p > 2$) is:*

(1) $1, 2, 3, \ldots, 2p$ (*standard labelling*);
(2) $1, 2, 2, 3, 3, \ldots, p, p, p+1$;
(3) $1, 3, 5, \ldots, p-2, p, p+1, p+2, \ldots, 2p-2, 2p-1, 2p, 2p+2, 2p+4, \ldots, 3p-1$.

Corollary 2. *The totality of solutions for an n-dice game with dice size p^2 is:*

(1) $1, 2, 3, \ldots, p^2$ (*standard labelling*);

(2) *labels*: $1, 2, 3, 4, \ldots, p-1, p, p+1, \ldots, 2p-2, 2p-1$
corresponding frequencies: $1, 2, 3, 4, \ldots, p-1, p, p-1, \ldots, 2, 1$;

(3) *labels*: $1, p+1, 2p+1, \ldots, (p-1)p+1, pp+1, \ldots, (2p-2)p+1$
corresponding frequencies: $1, 2, 3, 4, \ldots, p, p-1, \ldots, 1$.

(For example, for $p = 3$, (2) yields the labels 1, 2, 2, 3, 3, 3, 4, 4, 5.)

Theorem 3. *The standard die is the only solution for an n-dice game with dice-size m if and only if m is prime.*

Proof. If m is prime, then any solution $P(x)$ must have the form $x\lambda_m(x)$, so there is only one possibility for $P(x)$.

Now suppose $m = k \cdot l$ with $k, l \neq 1$. It suffices to show that there is a die of size m that is the solution to a 2-dice game. Let

$$P(x) = x\left(\frac{x^m - 1}{x^k - 1}\right)\left(\frac{x^m - 1}{x^l - 1}\right)$$

and

$$Q(x) = x\left(\frac{x^k - 1}{x - 1}\right)\left(\frac{x^l - 1}{x - 1}\right).$$

Since P and Q satisfy Theorem 1 and

$$P(x) \cdot Q(x) = x^2\left(\frac{x^m - 1}{x - 1}\right)^2,$$

P is the solution of a 2-dice game. But P has double roots, namely, the primitive mth roots of unity; so P is not the standard solution.

Before stating the next theorem, it is convenient to introduce the following notation: For a die with labels ranging from 1 to k, let α_i denote the number of times the label i occurs. For example, the octahedron labelled 1, 2, 2, 3, 5, 6, 6, 7 gives us $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 1$, $\alpha_4 = 0$, $\alpha_5 = 1$, $\alpha_6 = 2$, $\alpha_7 = 1$

Theorem 4. *For any solution die to an n-dice game with labels ranging from 1 to k, the sequence $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a palindrome.*

Proof. Let $P(x)$ be any solution to some game. Then $P(x)$ can be written as $x \prod \lambda_d(x)$ for some collection $\{\lambda_d(x)\}$ of cyclotomic polynomials (allowing repeats) with $d \neq 1$. The theorem now follows from that fact that all cyclotomic polynomials with $d \neq 1$ are palindromic and the product of palindromic polynomials is a palindrome.

Standard dice in the shape of a cube are always labelled so that the sum of opposing faces is 7. As an immediate consequence of Theorem 4, we see that all solution dice have the analogous arithmetic property.

Corollary. *If $a_1, a_2, \ldots, a_m$ are the m labels, listed in ascending order, of the solution to some game, then*

$$a_i + a_{m+1-i} = 1 + a_m \quad \text{for} \quad i = 1, \ldots, m.$$

In Section 3, we listed all of the solutions of an n-dice with dice-size 8. Solution h on that list is particularly interesting because of the relatively large gap between successive distinct labels. This raises the question of how large the gap between successive distinct labels can possibly be for a given dice size. The next result provides a bound on this gap.

Theorem 5. *If an m-sided die has a face labelled k, then the next largest label is at most $k+m$.*

Proof. In view of the palindrome property given in Theorem 4, it suffices to prove, instead, that if k is one of the labels on an m-sided die, then one of $k-1$, $k-2, \ldots, k-m+1$ or $k-m$ is also a label on the die. To prove this, we first recall some facts from the theory of equations. If a polynomial

$$P(x) = x^r + p_1 x^{r-1} + p_2 x^{r-2} + \cdots + p_r$$

has roots $\gamma_1, \gamma_2, \ldots, \gamma_r$ in some splitting field, let

$$\sigma_i = \gamma_1^i + \gamma_2^i + \cdots + \gamma_r^i.$$

Then Newton's Identities give (set $p_i = 0$ for $i > r$)

$$0 = \sigma_1 + 1p_1,$$

$$0 = \sigma_2 + \sigma_1 p_1 + 2p_2,$$

$$0 = \sigma_3 + \sigma_2 p_1 + \sigma_1 p_2 + 3p_3,$$

$$\vdots$$

Subtracting the $(i-m)$th equation from the ith $(i > m)$, we obtain

$$0 = (\sigma_i - \sigma_{i-m}) + (\sigma_{i-1} - \sigma_{i-m-1})p_1 + \cdots + \\ + (\sigma_m - [i-m])p_{i-m} + \sigma_{m-1}p_{i-m+1} + \cdots. \qquad (*)$$

Now take, in particular, $P(x)$ to be a polynomial corresponding to a die. Then, since any root γ of $P(x)$ is either 0 or an mth root of unity, we have $\gamma^i = \gamma^{i-m}$ and therefore $\sigma_i = \sigma_{i-m}$ for all $i > m$. Thus, (*) becomes

$$0 = (\sigma_m - [i-m])p_{i-m} + \sigma_{m-1}p_{i-m+1} + \cdots + \sigma_1 p_{i-1} + ip_i.$$

If we suppose $p_i = p_{i-1} = \cdots = p_{i-m+1} = 0$, then using the fact that

$$\sigma_m = \sum_{i=1}^{r} \gamma_i^m = (r-1)\cdot 1 + 1 \cdot 0 = r-1,$$

we have

$$0 = ([r-1] - (i-m))p_{i-m}.$$

Thus, either $i-m = r-1$ or $p_{i-m} = 0$. So, by choosing $i-m = r-k$, we see that the assumption

$$p_{r-k+1} = p_{r-k+2} = \cdots = p_{r-k+m} = 0$$

leads to $k = 1$ or $p_{r-k} = 0$. Since we have chosen our subscripts so that p_{r-k} is the number of faces labelled k, which by hypothesis is not zero, we see that, when $k \neq 1$, one of $p_{r-(k-1)}, p_{r-(k-2)}, \ldots, p_{r-(k-m)}$ is not zero. That is, some face has one of the labels $k-1, k-2, \ldots,$ or $k-m$. This completes the proof.

Numerous examples lead us to believe that Theorem 5 is true when the m in the conclusion is replaced by $\frac{1}{2}m$. Since there are dice of sizes 8 and 16 that have gaps between a pair of successive labels of 4 and 8 respectively, no better bound than $\frac{1}{2}m$ on the gap size is possible.

Our next result gives a bound on the magnitude of the labels of a die as a function of the size of the die.

Theorem 6. *No label on an m-sided die is larger than $m^2 - m + 1$.*

Proof. Let

$$P(x) = x^r + p_1 x^{r-n_1} + p_2 x^{r-n_2} + \cdots + p_s x^{r-n_s}$$

(where $p_i \neq 0$ for $i = 1, \ldots, s$) be a polynomial corresponding to an m-sided die. By Theorem 5, we know $n_1 \leq m$ and $(n_{i+1} - n_i) \leq m$ for all other i. Adding these successive gaps between labels, we obtain a sum that telescopes to $n_s \leq s \cdot m$. Since x divides $P(x)$ while x^2 does not, we have $r - n_s = 1$ and therefore $r \leq 1 + s \cdot m$. On the other hand,

$$m = P(1) = 1 + \sum_{i=1}^{s} p_i \geq 1 + s$$

so that $s \leq m-1$. Thus, $r \leq 1 + m(m-1)$ and the theorem is proved.

Our examples suggest that the bound on the largest label given in Theorem 6 is not a good one. It can be shown that when $m = p^k$, the largest label on an m-sided die is

$$1 + k(p-1)p^{k-1} = \frac{m \log m}{p \log p}(p-1) + 1,$$

and we conjecture that

$$\frac{m \log m}{2 \log 2} + 1$$

is actually an upper bound for the labels on an m-sided die for all m. Obviously, this bound, if correct, would be the best possible.

5. Results on game-size and the number of solution dice

For a fixed dice-size m, it would be nice to be able to predict, or at least bound, the game-size of a solution die and the number of solution dice as a function of m. In this section, we will give several results of this nature.

Theorem 7. *If the largest label on a die is L, then the game-size of the die is less than L.*

Proof. Write the polynomial P(x) corresponding to the die as

$$P(x) = x \prod_{\substack{d \mid m \\ d \neq 1}} \lambda_d(x)^{e_d}$$

and let n denote the game-size of $P(x)$. Since $\deg \lambda_d = \Phi(d)$,

$$1 + \sum_{\substack{d \mid m \\ d \neq 1}} \Phi(d) \cdot e_d = \deg P(x) = L$$

where $\Phi(d)$ is the Euler phi function of d. Thus,

$$\sum_{\substack{d \mid m \\ d \neq 1}} \Phi(d) e_d < L. \tag{1}$$

We wish to compare the sum given in (1) to the game-size n. Recalling that

$$\lambda_d(x) = \prod_{e \mid d} (x^{d/e} - 1)^{\mu(e)} = \frac{(x^d - 1)}{(x^{d/p} - 1) \cdots (x^{d/q} - 1)} \cdot \frac{(x^{d/p_1p_2} - 1) \cdots (x^{d/q_1q_2} - 1)}{(x^{d/p_1p_2p_3} - 1) \cdots (x^{d/q_1q_2q_3} - 1)} \cdots \tag{2}$$

where μ is the Möbius function and the p's and the q's are the distinct primes dividing d and letting $\omega(d)$ denote the number of distinct primes dividing d, we see that the number of terms in the numerator of (2) is

$$1+\binom{\omega(d)}{2}+\binom{\omega(d)}{4}+\cdots=\tfrac{1}{2}[(1+1)^{\omega(d)}+(1-1)^{\omega(d)}]=2^{\omega(d)-1}.$$

Therefore, if $P(x)=x\prod\lambda_d(x)^{e_d}$ is expanded using (2), the number of factors in the numerator is $\sum e_d\cdot 2^{\omega(d)-1}$. But the proof of Theorem 1 shows that if

$$P(x)=x\prod_{i=1}^{s}\left(\frac{x^{k_i}-1}{x^{l_i}-1}\right),$$

then the game-size n of $P(x)$ is at most s. It follows then that

$$n\leqslant\sum_{\substack{d\mid m\\ d\neq 1}} e_d\cdot 2^{\omega(d)-1}=\tfrac{1}{2}\sum_{\substack{d\mid m\\ d\neq 1}} 2^{\omega(d)}e_d. \tag{3}$$

Now, for any positive integer d,

$$\begin{aligned}2^{\omega(d)}=\prod_{p\mid d}2\leqslant 2\prod_{p\mid d}(p-1)&=2\prod_{p\mid d}p\cdot\prod_{p\mid d}\left(1-\frac{1}{p}\right)\\ &\leqslant 2d\cdot\prod_{p\mid d}\left(1-\frac{1}{p}\right)=2\Phi(d)\end{aligned} \tag{4}$$

Putting together (1), (3), and (4), we have

$$n\leqslant\tfrac{1}{2}\sum_{\substack{d\mid m\\ d\neq 1}} 2^{\omega(d)}e_d\leqslant\sum_{\substack{d\mid m\\ d\neq 1}}\Phi(d)e_d<L.$$

This completes the proof.

Theorems 6 and 7 together yield a bound on the game-size as a function of the dice-size.

Corollary 1. *A die with m labels has game-size at most m^2-m.*

Corollary 2. *There are only a finite number of solution dice with m sides.*

Proof. Theorems 1 and 7 show that any polynomial corresponding to an m-sided solution die must be a divisor of

$$x\left(\frac{x^m-1}{x-1}\right)^{m^2-m}.$$

The bound given in Corollary 1 of Theorem 7 is not at all sharp. For $m=30$, it says that the game-size of any solution die with 30 labels is at most 870. However, we conjecture that the maximum game-size for dice with 30 labels is actually 4. The next result gives a much sharper result for a certain large class of solution dice.

Theorem 8. *If a solution die $P(x)$ may be written*

$$P(x)=x\cdot\prod_{i=1}^{n}\left(\frac{x^{k_il_i}-1}{x^{l_i}-1}\right)$$

for some sets of integers $\{k_i\}$ and $\{l_i\}$, then the game-size of $P(x)$ is at most n. Moreover, if $P(x)$ can be written in the above form and if the prime-power decomposition of $m=P(1)$ is $m=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, then $n\leq\sum e_i$, giving an absolute bound on the game-size, knowing the dice size.

Proof. It suffices to produce $n-1$ polynomials satisfying the conditions of Theorem 1, such that the product of these polynomials and $P(x)$ is $x^n(x^m-1)^n/(x-1)^n$. We shall do this as in the proof of Theorem 1.

Since $P(x)$ is a solution die, we have from Theorem 1 that each k_il_i divides m. So, we define the polynomial

$$Q(x)=x^n\left(\frac{x^m-1}{x-1}\right)^n\Big/P(x)=x^{n-1}\prod\left(\frac{x^m-1}{x^{k_il_i}-1}\right)\cdot\left(\frac{x^{l_i}-1}{x-1}\right).$$

Repeatedly using the identity

$$\frac{x^{rst}-1}{x^r-1}=\frac{x^{rst}-1}{x^{rs}-1}\cdot\frac{x^{rs}-1}{x^r-1},$$

we may write this as

$$Q(x)=x^{n-1}\prod\left(\frac{x^{a_ip_i}-1}{x^{a_i}-1}\right)\qquad(*)$$

with each p_i prime.

Evaluating $(*)$ at $x=1$ gives $Q(1)=\prod p_i$. On the other hand,

$$P(1)\cdot Q(1)=x^n\left(\frac{x^m-1}{x-1}\right)$$

at $x=1$ is m^n, so $Q(1)=m^n/P(1)=m^{n-1}$.

Thus, $\prod p_i=m^{n-1}$, so that for each fixed prime p, the number of times $p_i=p$ in $(*)$ is

$$(n-1)\cdot(\text{number of times } p \text{ divides } m).$$

Therefore, we may partition the set of subscripts into $n-1$ subsets $S_1, S_2, \ldots S_{n-1}$ such that $\prod_{i \in S_j} p_i = m$ for each j. (This partition is unique only if $S = S_1$; i.e., if no partition is actually made!)

Define

$$Q_j(x) = \prod_{i \in S_j} \left(\frac{x^{a_i p_i} - 1}{x^{a_i} - 1} \right).$$

Then

$$Q_j(1) = \prod_{i \in S_j} p_i = m,$$

$$Q_j(x) = \prod_{i \in S_j} (1 + x^{a_i} + \cdots + x^{(p_i - 1)a_i})$$

is monic and has positive integral coefficients, and the roots of $Q_j(x)$ satisfy $x^{a_i p_i} - 1$ for some i, and, hence, $x^m - 1$. So we may use Theorem 1 to conclude that each $Q_j(x)$ actually corresponds to a die.

Moreover,

$$Q_1 \cdot Q_2 \cdot \cdots \cdot Q_{n-1} \cdot P = Q \cdot P = x^n \left(\frac{x^m - 1}{x - 1} \right)^n,$$

so that this set of dice actually constitutes an (n-dice) game; that is, the game-size of P is at most n.

The "moreover" part in the statement of the theorem follows from

$$\prod p_i^{e_i} = m = P(1) = x \cdot \prod^{n} \left(\frac{x^{k_i l_i} - 1}{x^{l_i} - 1} \right)_{\text{at } x=1} = \prod^{n} k_i,$$

so $n = \#$ factors $l_i \leq \#$ prime factors $p_i = \sum e_i$.

We remark that for certain m, for example p^k or pq, all solution dice may be written in the above form. However, among the 44 solution dice of size 30, there are four that can not be so written. Moreover, one of these has game-size 4, which is greater than $\sum e_i = 3$.

Note that for any m, if each of the $k_i l_i$ divides $m = P(1) = \prod k_i$, then by Theorem 1, the above polynomial does in fact give a solution die. This gives a method to generate many dice for each m.

The next theorem shows that there are dice with arbitrarily large game-size.

Theorem 9. *For any n, there are solutions dice of an n-dice game that are not solutions to any game with fewer than n dice. These dice can be chosen to have size p^n.*

Proof. For every $i \leq n$, let $P_i(x) = x(\lambda_{p^i}(x))^n$ for any prime p. Now $\lambda_{p^i}(x)$ has positive coefficients so $P_i(x)$ does, and $P_i(1) = p^n$ since $\lambda_{p^i}(1) = p$. Let $m = P_i(1)$. Then

$$P_1(x)P_2(x)\cdots P_n(x) = x^n(\lambda_p(x)\lambda_{p^2}(x)\cdots\lambda_{p^n}(x))^n$$
$$= x^n\left(\frac{x^m - 1}{x - 1}\right)^n$$

so that $P_1, P_2, \ldots, P_n$ taken together form an n-dice game. However, each P_i has roots of multiplicity n and so is not a factor of $(x^m - 1)^k/(x-1)^k$ for any $k < n$; that is, these dice are not solutions to a k-dice game for $k < n$.

Another general problem of interest is to find a formula for the number of solution dice of size m as a function of m or, more specifically, the prime-power decomposition of m. Again, this has already been done for $m = p, 2p, pq, p^2$. The next result handles the case where $m = p^k$.

Theorem 10. *There are exactly $\binom{2k-1}{k}$ solution dice of size p^k for all positive integers k and all primes p.*

Proof. Consider any polynomial of the form

$$P(x) = x \cdot \prod_{1 \leq i \leq k} (\lambda_{p^i}(x))^{e_i}.$$

By Theorem 1, $P(x)$ is the solution of a k-dice game if $P(1) = p^k$. Since $\lambda_{p^i}(1) = p$, we therefore have a one-to-one correspondence between the set of all solution polynomials $P(x)$ and the set of all n-tuples $(e_1, \ldots, e_k)$ such that $\sum e_i = k$. But, the number of such k-tuples is the same as the number of ways of putting k indistinguishable objects into i distinguishable boxes with $i = k$. This number is

$$\binom{k+i-1}{k-1} = \binom{2k-1}{k-1}.$$

Since the binomial coefficients are obviously unbounded, we have the following consequence of Theorem 10.

Corollary. *There exist integers m so that the number of dice of size m is arbitrarily large.*

The results obtained above for $m = p^n$ and $m = pq$ seem to suggest that the number of solution dice of size m may be a function of the prime-power structure of m alone and not the particular values of the primes themselves. We believe that this is true for the case $m = p^2q$ as well, but not true for the case $m = pqr$

(p, q, and r are distinct primes). For $m = p^2q$, we have shown that there always are at least 22 solution dice, and we conjecture that there are no more. On the other hand, we know there are at least 44 solution dice when $m = 30$ or 42; but for the general pqr case, we have only been able to establish the existence of 40. In fact, we conjecture that there are only 40 solution dice of size 105.

We conclude with a variation, which arose in a conversation with Roger Coleman, on the problem considered above. Given n and m, find n dice—not necessarily of size m or even the same size—so that these n dice yield the same probabilities as n standard dice of size m. For example, Coleman found that one die labelled 1, 1, 4, 4 and another labelled 1, 2, 2, 3, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 7, 7, 8 yield the same probabilities as an ordinary pair of cubes labelled 1 through 6.

Acknowledgements

The authors wish to express their gratitude to Kirby Stortz, Eric Anderson, and especially, Jon Grano for carrying out voluminous computer calculations.

References

[1] Martin Gardner, Mathematical games, Scientific American 238 (1978) 19–32.
[2] N. Jacobson, Basic Algebra I (W. H. Freeman, San Francisco, 1974).