MA294 Lecture

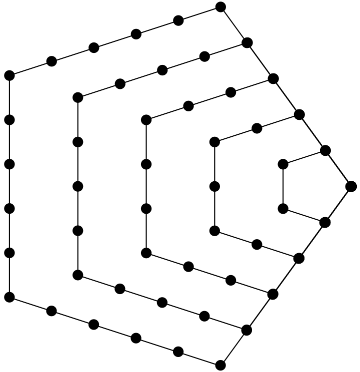
Timothy Kohl

Boston University

August 10, 2021

Pentagonal Numbers

Here is the origin of the 'Pentagonal Numbers' sequence we mentioned yesterday



which has the terms $1, 5, 12, 22, 35, 51, \ldots$, and in general $p_n = \frac{3n^2 - n}{2}$.

Applications of Partitions

The first application we shall explore has to do with probabilities, in particular, the distribution of outcomes from throwing two dice, say one red R and one green G.

What we are interested in is the possible sums one my obtain, given that $R \in \{1, 2, 3, 4, 5, 6\}$ and $G \in \{1, 2, 3, 4, 5, 6\}$.

As such $2 \leq R + G \leq 12$ so we may view the rolls as partitions of these numbers, which are restricted in that there are two parts.

We also label the dice two different colors to re-inforce the point that there is a distinction between $(R, G) = (2, 4)$ and $(R, G) = (4, 2)$ even though the sum in both cases is the same.

As such, this is not *exactly* a typical partition problem, but it does utilize many of the same tools as we used in the study of partitions and generating functions.

$G \downarrow \backslash R \rightarrow$	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

So the distribution is:

- $2 \rightarrow 1$
- $3 \rightarrow 2$
- $4 \rightarrow 3$
- $5 \rightarrow 4$
- $6 \rightarrow 5$
- $7 \rightarrow 6$
- $8 \rightarrow 5$
- $9 \rightarrow 4$
- $10 \rightarrow 3$
- $11 \rightarrow 2$
- $12 \rightarrow 1$

For a single die, the distribution is fairly simple, each number can appear just once so we can model this set of outcomes by the polynomial

$$D(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)$$

where each power represents an outcome of a single die, namely $\{1, 2, 3, 4, 5, 6\}$.

For two dice, since there are a finite number of outcomes (sums) and a finite number of parts, we can model this distribution using the polynomial:

$$
\begin{aligned}
(D(x))^2 &= (x + x^2 + x^3 + x^4 + x^5 + x^6)(x + x^2 + x^3 + x^4 + x^5 + x^6) \\
&= x^2 + 2x^3 + 3x^4 + 4x^5 + 5x^6 + 6x^7 \\
&+ 5x^8 + 4x^9 + 3x^{10} + 2x^{11} + x^{12}
\end{aligned}
$$

where the number of ways of achieving a given sum 's' is exactly the coefficient of x^s in $(D(x))^2$.

Indeed, in $(D(x))^2 = D(x)D(x)$ where the first factor is the 'red' die R, and the second corresponds to the 'green' die G.

Our question is, can we label the sides of two six sided dice with 'different' (positive) numbers say $R = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ and $G = \{b_1, b_2, b_3, b_4, b_5, b_6\}$ such that the resulting distribution of outcomes is identical?

We can answer this question using a similar polynomial. If we define

$$R(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}$$
$$G(x) = x^{b_1} + x^{b_2} + x^{b_3} + x^{b_4} + x^{b_5} + x^{b_6}$$

then what we want is to have $R(x)G(x) = (D(x))^2$ in that the coefficient of a given power is the number of ways of achieving that outcome (sum), viewed as an exponent.

Now, this does *not* mean that we try to expand out the product

$$R(x)G(x) = (x^{a_1}+x^{a_2}+x^{a_3}+x^{a_4}+x^{a_5}+x^{a_6})(x^{b_1}+x^{b_2}+x^{b_3}+x^{b_4}+x^{b_5}+x^{b_6})$$

and find conditions on the a_i and b_j to have it match $(D(x))^2$.

Note: It is possible that some of the a_i or b_j are repeated, i.e. one of the dice could have two sides with the same number of spots.

One fact we can ascertain is that since there are six, not necessarily distinct, terms in $R(x)$ and $G(x)$ then $R(1) = 6$ and $G(1) = 6$.

So how do we determine the possible choices for $R(x)$ and $G(x)$.

The key to this problem is the question of factorization.

So let's consider a specific class of rings relevant to this discussion.

This is a slight digression, but an interesting one, and we'll get back to the dice problem soon.

Definition

A integral domain R is a unique factorization domain (UFD) if for each non-unit $x \in R$, one may write

$$x = p_1 p_2 \cdots p_r$$

where the p_i are irreducible (i.e. cannot be factored) where the factorization is unique in that if

$$x = q_1 q_2 \cdots q_s$$

where the q_j are irreducible then $r = s$ and one may assume that $q_i = u_i p_i$ for units u_i for $i = 1, \ldots, r$.

That is, the irreducibles are 'associates' of one another. (i.e. each is a unit multiple of the other).

The most familiar example of a UFD is the integers $\mathbb{Z}$ where the irreducibles are exactly the prime numbers.

The factorization of 6 as $2 \cdot 3$ is unique, except for perhaps replacing 2 and 3 with -2 and -3 since $-2 = (-1)2$ and $-3 = (-1)3$ where -1 is the only other unit of $\mathbb{Z}$ (besides 1).

UFDs are of interest in number theory, besides just the example of $\mathbb{Z}$.

If d is an integer that is not divisible by the square of a prime then define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

for example $d = -1$ (whence $\sqrt{d} = \sqrt{-1} = i$) yields the so-called Gaussian Integers $\mathbb{Z}[i]$ which is a very important example of a UFD.

An example where this does **not** yield a UFD is the case of $\mathbb{Z}[\sqrt{-5}]$ where we have

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

is a factorization of 6 into irreducibles in two different ways, where $2, 3$ are not associates of $1 \pm \sqrt{-5}$.

Back to polynomials.

One of the other primary examples of a UFD is $\mathbb{Z}[x]$ which is relevant to our analysis of the dice example.

Namely that a polynomial like $(D(x))^2 \in \mathbb{Z}[x]$ is factorable into irreducible components, and since $(D(x))^2$ is monic, then so are the irreducible factors.

As is turns out

$$D(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 = x(x+1)(x^2+x+1)(x^2+x-1)$$

where $x, (x+1), (x^2+x+1), (x^2+x-1)$ are all irreducible, and like the way integers factor into unique prime power factors, so too is this factorization of $D(x)$ unique.

We have that

$$(D(x))^2 = x^2(x+1)^2(x^2+x+1)^2(x^2+x-1)^2$$

which equals $R(x)G(x)$.

As such, the irreducible factors of $R(x), G(x)$ lie in the set

$$\{x, (x+1), (x^2+x+1), (x^2+x-1)\}$$

which means that $R(x) = x^q(x+1)^r(x^2+x+1)^s(x^2+x-1)^t$ for some integers q, r, s, t.

So now,

$$\begin{aligned}R(x) &= x^q(x+1)^r(x^2+x+1)^s(x^2+x-1)^t\\ &\downarrow\\ G(x) &= x^{2-q}(x+1)^{2-r}(x^2+x+1)^{2-s}(x^2+x-1)^{2-t}\end{aligned}$$

So can we determine these values?

Yes, since $D(1) = 6$ then $(D(1))^2 = 36$ which means $R(1)G(1) = 36$ as well.

In particular

$$\begin{aligned}R(1) &= 1^q 2^r 3^s 1^t\\ G(1) &= 1^{2-q}2^{2-r}3^{2-s}1^{2-t}\end{aligned}$$

and, as observed earlier $R(1) = 6$ and $G(1) = 6$ which means $r = 1$ and $s = 1$, so that leaves q, t.

So we have established that

$$
\begin{aligned}
R(x) &= x^q(x+1)(x^2+x+1)(x^2+x-1)^t \\
G(x) &= x^{2-q}(x+1)(x^2+x+1)(x^2+x-1)^{2-t}
\end{aligned}
$$

and again $R(x)G(x) = (D(x))^2 = (x+x^2+x^3+x^4+x^5+x^6)^2$ which means $D(0) = 0$ so $(D(0))^2 = 0$ obviously.

As such $R(0)G(0) = 0$ which means at least one of the factors is 0, so assume $R(0) = 0$.

This implies that $q = 1$ *or* 2, however if $q = 2$ then $2 - q = 0$ which means $G(0) \neq 0$, but this implies that $G(x)$ has a constant term, which means the 'green' die has a face with no dots on it, which we don't allow.

Therefore $q = 1$ and $2 - q = 1$ so

$$R(x) = x(x+1)(x^2+x+1)(x^2+x-1)^t$$
$$G(x) = x(x+1)(x^2+x+1)(x^2+x-1)^{2-t}$$

so this leaves the choice for t (and $2 - t$), where $t = 0, 1, 2$.

If $t = 1$ we get

$$R(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$$
$$G(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$$

which corresponds to the usual dice labels.

However, if $t = 0$ we get

$$R(x) = x + 2x^2 + 2x^3 + x^4$$
$$G(x) = x + x^3 + x^4 + x^5 + x^6 + x^8$$

which means $R = \{1, 2, 2, 3, 3, 4\}$ and $G = \{1, 3, 4, 5, 6, 8\}$ (yes 8 !)

We note that if $t = 2$ then we simply exchange the two dice, i.e. $R(x) = x + x^3 + x^4 + x^5 + x^6 + x^8$ and $G(x) = x + 2x^2 + 2x^3 + x^4$. These non-standard dice, called Sicherman Dice, do indeed give the same distribution of sums:

$G \downarrow \backslash R \rightarrow$	1	2	2	3	3	4
1	2	3	3	4	4	5
3	4	5	5	6	6	7
4	5	6	6	7	7	8
5	6	7	7	8	8	9
6	7	8	8	9	9	10
8	9	10	10	11	11	12

as the usual dice:

$G \downarrow \backslash R \rightarrow$	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Probability Generating Functions

We can modify these polynomial generating functions to encode information about the probabilities of rolling a certain number (for one die) and sum for a pair of dice.

If we let $P(x) = \sum_{n=0}^{\infty} p_n x^n$ where $0 \leq p_n \leq 1$ is the probability of rolling a value of 'n' on a certain die (not necessarily six sided, or even a finite number of sides) then we have a function which actually *is* treated as a function.

In particular the basic tenets of probability also demand that $P(1) = 1$ as the likelihood of getting *some* number is 1. (i.e. each roll is a distinct event and so the probability for all the events viewed together is 1).

So this is a bit different type of generating function in that we do restrict the coefficients.

Note, if the die has only a finite number of sides (e.g. 6) then we have just a polynomial, where the coefficient in front of a power x^n is the probability of rolling that number on the die, which, if the die is fair, should be $\frac{1}{n}$.

We'll explore this more this in a moment.

We also note that if $P(x) = \sum_{n=0}^{\infty} p_n x^n$ then the average or 'expectation value' is $P'(1)$. Why?

Well

$$
\begin{aligned}
P(x) &= \sum_{n=0}^{\infty} p_n x^n = p_0 + p_1 x + p_2 x^2 + \dots \\
&\downarrow \\
P'(x) &= \sum_{n=1}^{\infty} n p_n x^{n-1} = p_1 + 2p_2 x + 3p_3 x^2 + \dots \\
&\downarrow \\
P'(1) &= p_1 + 2p_2 + 3p_3 + \dots
\end{aligned}
$$

which is the sum over the terms '(outcome)x(probability of that outcome)' which is the expectation value, i.e. average.

For the case of the normal six sided die, we have

$$
\begin{aligned}
P(x) &= \frac{1}{6}x + \frac{1}{6}x^2 + \frac{1}{6}x^3 + \frac{1}{6}x^4 + \frac{1}{6}x^5 + \frac{1}{6}x^6 \\
&\downarrow \\
P'(x) &= \frac{1}{6} + \frac{1}{6}2x + \frac{1}{6}3x^2 + \frac{1}{6}4x^3 + \frac{1}{6}5x^4 + \frac{1}{6}6x^5 \\
&\downarrow \\
P'(1) &= \frac{1}{6} + \frac{1}{6}2 + \frac{1}{6}3 + \frac{1}{6}4 + \frac{1}{6}5 + \frac{1}{6}6 \\
&= \frac{1}{6}\frac{6\cdot 7}{2} \\
&= 3.5
\end{aligned}
$$

which is a bit jarring until you realize this is just the average of the numbers $\{1,2,3,4,5,6\}$.

This line of reasoning also covers the case of two six sided dice.

In this case we can multiply $P(x) = \frac{1}{6}x + \frac{1}{6}x^2 + \frac{1}{6}x^3 + \frac{1}{6}x^4 + \frac{1}{6}x^5 + \frac{1}{6}x^6$ by itself to obtain

$$
\begin{aligned}
P(x)^2 = \frac{1}{36}x^2 + \frac{2}{36}x^3 + \frac{3}{36}x^4 + \frac{4}{36}x^5 + \frac{5}{36}x^6 + \frac{6}{36}x^7 \\
+ \frac{5}{36}x^8 + \frac{4}{36}x^9 + \frac{3}{36}x^{10} + \frac{2}{36}x^{11} + \frac{1}{36}x^{12}
\end{aligned}
$$

where the coefficients represent the outcomes of the different 'events', in this case the possible sums from rolling the two dice.

Indeed, if we consider the numerators of the coefficients in $P(x)^2$

$$\frac{1}{36}x^2 + \frac{2}{36}x^3 + \frac{3}{36}x^4 + \frac{4}{36}x^5 + \frac{5}{36}x^6 + \frac{6}{36}x^7$$
$$+ \frac{5}{36}x^8 + \frac{4}{36}x^9 + \frac{3}{36}x^{10} + \frac{2}{36}x^{11} + \frac{1}{36}x^{12}$$

we see the synchrony between these values and the distribution of sums for all 36 possible outcomes:

$G \downarrow \backslash R \rightarrow$	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Indeed this idea is true in general, if $P(x)$ and $Q(x)$ are probability generating functions for independent random variables (e.g. two distinct dice) then their product $P(x)Q(x)$ is the probability generating function for the combination of the two events.

The analogy is to the rule in probability that if A and B are independent events then $P(A\ and\ B) = P(A \cap B) = P(A) \cdot P(B)$.

Enumerating Finite Abelian Groups

We can use partitions to determine the number of abelian groups of a given order.

The first basic fact is the following.

Proposition

If G is a finite abelian group and $|G| = ab$ where $gcd(a, b)$ then there exists groups A and B such that $G \cong A \times B$, where $|A| = a$ and $|B| = b$.

One can actually define A and B as subgroups of G itself.

Let $A = \{g \in G \mid g^b = e\}$ and $B = \{g \in G \mid g^a = e\}$. These are both clearly subgroups of G, and if $z \in A \cap B$ then $|z|$ divides a and $|z|$ divides b but since $gcd(a, b) = 1$ this means $|z| = 1$ so $z = e$.

This implies that (literally) $G = AB = \{xy \mid x \in A; y \in B\}$. How?

If $z \in G$ then $z^{ab} = e$ which means $(z^a)^b = e$ and $(z^a)^b = e$ so $z^a \in A$ and $z^b \in B$.

Since $gcd(a, b) = 1$ there exists m, n such that $ma + nb = 1$ so let $x = z^{nb} = (z^a)^m \in A$ and $y = z^{na} = (z^b)^n \in B$.

Moreover $xy = z^{nb+ma} = z^1 = z$ so $z \in AB$, ergo $G = AB$.

Lastly we note (which we leave as an exercise) that $AB \cong A \times B$ so $G \cong A \times B$

So what this means for a finite abelian group G is that, if $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ for distinct primes p_i, then there exists groups (actually subgroups) $G_1, G_2, \ldots, G_k$ where $|G_i| = p_i^{n_i}$ such that

$$G \cong G_1 \times G_2 \times \cdots \times G_k$$

The remaining issue is to look at the structure of the individual (sub)groups G_i or order p^{n_i}.

Theorem

If G is an abelian group of order p^n where p is a prime then there exists integers $e_1, e_2, \ldots, e_t$ such that $G \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_t}}$ where $e_1 + e_2 + \cdots + e_t = n$, and each distinct paritition gives rise to a distinct abelian group.

The proof of this is not exceedingly difficult, but we won't go through it here.

The key observation though is that this 'decomposition' of G into a direct product of cyclic groups corresponds to a partition $\lambda = (e_1, e_2, \ldots, e_t)$ of n and the other important observation is that if one has two different partitions of n, $\lambda = (e_1, \ldots, e_t)$ and $\lambda' = (e'_1, e'_2, \ldots, e'_s)$ then the resulting groups are **not** isomorphic to each other.

The bottom line is this.

Corollary

For each $n \geq 1$ there $\mathcal{P}(n)$ distinct (i.e. non-isomorphic) abelian groups of order p^n.

So if $N = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ (for distinct primes p_i) there are exactly

$$\mathcal{P}(n_1) \cdot \mathcal{P}(n_2) \cdots \mathcal{P}(n_t)$$

abelian groups of order N, and what is rather interesting is that this number is only dependent on the exponents $n_1, \ldots, n_t$ and not on the primes p_i.

For example, the groups of order $540 = 2^2 \cdot 3^3 \cdot 5$ are

- $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

Partitions and Cycle Structure

Recall the problem of determining the possible orders of elements in S_n for a given n.

This is fundamentally tied to the partitions of n.

For example, in S_6, the partition $\lambda = (3, 3)$ corresponds to a product of two $3 - cycles$, for example $(1, 4, 5)(2, 3, 6)$ or $(1, 2, 3)(4, 6, 5)$, the elements in the cycles being less important than the length of the cycles corrsponding directly to the parts in the summand.

Specifically, if $\lambda = (i_1, i_2, \ldots, i_k)$ then one may find a product of cycles of lengths $i_1 \ldots i_k$ where one views a 1-cycle, e.g. (i_t) as the identity.

Recall that a 1-cycle is basically the identity, which is fine.

For example, for $n = 7$ if $\lambda = (3, 2, 1, 1)$ then a corresponding product of cycles in S_7 is, for example

$$(1, 2, 3)(4, 5)(6)(7)$$

which is operationally the same as $(1, 2, 3)(4, 5)$ but what is most useful is that the order calculation works out the same, since, for example

$$|(1, 2, 3)(4, 5)(6)(7)| = lcm(3, 2, 1, 1) = 6$$

as compared to

$$|(1, 2, 3)(4, 5)| = lcm(3, 2) = 6$$

since the order of each 1-cycle is 1 which is the order of I, which is consistent with our view of a 1-cycle as being the same as the identity.

So the main point of this discussion is that partition of n correspond to the possible cycle structure of elements in S_n and vice versa.

And with the knowledge of the partitions of n we have therefore a way of enumerating the orders of elements, namely $\lambda = (i_1, i_2, \ldots, i_k)$ corresponds to $lcm(i_1, i_2, \ldots, i_k)$.