WON Series in Discrete Mathematics and Modern Algebra Volume 7

FINITE ABELIAN GROUPS

Amin Witno

Abstract

We detail the proof of the fundamental theorem of finite abelian groups, which states that every finite abelian group is isomorphic to the direct product of a unique collection of cyclic groups of prime power orders. We briefly discuss some consequences of this theorem, including the classification of finite abelian groups of a given order.

These notes are presented in conjunction with a supplementary lecture in the Abstract Algebra 1 course (Math 342) at Philadelphia University, Jordan. The contents herein are structured in a way suitable as an independent reading project for students of group theory. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.[1]

What is direct product?

Let A and B be two arbitrary groups, not necessarily with the same binary operations. We define the *direct product* of A and B to be

$$A \times B = \{(a,b) \mid a \in A,\, b \in B\}$$

This two-dimensional set is again a group if we consider the operation where for every two elements $(a,b),(c,d) \in A \times B$, we set $(a,b)(c,d) = (ac, bd)$.

In some texts, our definition of direct product may be introduced by the name *external* direct product. You will soon see why the adjective is added, but first let us observe some elementary facts which are not hard to verify and which are intuitively clear anyhow.

Proposition 1. The following properties hold which concern the direct product of groups.

1. The commutative property: $A \times B \simeq B \times A$. Think of swapping places between the components; doing so does not affect the structure of the group.

Last Revision: 21–05–2012 awitno@gmail.com

2. The associative property: $A \times (B \times C) \simeq (A \times B) \times C$. This allows us to simply write multiple products without brackets, e.g., $A \times B \times C$.

3. The substitution property: If $A \simeq A'$ and $B \simeq B'$, then $A \times B \simeq A' \times B'$.

4. The cancellation property: If $A \simeq A'$ and $A \times B \simeq A' \times B'$, then $B \simeq B'$.

5. The identification property: We may treat the group A as a subgroup of $A \times B$ by identifying A with the subgroup $A \times \{e\}$, where e denotes the identity element. Of course, by symmetry, we may also call the coordinate B a subgroup of $A \times B$, i.e., $\{e\} \times B$.

Another result which we have not discussed in class is the useful criterion for expressing an arbitrary group as a direct product of its subgroups.

Theorem 2. Let G be a group with two normal subgroups H and K, with the conditions that $H \cap K = \{e\}$ and $HK = G$. Then $G \simeq H \times K$.

We remark first that we will be concerned with only abelian groups, where all subgroups are automatically normal.

The hypothesis of Theorem 2 is sometimes used as the definition of G being the *internal direct product* of H and K. In other words, Theorem 2 states that internal implies external. Conversely, given $G = H \times K$, we have two normal subgroups, i.e., $H \times \{e\} \simeq H$ and $\{e\} \times K \simeq K$, whose internal direct product recovers G. Hence, the two notions of external and internal direct products are actually equivalent.

Proof. We first show that every element of H commutes with any other of K. Let $h \in H$ and $k \in K$. We note that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$ because K is normal, and similarly $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$. However, $H \cap K = \{e\}$, so we see that $hkh^{-1}k^{-1} = e$, i.e., that $hk = kh$.

This result opens the way for a homomorphism $\theta : H \times K \to HK$ defined by $\theta(h, k) = hk$. As we can check,

$$\theta((h, k)(h', k')) = \theta(hh', kk') = hh'kk' = hkh'k' = \theta(h, k)\theta(h', k')$$

Since $HK = G$, we are only left with showing that θ is one-to-one and onto. Well, onto is quite obvious by the very definition of HK. For one-to-one, let $\theta(h, k) = \theta(h', k')$, so that $hk = h'k'$. Then $h^{-1}h' = k(k')^{-1}$. The left side belongs to H and the right to K. This is possible only if both be the identity element. Thus $h = h'$ and $k = k'$, completing the proof. ▽

To make the result complete, we need to extend Theorem 2 inductively to three or more subgroups. This is your exercise, and to help you with the induction step, why don't you start off with three subgroups.

Exercise 3. Let G be a group with three normal subgroups H, K, and L, such that $H \cap K = \{e\}$, $HK \cap L = \{e\}$, and $HKL = G$. Prove that $G \simeq H \times K \times L$.

The fundamental theorem

The fundamental theorem essentially states that every finite abelian group is isomorphic to a direct product of cyclic groups. Recall that every cyclic group of order n is given by the modular integers $\mathbb{Z}_n$ under addition mod n. Hence, to illustrate, an abelian group of order 1200 may actually be isomorphic to, say, the group $\mathbb{Z}_{40} \times \mathbb{Z}_6 \times \mathbb{Z}_5$.

Furthermore, let us recall the Chinese remainder theorem, which we shall abbreviate CRT, and which says that if $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. In the preceding example, we may then replace $\mathbb{Z}_{40}$ by $\mathbb{Z}_{2^3} \times \mathbb{Z}_5$, and $\mathbb{Z}_6$ by $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Therefore, we will state the fundamental theorem like this: every finite abelian group is the product of cyclic groups of prime power orders. The collection of these cyclic groups will be determined uniquely by the group G. Here is why.

Suppose we have two direct products of order 1200, e.g.,

$$\begin{aligned} A &= \mathbb{Z}_{2^3} \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ B &= \mathbb{Z}_{5^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \end{aligned}$$

It is easy to see why $A \not\simeq B$: the group A has an element of order 8, i.e., $(1, 0, 0, 0, 0)$. On the other hand if $(a, b, c, d) \in B$, then $(a, b, c, d)^m = (0, 0, 0, 0)$ where m is the least common multiple of 25, 4, and 3. Since m is not a multiple of 8, we conclude that there is no elements of order 8 in B.

In general, to show that such isomorphism is impossible, simply take any prime factor p for which there is a discrepancy between left and right. Say, $\mathbb{Z}_{p^j}$ and $\mathbb{Z}_{p^k}$ be the maximal components of A and B, respectively, with $j > k$. (If $j = k$, the cancellation property allows us to omit the factor $\mathbb{Z}_{p^k}$ and start over with the rest.) Then A would have an element of order p^j, whereas B would not, so the two can't possibly be the same groups.

Hence, we will now formally state the fundamental theorem of finite abelian groups, abbreviated FTFAG, as follows.

Theorem 4 (FTFAG)**.** Every finite abelian group is isomorphic to the direct product of a unique collection of cyclic groups, each having a prime power order.

To remark, by the word *collection* used in the theorem, we mean a multiset, i.e., where repetition of elements is allowed but ordering them is not important.

Elements of the proof

The uniqueness part in statement of FTFAG is already explained. To make the proof more readable, we go by step-by-step observations. As a matter of fact, the first one is an easy exercise for you to warm up before the long journey.

Exercise 5. Let G be a group with identity element e and a normal subgroup H, and let $x \in G$. Suppose that the element Hx has order n in the factor group G/H. Then x has order in G a multiple of n.

The truth is, the preceding exercise is needed to establish the next result, which is actually the famous Cauchy's theorem applied to abelian groups. We talk about Cauchy's theorem in the lecture but did not get to really prove it, so we have no choice but to buy the theorem right here.

Theorem 6 (Cauchy)**.** Let p be a prime number. If any abelian group G has order a multiple of p, then G must contain an element of order p.

Proof. Let $|G| = kp$ for some $k \geq 1$. In fact, the claim is true if $k = 1$ because any group of prime order is a cyclic group, and in this case any non-identity element will have order p. We proceed by induction. Take any non-identity element $x \in G$, say of order m. We are done if p divides m, for then $x^{m/p}$ will have order p. Otherwise, consider the factor group $G' = G/\langle x \rangle$, of order $|G'| = kp/m$. Since m is not a multiple of p, we may write $|G'| = jp$ for some $j < k$. We apply the induction hypothesis to conclude that G' contains an element of order p. According to the preceding exercise, then G contains an element of order a multiple of p, and that suffices. ▽

Lemma 7. Let G be an abelian group with identity e. For a fixed positive integer n, the set $H = \{x \in G \mid x^n = e\}$ is a subgroup of G.

Proof. If $a \in H$, so is $a^{-1} \in H$ since $(a^{-1})^n = (a^n)^{-1} = e$. Moreover, if $a, b \in H$ then being abelian, $(ab)^n = a^n b^n = e$ and $ab \in H$. Thus H passes the subgroup test. ▽

Now in order to conveniently refer to this subgroup H stated in the lemma, we shall give it a special notation.

Definition. Let G be an abelian group with identity e and let n be a fixed positive integer. We define the subgroup $G(n)$ of G by $G(n) = \{x \in G \mid x^n = e\}$.

Lemma 8. Suppose that $\gcd(m, n) = 1$, and let G be an abelian group of order mn. Then $G \simeq G(m) \times G(n)$.

Proof. To establish this lemma, we will employ Theorem 2, showing that $G(m)G(n) = G$ and $G(m) \cap G(n) = \{e\}$. The second part is easy: if $x \in G(m)$ then the order of x in G must divide m, and similarly with n in place of m. With $\gcd(m, n) = 1$, we see that $G(m) \cap G(n)$ contains only elements of order one, i.e., only the identity element.

Next, note that for every $x \in G$, we have $x^m \in G(n)$ because $(x^m)^n = x^{|G|} = e$. And similarly, $x^n \in G(m)$. Now $\gcd(m, n) = 1$ also implies that we can find $a, b \in \mathbb{Z}$ such that $1 = am + bn$. Then for every $x \in G$, we have

$$x = x^{am+bn} = (x^m)^a (x^n)^b \in G(n)G(m)$$

This establishes the claim that $G(m)G(n) = G$. ▽

Lemma 9. Suppose that $\gcd(m, n) = 1$, and let G be an abelian group of order mn. Then $|G(m)| = m$ and $|G(n)| = n$.

Proof. We already have $G \simeq G(m) \times G(n)$. The case $m = 1$ would be trivial, for then $G(m) = \{e\}$. So we assume there is a prime p which divides m. We claim that $|G(n)|$ is not a multiple of p, for otherwise by Cauchy's theorem, $G(n)$ would contain an element of order p. It would follow by the definition of $G(n)$ that p would divide n, which is impossible as m and n have no common factors. By symmetry, we also conclude that if a prime q divides $G(n)$, then q does not divide $G(m)$. However, we know that $|G(m)| \times |G(n)| = mn$. Hence by factoring mn into prime numbers, we see why it is necessary to have $|G(m)| = m$ and $|G(n)| = n$. ▽

The preceding two lemmas can be easily extended to three or more subgroups. If n is expressed as the product of distinct prime powers,

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

and if G is an abelian group of order n, then

$$G \simeq G(p_1^{e_1}) \times G(p_2^{e_2}) \times \cdots \times G(p_k^{e_k})$$

where each $|G(p_i^{e_i})| = p_i^{e_i}$. Thus, we will now establish FTFAG by showing just one more fact: that every abelian group of a prime power order is a direct product of cyclic groups, each having a prime power order.

Lemma 10. Let p be a prime number and let G be an abelian group of order p^k, for any integer $k \geq 1$. Then G is isomorphic to the direct product of cyclic groups.

Note that the cyclic groups satisfying the statement of the lemma will, of necessity, each have order a power of p.

Proof. We use induction on k. The case $k = 1$ gives a cyclic group G of order p, so there is nothing to prove. Otherwise, since there is only one prime involved, we may find an element $g \in G$ of order p^m, such that $x^{p^m} = e$ for all $x \in G$. Moreover, let H be a subgroup of G which is maximal with respect to the condition $\langle g \rangle \cap H = \{e\}$. We will show that $\langle g \rangle H = G$, so that $G \simeq \langle g \rangle \times H$. Then the proof will complete by applying the induction hypothesis on H since H itself is an abelian group of order a power of p, but less than that of G.

By contradiction, suppose there exists $c \in G$, but $c \notin \langle g \rangle H$. We may assume that $c^p \in \langle g \rangle H$, for if not, simply replace c by c^p. And if still $c^{p^2} \notin \langle g \rangle H$, replace c^{p^2} by c^{p^3}, etc. This process will not take more than m steps.

We may write $c^p = g^r h$, for some $h \in H$. Since $(c^p)^{p^{m-1}} = e$, we have $g^{rp^{m-1}} \in H$, and so $g^{rp^{m-1}} = e$ by the condition $\langle g \rangle \cap H = \{e\}$. In particular, g^r does not generate $\langle g \rangle$. It follows that $\gcd(r, p^m) > 1$, i.e., that p divides r.

Now let $s = -r/p$, and consider the subgroup K of G given by $K = \langle cg^s \rangle H$. We note that $cg^s \notin H$ because $c \notin \langle g \rangle H$. Thus, H is a proper subgroup of K. We will finish the proof by showing that $\langle g \rangle \cap K = \{e\}$, which contradicts the maximal choice of the subgroup H.

Every element $y \in K$ is of the form $y = (cg^s)^t h_2$ for some $h_2 \in H$. Since

$$(cg^s)^p = c^p (g^{-r/p})^p = c^p g^{-r} = h \in H$$

we note that if t is a multiple of p, then $y \in H$. In that case, we have that $y \notin \langle g \rangle$ unless $y = e$. On the other hand, suppose now $\gcd(t, p) = 1$. Then there exist $u, v \in \mathbb{Z}$ such that $tu = 1 + pv$. (Think of elements of the multiplicative group U_p.) It follows that

$$y^u = (cg^s)^{tu} h_2^u = (cg^s)^{1+pv} h_2^u = (cg^s)(cg^s)^{pv} h_2^u = (cg^s) h^v h_2^u$$

So if $y \in \langle g \rangle$, then $c \in \langle g \rangle H$, which is false. We have therefore shown that the only element in $\langle g \rangle \cap K$ is the identity. ▽

Consequences of FTFAG

The fundamental theorem readily gives us a means to the classification of all finite abelian groups according to their orders. We illustrate first with three examples.

1. The group $U_{12} = \{1, 5, 7, 11\}$ under multiplication mod 12 is not cyclic. By FTFAG, there are only two abelian groups of order 4, i.e., $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. We conclude that $U_{12} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. The group U_{60} has $\phi(60) = 16$ elements. There are five abelian groups of order 16, i.e.,

$$\begin{aligned} G_1 &= \mathbb{Z}_{2^4} \\ G_2 &= \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \\ G_3 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \\ G_4 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ G_5 &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \end{aligned}$$

Meanwhile, we look at the order $|x|$ for each element $x \in U_{60}$, i.e.,

x	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
$\lvert x\rvert$	1	4	2	4	4	2	4	2	2	4	2	4	4	2	4	2

Since we have elements of order 4, but not 8, we rule out G_1, G_2, and G_5. Whereas for G_3, only three elements have order 2, i.e., $(0, 2), (2, 0)$, and $(2, 2)$. Therefore, we go with G_4—thus $U_{60} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Consider the group U_{63} of order $\phi(63) = 36$, again not cyclic. There are four abelian groups of this order:

$$\begin{aligned} G_1 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \simeq \mathbb{Z}_{36} \\ G_2 &= \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\ G_3 &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \\ G_4 &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \end{aligned}$$

And again, we look at the table of orders in U_{63} and find only elements of orders 1, 2, 3, and 6. There is no doubt, $U_{63} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ($\simeq \mathbb{Z}_6 \times \mathbb{Z}_6$).

(Here is another way to study the orders in U_{63} in a glance. The group U_7 has order 6, hence $x^6 \equiv 1 \pmod 7$ for all integers x with $\gcd(x, 7) = 1$. Similarly, $x^6 \equiv 1 \pmod 9$ if $\gcd(x, 9) = 1$, because U_9 too has order 6. Since $\gcd(7, 9) = 1$, CRT applies and $x^6 = 1$ for all $x \in U_{63}$. This explains why the order of every element in U_{63} must divide 6.)

Exercise 11. For each given n, identify the group U_n by writing it as the direct product of cyclic groups of prime power orders.

(a) $n = 27$ (b) $n = 32$ (c) $n = 45$ (d) $n = 72$

An interesting question follows: Given a positive integer n, how do we determine the number of distinct abelian groups of order n? We can see in the three examples above a pattern that plays on the exponent of each prime appearing in the factorization of n. For example, the case $n = 16 = 2^4$ relies completely upon the different ways we partition the exponent 4 into positive integers. This leads us to the following definition.

Definition. Where n ranges through the positive integers, define the *partition function* $p(n)$ to stand for the number of different partitions of n into positive integers.

For instance $p(4) = 5$, having seen the five ways we can partition 4, i.e.,

$$\begin{aligned} 4 &= 4 \\ 4 &= 3 + 1 \\ 4 &= 2 + 2 \\ 4 &= 2 + 1 + 1 \\ 4 &= 1 + 1 + 1 + 1 \end{aligned}$$

This function enables us to better express the number of distinct abelian groups of a given order, as follows.

Theorem 12. *Let n denote a positive integer which factors into distinct prime powers, written $n = \prod p_k^{e_k}$. Then there are exactly $\prod p(e_k)$ distinct abelian groups of order n.*

In particular, when n is square-free, i.e., all $e_k = 1$, then there is a unique abelian group of order n given by $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$, which is just the cyclic group $\mathbb{Z}_n$, if we may borrow CRT again.

Exercise 13. Count how many distinct abelian groups of the given order n.
(a) $n = 1024$ (b) $n = 27000$ (c) $n = 30030$ (d) $n = 31104$

The next observation will lead to an alternate but equivalent form in which FTFAG can be presented. Let's say we work with the group

$$G = \mathbb{Z}_{2^4} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^3} \times \mathbb{Z}_{5^3} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

Let us write out these prime powers in matrix format, one row for each prime base, left-justified, ordered from the greatest exponent to the least, as follows.

$$\begin{array}{llll} 2^4 & 2^2 & 2 & \\ 3 & 3 & & \\ 5^3 & 5^3 & 5 & 5 \\ 7 & & & \end{array}$$

Observe that every column consists of distinct prime powers. As you probably have guessed, we then apply CRT columnwise, to conclude that

$$G \simeq \mathbb{Z}_{42000} \times \mathbb{Z}_{1500} \times \mathbb{Z}_{10} \times \mathbb{Z}_5$$

Now going from left to right, the columns successively lose some primes without ever gaining new ones. Hence, the sequence of the cyclic group orders, e.g., $42000, 1500, 10, 5$, consists of successive divisors—each number divides the preceding number. In other words, the direct product is now made up of nested cyclic subgroups, since each factor can be viewed as a subgroup of the preceding one. Thus, we state FTFAG alternately in this second form. Again, you can easily supply the proof for uniqueness.

Theorem 14 (FTFAG2)**.** *Every finite abelian group is isomorphic to the direct product of a unique collection of cyclic groups of the form $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, with the condition that each n_i is a multiple of n_{i+1} for $0 < i < k$.*

Exercise 15. Prove that if a group G is expressible as a direct sum such as described in FTFAG2, then the cyclic group factors are uniquely determined by G.

Another useful consequence of FTFAG is a statement concerning the subgroups of an abelian group. The result is somewhat an extension of Cauchy's Theorem 6. We will make this observation our last one for now.

Theorem 16. *Let m be any positive integer and let G be an abelian group of order a multiple of m. Then there exists a subgroup of G which has order m.*

We give first an illustration of this claim which will also serve as a model for writing the proof of Theorem 16. Suppose that G is a group of order 1,120,210,560, given by

$$G = \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_{7^3} \times \mathbb{Z}_7$$

This big number is a multiple of 6048; how do we find a subgroup of order 6048? First, we look at the factorization of 6048, i.e., $6048 = 2^5 \times 3^3 \times 7$. Then we select the cyclic group factors of G corresponding to these prime factors, i.e., 2, 3, 7, largest exponent first, just enough to exceed 2^5, 3^3, and 7. If necessary, we will take a subgroup of the cyclic group in order to match the total exponent that we need for each prime.

$$\begin{array}{ccccccccc} 2^3 & 2^3 & 2 & 3^2 & 3^2 & 3^2 & 5 & 7^3 & 7 \\ | & | & & | & | & & & | & \\ 2^3 & 2^3 & & 3^2 & 3^2 & & & 7^3 & \\ & | & & & | & & & | & \\ & 2^2 & & & 3 & & & 7 & \end{array}$$

In this way, the desired subgroup of order 6048 comes out to be

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_3 \times \mathbb{Z}_7$$

Note that we have freely used the fact that every cyclic group has a (unique) subgroup of order any number that divides the order of the group.

Exercise 17. Now write the proof of Theorem 16.

A bit more partitions

The partition function $p(n)$ is a fruitful topic in advanced number theory. It will not do justice, and rather out of place, if we attempt to write a short chapter on partitions simply because we encounter $p(n)$ in discussing finite abelian groups. Nevertheless, we just want to mention a few results which more or less relate to the evaluation of $p(n)$.

We inspect that $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, \ldots$ up to $p(10) = 42$. The sequence then increases quite rapidly, exceeding one million partitions with mere $n = 61$. In fact, the growth of $p(n)$ is known to be sub-exponential and, more specifically, $p(n)$ is asymptotically close to the function

$$P(n) = \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$$

What we mean is that $\lim \frac{P(n)}{p(n)} = 1$ as $n \to \infty$. For example, $P(10^4) \approx 36.32 \times 10^{105}$, and that is roughly how big $p(10,000)$ is.

In dealing with a rapidly growing sequence like $p(n)$, one would hope to find a recurrence relation of some sort. With $p(n)$, there is no explicit way to define a recurrence relation, but we may get help from the so-called intermediate partition functions.

Definition. Let $p_k(n)$ denote the number of partitions of n into positive integers, each no smaller than k, where $1 \le k \le n$. In particular, $p_1(n) = p(n)$.

Note that the partitions belonging to $p_{k+1}(n)$ form a subset of those belonging to $p_k(n)$. Moreover, if a partition belongs to $p_k(n)$ but not to $p_{k+1}(n)$, then the partition must be composed of a k term plus another partition belonging to $p_k(n-k)$, and vice versa. We express this relation into the following identity.

$$p_k(n) = p_{k+1}(n) + p_k(n-k) \tag{1}$$

This is our recurrence relation. To start off, note that $p_k(n) = 1$ whenever $n/2 < k \le n$ as it is impossible to partition n into two or more terms each of which is larger than half of n. We then build a table, rows for n and columns for k, and start filling in by rows according to (1), right to left, with the right half all 1's. The leftmost entry is what we are after, i.e., $p_1(n) = p(n)$. For convenience, we omit the terms $p_k(n) = 0$ which apply when $k > n$.

n	$p(n)$	$p_2(n)$	$p_3(n)$	$p_4(n)$	$p_5(n)$	$p_6(n)$	$p_7(n)$	$p_8(n)$	$p_9(n)$	$p_{10}(n)$
1	1									
2	2	1								
3	3	1	1							
4	5	2	1	1						
5	7	2	1	1	1					
6	11	4	2	1	1	1				
7	15	4	2	1	1	1	1			
8	22	7	3	2	1	1	1	1		
9				2	1	1	1	1	1	
10					2	1	1	1	1	1

To make yourself familiar with the recursive pattern, try to complete the remaining two rows, beginning with $p_3(9) = p_4(9) + p_3(9-3)$, and make sure you end with $p(10) = 42$.

Exercise 18. Extend this table until you find $p(20)$. Moreover, note and prove an alternate recurrence relation given by $p(n) = 1 + \sum p_k(n-k)$, where the sum ranges over k in the interval $1 \le k \le n/2$.

As a final remark, we mention that the partition function $p(n)$ can also be expressed in its generating function, i.e.,

$$\sum_{n=0}^{\infty} p(n)\, x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^n}$$

by setting $p(0) = 1$. To see this identity, note that each factor appearing on the right hand side is the expression for the sum of geometric series, i.e.,

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)\cdots$$

Hence, the coefficient of x^n is composed of how many 1's (from the first bracket), 2's (second bracket), 3's (third), etc., whose sum is n. The number of such combinations is just the number of ways we partition n into positive integers, thus $p(n)$.

Generating functions can sometimes be used to derive identities involving restricted partitions. For example, the generating function for $p_k(n)$ is given by

$$\sum_{n=0}^{\infty} p_k(n)\, x^n = \prod_{n=k}^{\infty} \frac{1}{1-x^n}$$

Then we could have established our recurrence relation (1) in this way:

$$\begin{aligned}
\sum_{n=0}^{\infty} p_{k+1}(n)\, x^n + \sum_{n=k}^{\infty} p_k(n-k)\, x^n &= \prod_{n=k+1}^{\infty} \frac{1}{1-x^n} + x^k \sum_{m=0}^{\infty} p_k(m)\, x^m \\
&= (1-x^k) \prod_{n=k}^{\infty} \frac{1}{1-x^n} + x^k \prod_{n=k}^{\infty} \frac{1}{1-x^n} \\
&= (1-x^k+x^k) \prod_{n=k}^{\infty} \frac{1}{1-x^n} \\
&= \sum_{n=0}^{\infty} p_k(n)\, x^n
\end{aligned}$$

Obviously, the combinatorial proof of (1) is much shorter and clean. Nevertheless, there are times when generating functions may seem to be the better approach—but that is another lecture series.

Exercise 19. Using generating functions, show that the number of partitions of n into odd positive integers equals the number of partitions of n into distinct positive integers.