Mathematics for Computer Scientists

Lecture notes for the module G51MCS

Venanzio Capretta
University of Nottingham
School of Computer Science

Chapter 6

Modular Arithmetic

6.1 Pascal's Triangle

One easy way to compute the binomial coefficients is by building *Pascal's triangle*. It is a triangular table containing in row n the values of $\binom{n}{k}$ for all possible values of k:

$n=$							
0				1			
1			1		1		
2		1		2		1	
3	1		3		3		1
4		1		4		6		4		1
5	1		5		10		10		5		1

So for example $\binom{4}{3}$ is the fourth element for the line for 4 (because the first element is $\binom{4}{0}$), that is, 4.

There is an easy recursive way of computing the triangle, based on the following fact.

Theorem 17 *For every natural number n and every natural number k such that $0 < k < n$, we have that:*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof. We can prove this theorem in two ways: by using the definition of binomial coefficient or by using the formula to compute it with factorials. Let's look at both proofs.

Proof 1: Remember that $\binom{n}{k}$ is the number of subsets of size k in a set of size n, for example in $\mathbb{Z}_n$. Now let's divide these subsets in two groups: those that contain $n-1$ and those that don't. The ones that don't contain $n-1$ are subsets of size k of $\mathbb{Z}_{n-1}$ and we know that there are $\binom{n-1}{k}$ ways of choosing them. The ones that contain $n-1$ will also have to contain $k-1$ elements of $\mathbb{Z}_{n-1}$; we know that there are $\binom{n-1}{k-1}$ ways of selecting the latter. Putting the

two groups together, we know that we have $\binom{n-1}{k} + \binom{n-1}{k-1}$ ways of selecting our subset, as the formula says.

Proof 2: Let's write out both sides of the equality in terms of factorials and verify that they are the same.

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{((n-1)-k)! \cdot k!} + \frac{(n-1)!}{((n-1)-(k-1))! \cdot (k-1)!} \\
&= \frac{(n-1)!}{(n-k-1)! \cdot k!} + \frac{(n-1)!}{(n-k)! \cdot (k-1)!} \\
&= \frac{(n-k) \cdot (n-1)! + k \cdot (n-1)!}{(n-k)! \cdot k!} \\
&= \frac{(n-k+k) \cdot (n-1)!}{(n-k)! \cdot k!} \\
&= \frac{n!}{(n-k)! \cdot k!}
\end{aligned}$$

Since we obtained the same result from both expressions, the equality must be true. □

The theorem allows us to give a recursive way to compute binomial coefficients; we use as base cases the fact that there is only one subset with zero elements, the empty set, and only one subset with n elements, the whole set.

Recursive computation of binomial coefficients:

$$\begin{aligned}
\binom{n}{0} &= 1 \\
\binom{n}{n} &= 1 \\
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \quad \text{if } 0 < k < n.
\end{aligned}$$

Pascal's triangle is constructed using this recursive definition. The "sides" of the triangle correspond to the base cases and are always 1. The internal values are obtained by adding the two values that are immediately above and to the left and right of the one we want to compute. So, for example, line number 6 is:

$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1.$$

6.2 Hilbert's Hotel

One of the consequences of the pigeonhole principle was that for a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$, injectivity is equivalent to surjectivity and, therefore, to bijectivity.

This is not true for infinite sets. In fact, a set X is infinite exactly when there is a function $f : X \to X$ that is injective but not surjective.

For example, for the natural numbers $\mathbb{N}$, we can show these two functions:

$$\begin{array}{ll} f : \mathbb{N} \to \mathbb{N} & \\ f(n) = n + 1 & \text{injective but not surjective;} \\ & \\ g : \mathbb{N} \to \mathbb{N} & \\ g(n) = \mathsf{quot}(n, 2) & \text{surjective but not injective.} \end{array}$$

The property of infinite sets of allowing injective but not surjective functions to themselves (which can be taken as the definition of infinity) is exploited in a whimsical tale about the "Hilbert's Hotel".

The hotel happens to have an infinite number of rooms, numbered 0, 1, 2, etc. There's a room for every natural number.

At present the hotel is completely booked. In the middle of the night a traveller comes to the reception and asks for accommodation. The hotel owner, Mr. Hilbert, tells him that, although at the moment all rooms are occupied, he can find a place for the new customer. (In reality, David Hilbert was a German mathematician who, around 1900, worked on the foundations of mathematics and the problems of the infinite.) Hilbert asks the tenant of room 0, let's call him Tenant 0, to move to room 1; he asks Tenant 1 to move to room 2; Tenant 2 to move to room 3 and so on. In this way every tenant is moved to a new room and room 0 is left free for the newcomer. You see that what Hilbert did is to apply the function $f(x) = x + 1$ to the tenants to determine what room to put them in. Since the function is injective, no two people are sent to the same room; and since it is not surjective, a new room is magically freed.

The properties of Hilbert's Hotel are even more astonishing. Some time later an "infinite bus" stops in front of the hotel. It contains an infinite number of travellers, let's call them Newcomer 0, Newcomer 1, Newcomer 2 and so on. They ask Mr. Hilbert to find them a place to stay. Again, Hilbert is unfazed: now he asks Tenant 1 to move to room 2, Tenant 2 to move to room 4, Tenant 3 to mover to room 6, and so on, Tenant n moves to room $2 \times n$. In this way, an infinite number of rooms becomes available: Newcomer 0 is accommodated in room 1, Newcomer 1 in room 3, Newcomer 2 in room 5 and so on, Newcomer m is accommodated in room $2 \times m + 1$.

6.3 Modular Arithmetic

The operations of addition and multiplication can be extended to the sets $\mathbb{Z}_n$ by "wrapping the result around", that is, by taking the remainder of the result after division by n. If two natural numbers a and b have the same remainder when they are divided by n then we say that they are *equivalent modulo* n and we write:

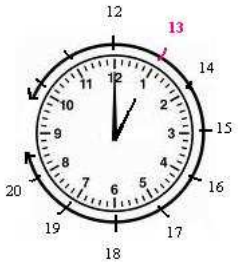
$$a \equiv b \ (\mathsf{mod}\ n).$$

By definition this mean that we can write both a and b as:

$$\begin{array}{l} a = q_1 \cdot n + r \\ b = q_2 \cdot n + r \end{array} \qquad \text{with } 0 \leq r < n.$$

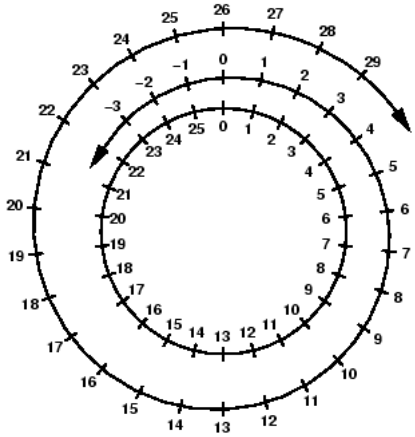
The remainder r is an element of $\mathbb{Z}_n$. If we are in a context in which it is clear that we are talking exclusively about elements of $\mathbb{Z}_n$, then we could consider also a and b as different ways of writing r.

We are all familiar with this way of seeing numbers: on a clock dial the hours 1 and 13 are represented by the same mark:



The clock actually represent the set $\mathbb{Z}_{12}$. We can perform addition on its elements: if two friends meet at 7 and agree to meet again 10 hours later, we know that the appointment is for 5 o'clock. This operation is performed by adding the numbers, $7 + 10 = 17$, and then taking the remainder of the division by 12, obtaining 5. (To be realistic we should distinguish between AM and PM, or use a clock with 24 hours instead, working in $\mathbb{Z}_{24}$.)

Imagine a planet that rotates around its axis in 26 hours. The inhabitants of that planet may have watches looking a bit like this:



The times on the planet are given as elements of $\mathbb{Z}_{26}$ (at least as long as we are happy with the hours and don't care about minutes and seconds). The number

29, for example, is considered just a different way of writing 3. The negative number -2 is a different way of writing 24.

We denote by the symbols $\oplus$ and $\otimes$ the operations of addition and multiplication in $\mathbb{Z}_{26}$. Remember that they are just the ordinary addition and multiplication, but taking the remainder of the division by 26 at the end. For example:

$$\begin{aligned} 9 \oplus 13 &= 22 \quad (\text{in } \mathbb{Z}_{26}) \\ 14 \oplus 15 &= 3 \quad (\text{in } \mathbb{Z}_{26}) \\ 8 \oplus 18 &= 0 \quad (\text{in } \mathbb{Z}_{26}) \\ 6 \otimes 3 &= 18 \quad (\text{in } \mathbb{Z}_{26}) \\ 6 \otimes 4 &= 24 \quad (\text{in } \mathbb{Z}_{26}) \\ 6 \otimes 5 &= 4 \quad (\text{in } \mathbb{Z}_{26}) \\ 2 \otimes 13 &= 0 \quad (\text{in } \mathbb{Z}_{26}) \end{aligned}$$

It is important that we always specify clearly that we are working on a specific set $\mathbb{Z}_n$, since the operations will generally have different results for different values of n. For example, if we take $n = 19$ the operations above give:

$$\begin{aligned} 9 \oplus 13 &= 3 \quad (\text{in } \mathbb{Z}_{19}) \\ 14 \oplus 15 &= 10 \quad (\text{in } \mathbb{Z}_{19}) \\ 8 \oplus 18 &= 7 \quad (\text{in } \mathbb{Z}_{19}) \\ 6 \otimes 3 &= 18 \quad (\text{in } \mathbb{Z}_{19}) \\ 6 \otimes 4 &= 5 \quad (\text{in } \mathbb{Z}_{19}) \\ 6 \otimes 5 &= 11 \quad (\text{in } \mathbb{Z}_{19}) \\ 2 \otimes 13 &= 7 \quad (\text{in } \mathbb{Z}_{19}) \end{aligned}$$

It is more common to use the normal symbols $+$ and $\times$ for addition and multiplication in $\mathbb{Z}_n$, but always remember to specify that they must be computed modulo n.

Modular Arithmetic satisfies most of the same properties as Arithmetic on the natural numbers and integers. But it has some surprising idiosyncrasies. Firs of all, there may be *zero divisors*. These are numbers x and y, both different from zero, but whose product $x \otimes y$ give zero. We have seen an example above: $2 \otimes 13 = 0$ (in $\mathbb{Z}_{26}$). This happens if n is a composite number: in our case it happens because $26 = 2 \times 13$.

It never happens if n is a prime number. But in that case something even more interesting occurs: every non-zero number has a *multiplicative inverse*:

Theorem 18 *If p is a prime number, then for every element $x \in \mathbb{Z}_p$, if $x \neq 0$ then there exists an element $x^{-1} \in \mathbb{Z}_p$ such that $x \otimes x^{-1} = 1$.*

For example, in $\mathbb{Z}_7$ we have that $5^{-1} = 3$ because $5 \otimes 3 = 1$ (in $\mathbb{Z}_7$). You may verify for yourself that the inverses of all non-zero elements of $\mathbb{Z}_7$ are the following:

$$1^{-1} = 1, \quad 2^{-1} = 4, \quad 3^{-1} = 5, \quad 4^{-1} = 2, \quad 5^{-1} = 3, \quad 6^{-1} = 6.$$

6.4 The Monkey and the Coconuts

On the first lecture I proposed the following puzzle:

> Five men and a monkey were shipwrecked on a desert island, and they spent the first day gathering coconuts for food. They piled them all up together and then went to sleep for the night.
>
> But when they were all asleep one man woke up and decided to take his share. He divided the coconuts in five piles. He had one coconut left and he gave it to the monkey. He took his pile and put the rest all back together.
>
> Later a second man woke up and acted in exactly the same way: He divided the coconuts into five piles; there was one coconut left that he tossed to the monkey; he took his pile and put the rest all back together.
>
> One after the other all five men do the same thing and every time there is one extra coconut that is given to the monkey.
>
> The next morning they divided what coconuts were left into five parts. Once again there was one coconut left that was given to the monkey.
>
> *How many coconuts were there at the beginning?*

If we call N the total number of coconuts at the beginning, we know that N must give remainder 1 when divided by 5:

$$N = 5 \cdot A + 1 \qquad \text{for some natural number } A.$$

The first man gives one coconut to the monkey and takes one fifth of the rest for himself. The number of the remaining coconuts is $4 \cdot A$.

When the second man comes, he starts with $4 \cdot A$ coconuts and proceed in the same way, so:

$$4 \cdot A = 5 \cdot B + 1 \qquad \text{for some natural number } B.$$

He gives one coconut to the monkey and takes one fifth of the rest for himself: the remaining coconuts are $4 \cdot B$.

The same process is repeated by every man, so we have five similar steps:

$$\begin{aligned}
N &= 5 \cdot A + 1 && \text{for some natural number } A \\
4 \cdot A &= 5 \cdot B + 1 && \text{for some natural number } B \\
4 \cdot B &= 5 \cdot C + 1 && \text{for some natural number } C \\
4 \cdot C &= 5 \cdot D + 1 && \text{for some natural number } D \\
4 \cdot D &= 5 \cdot E + 1 && \text{for some natural number } E
\end{aligned}$$

At the end of the night $4 \cdot E$ coconuts are left. The next morning they still give one coconut to the monkey and then divide the remaining in five equal parts:

$$4 \cdot E = 5 \cdot F + 1 \qquad \text{for some natural number } F.$$

To solve the puzzle we must find numbers N, A, B, C, D, E, F that satisfy these equation. Using some algebraic manipulation, we can reduce the six equations to a relation between the initial number N and the final share F:

$$1024 \cdot N = 15625 \cdot F + 11529.$$

We must solve it by finding two natural numbers N and F satisfying this equation. It is not easy to find the solution without trying all the possible values.

One way to solve the puzzle is, first of all, to notice that there are many, in fact infinite, different solutions. Suppose we have one solution, call it N_0. Since we divided the number of coconuts by 5 six times, it is easy to see that also $N_0 + 5^6$ must be a solution (try so substitute it for N in the equations, using the fact that N_0 already satisfies them).

But if we can obtain one solution by adding 5^6 to one that is already known, then we could also look at *negative solutions*, as long as they are still larger than -5^6. In particular we may notice that if we take $N_0 = -4$ we have that we can solve the first equation by taking $A_0 = -1$:

$$-4 = 5 \cdot (-1) + 1.$$

That would give that the number of coconuts left by the first man is $4 \cdot (-1) = -4$, that is, equal to the initial number. This, of course, doesn't make any sense in the real situation, since talking of negative coconuts is meaningless. But as a solution to the equations it is correct. The second equation can be solved in exactly the same way, since we have the same number -4 on its left. Indeed, by taking $N_0 = -4$ all six equations are solved in the same way.

So -4 is a solution, but not a realistic one. However, as we said earlier, when we have a solution we can get another one by adding 5^6 to it, therefore the number

$$-4 + 5^6 = -4 + 15625 = 15621$$

and this number is the solution we are looking for.