Chapter 9
Permutations, Cycles and Derangements

Permutations pervade much of mathematics including number theory. Besides innumerable peaceful uses, permutations were crucial in classical cryptography, such as the German *Geheimschreiber* (secret writer) and *Enigma* enciphering machines—and their demise. The *Geheimschreiber* was broken during World War II by the Swedish mathematician Arne Beurling—with the occasional help from the leading Swedish statistician Harald Cramér (see B. Beckman: *Codebreakers*).

Polish and British cryptanalysts were able to break the *Enigma* code by observing—among other factors—the cycle structure of the code. Cycles of permutations and their distributions are therefore considered in Section 9.4 of this chapter.\(^1\)

9.1 Permutations

The number of arrangements (“permutations”) of \(n\) distinct objects equals the *factorial* of \(n\):

\[
n! := 1 \cdot 2 \cdot 3 \cdots n, \quad (9.1)
\]

a formula easily proved by induction. Factorials grow very fast: while \(5!\) equals just 120, \(10!\) is already equal to 3,628,800. A good and relatively simple approximation is Stirling’s famous formula:

\[
n! \approx \sqrt{(2\pi n)n^n e^{-n}}, \quad (9.2)
\]

which yields 3,598,696 for \(n = 10\).

A better approximation multiplies the Stirling result by \(e^{1/12n}\), yielding \(10! \approx 3,628,810\) (for an error of less than 0.0003\%!).

Factorials are also related to the “Euler” integral. Repeated partial integration shows that

\(^1\) While the Germans, after a few years, became aware of the *Geheimschreiber*’s vulnerability and curtailed its use, the fact that the Allies had broken *Enigma* was one of the best-kept secrets of the war. The *Enigma* decrypts therefore continued to provide the Allies with invaluable information during the entire war.
\[ \int_0^\infty t^n e^{-t} \, dt = n! \quad (9.3) \]

The related gamma-function

\[ \Gamma(z) := \int_0^\infty t^{z-1} e^{-t} \, dt \]

is single-valued and analytic in the entire complex plane, except for the points \( z = -n \) \( (n = 0, 1, 2, \ldots) \) where it possesses simple poles with residues \( (-1)^n/n! \). \( \Gamma(z) \) obeys the recurrence formula

\[ \Gamma(z+1) = z\Gamma(z) \quad (9.4) \]

and the curious “reflection” formula

\[ \Gamma(z)\Gamma(1-z) = -z\Gamma(-z)\Gamma(z) = \pi\csc(\pi z), \quad (9.5) \]

which for \( z = 1/2 \) yields

\[ \Gamma(1/2) = \sqrt{\pi}. \]

### 9.2 Binomial Coefficients

As we learn in high school (?), the “binomial” \( (1+x)^n \) can be expanded (multiplied out) as follows:

\[ (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \quad (9.6) \]

where the \( \binom{n}{k} \) (read \( n \) choose \( k \)) are the binomial coefficients—

With 0! defined as 1, \( \binom{n}{0} = \binom{n}{n} = 1, \quad (9.7) \)

\( \binom{n}{1} \) equals \( n \) and \( \binom{n}{2} \) equals \( n(n-1)/2 = 0, 1, 3, 6, 10, 15, \ldots \) the “triangular” numbers (see Sec. 7.4). The binomial coefficient \( \binom{n}{2} = 1/2 \ n(n-1) \) is (by definition) the number of \textit{pairs} that can be selected from \( n \) distinct objects. Thus, at a party of \( n \) people, each guest clinking his glass with everyone else, produces a total of \( 1/2 \ n(n-1) \) clinkings. (Of course, for \( n = 1 \), the number of possible clinkings is zero, just as there is no applause with just one hand clapping. For two people (\( n = 2 \), there is just one clinking.)

Permutations when just two objects change places are called \textit{transpositions}. Every permutation can be decomposed into a unique (modulo 2) number of transpositions. If this number is odd, the permutation is called \textit{odd}. Otherwise it is called an \textit{even} permutation. The identity permutation is even because the number of transpositions is 0 (an even number). For example for \( n = 5 \), there are a total of \( n! = 120 \)