1. **Fermat primality test.** A number $m$ passes the Fermat primality test if $2^{m-1} \equiv 1 \pmod{m}$.

   a) Does $m = 2047$ pass the test?

   b) Did the test give the correct answer in this case?

2. **RSA encryption.** Using a public key $N = 55$ and an exponent $e = 3$ we want to transmit a message $m = 12$.

   a) What is the encryption $m^*$ of $m$ using RSA?

   b) Run the RSA decryption method to decrypt $m^*$.

3. **Bijection.** Give a bijection between the set of all integers and the set of all positive integers.

4. **Counting techniques.** How many ways are there to position two black rooks and two white rooks on an $8 \times 8$ chessboard so that no two pieces of different colors share a row or a column?

5. **Binomial coefficients.** What is the coefficient of $x^7y^5$ in

   a) What is the coefficient of $x^7y^5$ in $(x + y)^{12}$?

   b) What is the coefficient of $x^7y^5$ in $(2x - y)^{12}$?

6. **Combinatorial identity.**

   a) Using the formula for binomial coefficients prove that for all positive integers $k \leq r \leq n$

   $$\binom{n}{r} \binom{r}{k} = \binom{n}{k} \binom{n-k}{r-k}.$$

   b) Give a bijective proof of the above formula by interpreting both sides as enumerating certain pairs of subsets of an $n$-element set.