Problem 1 Let $G$ be a group and let $x, y \in G$. Show that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution: We have $xy(y^{-1}x^{-1}) = xyy^{-1}x^{-1} = xx^{-1} = id$ and $(y^{-1}x^{-1})xy = y^{-1}x^{-1}xy = y^{-1}y = id$, which shows that $y^{-1}x^{-1}$ is the inverse of $xy$.

Problem 2

1. Show that a group $G$ can only have one identity element.

2. Show that in a group $G$ every element has exactly one inverse.

Solution: This is Theorem 4.3.1 on page 170 of the textbook.

Problem 3 How many groups are there that have 11 elements (up to isomorphism)?

Solution: Let $G$ be a group with 11 elements, and let $a \in G$ be an element that is not the identity. Let $H$ be the subgroup generated by $a$, i.e. $H = \{a, a^2, a^3, \ldots, a^k = id\}$ (where $k$ is the order of $a$). Since $a$ is not the identity, $H$ cannot be the trivial subgroup that only consists of the identity element. By Lagrange’s theorem, the order of $H$ has to divide 11, and hence we must have $H = G$. Hence $G$ is cyclic, generated by $a$.

Any two cyclic groups of order 11 are isomorphic, by mapping the generator of the first group to the generator of the second group. Hence, up to isomorphism, there is only one group of order 11.

Problem 4 Show that if $\pi, \sigma$ are disjoint permutations in $S(n)$, then the order of $\pi\sigma$ is the least common multiple of the order of $\pi$ and the order of $\sigma$.

Solution: This is Lemma 4.2.5 on page 162 of the textbook.

Problem 5 What is the highest possible order of an element in $S(8)$?

Solution: By the previous problem and since a $k$-cycle has order $k$, the permutation $(123)(45678)$ has order 15. Since every permutation can be decomposed as a product of disjoint cycles, we can list all possible types of cycle decompositions and (by applying the previous problem several times) compute their orders.

(E.g., $\pi$ decomposes as a 4-cycle, a 3-cycle and a 1-cycle, or a 5-cycle, a 2-cycle and a 1-cycle or it decomposes as two 4-cycles, . . .) For each of these cycle decompositions we can compute the least common multiple of the cycle lengths involved and check that it is at most 15.
Problem 6  Determine the order and sign of each of the following permutations:

1. \((1\ 2\ 3\ 4\ 5)(8\ 7\ 6)(10\ 11)\)
2. \((1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10)\)

Solution: The first permutation has order 30 and is odd. The second permutation has order 30 and is odd.

Problem 7  Let \(\mathbb{H}_0\) be the group with 8 elements \(\mathbb{H}_0 = \{\pm 1, \pm i, \pm j, \pm k\}\) and multiplication rules

\[
i^2 = j^2 = k^2 = -1, \quad ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j.
\]

(You don’t have to check that these 8 elements together form a group.) (This is a subgroup of the famous quaternions.) Does \(\mathbb{H}_0\) have a subgroup of order 4? If so, is there a subgroup with 4 elements that is cyclic?

Solution: The subgroup \(K\) generated by \(i\) is cyclic of order 4, since \(K = \langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\}\).

Problem 8  Solve the simultaneous congruences

\[
3x \equiv 1 \pmod{5} \\
2x \equiv 6 \pmod{8}.
\]

Solution: The first equation is equivalent to \(x \equiv 2 \pmod{5}\), and the second equation is equivalent to \(x \equiv 3 \pmod{4}\).

The integers 5 and 4 are relatively prime, and we have

\[
5 \cdot 1 - 4 \cdot 1 = 1.
\]

By the proof of the Chinese remainder theorem this implies that the solution of this congruence modulo 20 is \(c := 5 \cdot 3 - 4 \cdot 2 = 7\), so \([7]_{20}\) is the unique solution.

Problem 9  Find all solutions (if there are any) of the congruence

\[
64x \equiv 32 \pmod{84}
\]

Solution: The gcd of 64 and 84 is 4 which divides 32, so this congruence has four distinct solutions modulo 84, or, equivalently, one unique solution modulo 84/4 = 21.

We divide the congruence by \(\gcd(64, 84)\) and obtain

\[
16x \equiv 8 \pmod{21}.
\]

Now we calculate the inverse of 16 mod 21, which is 4, so after multiplying by the inverse we get

\[
x \equiv 32 \pmod{21}
\]
or \(x \equiv 11 \pmod{21}\). Hence the unique solution modulo 21 is 11, and the solutions modulo 84 are 11, 32, 53 and 74.
Problem 10  A standard deck of 52 cards is dealt to four people, called North, South, East and West. Of the $52!$ permutations of the deck, for how many will it be the case that North has 2 Spades, East has 2 Spades, South has 4 Spades, and West has 5 Spades? (You may use the factorial notation to express your answer.)

Solution: There are \( \binom{13}{2,2,4,5} \) ways of choosing which Spades North gets, which Spades East gets, etc. Similarly, there are \( \binom{39}{11,11,9,8} \) ways of choosing which non-Spades North gets, which non-Spades East gets, etc. There are also $13!$ ways of permuting each players’ cards. Thus in all there are 
\[
\binom{13}{2,2,4,5} \binom{39}{11,11,9,8} 13!
\]
possible ways.

Problem 11  Two dice are thrown $n$ times in succession. Determine the probability that double 6 appears at least once.

Solution: The event “double 6 appears at least once in the $n$ trials” is the complement of the event “no double 6 appears in any of the $n$ rolls of the two dice”. Let $E_i$ be the event “the outcome of the $i$th roll is a double 6” (where $i$ takes values 1, 2, . . . , $n$); the probability of $E_i$ is $\frac{1}{36}$, which implies that $P(E_i^c) = \frac{35}{36}$.

In terms of the events $E_1, E_2, \ldots, E_n$, the probability of the event “no double 6 appears in any of the $n$ rolls of the two dice” is equal to the intersection of the events $E_1^c, E_2^c, \ldots, E_n^c$, whose probability equals the product of the probabilities for each $E_i^c$. (This is because the outcomes of the individual rolls of the two dice are independent of each other.)

\[
P(E_1^c \cap E_2^c \cap \cdots \cap E_n^c) = P(E_1^c) P(E_2^c) \cdots P(E_n^c) = \prod_{i=1}^{n} P(E_i^c) = P(E_1^c)^n = \left( \frac{35}{36} \right)^n.
\]

Therefore, the probability of the event “double 6 appears at least once in the $n$ trials” is

\[
1 - P(E_1^c \cap E_2^c \cap \cdots \cap E_n^c) = 1 - \left( \frac{35}{36} \right)^n.
\]

Problem 12

1. Suppose there are $n$ people in a room. What is the probability that no two of them celebrate their birthday on the same day?

2. How large does $n$ have to be so that the probability that at least two people share a birthday is $\geq 1/2$? (This part requires a calculator.)
Solution:

1. We assume that there are 365 days per year (so there is no February 29). Hence there are \((365)^n\) possible outcomes of this experiment. No two birthdays are on the same day in \(365 \cdot 364 \cdot 363 \cdot \cdots (365 - n + 1)\) cases. Hence the desired probability is

\[
\frac{365 \cdot 364 \cdot 363 \cdot \cdots (365 - n + 1)}{365^n}.
\]

2. When \(n \geq 23\), the above probability is \(< 1/2\), so in this case the probability that at least two people share a birthday is \(\geq 1/2\). This is often referred to as the \textit{birthday problem}.

Problem 13 In a poker game, what is the probability of being dealt two pairs?

Solution: If we are dealt two pairs, then the cards are \(a\ a\ b\ b\ c\) for some denominations \(a, b, c\) with \(a \neq b \neq c\). There are \(\binom{13}{2}\) to choose the two denominations \(a, b\) that form the two pairs, and for each pair there are \(\binom{4}{2}\) to choose two out of the four possible cards with the same denomination. There are \(\binom{44}{1}\) ways to choose the last remaining card \(c\). Hence the probability is

\[
\frac{\binom{4}{2} \binom{44}{1} \binom{13}{2}}{\binom{52}{5}}.
\]