1) Show by well-founded induction that every natural number greater than 1 can be divided by a prime number.

Solution:
We choose the well-founded relation $R = \{(m, n) \mid m < n \text{ with } m, n \in \mathbb{N}\}$.
Let $P(n)$ be the property that n can be divided by a prime number.
We want to show $P(n)$ for all natural numbers n greater than 1. We proceed by well-founded induction on n with respect to the relation R.
Consider a natural number $n > 1$ with the induction hypothesis that $P(m)$ holds for all m with $1 < m < n$. We have two cases:

- if n is a prime number: $P(n)$ holds since every prime number is divisible by itself.
- if n is not a prime number: n can be written as product of two natural numbers $n = m_1 \cdot m_2$ with $1 < m_1, m_2 < n$. Since we know $P(m_1)$ from our induction hypothesis and m_1 divides n we can conclude $P(n)$.

2) Are the following relations well-founded relations, well-founded partial orders, or neither? Explain why!

   a) The divisibility relation on natural numbers.
   b) The "<" relation on the interval $[0, 1]$ of real numbers (i.e. $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$)
   c) $R_1 = \{((a, b), (c, d)) \mid a, b, c, d \in \mathbb{N},\ a < c\}$
   d) $R_2 = \{((a, b), (c, d)) \mid a, b, c, d \in \mathbb{N},\ a < c \ \wedge\ b < d\}$
   e) $R_3 = \{((a, b), (c, d)) \mid a, b, c, d \in \mathbb{N},\ a < c \ \vee\ b < d\}$

Solution:

   a) This is not a well-founded relation because it is reflexive. However, as a partial order it is wellfounded. Recall that in the lecture we defined that a partial-order is well-founded if its strict part is well-founded. First, note that we cannot have an infinitely descending chain starting from a non-zero number a: since every number in such a chain strictly divides the next, the numbers must get smaller in every step. Since there are only finitely many numbers $\leq a$, the chain must be finite. We cannot have an infinite chain starting from 0 either, because after the first step we would end up at a non-zero number a, and we have already shown that this is not possible.
   b) This is not well-founded as a relation or as a partial order, since we have the infinitely descending chain $\ldots < \frac{1}{8} < \frac{1}{4} < \frac{1}{2} < 1$.
   c) This is well-founded as a relation (but not a partial order due to lack of reflexivity). Any infinitely descending chain in R_1 would give rise to an infinitely descending chain on the natural order on $\mathbb{N}$ by simply throwing away the second component.
   d) Again, well-founded as a relation but not a partial order. This is due to $R_2 \subseteq R_1$.
   e) Not well-founded since e.g. $\ldots\ R_3\ (0, 1)\ R_3\ (1, 0)\ R_3\ (0, 1) R_3$ is an infinitely descending chain.

3) Let Σ be a finite set of symbols. Let us define the *maximo-lexicographical ordering* $<_{\text{mlex}}$ on the set of all finite words $\Sigma^\star$ as follows:

$$x <_{\text{mlex}} y \quad \iff \quad \ell(x) < \ell(y) \ \lor \ (\ell(x) = \ell(y) \ \land \ x <_{\text{lex}} y)$$

where $<_{\text{lex}}$ is the lexicographical ordering from the lecture. Prove that $<_{\text{mlex}}$ is a well-founded total strict order.

Solution:
We need to show that $<_{\text{mlex}}$ is (1) *irreflexive*, (2) *transitive*, (3) *total*, and (4) *well-founded.*

(1) Follows from the irreflexivity of $<_{\text{lex}}$.

(2) Let $x <_{\text{mlex}} y$ and $y <_{\text{mlex}} z$. Clearly $\ell(x) \leq \ell(y) \leq \ell(z)$ and hence $\ell(x) \leq \ell(z)$. When $\ell(x) < \ell(z)$ we have $x <_{\text{mlex}} z$. When $\ell(x) = \ell(z)$ then also $\ell(x) = \ell(y)$ and hence both $x <_{\text{lex}} y$ and $y <_{\text{lex}} z$ must hold. From the transitivity of $<_{\text{lex}}$ we obtain $x <_{\text{lex}} z$. Hence $x <_{\text{mlex}} z$ holds as well.

(3) Let $x, y \in \Sigma^\star$. When $\ell(x) \neq \ell(y)$ then we have either $x <_{\text{mlex}} y$ or $y <_{\text{mlex}} x$. When $\ell(x) = \ell(y)$ then the claim follows from the totality of $<_{\text{lex}}$.

(4) For a contradiction, let us consider an infinite descending chain $x_0 >_{\text{mlex}} x_1 >_{\text{mlex}} x_2 >_{\text{mlex}} \cdots$. It must hold that $\ell(x_i) \leq \ell(x_0)$ for all $i \in \mathbb{N}$, that is, that all the words x_i are shorter or equal in length to x_0. But there are only finitely many such words because Σ is finite. Since $<_{\text{mlex}}$ is irreflexive, this means that the chain cannot be infinite.

4*) In the following, let R and S be relations over some set A. Which of these statements are true? Give an informal explanation for true statements and a counterexample for false ones.

a) If R is well-founded, then every subset $R' \subseteq R$ is well-founded.

b) If R and R' are well-founded, then $R \cup R'$ is well-founded.

c) If R and S are well-founded, RS is well-founded.

d) If R is well-founded, then for any function $f : B \to A$, the relation $R' = \{(x, y) \mid (f(x), f(y)) \in R\}$ is also well-founded.

e) For any $n > 0$, R^n is well-founded if and only if R is well-founded.

f) If R is well-founded, then R is acyclic (i.e. there is no x with $(x, x) \in R^+$).

g) If A is finite and acyclic, then R is well-founded.

Solution:

a) True. Any infinite descending chain in R' would also be one in R.

b) False. Consider e.g. $R = \{(i, i+1) \mid i \text{ even}, \ i \in \mathbb{Z}\}$ and $S = \{(i, i+1) \mid i \text{ odd } i \in \mathbb{Z}\}$. Both of these have no descending chains of length > 2, but their union is the "successor" relation on $\mathbb{Z}$, which clearly has an infinite descending chain $\ldots, -3, -2, -1, 0$.

c) False. If we take R and S to be the same as in our counterexample in b), we get $RS = \{(i, i+2) \mid i \text{ even}, \ i \in \mathbb{Z}\}$, which has the infinite descending chain $\ldots, -6, -4, -2, 0$.

d) True. If $\ldots, x_3, x_2, x_1, x_0$ were an infinite descending chain in our new relation, $\ldots, f(x_3), f(x_2), f(x_1), f(x_0)$ would be an infinite descending chain in R.

e) True. Any infinite descending chain in R^n can be "unravelled" into an infinite descending chain on R. Vice versa, every infinite descending chain on R can be "condensed" into one on R^n.

f) True. If $(x, x) \in R^+$ then there would be some chain of the form $x < \ldots < x$. By repeating that chain infinitely often we would get an infinitely descending chain.

g) True. Because A is finite, some x would have to appear multiple times in any infinite descending chain, and that would imply $(x, x) \in R^+$.