Exercise 13.1.  [Presburger Arithmetic]
Eliminate the quantifiers from the following formulas, according to Presburger arithmetic:

1. $\forall y (3 < x + 2 \cdot y \lor 2 \cdot x + y < 3)$
2. $\forall x (\exists y (x = 2 \cdot y) \rightarrow (2 \cdot x \geq 0 \lor 3 \cdot x < 2))$

Solution:

$\forall y (3 < x + 2 \cdot y \lor 2 \cdot x + y < 3)$
$\iff \neg \exists y \neg (3 < x + 2 \cdot y \lor 2 \cdot x + y < 3)$
$\iff \neg \exists y (3 \geq x + 2 \cdot y \land 2 \cdot x + y \geq 3)$
$\iff \neg \exists y (2 \cdot y \leq 3 - x \land 3 - 2 \cdot x \leq y)$
$\iff \neg \exists y (2 \cdot y \leq 3 - x \land 6 - 4 \cdot x \leq 2 \cdot y)$
$\iff \neg \exists z (z \leq 3 - x \land 6 - 4 \cdot x \leq z \land 2 \mid z)$
$\iff \neg ((6 - 4 \cdot x \leq 3 - x \land 2 \mid 6 - 4 \cdot x) \lor (7 - 4 \cdot x \leq 3 - x \land 2 \mid 7 - 4 \cdot x))$

$\forall x (\exists y (x = 2 \cdot y) \rightarrow (2 \cdot x \geq 0 \lor 3 \cdot x < 2))$
$\iff \forall x (2 \mid x \rightarrow (2 \cdot x \geq 0 \lor 3 \cdot x < 2))$
$\iff \neg \exists x \neg (2 \mid x \rightarrow (2 \cdot x \geq 0 \lor 3 \cdot x < 2))$
$\iff \neg \exists x (2 \mid x \land 2 \cdot x < 0 \land 3 \cdot x \geq 2)$
$\iff \neg \exists x (2 \mid x \land 2 \cdot x \leq -1 \land 2 \leq 3 \cdot x)$
$\iff \neg \exists x (2 \mid x \land 6 \cdot x \leq -3 \land 4 \leq 6 \cdot x)$
$\iff \neg \exists z (12 \mid z \land z \leq -3 \land 4 \leq z) \iff \bot$
Exercise 13.2. [Quantifier Elimination for $Th(\mathbb{N}, 0, S, =)$]

Give a quantifier-elimination procedure for $Th(\mathbb{N}, 0, S, =)$ where $S$ is the successor operation on natural numbers, i.e. $S(n) = n + 1$.

Hint: $a = b$ iff $S^k(a) = S^k(b)$ for any $a, b, k \in \mathbb{N}$.

Solution:
We assume $F = \exists x (A_1 \land \ldots \land A_n)$ where $x$ occurs in all $A_i$ and each $A_i$ is of the form

$$S^k(x) = S^m(t) \text{ or } S^k(x) \neq S^m(t)$$

where $t$ is 0 or a variable (using symmetry of $=$).

If $x$ occurs on both sides of an atom $A_i$, we can compare the number of successors and replace it with $\bot$ or $\top$. Formally, $Th(\mathbb{N}, 0, S) \models (S^k(x) = S^k(x)) \leftrightarrow \top$ and $Th(\mathbb{N}, 0, S) \models (S^k(x) \neq S^k(x)) \leftrightarrow \bot$, and similarly for different numbers of successors.

Hence, we may further assume that $x \neq t$.

We have to distinguish two cases:

1. All $A_i$ only use $\neq$, but not $=$. Then return $\top$, because

$$Th(\mathbb{N}, 0, S) \models (\exists x (A_1 \land \ldots \land A_n)) \leftrightarrow \top$$

2. There is at least one $A_i$ of the form $S^m(x) = t$ where $x \neq t$.

We replace $A_i$ as follows:

- If $k > 0$, we add the constraints $t \neq 0 \land \ldots \land t \neq S^{m-1}(0)$ to ensure that the solution for $x$ is non-negative.
- Otherwise, replace it with $\top$.

The other $A_j$ ($i \neq j$) can be replaced as follows: Let $A_j$ be $S^k(x) = u$. Using the hint, first increment both sides by $m$: $S^{k+m}(x) = S^m(u)$. Then, substitute $A_i$, resulting in $S^k(t) = S^m(u)$.

This works similarly for inequality, resulting in $S^k(t) \neq S^m(u)$.

For optimization purposes, we could also assume that either side of the equalities/inequalities contains no successor application. If they do, we can decrement until at least one side is 0 or a variable.

Exercise 13.3. [Brainstorming]
Collect about 30 important pieces of terminology that were used in the lecture and that you want to remember for the exam.

Also collect the three results that you find most interesting.
Homework 13.1.  [Quantifier Elimination]  (8 points)
Perform Presburger arithmetic quantifier elimination for each formula:

1. $\forall x \forall y (0 < y \land x < y \rightarrow x + 1 < 2 \cdot y)$
2. $\forall x (\exists y (x = 2 \cdot y \land 2 \mid y) \rightarrow 4 \mid x)$

Homework 13.2.  [Quantifier Elimination for $Th(\mathbb{Z}, 0, S, P, =, <)$]  (8 points)
Give a quantifier-elimination procedure for $Th(\mathbb{Z}, 0, S, P, =, <)$ where $S$ is the successor and $P$ the predecessor operation on integers, i.e. $S(n) = n + 1$ and $P(n) = n - 1$. Do not use Presburger arithmetic; give a direct algorithm.