List of the parts of the lecture notes that are needed for the exam

Everything that was covered in the lecture may be needed for the solution of the problems in the exams. The notes contain a little more than I told in this semester, and the list below describes precisely what is needed.

Number theory:

- **Basics of number theory:** In Section 1.1 some proofs were omitted. The proof of the uniqueness part of the fundamental theorem and the proofs of Proposition 1.1.4, Corollary 1.1.5, Theorem 1.1.6 were not given in the lecture (though it is maybe useful to understand them, the proof of the uniqueness part is harder than the other proofs). Exercise 1.1.1 is not needed. Everything else is needed in the exam.

- **Congruences:** Section 1.2 was covered completely except for Exercise 1.2.1 which is basic and the method of its solution may needed in the exam.

- **The Euler-Fermat theorem:** Most parts of Section 1.3 were covered. The remark below Lemma 1.3.4 and the proof of that lemma are not needed.

- **Linear congruences:** Section 1.4 was covered completely except for some examples and the exercises of this section that are basic and may needed in the exam.

- **Polynomial algorithms:** Section 1.5.1 and Section 1.5.2 were covered completely except for Exercise 1.5.1.

- **Modular exponentiation:** In Section 1.5.3 everything was covered except for the paragraph after the pseudocode.

- **Euclidean algorithm (for the computation of the gcd):** Section 1.5.4 was covered completely except for the proof of Proposition 1.5.2 that is not needed.

- **Euclidean algorithm for the solution of linear congruences:** Section 1.5.5 was covered except for the pseudocode and the number of steps.

- **Primality tests:** Only the Fermat test is needed in the exam (the Miller-Rabin test, the prime generating algorithms, Proposition 1.5.4, Theorem 1.5.5 and Theorem 1.5.6 are not needed). The proof of Theorem 1.5.3 is not needed.

- **The RSA algorithm:** Section 1.5.7 was covered completely, the last paragraph of the section is a remark and not needed in the exam.

Linear Algebra:

- **Analytic geometry:** Section 2.1 was covered completely in the lecture.

- **The space \( \mathbb{R}^n \):** In Section 2.2 everything was told in the lecture except for some exercises and remarks. Note that all the exercises in this section are basic and similar problems can occur in the exam. On the other hand, the content of the paragraphs marked as a "Remark" on page 38 and page 41 will not be part of the exam.
- **Gaussian elimination:** Section 2.3 was covered almost completely except for the last 3 paragraphs of the section (about the running time) that are not needed in the exam. Note that the pseudocode for the algorithm was not given in the lecture but hopefully it is helpful and one should understand it.

- **The determinant:** Section 2.4 was covered almost completely. The 3 paragraphs that are marked as a "Remark" (page 59, page 63 and page 71) are not needed in the exam. Exercise 2.4.1 and Exercise 2.4.2 were not covered in the lecture, but these are easy exercises and the solution of similar problems can be a part of the exam.

- **Matrices:** Section 2.5.1 and Section 2.5.2 were covered completely except for Lemma 2.5.6, the proof of Theorem 2.5.5 and some examples that belong to the main part of the material and only help the understanding of the notions.

- **The inverse of a matrix:** Section 2.5.3 was covered completely except for Corollary 2.5.14 and the paragraph above it.

- **Rank of the matrix:** Section 2.5.4 was covered completely except for Exercise 2.5.2.

- **Linear maps:** Sections 2.6.1 and 2.6.2 were covered completely. Section 2.6.3 was covered almost completely, the proof of the independence of the chosen basis vectors in \( \ker f \) in the algorithm on page 97 is not needed, the paragraph above Example 2.6.4 is not important for the exam, and Exercise 2.6.1 is also optional. Section 2.6.4 contains more than you have to know in the exam. Definition 2.6.5 was given in the lecture only in the special case when the functions are linear. The remark below the definition is not needed. The proof of Theorem 2.6.10 is not needed. The first two paragraphs after the proof of Theorem 2.6.11 are not needed. In Section 2.6.5 the proof of Theorem 2.6.15 and the paragraph after this proof are not needed. On page 107 in Section 2.6.6 only Definition 2.6.9 and the paragraph below it are needed, the remaining part of the page was not covered. Exercise 2.6.2 and Exercise 2.6.3 are not needed. The remaining parts of the last 3 sections were covered in the lecture.