3 Proofs

We have on several occasions in the lectures discussed various kinds of proofs. Let us summarize these discussions, and also add a few things. Hopefully this will help you to prove things in the exam, and to understand the proofs given in the course. I also hope it will help you to understand books in pure mathematics in the future.

3.1 Theorems

In mathematics, the word "Theorem" means "true statement". We have seen many examples in the course. Sometimes we use a different word, as we have seen on a few occasions. Here are the words that are in common use in mathematical literature. We could (as we have done almost everywhere in these notes) use the word Theorem for all true statements, but the use of different words can help us to understand the structure of a chapter or a research paper, and to know what statements are more important than others.

- **Lemma** A lemma is a "small" theorem, that we want to use to prove a more important theorem later. Usually, the lemma is not really interesting in itself. Most lemmas have very short proofs. Sometimes, one proves several lemmas, and then uses all of them to prove an important theorem.
- **Corollary** A corollary is a theorem that follows immediately from a theorem we already have proved, for example by applying the theorem to a particular situation. For example, in these notes, Bezout's theorem (Theorem 8) can be regarded as a corollary to Theorem 7 (see page 23).
- **Proposition** A proposition is a theorem that is of interest in itself, but it is still not a major, very important theorem.
- **Theorem** In many textbooks, the word Theorem is used only for statements that are of a major importance.
- **Fact** In any serious textbook in pure mathematics, any theorem/lemma/proposition/corollary should be followed by a proof. Many authors use the word Fact when they for some reason want to state a theorem without giving the proof.

3.2 Proofs

A proof is a correct argument that shows that a certain statement must be true. Whenever we state a theorem, we should also give a proof to justify

our claim that the statement is true.
In a proof you are free to use anything you know is true, such as

- Obvious facts
- Theorems that are already proved
- The definitions of the concepts involved in the theorem

For example, in the proof of Theorem 7, we used the obvious fact that if two positive integers divide each other, then they are equal. We also used the definition of GCD, the definition of linear combination, and the definition of generator. To prove Theorem 5, we used Theorem 6.

Suppose we have defined a concept, for example prime number, or ideal, or the Euler φ-function. To prove something about this concept, we MUST use either the definition, or something we have already proved about the concept. Just after we defined a concept we know *nothing* about that concept except the definition.

It is common practice to indicate the end of a proof either by a small square, as in these notes, or by the letters QED, which is an abbreviation of the Latin expression *quod erat demonstrandum* ("which was to be proved").

Many times in this course (including in the exam!), and also in future courses in pure mathematics, you will be asked to prove something. We shall look at a few common types of theorems, and discuss what kinds of proof can be suitable in these various situations.

3.3 Different kinds of theorems

It is impossible to list all kinds of theorems that occur in mathematics. And it is "even more impossible" to list all kinds of proofs. However, we can list a few of the most common kinds of theorems, and discuss some basic methods of proof.

3.3.1 If "hypotheses" then "conclusion"

This is perhaps the most common type of theorem. We are given some assumptions, (called the "hypothesis") and are asked to prove some consequence of the assumptions (a "conclusion"). In other words, we are asked to prove that the hypotheses implies the conclusion. For example, we have the following very simple theorem: If n is an odd integer, then n^2 is also odd. Here the hypothesis is "n is an odd integer" and the conclusion is "n^2 is odd". To prove a theorem of this kind, the following steps may help:
Step 1: Identify and write down the hypotheses. These are the assumptions

that we start with.
Step 2: Identify and write down the conclusion. This is what we are asked to prove.
Step 3: Identify and write down the definitions of the terms involved in the theorem. These definitions will probably be used in the proof.
Step 4: Try to think about consequences of the hypothesis. For example, if the hypothesis is that "p is a prime number", then there are the following consequences:

- The only positive divisors of p are 1 and p.
- p is either equal to 2, equal to 3, congruent to 1 mod 6, or congruent to 5 mod 6.
- $\varphi(p) = p - 1$
- $a^p \equiv a \pmod{p}$ for any positive integer a.

Step 5: Try to think about theorems that seem related to the statement you are asked to prove. For example, if you are asked to prove something involving a congruence, you know about the following theorems:

- The rules for congruences (Theorems 13, 14, 15)
- The five equivalent formulations of congruence (page 28)
- Euler's theorem and Fermat's theorem
- Congruence mod m is an equivalence relation
- A criterion for solvability of linear congruences (Theorem 18)
- The Chinese Remainder Theorem (Theorem 19)

Can you combine any of these theorems with the hypotheses to get somewhere?
Step 6: With the help of the previous points, try to find an argument which starts with the hypothesis, and from there proves that the conclusion must be true.

Example 48. Theorem: For every integer $n \geq 4$, we have the inequality $2^n \geq n^2$. Here the hypothesis is "n is an integer greater than or equal to 4". The conclusion is "$2^n \geq n^2$".

Example 49. Theorem: If a divides b and b divides c, then a divides c. Here the hypothesis is "a divides b and b divides c", and the conclusion is "a divides c".

IMPORTANT: You must never start by assuming that the conclusion is true! Also, you may never use a hypothesis that is not stated in the theorem.

3.3.2 Statement 1 is equivalent to Statement 2

With this kind of statement, we are asked to prove that one statement is true if and only if another statement is true. For example, see Theorem 11. To do this we must

- Prove that Statement 1 implies Statement 2
- Prove that Statement 2 implies Statement 1

For each of these points, you can use the ideas above. In the first point, you treat Statement 1 as the hypothesis, and Statement 2 as the conclusion. In the second point, you reverse the roles of the statements.

3.4 Some general methods of proof

Not all theorems are of the forms mentioned above. There are a few general strategies that often can be used to prove things, regardless of what kind of theorem we are dealing with. Here are some examples:

3.4.1 Proof by cases

In many situations, it might be useful to distinguish between separate cases, and give a separate proof for each case. We have seen the following examples:

- In Theorem 7, we had to prove something about an ideal. We considered the case of the zero ideal, and the case of a nonzero ideal, and gave different proofs for the two cases.
- In Theorem 16, we wanted to prove something about odd integers. We considered the case where the integer is congruent to 1 mod 4, and the case where the integer is congruent to 3 mod 4.
- In proving Fermat's little theorem, we considered the case where $p|a$ and the case where $p \nmid a$.

In elementary number theory, it is very often useful to consider the various possible cases of remainder mod m, for some number m. For example, we could consider the cases of odd numbers and even numbers.

The method of proof by cases can be thought of as a method to gain more information than was originally given in the statement of the theorem. For example, it might be hard to prove a statement about a general integer n, while it is easier to prove the statement when n is odd, or when n is even, because in each of these cases we have some additional information about n, that can be used in the proof.

3.4.2 Proof by contradiction

The idea of this proof method is to *assume* that the theorem is *not true*, and then show that this implies some false statement (a *contradiction*). This false statement could for example be $0 = 1$, or any other statement that we *know* is false. We give one example of a proof using this method.

Theorem 27. There are infinitely many prime numbers.

Proof. To prove this, we shall assume that the theorem is not true, and arrive at a contradiction. Assume that the set of prime numbers is a finite set. Then we can list all the primes as $p_1, p_2, \ldots, p_r$. Let their product be m. Consider the number

$$n = p_1 p_2 \cdots p_r + 1$$

that is, the number $m + 1$. This number is clearly greater than each of the primes p_i, so it can not be prime. Hence it is composite. Take a prime p which divides n. This prime also divides m, because p is among the primes $p_1, p_2, \ldots, p_r$. Therefore, p divides $n - m$, in other words $p|1$. This is clearly false, so we have obtained a contradiction. Therefore the theorem is true. □

3.4.3 Proof by induction

This has been explained earlier in these notes.

3.4.4 Some further advice

Here are some further ideas that might be helpful if you try to prove something.

- Try to find out what the theorem says in particular cases, in order to understand why it must be true in general.
- Make sure that you know the definitions of the concepts involved in the statement of the theorem.
- Can you reformulate the theorem? For example, if you are asked to prove something about divisibility or congruences, you may use all of the five equivalent statements on page 28.
- Try to find a counterexample to the theorem, that is an example which shows the theorem to be false. If the theorem is true, this will not be possible, but by trying you will develop a better understanding of why the theorem is true, and perhaps also find a proof of the theorem.
- Try to think about related theorems that you know are true - can you use any of them?

3.5 Exercises

Identify the hypotheses and conclusions in the following statements. (You don't have to prove the theorems.)

E219 If x and y are positive real numbers, then the inequality

$$\frac{x}{y} + \frac{y}{x} \geq 2$$

holds.

E220 For any positive integer n, the sum of the integers $1, 2, 3, \ldots n$ is equal to $\frac{n(n+1)}{2}$.

E221 If $n > 2$ is an integer, then there are no positive integers x, y and z, such that $x^n + y^n = z^n$.

E222 Let m be an integer. Then $m^2 + m + 1$ is an odd number.

3.6 Problems

Here are some theorems with proofs, but the proofs are not correct! For each proof, identify the mistake made.

P22. Theorem:
If m is an even integer, then $m^2 + 2m$ is also even.

Proof. Since $m^2 + 2m$ is even and $2m$ is always even, the number m^2 must also be even. Therefore m must be even. □

P23. Theorem:
For every positive integer n, the number $n^3 - n$ is divisible by 3.

Proof. We consider different possible cases of remainder when n is divided by 3.

Case 1: $n \equiv 1 \pmod 3$.
Raising both sides of this congruence to 3, we get

$$n^3 \equiv 1 \pmod 3$$

Subtract the first congruence from the second. This gives

$$n^3 - n \equiv 0 \pmod 3$$

so the theorem is true in this case.

Case 2: $n \equiv 2 \pmod 3$.
Again, we raise both sides of this congruence to 3, to get

$$n^3 \equiv 8 \pmod 3$$

Subtracting the first congruence from the second gives

$$n^3 - n \equiv 6 \pmod 3$$

so the theorem is true also in this case, since $6 \equiv 0 \pmod 3$. This completes the proof. □

P24. Theorem:
A positive integer n is a prime number if and only if the following congruence holds:

$$(n-1)! \equiv -1 \pmod{n}$$

(Recall that $k! = 1 \cdot 2 \cdot 3 \cdots k$.)

Proof. Suppose that the given congruence holds. We want to show that n is prime. Let d be a positive divisor of n such that $d < n$. Then d is among the numbers 1, 2, ..., $(n-1)$. Therefore d divides n and d divides $(n-1)!$. By the congruence, -1 is a linear combination of n and $(n-1)!$, so d divides -1. Since d is positive, d must be equal to 1. This argument shows that n has no positive divisors except 1 and n itself. So n is prime. □

P25. Theorem:
If $x^2 \equiv 3 \pmod{6}$, then $x \equiv 3 \pmod{6}$.

Proof. If $x^2 \equiv 3 \pmod{6}$, then because $3 \equiv 9 \pmod{6}$, we also have

$$x^2 \equiv 9 \pmod{6}$$

Raise both sides of this congruence to $\frac{1}{2}$. This gives

$$x \equiv 3 \pmod{6}$$

which completes the proof. □

3.7 Answers and solutions

E219
The hypothesis is

> "x and y are positive real numbers."

The conclusion is

> "The inequality
> $$\frac{x}{y} + \frac{y}{x} \geq 2$$
> holds."

E220
Hypothesis: " n is a positive integer".
Conclusion:

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

E221
Hypothesis:

n is an integer and $n > 2$.

Conclusion:

There are no positive integers x, y and z, such that $x^n + y^n = z^n$

E222
Hypothesis:

m is an integer.

Conclusion:

$m^2 + m + 1$ is odd.

P22
We are supposed to start with the hypothesis and from there prove the conclusion. The proof given starts with the conclusion and proves the hypothesis, which is completely wrong.
P23
If we prove something by cases, we must consider *all* possible cases. In the given situation, we should consider the cases of remainder 0, 1, and 2. The proof given only covers the cases of remainder 1 and 2. It would be correct if we added a proof for the case $n \equiv 0 \pmod 3$.
P24
This is an "if and only if" theorem. This means that we must prove two things: That Statement 1 implies Statement 2 and the other way around. The given proof proves that if the congruence holds, then n is prime. There should also be a proof showing that if n is prime, then the congruence holds.
P25
We are allowed to raise both sides of a congruence to a positive integer, but we cannot raise both sides to $\frac{1}{2}$, or take square roots. To see why, let $x = 3$. Then $x^2 \equiv 4 \pmod 5$, but it is NOT true that

$$x \equiv 2 \pmod 5$$