# M1F Notes

David Burgschweiger

November 1, 2015

# Contents

**1 Sets** **2**
1.1 Set Operators . . . . . 2
1.2 Intervals in $\mathbb{R}$ . . . . . 3
1.3 Infinite Unions and Intersections . . . . . 3

**2 Proofs** **3**
2.1 Elements of the propositional calculus . . . . . 3
2.2 Inference rules . . . . . 5
2.3 Proof-Practice . . . . . 6
2.4 Dis-Proving . . . . . 9

**3 Natural Numbers** **9**
3.1 Proof by Induction . . . . . 10
3.2 Prime numbers . . . . . 13

# 1 Sets

**Definition 1.0.1.** A set $S$ is a collection of objects (called *elements* of the set). If $x$ is an *element* of $S$ let us write $x \in S$ otherwise $x \notin S$.

**Remark 1.1.** The order of the elements or any repetition is unimportant.

**Example 1.1.**

$$\{1, 3\} = \{3, 1, 1\}$$

**Definition 1.0.2.** For two sets $S$ and $T$ let us write $S \subseteq T$ ($S$ is contained in $T$) if

$$x \in S \Rightarrow x \in T$$

**Result 1.0.1.** $S = T$ iff $S \subseteq T$ and $T \subseteq S$.

**Remark 2.1.** $S \notin S$ (Foundation Axiom)
Nonetheless, elements can be sets.

**Definition 1.0.3.** $\emptyset$ is the set with no elements.

**Property 3.1.** $\emptyset \subseteq S$ and $S \subseteq S$ for all sets S

## 1.1 Set Operators

**Definition 1.1.1.** The intersection $S \cap T$ of two sets $S$ and $T$ is

$$\{x |\ x \in S \,\text{and}\, x \in T\}$$

**Definition 1.1.2.** The union $S \cup T$ of two sets $S$ and $T$ is

$$\{x |\ x \in S \,\text{or}\, x \in T\}$$

**Definition 1.1.3.** The difference $S \backslash T$ of two sets $S$ and $T$ is

$$(S \cup T) \backslash (S \cap T)$$

**Definition 1.1.4.** The symmetric difference $S \triangle T$ of two sets $S$ and $T$ is

$$\{x |\ x \in S \,\text{and}\, x \in T \,\text{but not both}\}$$

**Definition 1.1.5.** In $A \subseteq \Omega$ then

$$A^C = \{x \in \Omega | x \notin A\} \qquad = \Omega \backslash A$$

**Remark 5.1.** The complement is only used when the reference set $\Omega$ is clear.

Some sets we will work with in this course are

$$\begin{aligned}
&\mathbb{N} = \{0, 1, 2, \dots\} \\
&\mathbb{Z} = \{0, 1, -1, 2, -2 \dots\} \\
&\mathbb{Q} = \left\{\frac{p}{q} |\ p \in \mathbb{N}, q \in \mathbb{Z}\backslash\{0\}\right\} \\
&\mathbb{R}\ \text{ reals} \\
&\mathbb{C}\ \text{ complex numbers}
\end{aligned}$$

**Definition 1.1.6.** $\mathbb{N}$ is defined by two axioms:

1. $0 = \emptyset \in \mathbb{N}$
2. If $n \in \mathbb{N}$ then $n + 1 \stackrel{def}{=} n \cup \{n\} \in \mathbb{N}$

**Example 6.1.**

$$\begin{aligned}
1 &= 0 + 1 = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
2 &= 1 + 1\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}
\end{aligned}$$

## 1.2 Intervals in $\mathbb{R}$

**Definition 1.2.1.** If $a, b \in \mathbb{R},\ a \leq b$:

$$\begin{aligned}
[a, b] &= \{t \in \mathbb{R} | a \leq t \leq b\} \\
(a, b) &= \{t \in \mathbb{R} | a < t < b\} \\
[a, b) &= \{t \in \mathbb{R} | a \leq t < b\} \\
(a, b] &= \{t \in \mathbb{R} | a < t \leq b\} \\
[a, \infty) &= \{t \in \mathbb{R} | a < t\} \\
(-\infty, b] &= \{t \in \mathbb{R} | t \leq b\}
\end{aligned}$$

## 1.3 Infinite Unions and Intersections

**Definition 1.3.1.** Suppose that, for all $n \in \mathbb{N}$, we are given a set $A_n$.

$$\begin{aligned}
\bigcup_{n=a}^{\infty} A_n &= \{x |\ \text{there exists a}\, n \in \mathbb{N}, n \geq a : x \in A_n\} \\
\bigcap_{n=a}^{\infty} A_n &= \{x |\ \text{for all}\, n \in \mathbb{N}, n \geq a : x \in A_n\}
\end{aligned}$$

**Example 1.1.**

$$\begin{aligned}
\bigcup_{n=1}^{\infty} \left[0, 1 - \frac{1}{n}\right] &= [0, 1) \\
\bigcap_{n=1}^{\infty} \left(1 - \frac{1}{n}, 1 + \frac{1}{n}\right) &= \{1\}
\end{aligned}$$

# 2 Proofs

## 2.1 Elements of the propositional calculus

**Definition 2.1.1.** A statement (proposition) is an assertion that can be either true (T) or false (F).

**Remark 1.1.** In maths such an assertion usually takes the form: "If such and such assumptions are made, then we can infer such and such conclusions."

**Example 1.1.**

- $n = 3$
- $(A+B)^2 = A^2 + 2AB + B^2$
- If it $n^2$ is odd, then $n$ is odd too.
- If it rains, then it is cloudy.
- For all real numbers $\geq 0$ there exists a square root.

**Definition 2.1.2.** A proof is a chain of statements linked by logical implications (inferences) that establish the truth of the last statement. In the course of the proof one is allowed to "call up"

- assumptions that are made.
- statements proven previously.
- axioms (statements that are generally accepted and never proven).

"Grammar elements" of mathematical statements are Quantifiers:

| Type | Sign | Meaning |
|---|---|---|
| Existential | $\exists$<br>$\exists_1$ | there exists<br>there exists a unique |
| Universal | $\forall$ | for all |
| | :, $\mid$ | such that |

Ways to form new statements from old ones:

- If $P$ is a statement then $\overline{P}$ "non-P" is the statement which is true if $P$ is false and false if $P$ is true.
- If $P$ and $Q$ are statements then we can form:

| Sign | Meaning |
|---|---|
| $P \wedge Q$, $P\&Q$ | $P$ and $Q$. |
| $P \vee Q$ | Either $P$ or $Q$ or both. |
| $P \veebar Q$ | Either $P$ or $Q$ but not both. |
| $P \Rightarrow Q$ | If $P$ then $Q$. |
| $P \Leftrightarrow Q$ | $P$ if and only if $Q$. |

**Remark 2.1.** $P \Rightarrow Q$ means any of the following:

- If $P$ then $Q$.
- $Q$ if $P$.
- $P$ is true only if $Q$ is true.
- $P$ only if $Q$.
- $P$ is sufficient for $Q$.
- $Q$ is necessary for $P$.
- If $Q$ is false then $P$ is false.
- $\overline{Q} \Rightarrow \overline{P}$

Similarly, $P \Leftrightarrow Q$ means any of the following:

- $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

- $P$ if and only if $Q$.
- $P$ is necessary and sufficient for $Q$.

The rigorous definition of $P \wedge Q$, $P \Rightarrow Q$ can be made through a truth table

**Definition 2.1.3.** $P \wedge Q$ is defined by:

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

**Definition 2.1.4.** Also, $P \Rightarrow Q$ is defined by:

| $P$ | $Q$ | $P \Rightarrow Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

**Example 4.1.** The statement "If $x \in \{n \in \mathbb{N}|\ n^2 < 0\}$ then x is a sheep." is true as well as the statement "If $x \in \{n \in \mathbb{N}|n^2 < 0\}$ then x is not a sheep."

## 2.2 Inference rules

**Example 0.2.** *Premise 1.* If it is raining then it is cloudy.
*Premise 2.* It is raining.
*Conclusion.* It is cloudy.

We can write this more abstractly as follows:
P: it is raining
Q: it is cloudy
In this form:
*Premise 1.* $P \Rightarrow Q$
*Premise 2.* $P$
*Conclusion.* $Q$

This is an example of an inference rule which we write like this:

$$((P \Rightarrow Q) \wedge P) \Rightarrow Q$$

There are other inference rules:

$$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$$
$$\left((P \vee Q) \wedge \overline{P}\right) \Rightarrow Q$$
$$(P \wedge Q) \Rightarrow P$$
$$((P \Rightarrow Q) \vee (P \Rightarrow R)) \Rightarrow P \Rightarrow (Q \vee R)$$
$$((P \vee Q) \wedge (P \Rightarrow (P \wedge Q))) \Rightarrow (R \Rightarrow R)$$
$$\left((P \Rightarrow Q) \wedge \left(P \Rightarrow \overline{Q}\right)\right) \Rightarrow \overline{P}$$
$$P \wedge (Q \vee R) \Rightarrow (P \wedge Q) \vee (P \wedge R)$$

**Exercise 1.** Proof that

$$\forall n \in \mathbb{N}, n^2 \,\text{odd} \Rightarrow n \,\text{odd} \quad .$$

**Example 0.3.** Is the following a valid argument:

1. If a movie is not worth seeing, then it is not made in the UK.

2. A movie is worth seeing only if Prof Corti reviews it.
3. "The Maths Graves" was not not reviewed by Prof Corti.
4. Therefore, "The Maths Graves" is not made in the UK.

In order to determine this, let us rewrite the argument in a more formal way:

| Variable | Meaning |
|---|---|
| $M$ | the set of all movies |
| $W(x)$ | "$x$ is worth seeing" |
| $UK(x)$ | "$x$ is made in the UK" |
| $C(x)$ | "Prof Corti reviews $x$" |
| $m$ | "The Maths Games" $\in M$ |

Now the argument can be expressed as:

$$\begin{aligned}
&\forall x \in M : && \overline{W(x)} \Rightarrow \overline{UK(x)} && (1)\\
&\forall x \in M : && W(x) \Rightarrow C(x) && (2)\\
& && \overline{C(m)} && (3)\\
&((1) \wedge (2) \wedge (3)) \Rightarrow && \overline{UK(x)} && (4)
\end{aligned}$$

Yes it is a valid argument. Indeed, it is the same as:

$$\begin{aligned}
&\forall x \in M : && UK(x) \Rightarrow W(x)\\
&\forall x \in M : && W(x) \Rightarrow C(x)
\end{aligned}$$

Then you say:

$$\begin{aligned}
&\forall x \in M && \overline{C(x)} \Rightarrow \overline{UK(x)}\\
& && \overline{C(m)}\\
& && \Rightarrow \overline{UK(m)}
\end{aligned}$$

**Result 2.2.1.** What can we learn from this? If we want to be understood, we have to learn to present our arguments better. For instance, try to put everything in the positive. Use "if then" throughout. A better way of writing would be:

1. If $x$ is made in the UK, then $x$ is worth seeing.
2. If $x$ is worth seeing then Prof Corti reviews it.
3. Prof Corti did not review $m$.
4. Therefore $m$ is not made in the UK.

## 2.3 Proof-Practice

**Theorem 2.3.1.** Let $A$, $B$, $C$, $\Omega$ be sets with $A, B \in \Omega$. Then:

$$\begin{aligned}
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) && (1)\\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) && (2)\\
(A \cup B)^C &= A^C \cap B^C && (3)\\
(A \cap B)^C &= A^C \cup B^C && (4)
\end{aligned}$$

**Exercise 2.** Draw pictures of these statements.

*Proof.* Consider (1). We show first:

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$

Suppose that $x \in A \cap (B \cup C)$ then $x \in A$ and $x \in B \cup C$.

That is:

$$\begin{aligned} & x \in A \wedge (x \in B \vee x \in C) \\ \Leftrightarrow \quad & x \in A \cap B \vee x \in A \cap C \\ \Leftrightarrow \quad & x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

This shows $\subseteq$. Now we show:

$$A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

Suppose $x \in (A \cap B) \cup (A \cap C)$ then $x \in A \cap B$ or $x \in A \cap C$. We now distinguish between two cases:

1. $x \in A \cap B$. Then $x \in A$ and $x \in B$. Therefore, $x \in A$ and $x \in B \cup C$. Hence, $x \in A \cap (B \cup C)$
2. $x \in A \cap C$. Then $x \in A$ and $x \in C$. Therefore, $x \in A$ and $x \in B \cup C$. Hence, $x \in A \cap (B \cup C)$.

**Remark 0.1.** We split the proof of $C$ in two cases. In doing so we used the inference rule:

$$(P \vee Q, P \Rightarrow R, Q \Rightarrow R) \Rightarrow R$$

Please finish the proof of the other statements in your own □

**Axiom 1.** *Archimedeon Axiom*

$$\forall r \in \mathbb{R}\ \exists n \in \mathbb{N}: \quad n > r$$

**Lemma 2.1.**

$$\forall a \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad \left( \forall n \in \mathbb{N}, n \geq 1: \quad x \geq a - \frac{1}{n} \right) \quad \Rightarrow \quad x \geq a$$

*Proof.* We argue by contradiction. Hence we want to show

$$\left( \exists n \in \mathbb{N}, n \geq 1: \quad x < a - \frac{1}{n} \right) \quad \Leftarrow \quad x \leq a$$

By the Archimedeon Axiom

$$\exists n: \quad n > \frac{1}{a - x}$$

And then also

$$\frac{1}{n} < a - x$$

Therefore

$$x < a - \frac{1}{n}$$

□

$$\bigcup_{n=1}^{\infty} \left[ 0, 1 - \frac{1}{n} \right] = [0, 1) \tag{1}$$

$$\bigcap_{n=1}^{\infty} \left( 1 - \frac{1}{n}, 1 + \frac{1}{n} \right) = \{1\} \tag{2}$$

*Proof.* (2) By definition

$$\bigcap_{n=1}^{\infty} A_n = \{a |\ \forall n,\ a \in A_n\}$$

Then

$$L = \bigcap_{n=1}^{\infty} \left(1 - \frac{1}{n}, 1 + \frac{1}{n}\right) = \left\{x \in \mathbb{R} |\ \forall n \in \mathbb{N} :\ 1 - \frac{1}{n} < x < 1 + \frac{1}{n}\right\}$$

Clearly $1 \in L$. This proofs $\supseteq$.

No we are going to prove $\subseteq$. We need to show

$$\left(\forall n \in \mathbb{N} \quad 1 - \frac{1}{n} < x < 1 + \frac{1}{n}\right) \Rightarrow x = 1$$

By the lemma, $x \geq 1$. There is a similar lemma that states

$$\left(\forall n, \quad x \leq 1 + \frac{1}{n}\right) \Rightarrow x \leq 1$$

So in fact $x \geq 1$ and $x \leq 1$. Thus $x = 1$. This shows $\subseteq$.

(1) Recall that by definition

$$\bigcup_{n=1}^{\infty} A_n = \{a |\ \exists n :\ a \in A_n\}$$

It is easy to see

$$\bigcup_{n=1}^{\infty} \left[0, 1 - \frac{1}{n}\right) \subseteq [0, 1)$$

Indeed if

$$\exists n : \quad 0 \leq x \leq 1 - \frac{1}{n}$$

then

$$0 \leq x < 1$$

This shows $\supseteq$, as next we show $\subseteq$. This means exactly

$$(0 \leq x < 1) \Rightarrow \left(\exists n :\ 0 \leq x \leq 1 - \frac{1}{n}\right)$$

By the Archimedeon axiom

$$\exists n : \quad n > \frac{1}{1 - x}$$

Hence $\frac{1}{n} < 1 - x$ and then $x < 1 - \frac{1}{n}$. □

Show that for $n \in \mathbb{N}$, $n^2$ odd $\Rightarrow$ $n$ odd.

*Flawed proof.* If $n$ is odd then $n = 2k + 1$ for some $k \in \mathbb{N}$ and then

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\left(2k^2 + 2k\right) + 1 \end{aligned}$$

So $n^2$ is odd.

*Proof.* We need to take the following statement for granted, which will be proven later in the document:

$$\forall n \in \mathbb{N} : \quad \exists k \in \mathbb{N} :\ n = 2k \quad \vee \quad \exists k \in \mathbb{N} :\ n = 2k + 1$$

Assuming that we argue by contradiction:

$$\begin{gathered} n \,\text{even} \Rightarrow n^2 \,\text{even} \\ n = 2k \Rightarrow n^2 = 2\left(2k^2\right) \end{gathered}$$

□

### 2.4 Dis-Proving

How to form the negation of a statement? Given $P$, how to form $\overline{P}$? Rule 1

$$\begin{aligned} & P = (\forall x \in A, Q(x)) \\ \Rightarrow \quad & \overline{P} = (\exists x \in A, \overline{Q(x)}) \end{aligned}$$

Rule 2

$$\begin{aligned} & P = (\exists x \in A, Q(x)) \\ \Rightarrow \quad & \overline{P} = (\forall x \in A, \overline{Q(x)}) \end{aligned}$$

**Exercise 3.** Show that Rule 2 is the same as Rule 1.

**Remark 0.2.** An element $a \in A$ such that $\overline{Q(a)}$ is called a counterexample to the statement

$$(\forall x \in A, Q(x))$$

Indeed the very existence of this example $a \in A$ shows that $P$ is false (it "counters" P).

A typical exam question is:
Prove or disprove the following statement:
If $p \in \mathbb{N}$ is prim then $\exists a, b \in \mathbb{Z}: \; p = a^2 + b^2$
This statement is false. Counterexample: 3

$$\begin{aligned} P &= (\forall p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad (\exists (a,b) \in \mathbb{Z}^2 : p = a^2 + b^2)) \\ \overline{P} &= (\exists p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad \overline{(\exists (a,b) \in \mathbb{Z}^2 : p = a^2 + b^2)}) \\ \overline{P} &= (\exists p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad (\forall (a,b) \in \mathbb{Z}^2 : p \neq a^2 + b^2)) \end{aligned}$$

We prove $\overline{P}$ thus we have to name a particular prime name $p = 3$. We claim:

$$\forall a, b \in \mathbb{Z}: \quad a^2 + b^2 \neq 3$$

*Proof.* Suppose for contradiction that for some $a, b \in \mathbb{Z}$, $a^2 + b^2 = 3$. Note that $a^2, b^3 \geq 0$ so both $a^2, b^2 \leq 3$ This means that $|a|, |b| \leq 1$ but then $a^2, b^2 \leq 1$ and $a^2 + b^2 \leq 2$. □

## 3 Natural Numbers

**Axiom 2.** *Smallest element axiom.*
Let $\emptyset \neq S \subseteq \mathbb{N}$. Then $S$ has a smallest element.

($a \in S$ is smallest if $\forall b \in S: \; a \leq b$. A smallest element is clearly unique.)

**Theorem 3.0.1.**

$$\forall n, p \in \mathbb{N}, \quad \exists_1 q, r \in \mathbb{N}: \quad n = pq + r, 0 \leq r < p$$

Special case
For $p = 2$ this says that there exists a $q$ such that either $n = 2q$ or $n = 2q + 1$ (but not both).

*Proof.*

$$S = \{q \in \mathbb{N} |\; \exists k \in n : \quad y = n - pk\}$$

$S \neq \emptyset$ because $n \in S$ The axiom says that $S$ has a smallest element.
Take $k$ =0. Claim: $0 \leq r < p$. Indeed if $r \geq p$ then

$$r' = r - p = r - pk_0 - p = r - p(k_0 + 1) \in S$$

and $r' < r$ so $r$ is not the smallest element. Take $q = k_0$ then:

$$n = pq + r \qquad\qquad 0 \leq r < p$$

it remains to shows uniqueness. To show uniqueness suppose

$$n = pq_1 + r_1$$
$$n = pq_2 + r_2 \qquad 0 \le r_1, r_2 < p$$

Without loss of generality we may assume $r_1 \le r_2$.

$$0 \le r_2 - r_1 = (q_1 - q_2)p < p$$

So $0 \le q_1 - q_2 < 1 \quad \Rightarrow \quad q_1 = q_2$ and $r_1 = r_2$ □

## 3.1 Proof by Induction

Principle of induction: Suppose that $\forall n \in \mathbb{N}$ we are given a statement $P_n$. Assume that:

1. $P_0$ holds;
2. $\forall n \in \mathbb{N}, (Pn \Rightarrow P_{n+1})$ holds

Then $\forall n \in \mathbb{N}$, $P_n$ holds.

**Example 0.4.**

$$P_n : \qquad 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Let us show $P_n \Rightarrow P_{n+1}$. Assume that

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

then

$$0 + 1 + 2 + \cdots + n + (n+1) = (0 + 1 + 2 + \cdots + n) + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

$P_0$ is the statement that $0 = 0$. Therefore $\forall n$ the formula is true.

*Proof.* We argue by contradiction. Suppose that the conclusion is false. That means:

$$\exists n \in \mathbb{N} : \qquad \overline{P_n}$$

In other words:

$$S = \{n \in \mathbb{N} | \ \overline{P_n}\} \neq \emptyset$$

Let $k$ be the smallest element of $S$. $k$ exists by the smallest element axiom. $k - 1 < k$, therefore $k - 1 \in S$, thus $P_{k-1}$ holds. But:

$$P_{k-1} \Rightarrow P_k$$

□

**Example 0.5.** The Fibonacci sequence. $\forall n \in \mathbb{N}$ define $F_n$ inductively by the formula:

$$F_0 = 0, \quad F_1 = 1, \quad \forall n \ge 2 F_n = F_{n+1} + F_{n+2}$$

Let us prove by induction that:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

The really interesting thing would be to understand how one can "come up" with a formula like this. Another interesting thing would be to "stare" at the formula and see what we can learn from it about life. Instead wo focus on a "minor" print of logic.

*Wrong proof.* To prove by induction you need to declare at the outset, $\forall n$ what is $P_n$. Your instinct here will be to say

$$P_n : \qquad F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Then you will write:

$$\begin{aligned} F_{n+1} &= F_n + F_{n+1} \\ &= (\dots) + (\dots) \end{aligned}$$

**Remark 0.3.** You have used both, $P_{n-1}$ and $P_n$. However, for induction you can only use $P_n$.

*Proof.* We use the principle of induction with:

$$Q_n = (P_n \wedge P_{n+1})$$

We need to show $\forall n: \ Q_n \Rightarrow Q_{n+1}$. Suppose $(P_n \wedge P_{n+1} \Rightarrow P_{n+1}) \Rightarrow ((P_n \wedge P_{n+1}) \wedge (P_{n+1} \wedge P_{n+2}))$. Hence we only need to proof that $P_n \wedge P_{n+1} \Rightarrow P_{n+2}$ Assume $P_n \wedge P_{n+1}$, then:

$$\begin{aligned} F_{n+1} = F_{n+1} + F_n =& \frac{1}{\sqrt{5}}\left(\varphi^{n+1} - \psi^{n+1}\right) + \frac{1}{\sqrt{5}}\left(\varphi^n - \psi^n\right) \\ =& \frac{1}{\sqrt{5}}\varphi^n(\varphi+1) + \frac{1}{\sqrt{5}}\psi^n(\psi+1) \end{aligned}$$

Since $\varphi$ and $\psi$ are solutions of the equation $x^2 - x - 1 = 0$ we can rewrite that as:

$$\begin{aligned} &\frac{1}{\sqrt{5}}\varphi^n\varphi^2 + \frac{1}{\sqrt{5}}\psi^n\psi^2 \\ =& \frac{1}{\sqrt{5}}\varphi^{n+2} + \frac{1}{\sqrt{5}}\psi^{n+2} \end{aligned}$$

So $P_{n+2}$ holds. We have shown that $\forall n: \ Q_n \Rightarrow Q_{n+1}$. To finish the proof we need $Q_0 = (P_0 \wedge P_1)$.

$$P_0 \qquad F_0 = \frac{1}{\sqrt{5}}\left(\varphi^0 - \psi^0\right) = 1$$

$$P_1 \qquad F_1 = \frac{1}{\sqrt{5}}\left(\varphi^1 - \psi^1\right) = 1$$

□

**Theorem 3.1.1.** Principle of strong induction.
Suppose that $\forall n \in \mathbb{N}$ we are given a statement $Q_n$. Assume that:

1. $Q_0$ holds;
2. $\forall n, \ (\forall k \leq n : \ Q_k) \Rightarrow Q_{n+1}$

Then $\forall n \in \mathbb{N}, \ Q_n$ holds.

*Proof.* Apply induction with:

$$(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_n)$$

□

**Definition 3.1.1.** $n \neq 0, 1 \in \mathbb{N}$ is irreducible if:

$$\forall u, v \in \mathbb{N}: \quad n = uv \quad \Rightarrow \quad u = 1 \vee v = 1$$

**Theorem 3.1.2.** Every $n \in \mathbb{N}, n \neq 0, 1$ is the product of irreducibles.

*Proof.* We are going to prove the statement by strong induction. Let $Q_n$ be the statement that $n$ is the product of irreducibles.

$Q_0$ clearly holds.

Assume $Q_n$ for $k \leq n$. If $n+1$ is irreducible then $Q_{n+1}$. Otherwise $n+1 = u \cdot v$ where $1 < u < n+1$ and $1 < v < n+1$. By $Q_u, u$ is prod of irreducibles. By $Q_v, v$ is the product if irreducibles. Therefore, $Q_{n+1}$ holds. $\square$

**Definition 3.1.2.** For $c, a \in \mathbb{Z}$ we say that $c$ divides $A$ and write $c|A$ if

$$\exists R \in \mathbb{Z}: \quad cR = A$$

**Remark 2.1.**

$$c|A_1 \wedge c|A_2 \Rightarrow c|(A_1 + A_2)$$
$$c|A \Rightarrow \forall B \in \mathbb{Z}, c|AB$$

**Definition 3.1.3.**

$$\forall a, b \in \mathbb{Z}: \quad hcf(a,b) = \text{Highest Common Factor} = \max\{t \in \mathbb{Z}| \quad t|a \wedge t|b\}$$

**Remark 3.1.**

$$\text{hcf}(a,b) = \text{hcf}(\pm a, \pm b) \in \mathbb{N} = \text{hcf}(b,a)$$

Let us now consider the *Division Algorithm* to compute the highest common factor.
Suppose $a, b \in \mathbb{N}$ with $a \geq b$. We know from last time:

$$\exists q, r \in \mathbb{N}, \quad 0 \leq r < b: \quad a = bq + r$$

Note that

$$(t|a \wedge t|b) \quad \Leftrightarrow \quad (t|b \wedge t|r)$$

This implies that $\text{hcf}(a,b) = \text{hcf}(b,r)$. $a \geq b > r$ so the pair $(b,r)$ is smaller than the pair $(a,b)$, hence our algorithm will eventually come to an end. And I can assume by induction that I know to compute $k$ and $(b,r)$.

**Theorem 3.1.3.** If $c = \text{hcf}(a,b)$ then

$$\exists y, x \in \mathbb{Z}: \quad c = ac + by$$

*Proof.* Assume $a \geq b > 0$ then write $a = bq + r$. But what we said:

$$\text{hcf}(a,b) = \text{hcf}(q,r) = c$$

$(q,r)$ is smaller than $(a,b)$ so by induction there exist $x_0, g_0$ such that

$$\begin{aligned} c &= rx_0 + by_0 \\ &= (a - bq)x_0 + by_0 \\ &= ax_0 + b(y_0 - qx_0) \end{aligned}$$

$\square$

**Example 3.1.** Compute $\text{hcf}(1734, 371) = c$ and $x, y \in \mathbb{Z}$ such that $1734 + 371y = c$

$$\begin{aligned} & & 1734 &= 4 \cdot 371 + 250 \\ \Rightarrow & & \text{hcf}(1734, 371) &= \text{hcf}(371, 250) \\ & & 371 &= 1 \cdot 250 + 121 \\ \Rightarrow & & \text{hcf}(371, 250) &= \text{hcf}(250, 121) \\ & & 250 &= 2 \cdot 121 + 8 \\ \Rightarrow & & \text{hcf}(250, 121) &= \text{hcf}(121, 8) \\ & & 121 &= 15 \cdot 8 + 1 \\ \Rightarrow & & \text{hcf}(121, 8) &= \text{hcf}(8, 1) \end{aligned}$$

So $c = 1$.

$$\begin{aligned}1 &= -15 \cdot 8 + 121\\ &= -15(-2 \cdot 121 + 250) + 121\\ &= 31 \cdot 121 - 12 \cdot 250\\ &= 31 \cdot (-1 \cdot 250 + 371) - 15 \cdot 250\\ &= -46 \cdot 250 + 31 \cdot 371\\ &= -44(-4 \cdot 371 + 1734) + 31 \cdot 371\\ &= 215 \cdot 371 - 46 \cdot 1734\end{aligned}$$

**Definition 3.1.4.** We say that $a, b \in \mathbb{Z}$ are *co-prime* if $\operatorname{hcf}(a, c) = 1$.

## 3.2 Prime numbers

**Definition 3.2.1.** $p \in \mathbb{N}\backslash\{0, 1\}$ is prime if:

$$\forall A, B \in \mathbb{Z} : \quad p|AB \Rightarrow p|A \vee p|Q$$

**Theorem 3.2.1.** $P \in \mathbb{N}$ is irreducible if and only if it is prime.

*Proof.* Suppose $p$ is prime, i.e.

$$p|uv \quad \Rightarrow \quad (p|u \vee p|v)$$

If $p|u$ then $u = kp$ and

$$p = uv = (kv)p \quad \Rightarrow \quad 1 = kv \quad \Rightarrow \quad v = 1$$

Similarly if $p|v$ then $u = 1$. This shows $p$ is irreducible.

Now suppose $p$ is irreducible. Suppose $p|AB$. Because $p$ is irreducible, the positive divisors of $p$ are just 1 and $p$. Therefore, either $\operatorname{hcf}(p, A) = 1$ or $\operatorname{hcf}(p, A) = p$.

If $\operatorname{hcf}(p, A) = p$ then $p|A$ and we can close. Suppose $hcf(p, A) = 1$. Then $\exists x, y \in \mathbb{Z}$ such that:

$$xp + yA = 1$$

But then

$$xpB + yAB = B$$

$p$ divides the first part because there is a $p$ there. $p$ divides the second part because we are assuming $p|AB$. So $p|B$. □

**Definition 3.2.2.** Let $p$ be prime. Then

$$\forall N \in \mathbb{Z}, \quad \operatorname{ord}_p N = \max\left\{k \in \mathbb{N} | \quad p^k | N\right\}$$

= exponent of the largest power of $p$ that divides $n$.

**Example 2.1.**

$$\begin{aligned}\operatorname{ord}_2 3 &= 0\\ \operatorname{ord}_2 24 &= 3\end{aligned}$$

**Property 2.1.**

$$\forall N_1, N_2 \in \mathbb{Z} \qquad \operatorname{ord}_p(N_1 + N_2) \geq \min\{\operatorname{ord}_p N_1, \operatorname{ord}_p N2\} \tag{1}$$

$$\operatorname{ord}_p(N_1, N_2) = \operatorname{ord}_p N_1 + \operatorname{ord}_p N_2 \tag{2}$$

*Proof.* (1) If $p^k|N_1$ and $p^k|N_2$ then $p^k|N_1 + N_2$.

(2)

$$a_1 = \operatorname{ord}_p N_i$$

means

$$p^{a_i}|N_i \quad \wedge \quad p^{a_i+1} \nmid N_i$$

It is clear that

$$(p^{a_i}|N \wedge p^{a_2}|N_2) \quad \Rightarrow \quad p^{a_1+a_2}|N_1 N_2$$

What we need to show is:

$$p^{a_1+a_2+1} \nmid N_1 N_2$$

Write $N_i = p^{a_i} A_i$ where $p_i \nmid A_i$. Then

$$N_1 N_2 = p^{a_1+a_2} A_1 A_2$$

and

$$p \nmid A_1, p \nmid A_2 \quad \Rightarrow \quad p \nmid A_1 A_2$$

□

**Result 3.2.1.** If $p$ is a prime then $\sqrt{p}$ is irrational.

*Proof.* Suppose for contradiction that $r^2 = p$ with $r = \frac{k}{n} \in \mathbb{Q}$.

$$\frac{k^2}{n^2} = p$$

or equivalently:

$$k^2 = pn^2$$
$$2 \operatorname{ord}_p k = \operatorname{ord}_p(pn^2) = 1 + 2 \operatorname{ord}_p n$$

This is a contradiction. ( A number can only be either odd or even but not both.) □

**Definition 3.2.3.** $N \in \mathbb{Z}$ is a perfect square if $\exists k \in \mathbb{Z} : N = k^2$.

**Exercise 4.** $N$ is a perfect square iff for all primes $p$, $\operatorname{ord}_p N$ is even.

**Example 3.1.** $\sqrt{N} \in \mathbb{Q} \Leftrightarrow N$ is a perfect square.

*Proof.* $\Leftarrow$ is obvious.

We need to deal with $\Rightarrow$. Suppose $\exists r = \frac{k}{n} \in \mathbb{Q}$ such that $r^2 = N$.

Suppose for contradiction that $N$ is not a perfect square. i.e. there exists a prime $p$ such that $\operatorname{ord}_p N$ is odd. As before we write:

$$k^2 = n^2 N$$
$$2 \operatorname{ord}_p k = \operatorname{ord}_p k^2 = 2 \operatorname{ord}_p n + \operatorname{ord}_p N$$

This is a contradiction because we have an even number on the left and an odd number on the right hand side. □

**Theorem 3.2.2.** The fundamental theorem of arithmetic.
Every $n \in \mathbb{N}$ can be written uniquely in the form:

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

where $p_1 < p_2 < \cdots < p_r$ are primes and $a_i \in \mathbb{N}\backslash 0$ for $i \in \mathbb{N}\backslash\{0\}$.

*Proof.* We already know that $n$ can be written like this. For uniqueness:

$$a_i = \operatorname{ord}_{p_i} n$$

□

**Remark 3.1.** What you are really doing is:

$$\begin{aligned} n &= p_1^{a_1} \dots p_r^{a_r} \\ \Rightarrow \qquad \operatorname{ord}_{p_i} n &= \operatorname{ord}_{p_i} (p_1^{a_1} \dots p_r^{a_r}) \\ &= a_1 \operatorname{ord}_{p_i} p_1 + \dots a_{i-1} \operatorname{ord}_{p_i} p_{i-1} + a_i \operatorname{ord}_{p_i} p_i + a_{a+1} \operatorname{ord}_{p_i} p_{i+1} + \dots + a_r \operatorname{ord}_{p_i} p_r = a_i \end{aligned}$$

because $\operatorname{ord}_{p_i} p_i = 1$ and $\operatorname{ord}_{p_j} p_j = 0$ if $i \neq j$.

**Example 3.2.** There are infinitely many primes. Suppose for a contradiction that:

$$P = \{\text{all primes}\} = \{p_1 < p_2 < \dots < p_r\}$$

Consider $N = p_1 p_2 \dots p_r + 1$. Claim $\operatorname{hcf}(N, p_i) = 1$ for all $i = 1, \dots, r$. Manifestly $\exists x, y \in \mathbb{Z}$ such that $xN + yp_i = 1$. Hence, $N$ contradicts the prime decomposition theorem.

New things about hcf.

**Lemma 3.1.** Suppose $\operatorname{hcf}(a, b) = 1$. Then for all $C \in \mathbb{N}$

$$(a|C \wedge b|C) \Rightarrow ab|C \tag{1}$$
$$a|bC \Rightarrow a|C \tag{2}$$

*Proof.*

$$\exists x, y \in \mathbb{Z} : \quad ax + by = C \tag{$*$}$$

For (1) multiply ($*$) with $C$. We get

$$axC + byC = C$$

$b|C \Rightarrow ab|aC$ so $ab$ divides $axC$. $a|C \Rightarrow ab|bC$ so $ab$ divides $byC$. Therefore, $ab|C$.
For (2) again

$$axC + byC = C$$

$a$ obviously divides $axC$ and $byC$ as well because of our assumption. Thus $a|C$. □

**Theorem 3.2.3.** Suppose $c|a$ and $c|b$. Then $c| \operatorname{hcf}(a, b)$.

*Proof.* Indeed let $d = \operatorname{hcf}(a, b)$. We know $\exists x, y \in \mathbb{Z}$ such that

$$ax + by = d$$

$c$ divides $ax$ as well as $bx$. Thus, $c|d$ □

It follows easily from unique prime factorization that for all $p$, $\operatorname{ord}_p \operatorname{hcf}(a, b) = \min\{\operatorname{ord}_p a, \operatorname{ord}_p b\}$. Another way to say this is: if

$$a = \Pi p_i^{r_i}, b \qquad\qquad = \Pi p_i^{s_i}$$

Then

$$\operatorname{hcf}(a, b) = \Pi p_i^{\min\{r_i, s_i\}}$$

**Remark 3.2.** This is a really bad method for computing the hcf.

**Example 3.3.** • (a Diophantine equation)
Solve for $x, y \in \mathbb{N}$:

$$4y^2 = x^3 + 1$$

Write this as:

$$x^3 = 4y^2 - 1 = (2y + 1)(2y - 1)$$

Note that $\mathrm{hcf}(2y + 1, 2y - 1) = c = 1$:

$$(c|2y + 1 \ \wedge \ c|2y - 1) \quad \Rightarrow \quad c| \ (2y + 1) - (2y + 1) = 2$$

but both numbers are odd so $c = 1$.

Suppose $\mathrm{hcf}(A, B) = 1$ and $AB = x^3$ is a perfect cube. Then both $A, B$ are perfect cubes. Indeed, if $p$ prime, $\mathrm{ord}_p\, AB = 3k$ and at least one of $\mathrm{ord}_p\, A,\ \mathrm{ord}_p\, B = 0$.

So $2y - 1, 2y + 1$ are both perfect cubes. Only small cubes can have such a small distance.

$$\ldots \quad -27 \quad -8 \quad -1 \quad 0 \quad 1 \quad 8 \quad 27 \quad \ldots$$

At the end:

$$\begin{aligned} 2y - 1 &= -1 \\ 2y + 1 &= 1 \\ \Rightarrow \qquad y = 0 &\quad \wedge \quad x = -1 \end{aligned}$$

These are all the solutions!

- Suppose $A, B, C \in \mathbb{Z}$. We want to find all solutions $x, y \in \mathbb{Z}$ of:

$$Ax + By = C$$

Sometimes we may want to look for $x, y \in \mathbb{N}$. Let us consider the more special example

$$3x + 7y = 18 \tag{1}$$

Ordinarily, you would use Euklid's algorithm to find one solution. This one solution can then help to find the general solution. In this case it is easy to spot one: $(x, y) = (6, 0)$. Write $(x, y) = (x_0, y_0) + (x', y')$ and

$$\begin{aligned} 3x + 7y &= 18 \\ \Leftrightarrow 3x' + 7y' &= 0 \end{aligned} \tag{2}$$

Thus, finding all solutions of (2) is the same as finding all solutions of (1). Note: $7y' = -3x'$.

$$(\mathrm{hcf}(7, 3) = 1 \quad \wedge \quad 7|3x') \qquad \Rightarrow 7|x'$$

Therefore, there exists a $t \in \mathbb{Z} : x' = 7t$. Then $7y' = -3t$ The set of all solutions is precisely:

$$\{(x, y)| \quad (x, y) = (6, 0) + t(7, -3), \quad t \in \mathbb{Z}\}$$

We think of this as a parametrised 'integral line'.