Numbers & Sets

Lectured by Prof Imre Leader

Michaelmas 2013

Contents

1 Proofs

Defintion. A *proof* is a sequence of (mathematical) statements that logically establishes a conclusion.

We need proofs for two reasons:

1. To be *sure* that statements are true.

2. To understand *why* they are true.

1.1 Examples

Theorem. For any positive integer n, $n^3 - n$ is a multiple of 3.

Proof. For an positive integer n, $n^3 - n = n(n-1)(n+1)$ which is the product of 3 consecutive integers, one of which must therefore be a multiple of 3. So $n(n-1)(n+1) = n^3 - n$ is a multiple of 3. □

Note that proving $A \Rightarrow B$ is different to proving $B \Rightarrow A$.

2 Elementary Number Thoery

2.1 The Natural Numbers

Intuitively, the natural numbers consists of

$$1, (1+1), (1+1+1), (1+1+1+1), ...$$

a list of distinct numbers, going on forever.

More formally, the natural numbers consists of a set $\mathbb{N}$ with an element '1' and an operation '+1' satisfying:

1. $\forall n : n + 1 \neq 1$
2. $\forall n, m : n \neq m \implies n + 1 \neq m + 1$
3. For any property P, if $P(1)$ holds and $\forall n : P(n) \implies P(n+1)$, then $P(n)$ holds for all n. (This is known as 'induction')

Intuitively, this last axiom captures the idea of 'that list is everyting, and nothing more', by taking the property P to be "is on the list".

Together, these three axioms are called the *peano axioms*.

2.1.1 Operations on the Natural Numbers

To save us having to write out '+1' many times, we can write:
2 for $1 + 1$,
3 for $1 + 1 + 1$
etc.
We can also define an operation '+2' by $n+2 = n+1+1$. Having defined '$+k$', we define '$+(k+1)$' by $n + (k+1) = (n+k) + 1$. This defines '$+k$ ' for all k, by induction.

Multiplication, powers, etc. can be defined in a similar way.

2.1.2 Properties

We can prove the usual algebraic rules:

1. $\forall a, b : a + b = b + a$ (addition is commutitive)
2. $\forall a, b, c : a + (b + c) = (a + b) + c$ (addition is associative)
3. $\forall a, b : ab = ba$ (multiplication is commutative)

4. $\forall a, b, c : a(bc) = (ab)c$ (multiplication is associative)

5. $\forall a, b, c : a(b + c) = ab + ac$ (multiplcation is distributative over addition)

6. $\forall a : 1.a = a$ (identity for multiplication)

2.1.3 Inequalities

Define $a < b$ to mean: $a + c = b$ for some natural number c. From this, we can prove:

1. $\forall a, b, c : a < b \implies a + c < b + c$
2. $\forall a, b, c : a < b \implies ac < bc$
3. $\forall a, b, c : a < b \ \& \ b < c \implies a < c$
4. $\forall a : \neg(a < a)$

2.2 Strong Induction

Induction says that if we know $P(1)$ and that for all n, $P(n) \implies P(n+1)$ then $P(n)\forall n$.

A more useful form, *strong induction* is: if $P(1)$ and for all n, $P(m)\forall m < n \implies P(n)$, then $P(n)\forall n$.
To see why strong induction is valid, just apply (ordinary) induction to $Q(n)$, defined as $P(m)\forall m \leq n$.

To show $P(n)$, we would normally take an arbitrary n and prove $P(n)$. Induction says: if, during that proof, it would help you to assume that $P(m)$ for some $m < n$, feel free to do so. This is the correct view of induction.

There are two equivalent forms of strong induction:

1. If $P(n)$ false for some n then there exists n with $P(n)$ false but $P(m)$ true $\forall m < n$. ('If there's a counter-example, then there's a minimal counter-example')
2. If $P(n)$ for some n, then there is a least n with $P(n)$ holding. ('Well-ordering principle')

2.3 The Integers

The integers, written $\mathbb{Z}$, consist of all expressions n and $-n$ (n a natural number) and 0.

2.3.1 Operations and Properties

We can define $+$, $\cdot$ (from $\mathbb{N}$) and have the previous algebraic rules, together with:

7. $\forall a : a + 0 = a$ (identity for addition)

8. $\forall a \exists b : a + b = 0$ (inverses for addition)

Define $a < b$ if $a + c = b$, for some *natural* number c. We then have the same rules as with natural numbers of $<$ except:

$$\forall a, b, c : a < b \ \& \ 0 < c \implies ac < bc$$

2.4 The Rationals

The rationals, written $\mathbb{Q}$, consist of all expressions $\frac{a}{b}$ (a horizontal line b), where a and b are integers with $b \neq 0$, and $\frac{a}{b}$ and $\frac{c}{d}$ regarded as equal if $ad = bc$. We can view $\mathbb{Z}$ as being inside $\mathbb{Q}$ (viewing n as $\frac{n}{1}$).

2.4.1 Operations

We can define $+$ on $\mathbb{Q}$ by:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and $\cdot$ on $\mathbb{Q}$ as:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We then get all the previous algebraic rules, plus:

9. $\forall a \neq 0 : \exists b$ with $ab = 1$. (inverses for $\cdot$)

Define $\frac{a}{b} < \frac{c}{d}$ $(b, d > 0)$ if $ad < bc$. The inequality rules are then the same as for $\mathbb{Z}$.

2.5 Prime Numbers

Let k be a natural number. The *multiples* of k are all integers of the form km, for some integer m.

If n is a multiple of k, we can say that k *divides* n or k is a *factor* / *divisor* of n, and write $k \mid n$.

A natural number $n \geq 2$ is a *prime* if its only factors are 1 and n. Otherwise, n is *composite*.

Proposition 1. Every natural number $n \geq 2$ is expressible as a product of primes.

Proof. Induction on n:

Base case $n = 2$ is prime so is a product of primes.

Now assume that every number less than n is expressible as a product of primes. If n is a prime, we are done. If not, write $n = ab$ for some $1 < a, b < n$. Suppose that $a = p_i p_2 \ldots p_k$ and $b = q_1 q_2 \ldots q_l$ for some primes p_i, q_i. Then $n = p_1 \ldots p_k q_1 \ldots q_n$, which is a product of primes. □

Theorem 2. There are infinitely many primes.

Proof. Suppose not: let $p_1, p_2, \ldots p_k$ be all the primes. Let $n = p_1 p_2 \ldots p_k + 1$. Then no p_i divides n. So n has no prime factors, contradicting Proposition 1. □

Remarks

1. If we consider 1 as the 'empty product', then Prop. 1 would say 'for all $n \geq 1$'.
2. There is no 'pattern' to the primes - there is no (algebraic) formula for the nth prime.

2.6 Highest Common Factors

Let a, b be natural numbers. A nautral number c is a *highest common factor* of a and b, written $\text{hcf}(a, b)$ or (a, b), if:

1. $c \mid a$ and $c \mid b$ (c is a common factor of a and b)
2. For any natural number d: if $d \mid a$ and $d \mid b$ then $d \mid c$ (every common factor of a and b divides c)

N.B. If the hcf exists, then it is the greatest of all common factors.
If $(a, b) = 1$, we say that a and b are coprime.

Proposition 3 (Division algorithm)**.** Let k, n be natural numbers. Then $n = qk + r$, for some integers q, r with $0 \leq r \leq k - 1$.

Proof. Induction of n:
Base case $n = 1$: if $k. = 1$, use $q = 1, r = 0$. If $k > 1$, use $q = 0, r = 1$.
Now assume that given $n > 1$ we can write $n - 1 = qk + r$, for some integers q, r with $0 \leq r \leq k - 1$.
If $r < k - 1$, we have $n = qk + (r + 1)$.
If $r = k - 1$, we have $n = (q + 1)k + 0$. □

2.6.1 Euclid's Algorithm

Take two positive integers a and b (say $a \geq b$). Euclid's algorithm is used to find the highest common factor of a and b.
Write $a = q_1 b + r_1$ ($q_1, r_1 \in \mathbb{Z}, 0 \leq r < b$).
Then write $b = q_2 r_1 + r_2$ ($q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < 1$).
And write $r_1 = q_3 r_2 + r_3$ ($q_r, r_3 \in \mathbb{Z}, 0 \leq r_3 < r_2$).
Continue until $r_{n-1} = q_{n+1} r_n + r_{n+1}$ with $r_{n+1} = 0$. Output r_n.
N.B. Since $b < r_1 < r_2 < \ldots$ this process does terminate (in fewer than b steps).

Proposition 4. The output of Euclid's algorithm on a, b is a hcf of a, b.

Proof. Let c be the output.

1. Have $c \mid r_{n-1}$ (from last line of Euclid)
   So $c \mid r_{n-2}$ (from 2nd-last line)
   So $c \mid r_i \forall i$ (inductively)
2. Given $d \mid a, d \mid b$. Have $d \mid r_1$ (from top line)
   So $d \mid r_2$ (from second line)
   So $d \mid r_i \forall i$ (inductively)

In particular, $d \mid c$. □

N.B. Euclid's algorithm shows both that the hcf exists and gives a way to calculate it.

Proposition 5. $\forall a, b \in \mathbb{N}\ \exists x, y \in \mathbb{Z}$ with $ax + by = (a, b)$.

Proof. Having run Euclid's algorithm on a and b with output $c = r_n$ ...

We have c as a linear combination of r_{n-1} and r_{n-2} (from 2nd-last line). And so we have c as a linear combination of r_{n-2} and r_{n-3} (substituting for r_{n-1} using the 3rd-last line).

Therefore, inductively, we have c as a linear combination of r_i and r_{i-1}. In particular, we have c as a linear comination of a and b. $\square$

Proof. Alternatively ...

Let h be the least positive integer of the form $xa + yb$, for some x, y in $\mathbb{Z}$. We claim that h is the hcf of a and b. To prove this:

1. If $d \mid a$ and $d \mid b$, then d divides every linear combination of a and b, so certainly $d \mid h$.

2. To show $h \mid a$: suppose $h \not| a$. Then write $a = qh + r$ for some $q, r \in \mathbb{Z}$ with $1 \leq r < h$. Then $r = a - qh = a - q(xa + yb)$, so r is a linear combination of a and b, contradicting the minimality of h. So $h \mid a$ and by similar reasoning, $h \mid b$.

$\square$

2.7 Solving Integer Equations

Let $a, b \in \mathbb{N}$. When is there an *integer* solution to the equation $ax = b$? Clearly, only when $a \mid b$.

What about $ax + by = c$ for $a, b, c \in \mathbb{N}$.
e.g. $102x + 52y = 37$ - not in this case, as the LHS is even, and the RHS is odd!

What about $57x + 82y = 5$?

In this case there is a solution: we have $82.16 - 57.23 = 1$ by Euclid's algorithm. So, multiplying through by 5, we get $82(5.16) - 57(5.23) = 5$.

Corollary 6 (Bezout's Theorem)**.** Let $a, b, c \in \mathbb{N}$. Then $\exists x, y \in \mathbb{Z}$ with $ax + by = c$ if and only if $\text{hcf}(a, b) \mid c$.

Proof. Let $h = \text{hcf}(a, b)$.

($\Longrightarrow$): Have $h \mid a$ and $h \mid b$, so $h \mid ax + by$, i.e. $h \mid c$.

($\Longleftarrow$): Have $h \mid c$, and have $h = ax + by$ for some $x, y \in \mathbb{Z}$. So $c = \frac{c}{h}(ax + by)$. $\square$

2.8 Fundamental Theorem of Arithmetic

Proposition 7. Let $a, b \in \mathbb{N}$ and p be a prime. Then $p \mid ab \implies p \mid a$ or $p \mid b$.

Proof. Suppose without loss of generality that $p \nmid a$ (then we want to show that $p \mid b$). So $(p, a) = 1$ (as p is prime). Thus $px + ay = 1$ for some $x, y \in \mathbb{Z}$. So, $bpx + bay = b$. Clearly, $p \mid bpx$ and $p \mid bay$ (since $p \mid ab$), so b is a multiple of p. i.e. $p \mid b$. $\square$

Remarks

1. We do need that p is prime for the above to hold.

2. Similarly, $p \mid a_1 \dots a_n \implies p \mid a_i$ for some i (provable inductively).

Theorem 8 (Fundamental Theorem of Arithmetic)**.** Let $n \geq 2$ be a natural number. Then n can be written as a product of primes, *uniquely* (up to reordering).

Proof.

- Existence: See Proposition 1.
- Uniqueness: Induction on n:

  Base case $n = 2$ obviously holds.

  Given $n > 2$ and that $n = p_1 \dots p_k = q_1 \dots q_l$ for some $k, l \in \mathbb{N}$ and primes p_i, q_j, we must show that $k = l$ and (after reordering) $p_i = q_i \; \forall i$.

  We have $p_i \mid q_1 q_2 \dots q_l$ (as $q_1 \dots q_l = p_1 \dots p_k$), so $p_1 \mid q_i$ for some i (by the above Proposition). Reordering, we have assume that $p_1 = q_1$. So $p_2 \dots p_k = q_2 \dots q_l$. By induction, we have $k = l$ and (after reordering) that $p_2 = q_2$, $p_3 = q_3$, $\dots$ $p_k = q_k$.

$\square$

Applications of F.T.A.

- HCFs

  The common factors of $2^3.3^5.7.11$ and $2^6.3^2.7.13$ are all numbers of the form $2^a.3^b.7^c$ $(0 \leq a \leq 3, 0 \leq b \leq 2, 0 \leq c \leq 1)$, so HCF is $2^3.3^2.7$.

  In general, suppose $m = p_1^{a_1} \dots p_k^{a_k}$ and $n = p_1^{b_1} \dots p_k^{b_k}$ where $p_1 \dots p_k$ are distinct primes, and $a_1, b_i \geq 0 \; \forall i$. Then $\text{hcf}(m, n) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_k^{\min(a_k, b_k)}$.

- LCMs

  In the preceding example, the common multiples of our two numbers are all numbers that are multiples of $2^6.3^5.7.11.13$ - so the *least* common multiple (LCM) is $2^6.3^5.7.11.11$.

  In general, for m, n as above, $\text{lcm}(m, n) = p_1^{\max(a_1, b_1)} \dots p_k^{\max(a_k, b_k)}$.

- Interestingly, $\text{hcf}(m, n).\text{lcm}(m, n) = mn$ because $p^{\max(a,b)}.p^{\min(a,b)} = p^a.p^b = p^{a+b}$.

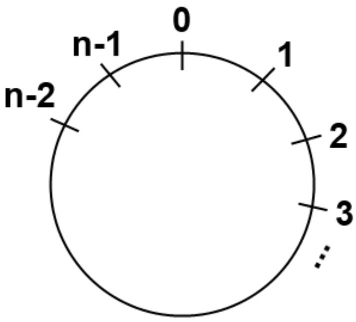
3 Modular Arithmetic

Let $n \geq 2$ be a natural number. The integers mod n, written $\mathbb{Z}_n$, consists of the integers, where two numbers are regarded as the same if they differ by a multiple of n. For example, in $\mathbb{Z}_7$, 2 and 16 are the same.

If a and b are the same in $\mathbb{Z}_n$, we can write $a \equiv b \pmod{n}$, read 'a is congruent to b mod a'. Or $a \equiv b \; (n)$ or $a = b$ in $\mathbb{Z}_n$.

So, $0, 1, \dots n-1$ are all distinct mod n, and *every* a is congruent to one of these (mod n), by the division algorithm.

The correct mental picture of $\mathbb{Z}_n$ is as a loop:



3.1 Operations

Do $+$ and $\cdot$ make sense in $\mathbb{Z}_n$? (Note that 'even' does not make sense in $\mathbb{Z}_n$ since e.g. $2 \equiv 9 \pmod 7$.)

We'd need that if $a \equiv a'$ (n) and $b \equiv b'$ (n) then $a + b \equiv a' + b'$ (n) and $ab \equiv a'b'$ (n).

We have that $a' = a+ni$ and $b' = b+nj$ for some $i, j \in \mathbb{Z}$. So $a'+b' = a = b+n(i+j)$, so $a'+b' \equiv a+b$ (n). Also, $a'b' = (a+ni)(b+nj) = ab+n(ib+ja+nij)$, so $a'b' \equiv ab$ (n).

The usual algebraic rules (such as $a + b \equiv b + a$ (n) are inherited from $\mathbb{Z}$.

3.2 Earlier results

Some things we've already seen can be expressed nicely in this language.

e.g. For p prime, $p \mid ab \implies p \mid a$ or $p \mid b$. In this new language, we can write:

If $ab \equiv 0$ (p) then $a \equiv 0$ (p) or $b \equiv 0$ (p). Or, in $\mathbb{Z}_p$, $ab = 0 \implies a = 0$ or $b = 0$.

3.3 Inverses

We say that an integer a is *invertible* (or a *unit*) mod n if there exists an integer b with $ab \equiv 1$ (n). We can say that b is an *inverse* of a and write it as a^{-1}.

For example, mod 10, the inverse of 3 is 7 (since $3.7 = 21 = 1$ (10)), and the inverse of 4 does not exist (since cannot have $4b = 1 + 10k$ as LHS even, RHS odd).

Proposition 9. Let p be prime. Then every integer $a \neq 0$ (p) is invertible mod p. (i.e. in $\mathbb{Z}_p : a \neq 0 \implies a$ invertible.

Proof 1. Have $(a, p) = 1$ (since a not a multiple of p), so $ax + py = 1$ for some $x, y \in \mathbb{Z}$. Thus $ax \equiv 1$ (p). □

Proof 2. Consider, in $\mathbb{Z}_p$, the numbers $a.0, a.1, a.2, \dots a.(p-1)$.

They are distinct as:

$$\begin{aligned} a_i \equiv a_j \ (p) &\implies a(i-j) \equiv 0 \ (p) \\ &\implies a \equiv 0 \ (p) \text{ or } (i-j) \equiv 0 \ (p) \\ &\implies i \equiv j \ (p) && (\text{as } a \not\equiv 0) \\ &\implies i = j && (\text{as } 0 \leq i, j \leq p-1) \end{aligned}$$

Thus $a.0, a.1, \dots a(p-1)$ are $0, 1, 2, \dots (p-1)$ in some order. In particular, $ax = 1$ for some x. □

What about in $\mathbb{Z}_n$?

Proposition 10. Let a be an integer. Then a is invertible in $\mathbb{Z}_n$ if and only if $(a, n) = 1$ (i.e. a is coprime to n).

Proof.

$$\begin{aligned} a \text{ is invertible} &\iff ax \equiv 1 \ (n) && \text{some } x \\ &\iff ax + ny = 1 && \text{some } x, y \\ &\iff (a, n) \mid 1 && \text{(Bezout)} \\ &\iff (a, n) = 1 \end{aligned}$$

□

Remarks

1. Inverses are unique (if they exist).

   Indeed, suppose $ab \equiv 1 \ (n)$ *and* $ac \equiv 1 \ (n)$. Multiply by b: $bac \equiv b \ (n)$, so $c \equiv b \ (n)$ (since $ab \equiv ba \equiv 0 \ (n)$).

2. In $\mathbb{Z}_n$, we can 'cancel an invertible': if a is invertible, and $ab \equiv ac \ (n)$, then $b \equiv c \ (n)$ (multiplying by a^{-1}).

   But, for example, $4.5 \equiv 6.5 \ (10)$ but $4 \not\equiv 6 \ (10)$ since 5 is not invertible.

3. For $n \geq 1$, the Euler totient function $\phi(n)$ is the number of $1, 2, \dots n$ that are coprime to n. So, $\phi(n)$ is the number of invertibles, or 'units' in $\mathbb{Z}_n$.

   For example, for p prime, $\phi(p) = p - 1$, and $\phi(p^2) = p^2 - p$.

3.4 Fermat's Little Theorem

Theorem 11 (Fermat's Little Theorem)**.** Let p be prime. Then, in $\mathbb{Z}_p$, $a^{p-1} = 1 \ \forall a \neq 0$.
[i.e. $a \not\equiv 0 \ (p) \implies a^{p-1} \equiv 1 \ (p)$]

Proof. In $\mathbb{Z}_p$: consider $a.1, a.2, \dots a(p-1)$. They are distinct (as a is invertible) and non-zero (as $ab = 0 \implies 1a = 0$ or $b = 0$). So they are $1, 2, \dots p - 1$ in some order.

Multiplying them together: $a^{p-1}(p-1)! = (p-1)!$, so $a^{p-1} = 1$ as $(p-1)!$ invertible (as a product of invertibles is invertible). □

Theorem 12 (Fermat-Euler Theorem)**.** For a invertible in $\mathbb{Z}_n$, $a^{\phi(n)} = 1$.
[i.e. if $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \ (n)$]

Proof. Let $x_1, x_2, \dots x_{\phi(n)}$ be the invertibles in $\mathbb{Z}_p$. Then, in $\mathbb{Z}_n$: $ax_1, ax_2, \dots ax_{\phi(n)}$ are distinct (as a invertible) *and* invertible (as they are products of invertibles). So they are $x_1, x_2, \dots x_{\phi(n)}$ in some order. Thus $a^{\phi(n)}x_1x_2 \dots x_{\phi(n)} = x_1, x_2, \dots x_{\phi(n)}$, so $a^{\phi(n)} = 1$ (cancelling each x_i in turn). □

3.5 Wilson's Theorem

In the proof of Fermat's Little Theorem, we cancel through by $(p-1)!$ since we know that it is invertible in $\mathbb{Z}_p$. But what *is* $(p-1)!$ mod p? Trying a couple of examples, we find that $4! = 24 = -1\ (5)$ and $6! = 720 = -1\ (7)$. This suggests that $(p-1)! \equiv -1\ (p)$.

Lemma 1. Let p be prime. Then in $\mathbb{Z}_p$, $x^2 = 1 \implies x = 1$ or -1.

Proof. Have $x^2 = 1$ i.e. $x^2 - 1 = 0$, which is $(x+1)(x-1) = 0$.
Since p is prime, it follows that $x + 1 = 0$ or $x - 1 = 0$, so $x \pm 1$. □

Note: In fact, one can show that in $\mathbb{Z}_p$ (p prime), a polynomial of degree d has $\leq d$ roots.

Theorem 13. Let p be prime. Then $(p-1)! = -1$ in $\mathbb{Z}_p$ (i.e. $(p-1)! \equiv 1\ (p)$).

Proof. We may assume that $p > 2$ (since $p = 2$ is easily verified).
We can pair each $1 \leq a \leq p-1$ with a^{-1} (in $\mathbb{Z}_p$). The lemma above implies that the only values of a for which $a^{-1} \neq a$ (i.e. $1 = a^2$) are $a = 1, -1$. Thus the numbers $1, 2, 3, \ldots (p-1)$, excluding ± 1, can be arranged in distinct pairs such that the product of each pair $\equiv 1\ (p)$. Then we have $(p-1)! = 1 \times 1 \times \ldots 1 \times -1 = -1\ (p)$. □

Theorem 14. Let $p > 2$ be prime. Then -1 is a square mod p if and only if $p \equiv 1\ (4)$.

Proof. For $p = 4k+3$: Suppose $x^2 = -1$ in $\mathbb{Z}_p$. By Fermat's Little Theorem, $x^{4k+2} = 1$. But $x^{4k+2} = (x^2)^{2k+1} = (-1)^{2k+1} = -1$, which is a contradiction.
For $p = 4k+1$: □