Number theory summary

MAT 221, fall 2014

David Pierce

November 3, 2014

http://mat.msgsu.edu.tr/~dpierce/Dersler/

The set $\mathbb{N}$ of **natural numbers** is postulated to be such that

(i) $1 \in \mathbb{N}$;

(ii) $x \mapsto x' \colon \mathbb{N} \to \mathbb{N}$ (where x' is called the **successor** of x);

(iii) **proof by induction** is possible: If $A \subseteq \mathbb{N}$, and

- $1 \in A$,
- for all n in $\mathbb{N}$, if $n \in A$, then $n' \in A$,

then **by induction** $A = \mathbb{N}$.

Theorem. *The binary operations* $+$ *and* $\cdot$ *can be defined on* $\mathbb{N}$ *by*

$$x + 1 = x', \qquad x + y' = (x + y)',$$
$$x \cdot 1 = x, \qquad x \cdot y' = x \cdot y + x,$$

(Proof not required.)

Theorem. $+$ *and* $\cdot$ *are commutative and associative, and* $\cdot$ *distributes over* $+$.

We postulate now

(iv) 1 is not a successor ($\forall x\ 1 \neq x'$),

(v) $x \mapsto x'$ is injective ($\forall x\ \forall y\ (x' = y' \Rightarrow x = y)$).

Recursion Theorem. *If A is a set, and*

$$b \in A, \qquad\qquad f\colon A \times \mathbb{N} \to A,$$

then there is a unique function g from $\mathbb{N}$ to A such that

- *$g(1) = b$,*
- *for all n in $\mathbb{N}$, $g(n+1) = f(g(n), n)$.*

(Proof not required.) We now obtain some new operations by the **recursive definitions**

$$\begin{aligned}
x^1 &= x, & x^{n+1} &= x^n \cdot x, \\
1! &= 1, & (n+1)! &= n! \cdot (n+1), \\
\sum_{k=1}^{1} a_k &= a_1, & \sum_{k=1}^{n+1} a_k &= \sum_{k=1}^{n} a_k + a_{n+1}, \\
\prod_{k=1}^{1} a_k &= a_1, & \prod_{k=1}^{n+1} a_k &= \prod_{k=1}^{n} a_k \cdot a_{n+1}, \\
(\mathrm{F}_1, \mathrm{F}_2) &= (1, 1), & (\mathrm{F}_{n+1}, \mathrm{F}_{n+2}) &= (\mathrm{F}_{n+1}, \mathrm{F}_n + \mathrm{F}_{n+1}).
\end{aligned}$$

We introduce 0 such that $0 \notin \mathbb{N}$, but $0' = 1$; and we let

$$\mathbb{N} \cup \{0\} = \omega.$$

Then the structure $(\omega, 0, {}')$, like $(\mathbb{N}, 1, {}')$, satisfies Postulates (i–v), which are called the **Peano Axioms.** We define

$$x + 0 = x, \quad x \cdot 0 = 0, \quad x^0 = 1, \quad 0! = 1, \quad \sum_{k=1}^{0} a_k = 0, \quad \prod_{k=1}^{0} a_k = 1.$$

By a double recursion, we define

$$\binom{0}{0} = 1, \quad \binom{0}{k+1} = 0, \quad \binom{n+1}{0} = 1, \quad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

By induction, we can prove results like

1) $\sum_{k=1}^{n} 1 = n$,

2) $2 \cdot \sum_{k=1}^{n} k = n \cdot (n+1)$,

3) $6 \cdot \sum_{k=1}^{n} k^2 = n \cdot (n+1) \cdot (2n+1)$,

4) $\sum_{k=0}^{n} (2k+1) = (n+1)^2$,

5) $1 + \sum_{k=1}^{n} \mathrm{F}_k = \mathrm{F}_{n+2}$,

6) if $k + \ell = n$, then

$$\binom{n}{k} = \binom{n}{\ell}, \qquad\qquad \binom{n}{k} \cdot k! \cdot \ell! = n!.$$

On $\mathbb{N}$, we write $x < y$ and say x **is less than** y if for some z in $\mathbb{N}$, $x + z = y$. We prove that $<$ is an **irreflexive** and **transitive** relation on $\mathbb{N}$; thus it is an **ordering** of $\mathbb{N}$. It respects also the **trichotomy** law, so it is a **linear** ordering of $\mathbb{N}$. We write $x \leqslant y$ to mean $x < y$ or $x = y$. Then by definition $0 \leqslant x$ for all x in ω. Now can prove by induction that, for example, for all n in ω,

$$2^n \geqslant 2n, \qquad\qquad 2^n + 1 \geqslant n^2.$$

If $x \leqslant y$, then the z in ω such that $x + z = y$ is unique and is denoted by $y - x$. Now we can state and prove the **Binomial Theorem:**

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

We use the notation $\{x \in \mathbb{N} \colon x < n\} = \{1, \dots, n-1\}$.

Strong Induction Theorem. *if* $A \subseteq \mathbb{N}$ *and*

- *for all* n *in* $\mathbb{N}$, *if* $\{1, \dots, n-1\} \subseteq A$, *then* $n \in A$,

then $A = \mathbb{N}$.

In ω, the notation $k \mid n$ means that, for some ℓ, $k \cdot \ell = n$. In this case, k is a **divisor** or **factor** of n. If $p > 1$, and the only factors of p are 1 and p, then p is called **prime.** If $n > 1$, but n is not prime, then it is **composite.** By strong induction, every natural number greater than

1 has a prime factor. Similarly, every natural number n has a **prime factorization:** there is m in ω and a function $k \mapsto p_k$ on $\{1, \ldots, m\}$ such that each p_k is prime and $n = \prod_{k=1}^{m} p_k$.

Well Ordering Theorem. *Each* nonempty *subset of* ω *has a least element.*

Division Theorem. *For all m in $\mathbb{N}$ and n in ω, there are unique q and r in ω such that*

$$n = m \cdot q + r \ \& \ 0 \leqslant r < m.$$

Here r is the **remainder** when n is divided by m. Given a_0 and a_1 in $\mathbb{N}$, where $a_0 > a_1$, we find their **greatest common divisor** by the **Euclidean Algorithm:** if $a_{k+1} > 0$, let a_{k+2} be the remainder when a_n is divided by a_{k+1}. For some least n, a_{n+1} will be 0; and then a_n is the greatest common divisor of a_0 and a_1.

If $n \in \mathbb{N}$, and $n \mid a - b$ or $n \mid b - a$, we say a and b are **congruent *modulo*** n, writing

$$a \equiv b \pmod{n},$$

or $a \equiv b$ if n is understood. Congruence *modulo* n is an **equivalence relation** (it is **reflexive, symmetric,** and **transitive**). The congruence class of a *modulo* n can be denoted by $\bar{a}$; the set of all congruence classes, by $\mathbb{Z}_n$. Then $\mathbb{Z}_n = \{\bar{1}, \ldots, \bar{n}\}$. Also, if $x \equiv y$, then $x' \equiv y'$. Thus we can define $(\bar{x})' = \overline{x'}$. The structure $(\mathbb{Z}_n, \bar{1}, ')$ allows proofs by induction. Therefore

$$a \equiv b \ \& \ c \equiv d \implies a + c \equiv b + d \ \& \ a \cdot c \equiv b \cdot d.$$

However, $1 \equiv 4 \ \& \ 2^1 \not\equiv 2^4 \pmod 3$. This shows that recursive definitions may require more than induction.