Math 312, lecture 1

Identity: take two primes p, q, let $N = pq$

Say "I'm the person who can factor N".

Implementation: Browser trusts N_{CA}

Bank gets from CA "certificate" saying:

~~the~~ "we (who can factor N_{CA}) say that whoever can factor N_{bank} owns https://www.yourbank.ca".

Today: The integers

Def: The integers are a sextuple $(\mathbb{Z}, +, \cdot\,; 0, 1, <)$

where: (0) $\mathbb{Z}$ is a set, $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$,

$0, 1 \in \mathbb{Z}$, $<$ is a binary relation

(1) Addition is commutative, associative, $a + 0 = a$, has negatives: $a + (-a) = 0$

(2) Multiplication is commutative, associative, $a \cdot 1 = a$

(3) $<$ is a linear order: if $a < b$, $b < c$ then $a < c$ and for any a, b one of $a < b$, $b < a$, $a = b$ holds

(7) if $a, b > 0$ then $a \cdot b,\ a+b > 0$

(8) Well-ordering: if $A \subset \mathbb{Z}_{\geq 0}$ is non-empty then A has a least element.

restatement of induction

Example of induction

Lemma: There is no integer b s.t. $0 < b < 1$

Pf: let $A = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. If A was non-empty, it would have a least element, b. The $0 < b \cdot b < b < 1$ so $b \cdot b \in A$, $b \cdot b < b$, which contradicts the minimality of b. It follows that A is empty.

power: went down from b to $b \cdot b$ not $b-1$

Cor: For any $n \in \mathbb{Z}$ no $a \in \mathbb{Z}$ s.t. $n < a < n+1$

Pf: If $n < a < n+1$ then $0 < b = n - a < 1$.

Theorem: (Induction) let $P \subset \mathbb{N} = \mathbb{Z}_{\geq 0}$ ($\mathbb{Z}_{\geq 1}$ positive integers) satisfy: $0 \in P$, and if $n \in P$ then $n+1 \in P$. Then $P = \mathbb{N}$.

Pf: Let $A = \{n \in \mathbb{N} \mid n \notin P\}$. If A ~~was~~ was non-empty, it would have a least element, a. Now $a \neq 0$ ($0 \in P$) so $a \geq 1$ (by lemma) so $a - 1 \geq 0$, i.e. $a - 1 \in \mathbb{N}$.

Also, $a-1 \notin P$: if it were, then $a=(a-1)+1 \in P$ too, but $a \notin P$. This means $a-1 \in A$, contradicting the minimality of a.

Division and divisibility

Def: Call $n \in \mathbb{Z}$ even if $n = 2k$ for some $k \in \mathbb{Z}$.

Prop: For any $n \in \mathbb{Z}$, one of $n, n+1$ is even

Pf: Claim is true for $n=0$ (among $0, 1$ one is even: $0 = 2 \cdot 0$)

Suppose one of $n, n+1$ is even. If $n+1$ is even, the claim holds for $n+1$. Otherwise, n is even. Say $n = 2k$. Then $(n+1)+1 = n+2 = 2(k+1)$ so $n+2$ is even and claim holds for $n+1$ anyway.

By induction, claim holds for all $n \geq 0$. Now suppose that $n < 0$. Then $n+1 \leq 0$ so $-(n+1), (-n)$ are consecutive non-neg integers, one of which is even.

Finally, if $m = 2k$ then $-m = 2(-k)$

<u>Theorem:</u> (Division thm) Let $n, a \in \mathbb{Z}$ with $a > 0$. Then there exist <u>unique</u> $q, r \in \mathbb{Z}$ with $0 \le r < a$ and

$$n = q \cdot a + r$$

(Call q the "quotient", r "remainder")

(Eg. $7 = 2 \cdot 3 + 1$)

<u>Pf:</u> Let $A = \{ m \in \mathbb{N} \mid m = n - ka \text{ for some } k \in \mathbb{Z} \}$

(= all $m \in \mathbb{N}$ which differ from n by a mult of a)

* A is non-empty: if k is negative enough, $n - ka$ is large, eg. $a \ge 1$, so if $k = -|n|$ then

$n - ka = n + |n| \cdot a \ge n + |n| \ge 0.$

Let $r \in A$ be the least member. Then $r \ge 0$,

and $r = n - qa$ for some $q \in \mathbb{Z}$

Also, $r < a$: if $r \ge a$ held, then $r - a \ge 0$ would have form $r - a = n - (q+1) a \in A$, contradiction.

Next, suppose $n = q \cdot a + r = q' a + r'$. Wlog, $r \ge r'$

Then $0 \le r - r' \le r < a$ also $r - r' = (q' - q) \cdot a$

If $r \ne r'$ then $q' \ne q$, so $q' - q \ge 1$ so $r - r' \ge a$ <u>impossible</u>

so $r = r'$, then $q = q'$

Divisibility

Def: Let $a, b \in \mathbb{Z}$. Say "a divides b", write $a \mid b$ if there is $c \in \mathbb{Z}$ s.t. $b = ac$. If not, say "a does not divide b", write $a \nmid b$.

E.g. $2 \mid 6$, $2 \nmid 3$, $0 \mid 0$, $-3 \mid 6$, $2 \mid -6$.

($\Leftrightarrow$ the equation $a \cdot x = b$ has a solution in $\mathbb{Z}$)

Notation: If $a \mid b$, $a \neq 0$ write $\frac{b}{a}$ for the unique solution.

Examples: $a-b \mid a^2 - b^2$ for all $a, b \in \mathbb{Z}$

$a^2 - b^2 = (a-b)(a+b)$

e.g. $2^{2^n} - 1 \mid 2^{2^{n+1}} - 1$

Lemma: Let $b \neq 0$, and $a \mid b$. Then $|a| \leq |b|$

Pf: Say $b = ac$. Then $|b| = |a| \cdot |c|$. If $b \neq 0$ then $c \neq 0$ so $|c| \geq 1$, so $|b| \geq |a|$.

Def: Let $a, b \in \mathbb{Z}$. Say $d \in \mathbb{Z}$ is a <u>common divisor</u> of a, b if $d \mid a$, $d \mid b$.