Math 403 Fall 2011 UMD
Lecture 2
Elementary Number Theory

Well ordered Property of $\mathbb{N}$

Axiom Let $S \subseteq \mathbb{N}$ be a non-empty subset. Then there exists $s \in S$ st $\forall\, t \in S$ $s \leq t$.

In other words, every non-empty subset of $\mathbb{N}$ has a smallest element.

In math, you prove this by looking at def of $\mathbb{N}$, but we'll take it as an axiom. It is ~~similar to the principle~~ closely related to the following

Principle of Math Induction Let P be a property of natural numbers. Assume

(a) $P(0)$ holds
(b) $\forall n \in \mathbb{N}$ $P(n) \Rightarrow P(n+1)$

Then $P(n)$ holds for all $n \in \mathbb{N}$.

__Pf__ Set $S = \{n \in \mathbb{N} : P(n) \text{ does not hold}\}$. Assume, to get contr., $S \neq \emptyset$. Then there exists a smallest $n \in S$. Since $P(0)$ holds, $n > 0$. So $n-1 \in \mathbb{N}$ and, since n is smallest elt of S, $P(n-1)$ holds. But then (b) $\Rightarrow$ $P(n)$ holds. Contradiction.

__Rmk__ In fact, the principle of math induction also implies the well ordered property of $\mathbb{N}$. The two are equivalent.

__Prop__ (Division Algorithm) Suppose $a, q \in \mathbb{Z}$, $q \neq 0$. Then there exist unique numbers $d, r \in \mathbb{Z}$ satisfying

(i) $a = dq + r$

(ii) $0 \leq r < |q|$.

__Pf__ Assume first that $a, q \geq 0$. Set

$$S = \{a - dq : d \in \mathbb{Z}\} \cap \mathbb{N}.$$

Then S is non-empty (b/c for ex $a + (a^2+1)q > 0$ ~~$a - (-1)a^2q = a + a^2q \geq$~~ ~~$a =$ and $a - 0q$~~ $\in S$.)

Thus S has a smallest element r. By def we have

$$r = a - dq \quad \text{for some } d \in \mathbb{Z},$$

So (i) holds.

To see that (ii) holds, suppose $r \geq q$. Then $r - q \geq 0$ and

$$a = dq + q + (r-q)$$
$$= (d+1)q + (r-q) \Rightarrow r-q = a - (d+1)q$$

So $r' = r - q \in S$. But, since $q > 0$, this contradicts the assumption that r was the smallest elt of S.

~~Addendum~~ 1

Uniqueness suppose $a = dq + r = d'q + r'$ with $d, r; d', r'$ satisfying (i) and (ii). ~~The~~ ~~[illegible]~~ If $r \neq r'$ then we can assume $0 < r < r' < q$. But we have

$$r' - r = (d - d')q \Longrightarrow |r - r'| > |q|$$

So this is impossible. So $r = r'$. But then $(d-d')q = 0$ $\Rightarrow d - d' = 0 \Rightarrow d = d'$.

~~Addendum~~

I leave the case when ~~a or~~ q is negative ~~to~~ as exercise.

~~Sol~~ Sol If $q < 0$, then can write $a = d(-q) + r$ ~~with~~ $= (-d)q + r$ with $0 \leq r < |q|$.

~~Sol Suppose $a, q \in \mathbb{Z}$ and $q \neq 0$. If $q < 0$, then.~~ .

~~Suppose $a < 0$. Then~~

~~$$-a = dq + r \Rightarrow a = -dq - r$$~~
~~$$= -dq - q + q - r$$~~
~~$$= -(d+1)q + (q-r)$$~~

~~If $0 \leq r < q$ then~~

Def If $a = dq + r$ as in prop, we say that d is the *quotient* of division of q into a and r is the remainder. If $r = 0$, we say that q *divides* a and write $q \mid a$. Else we write $q \nmid a$.
If $q \mid a$ then q is said to be a *divisor* of a.

Factoid If $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for all $m, n \in \mathbb{Z}$

Def A pos int c is called the gcd of a and b if

1. $c \mid a$ and $c \mid b$
2. Any divisor of a and b divides c.

We write (a,b) for the gcd assuming it exists

Ex $(8,12) = 4$, $(2,3) = 1$.

Thm (Euclid) Suppose $a, b \in \mathbb{Z}$ not both 0. Then the gcd exists ~~[illegible]~~ and is unique. Moreover we can find $m, n \in \mathbb{Z}$ s.t.

$$(a,b) = ma + nb.$$

Ex $(8,12) = 4 = (-1)8 + (1)12$

$(2,3) = 1 = (-1)2 + (1)3.$

Pf Set $M = \{ma + nb : m, n \in \mathbb{Z}\}$

$M^+ = M \cap \mathbb{Z}_+.$

Then M^+ is non-empty b/c $a^2 + b^2 \in M^+$. ~~and a^2+b^2~~
Let $c = ma + nb$ be the smallest element of M^+.
I claim that $c \mid a$ and $c \mid b$.
To see this, suppose not to get a contradiction.
So suppose $c \nmid a$. Then

$$a = dc + r \quad \text{for some } 0 < r < c.$$

But then $r = a - dc$

$= a - d(ma + nb)$

$= (1 - dm)a + (-d)b$

$\Rightarrow r \in M_+$. Since $r < c$ this contradicts assumption that c is smallest elt of M_+.

Now by fact any divisor of a and b divides c since $c = ma + nb$. So by def c is gcd of a and b.

It is clearly unique b/c if c and c' are both gcds then $c \mid c'$ and $c' \mid c$. Since $c, c' > 0$ this ~~shows~~ implies $c = c'$.

~~Cor If~~

Def We say that ~~Gos~~ a and b are relatively prime if $(a,b)=1$.

Cor If a and b are rel. prime $\exists\ m,n \in \mathbb{Z}$ st $ma+nb=1$.

Ex $(3,4)=1$ and $(-1)3+(1)4=1$
$(3,5)=1$ and ~~β~~ $(2)(3)+(-1)5=1$.

etc.

~~Recall that a pos. int. greater than 1 is prime if it has exact~~

Recall that a pos. int $p \in \mathbb{Z}_+$ is prime if it has exactly 2 ~~prime~~ pos. divisors: 1 and itself.

Lemma (Euclid) If p is a prime and $p \mid ab$ for $a,b \in \mathbb{Z}$ then ~~we have~~ $p \mid a$ or $p \mid b$.

Pf Suppose $p \nmid a$. Then ~~$(p,a)=1$ Since there is no divisor of p~~ since $(p,a) \mid p$ we must have $(p,a)=1$. Therefore $\exists\ m,n \in \mathbb{Z}$ st $mp+na=1$. So $b = nab + mpb$. Since $p \mid ab$, we have $p \mid b$.

Lemma (Euclid) If $a,b,c \in \mathbb{Z}$ and a is rel. prime to b and c but $a \mid bc$ ~~then~~ then $a \mid b$ or $a \mid c$.

Pf ~~Since (a,b)~~ Suppose $a \nmid b$. Since $(a,b)=1$ we can find $m,n \in \mathbb{Z}$ s.t. $ma+nb=1$. Then multiplying through $c = mac + nbc$. Since $a \mid mac$ and $a \mid bc$, we have $a \mid c$.

Cor Suppose p is a prime and $a,b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Pf Since p is ~~not~~ ~~prim~~ prime, $p \nmid a \Rightarrow (p,a)=1$ and similarly $p \nmid b \Rightarrow (p,b)=1$. Now use lemma.

Thm (Fundamental Thm of Arithmetic) Every integer $n \in \mathbb{Z}_+$ is a product

$$\boxed{n = p_1 p_2 \cdots p_r}$$

of primes. If we have

$$\begin{aligned} n &= p_1 p_2 \cdots p_r \\ &= q_1 q_2 \cdots q_s \end{aligned}$$

with

$$p_1 \le \cdots \le p_r$$
$$q_1 \le \cdots \le q_s$$

and all p_i, q_i primes; then $r=s$ and $\forall i \; p_i = q_i$.

Pf (Existence) To get a contradiction, let S denote the set of all pos ints ~~[illegible]~~ $n > 1$ st n cannot be written as a product

$$n = p_1 \cdots p_r$$

with p_i prime.

If $S \neq \emptyset$, ~~then~~ there is a smallest element $n \in S$.
~~If $a \in \mathbb{Z}_+$ and $a \mid n$ then we must have either $a = 1$ or $a = n$ b/c otherwise a~~

Suppose $\boxed{n = ab \text{ with } 1 < a \leq b < n.}$ Then since $a, b < n$ we have

$$a = q_1 \cdots q_s$$
$$b = r_1 \cdots r_t$$

with q_i, r_i prime. But then $n = (q_1 \cdots q_s)(r_1 \cdots r_t)$. This is a contradiction. It follows that n ~~itself is prime~~ cannot be written as in the box. Therefore n ~~itself~~ is prime, again a contradiction. We conclude that $S = \emptyset$. So every pos int can be written as a product of primes.

(Uniqueness) Suppose $n = p_1 \cdots p_r$
$= q_1 \cdots q_s$

with p_i, q_i prime, ~~[illegible]~~ ~~and $1 \leq s \leq$~~ ~~$1 \leq r \leq s$.~~
~~Then If $r = 1$~~ p_1 Without loss of generality we ~~[illegible]~~ can assume that p_1 is the smallest prime in the p_i, q_j.
Assume that n is smallest ~~[illegible]~~ pos integer with 2 distinct factorizations. Then, since $p_1 \mid n$, we have

$$p_1 \mid q_1 \quad \text{~~or~~ or} \quad p_1 \mid (q_2 \cdots q_s)$$

~~Since p_1 is smallest in list, must have~~ have

If $p_1 \mid q_2 \cdots q_s$ then $p_1 \mid q_i$ for some $i \geq 2$

But p_1 is smallest in the list so this implies $p_1 = q_i$

Therefore $p_2 \cdots p_r = q_2 \cdots q_s$.

But this means that $m = p_2 \cdots p_r$ has two distinct prim factorizations. This contradicts ~~minimality~~ assumpton that n was smallest such pos integer.