Last time: Proved that if $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$ then $\exists!\ d \geq 1$ st

1) $d \mid a$ and $d \mid b$
2) if $c \mid a$ and $c \mid b$ then $c \mid d$.

$d := \gcd(a,b)$, the greatest common divisor of a & b.

Also, $\exists\, x, y \in \mathbb{Z}$ (not unique) st $d = xa + yb$

[Note: $ba + (-a)b = 0 \Rightarrow d = (x+b)a + (y-a)b$ etc...]

Lemma 2.3: $\gcd(n,m) = \gcd(n-km, m)$ $\forall\, k, n, m$ $((n,m) \neq (0,0))$

Thm 2.5: If $\gcd(a,m) = 1$ and $a \mid (mn)$ then $a \mid n$.

Def: An integer $p \geq 2$ is prime iff $p = ab$, $a, b > 0$, $\Rightarrow a = 1$ or $b = 1$.

[strictly speaking this is a definition of an irreducible element of $\mathbb{Z}$]

Remark: For any $n \in \mathbb{Z}$ and any prime p, $\gcd(n,p) = 1$ or p

This is because $\gcd(n,p) \mid p$ (and $\gcd(n,p) \geq 1$).

HW1: If p is prime, $n, m \in \mathbb{Z}$ and $p \mid (nm)$ then either $p \mid n$ or $p \mid m$ (or both). Hint: Remark above and Thm 2.5

Remark: In general (rings) the property $p \mid nm \Rightarrow p \mid n$ or $p \mid m$ is used as a definition of a prime.

Thm 3.1 (Euclid's lemma; see Nicholson, p 37). Suppose p is prime, $k \geq 1$, $m_1 \ldots m_k \in \mathbb{Z}$ and $p \mid (m_1 \cdots m_k)$. Then $p \mid m_i$ for some i, $1 \leq i \leq k$.

Proof: Induction on k. If $k = 1$, nothing to prove.

Suppose true for $k = n$ and $p \mid (m_1 \cdots m_n m_{n+1})$. Then $p \mid (m_1 \cdots m_n) \cdot m_{n+1}$. By HW, $p \mid (m_1 \cdots m_n)$ or $p \mid m_{n+1}$.

If $p \mid (m_1 \cdots m_n)$ then $p \mid m_i$ for some i, $1 \leq i \leq n$ by inductive assumption. Otherwise, $p \mid m_{n+1}$ $\square$

<u>Thm 3.2</u> (Nicholson, Thm 7, p 37)

1) Every integer $n \geq 2$ is a prime or a product of primes.

2) Factorization of integers ≥ 2 into prime factors is unique up to order. That is, if $n = p_1 \cdots p_r = q_1 \cdots q_s$ then $r = s$, and q_j's can be re-ordered so that $q_j = p_j$ $\forall j$.

<u>Proof</u> (1) Suppose not: $\exists m \geq 2$, $m \in \mathbb{Z}$ which is not a prime or a product of primes. Then

$$S = \{ n \in \mathbb{N} \mid n \geq 2, \ n \text{ is not a prime or a product of primes} \}$$

is nonempty. By well-ordering $k = \min S$ exists.

Then k is not a prime, so it can be factored as $k = ab$, $a, b > 0$, $a, b \neq 1$. Then $a, b < k = \min S$

$\Rightarrow$ a, b a primes or products of primes.

$\Rightarrow$ k is a product of primes. Contradiction.

(2) Suppose there is $n \geq 2$ which has two distinct factorizations. By well-ordering there is the smallest integer $m \geq 2$ two distinct factorizations $m = p_1 \cdots p_r = q_1 \cdots q_s$, $r, s > 0$, $p_1 \cdots p_r$, $q_1 \cdots q_s$ primes

$p_1 \mid (p_1 \cdots p_r) \Rightarrow p_1 \mid (q_1 \cdots q_s)$. By Euclid's lemma, $p_1 \mid q_j$ for some j. We may assume $p_1 \mid q_1$. q_1 is a prime, $p_1 > 1$. $\Rightarrow p_1 = q_1$. Contradiction.

<u>Case 1</u> $r = 1$. Then $p_1 = p_1 q_2 \cdots q_s$. $\Rightarrow 1 = q_2 \cdots q_s$, which is impossible if $s \geq 2$. Hence if $r = 1$, $s = 1$ and we're done.

<u>Case 2</u> $r > 1$. Then $m = p_1 \cdots p_r = p_1 q_2 \cdots q_s$

$\Rightarrow \frac{m}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$. Since $\frac{m}{p_1} < m$, $\frac{m}{p_1}$ has a unique factorization into primes (up to order)

$\Rightarrow r = s$ and $p_i = q_i$ $(i \geq 2)$ after reordering.

Factorization of m into primes is unique, after all. $\square$

Theorem 3.3 (Euclid) There are infinitely many primes.

Proof Suppose not. Then there are finitely many primes:

$p_1 \cdots p_n$ for some $n \in \mathbb{N}$.

Consider $m = p_1 \cdots p_n + 1$.

By Thm 3.2 (1) m is a prime or a product of primes

Since $p_1 \cdots p_n + 1 > p_i$ for all i, m is not a prime.

If $p_i \mid m$ for some i, Then $p_i \mid m - (p_1 \cdots p_n) = 1$

which is impossible since $p_j \geq 2$.

m cannot be a product of primes either. Contradiction.

$\therefore$ there are infinitely many primes

Review Equivalence relations, equivalence classes, partitions

Recall A (binary) relation R on a set X is a subset of $X \times X$

We write $x \sim y$ if $(x, y) \in R$.

Def A relation R on a set X is an equivalence relation iff

1) $x \sim x \quad \forall x \in X$ (R is reflexive)

2) $x \sim y \Rightarrow y \sim x$ (R is symmetric)

3) $(x \sim y) \& (y \sim z) \Rightarrow x \sim z$ (R is transitive)

Def A partition of a set X is a collection of subsets $\{C_\alpha\}_{\alpha \in A}$ of X st

1) $\bigcup_{\alpha \in A} C_\alpha = X$

2) $C_\alpha \cap C_\beta \neq \emptyset \Rightarrow C_\alpha = C_\beta$.

Thm Every equivalence relation on X gives rise to a partition of X

Every partition of X gives rise to an equivalence relation

There is a bijection: $\{$equiv relations on $X\} \leftrightarrow \{$partitions of $X\}$.

[compare with Nicholson, p 19]

Sketch of proof

Given an equivalence relation $\sim$ on X, given $x \in X$ let

$[x] = \{ y \in X \mid y \sim x \}$, the equivalence class of x.

Then $x \in [x]$ since $x \sim x$. $\Rightarrow \bigcup_{x \in X} [x] = X$.

Also if

$[x] \cap [y] \neq \emptyset$ then $\exists z \in [x] \cap [y]$ ie $\exists z$ s.t. $z \sim x$ and $z \sim y$.

Then if $w \in [x]$, $w \sim x$. Since $x \sim z$ and $z \sim y$, $w \sim y$. $\Rightarrow w \in [y]$

$\Rightarrow [x] \subseteq [y]$. Similarly $[y] \subseteq [x]$.

$\therefore \{[x]\}_{x \in X}$ is a partition of X.

[The indexing of the equivalence classes is redundant]

Conversely suppose $\{C_\alpha\}_{\alpha \in A}$ is a partition of X.

Define a relation R on X by $x \sim y \Leftrightarrow \exists \alpha$ s.t. $x, y \in C_\alpha$.

Then $\sim$ is reflexive and symmetric

Moreover if $x \sim y$ and $y \sim z$ $\exists \alpha, \beta$ s.t. $x, y \in C_\alpha$, $y, z \in C_\beta$.

$\Rightarrow y \in C_\alpha \cap C_\beta$. $\Rightarrow C_\alpha \cap C_\beta \neq \emptyset$. $\Rightarrow C_\alpha = C_\beta$. $\Rightarrow x \sim z$.

$\therefore \sim$ is transitive

Ex Let $n \in \mathbb{Z}$, $n > 1$. Define $\sim_n$ on $\mathbb{Z}$ by $x \sim y \Leftrightarrow n \mid (x - y)$

Then $\sim$ is an equivalence relation: $x \sim x$ since $n \mid x - x = 0$

$x \sim y \Rightarrow n \mid (x-y) \Rightarrow n \mid (-(x-y)) \Rightarrow y \sim x$.

$x \sim y$ and $y \sim z \Rightarrow n \mid (x-y) + (y-z) = x - z. \Rightarrow x \sim z$.

We get a partition of $\mathbb{Z}$: $\mathbb{Z} = \{[k]\}_{k \in \mathbb{Z}}$.

Claim: $\{[k]\}_{k \in \mathbb{Z}} = \{[0], \ldots, [n-1]\}$.

Reason: $\forall k \in \mathbb{Z}$ $\exists! q, r \in \mathbb{Z}$, $0 \le r < n$ st

$k = qn + r. \Rightarrow n \mid qn = k - r \Rightarrow [k] = [r]$.