MATH 417 09/12/2018 We

Quiz Friday on equiv. relations, equivalence classes...
HW #3 posted.

7.1

Last time existence of gcd's, computing of gcd's.

If p is prime and $p|(ab)$ then either $p|a$ or $p|b$.

Every $n \in \mathbb{N}$, $n>1$ is a prime or a product of primes

Thm 1.6.21 Factorization into primes is unique (up to order)

Proof Suppose not; suppose there are intergers ≥ 2 with a nonunique factorization into primes. By well-ordering there is the smallest one such integer, call it m.

Then $\exists r, s \in \mathbb{N}$ and primes $p_1, \dots, p_r, q_1, \dots, q_s$ s.t.

$$m = p_1 \cdots p_r = q_1 \cdots q_s.$$

Since $p_1 | (p_1 \cdots p_r)$, $p_1 | (q_1 \cdots q_s)$

Homework (#1.6.9) $\Rightarrow$ $p_1 | q_j$ for some j. After renumbering we may assume: $j=1$. Since q_1 is prime and $p_1 | q_1$, $p_1 = q_1$

$\Rightarrow p_1 (p_2 \cdots p_r) = p_1 (q_2 \cdots q_s)$.

$\Rightarrow p_2 \cdots p_r = q_2 \cdots q_s$

But $p_2 \cdots p_r = m/p_1 < m$. $\Rightarrow$ Factorization of m/p_1 into primes is unique up to order, ie $r=s$ and after renumbering q_j's we may assume $p_2 = q_2, p_3 = q_3 \dots p_r = q_r$

$\Rightarrow$ factorization of m into primes is also unique (up to order). Contradiction.

$\therefore$ all integers ≥ 2 have a unique factorization into primes. $\square$

Intergers modulo n ($n \in \mathbb{Z}$, $n \geq 1$)

Definition Two intergers $a, b \in \mathbb{Z}$ are congruent modulo n if $n | (b-a)$. We write $a \equiv b \mod n$ or $a \equiv_n b$.

$\equiv_n$ is a relation on $\mathbb{Z}$

<u>Recall</u> A <u>relation</u> on a set X is a subset R of $X \times X$,

ie R is a set of ordered pairs of the form (x_1, x_2) with $x_1, x_2 \in X$.

We write $x_1 \sim x_2$ or $x_1 \sim_R x_2$ if $(x_1, x_2) \in R$.

A relation $R \subseteq X \times X$ is an <u>equivalence relation</u> if

1) $\forall x \in X$, $x \sim x$ (i.e. $(x, x) \in R$) (reflexivity)
2) if $x \sim y$ then $y \sim x$ (symmetry)
3) if $x \sim y$ and $y \sim z$ then $x \sim z$. (transitivity)

<u>Lemma</u> 1.7.2 Congruence modulo n is an equivalence relation.

<u>Proof</u> See textbook.

<u>Recall</u> Given an equivalence relation $\sim$ on a set X the <u>equivalence class</u> of $x \in X$ is the set

$$[x] = \{ y \in X \mid y \sim x \} = \{ y \in X \mid x \sim y \}.$$

<u>IMPORTANT FACT</u> For two equivalence classes $[x], [y]$, if $[x] \cap [y] \neq \emptyset$ then $[x] = [y]$.

<u>Proof</u> Suppose $[x] \cap [y] \neq \emptyset$. Then $\exists z$ s.t. $z \in [x] \cap [y]$.

$\Rightarrow x \sim z$ and $z \sim y$.

Now given $u \in [x]$, $u \sim x$. $u \sim x$ and $x \sim z \Rightarrow u \sim z$ by transitivity

$u \sim z$ and $z \sim y \Rightarrow u \sim y$ by transitivity. $\Rightarrow u \in [y]$

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

Ex (Back to $\equiv_n$). Let $a \in \mathbb{Z}$.

$[a] = \{ b \mid a \equiv b \bmod n \} = \{ b \mid n \mid (b-a) \}$

$= \{ b \in \mathbb{Z} \mid b - a = qn \text{ for some } q \in \mathbb{Z} \} = \{ a + nq \mid q \in \mathbb{Z} \}$

$=: a + n\mathbb{Z}$

Notation $\mathbb{Z}_n$ = the set of all equivalence classes modulo n.

$\mathbb{Z}_2 = \{ \underset{\text{evens}}{[0] = 2\mathbb{Z}}, \underset{\text{odd}}{[1] = 2\mathbb{Z}+1} \}$

$\mathbb{Z}_3 = \{ [0] = 3\mathbb{Z}, [1] = 3\mathbb{Z}+1, [2] = 3\mathbb{Z}+2, [3] = [0], [4] = [1], [5] = [2]$

$= \{ [0], [1], [2] \}$

Corollary 1.7.4 For any $n \geq 2$, $\mathbb{Z}_n = \{ [0], [1], \ldots [n-1] \}$

Moreover, the classes $[0], [1], \ldots [n-1]$ are all distinct.

Proof (1) By the division algorithm, for any $a \in \mathbb{Z}$ there are (unique) $q, r \in \mathbb{Z}$ s.t. $a = qn + r$ and $0 \leq r < n$.

$\Rightarrow a - r = qn \Rightarrow a \equiv r \bmod n \Rightarrow [a] = [r]$.

$\Rightarrow \mathbb{Z}_n = \{ [0], \ldots [n-1] \}$

Moreover, $\forall r_1, r_2 \in \mathbb{Z}$ s.t. $0 \leq r_1, r_2 < n$

$[r_1] = [r_2] \iff n \mid (r_1 - r_2) \iff r_1 - r_2 = 0$ since $0 \leq |r_1 - r_2| < n$ $\square$

Lemma (1.7.5) Fix $n \in \mathbb{N}$, $n \geq 2$. For any $[a], [b] \in \mathbb{Z}_n$

$[a] + [b] := [a+b]$ and $[a] \cdot [b] = [a \cdot b]$

are well-defined:

if $[a] = [a']$, $[b] = [b']$ then $[a] + [b] = [a'] + [b']$ and $[a] \cdot [b] = [a'] \cdot [b']$.

Ex $n = 5$. Then $[3] = [8]$ and $[1] = [6]$

$[3] + [1] = [4]$ and $[3] \cdot [1] = [3]$

$[8] + [6] = [14]$ and $[8] \cdot [6] = [48]$

But in $\mathbb{Z}_5$ $[4] = [14]$ since $5 \mid 14 - 4$ and $[3] = [48]$, since $5 \mid 45$

<u>Proof of lemma</u> Suppose $[a] = [a']$, $[b] = [b']$.
Then $a \equiv a' \bmod n$, $b \equiv b' \bmod n$, ie
$\exists\, k, l \in \mathbb{Z}$ st $a = kn + a'$, $b = ln + b'$.

Now

$$a+b = (kn+a') + (ln+b') = a'+b' + (k+l)n$$

$\Rightarrow$ $a+b \equiv a'+b' \bmod n$

$\Rightarrow$ $[a+b] = [a'+b']$.

Similarly

$$a \cdot b = (kn+a') \cdot (ln+b') = a' \cdot b' + kb'n + a'ln + klnn$$
$$= a'b' + (kb' + a'l + kln) \cdot n$$

$\Rightarrow$ $a \cdot b \equiv a' b' \bmod n$

$\Rightarrow$ $[a \cdot b] = [a' \cdot b']$. $\square$

<u>Ex</u> $4^{1237} = q \cdot 5 + r$ for some $q, r \in \mathbb{Z}$, $0 \le r < 5$.
What's r?

$[r] = [4^{1237}]$ in $\mathbb{Z}_5$

Since $[a] \cdot [b] = [ab]$ in $\mathbb{Z}_n$, $[a^k] = ([a])^k$ in $\mathbb{Z}_n$ for any $k \in \mathbb{N}$.

$\Rightarrow$ $[4^{1237}] = [4]^{1237}$

Now $[4] = [-1]$ in $\mathbb{Z}_5$. $\Rightarrow [4]^2 = [(-1)]^2 = [(-1)^2] = [1]$.

$\Rightarrow$ $[4]^{1237} = [4] \cdot ([4])^{1236} = [4] \cdot ([4]^2)^{618} = [4]([1])^{618}$

$= [4] \cdot [1] = [4]$.

$\Rightarrow$ $4^{1237} = q \cdot 5 + 4$ for some $q \in \mathbb{Z}$.

<u>Ex</u> 122013 is divisible by 3.

<u>Reason</u> In $\mathbb{Z}_3$ $[10] = [1]$. $\Rightarrow [10^n] = ([10])^n = [1]^n = 1$ $\forall n$

$\Rightarrow$ $[122013] = [10^5] + [10^4 \cdot 2] + [10^3 \cdot 2] + [10] + [3]$

$= [1] + [2] + [2] + [1] + [0] = [6] = [0]$.

$\Rightarrow$ $122013 \equiv 0 \bmod 3$ ie.

$3 \mid 122013$.