15-151: Midterm 2

Induction

→ let $p(n) =$ "..." . WTS $p(n)\ \forall n \in \mathbb{N}$ ← DO NOT quantify n in predicate

B.C. $n=0$, ... ⇒ $p(0)$ is true

I.S. I.H. fix $n \geq 0$. assume $p(n)$. WTS $p(n+1)$

$RHS = \ldots \overset{I.H.}{=} \ldots = LHS$ ⇒ $p(n+1)$ is true

→ if $p(x_0)$ is true and $\forall n \geq x_0,\ (p(x_0) \wedge p(x_0+1) \wedge \ldots \wedge p(n) \Rightarrow p(n+1))$

⇒ $p(n)$ is true $\forall n \geq x_0$. (SPMI)

Relations

→ a relation on a set S is a subset of $S \times S$

→ equivalence relation ⇔

1. reflexivity: $x \sim x\ \forall x \in S$
2. symmetry: $x \sim y \Rightarrow y \sim x\ \ \forall x, y \in S$
3. transitivity: $x \sim y \wedge y \sim z \Rightarrow x \sim z\ \ \forall x, y, z \in S$

→ order relation ⇔ reflexivity, antisymmetry, transitivity

$x \sim y \wedge y \sim x \Rightarrow x = y\ \ \forall x, y \in S$

→ equivalence class of x: $[x]_\sim = \{y \in S : x \sim y\}$

↳ equivalence classes partition S ∧ any partition of S can be made into an equivalence relation

→ set of all equivalence classes for some relation R on set S forms a partition of set S

→ Quotient: $X/\sim\ = \{[x]_\sim \mid x \in X\}$ ← "partition" "set of all equiv. classes"

★ n with last digit x, $m = \frac{n-x}{10} - 2x$ ⇒ $7 \mid n \Leftrightarrow 7 \mid m$

$10^k \equiv (-1)^k \bmod 11$ ⇒ $246837 \equiv (7-3+8-6+4-2) \equiv 8 \bmod 11$

$1001 = 7 \times 11 \times 13$

Number Theory

→ Division theorem: $\forall a, b \in \mathbb{Z}$, $b \neq 0$, $\exists!\, q, r \in \mathbb{Z}$ s.t. $a = bq + r \wedge 0 \le r < |b|$

→ definition of gcd: $\forall a, b, d \in \mathbb{Z}$, d is a gcd of a and b

$\Leftrightarrow$ (1) $d | a \wedge d | b$

(2) $\forall e \in \mathbb{Z}$ with $e|a \wedge e|b$, $e|d$

→ big theorem, $\forall a, b, q \in \mathbb{Z}$, $\gcd(a,b) = \gcd(a-bq, b)$ ⤳ Euclidean algorithm

→ for $a, b \in \mathbb{Z}$, $b|a \Leftrightarrow a = bk$ for some $k \in \mathbb{Z}$

a and b are relatively coprime iff $\gcd(a,b) = 1$

→ Euclid's Lemma: let $a, b, c \in \mathbb{Z}$. if $a \perp b$ and $a | bc$, then $a | c$

→ linear diophantine equation: $ax + by = c$, WTF x, y

↳ given a solution (x_0, y_0), $x = x_0 + k\left(\frac{b}{\gcd(a,b)}\right)$

$y = y_0 - k\left(\frac{a}{\gcd(a,b)}\right)$ $k \in \mathbb{Z}$

→ Bezout's Lemma: let $a, b, c \in \mathbb{Z}$. then $ax + by = c$ has a solution $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ iff $\gcd(a,b) | c$

→ in a number system, u is a unit $\Leftrightarrow \exists\, v$ in # system s.t. $uv = 1$ (u has multiplicative inverse)

a nonzero, nonunit p is prime $\Leftrightarrow p|uv \Rightarrow p|u$ or $p|v$

a nonzero, nonunit p is irreducible $\Leftrightarrow p = uv \Rightarrow u$ or v is a unit

↳ in all number systems, prime $\Rightarrow$ irreducible. --- (1)

in $\mathbb{Z}$, units are $\{-1, 1\}$ and irreducible $\Rightarrow$ prime --- (2)

(1) $p = ab \Rightarrow p | ab \overset{\text{WLOG}}{\Rightarrow} p|a \Rightarrow pk = a$, $k \in \mathbb{Z} \Rightarrow p = pkb \Rightarrow 1 = k \cdot b \Rightarrow b$ is a unit

(2) let p be irreducible and $p | ab$, $a, b \in \mathbb{Z}$ → ① $p|a$ ✓

factors of $p = \{\pm 1, \pm p\}$

↳ ② $p \nmid a \Rightarrow \gcd(a, p) = 1 \Rightarrow p \perp a \wedge p | ab \Rightarrow p | b$ by coprime lemma

→ factorization is unique: assume 2 through n has unique factorization for some $n \in \mathbb{N}$

suppose we can write $n+1 = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ both in non-decreasing order (p, q are positive primes)

WLOG, suppose $p_1 \le q_1$, WTS $p_1 = q_1$: $p_1 | q_1 \cdots q_\ell \Rightarrow \exists\, q_j$, $j \in [\ell]$ s.t. $p_1 | q_j \Rightarrow p_1 = q_j$ (both primes)

so $p_1 \le q_1 \le q_j = p \Rightarrow p_1 = q_1 \Rightarrow p_2 \cdots p_k = \overset{=m}{q_2 \cdots q_\ell}$ $(p_1 = q_1 > 0) \Rightarrow 2 \le m \le n$ $(m < n+1)$ → apply I.H.