CS 70 M11

cardinality = $|A|$ = size | $\subseteq$ subset $\supseteq$ superset | relative complement of A in B, $B \setminus A$ | in B but not A | $\mathbb{N}$ natural | $\mathbb{Z}$ integers | $\mathbb{Q}$ rational | $\mathbb{R}$ real | $\mathbb{C}$ complex

powerset = all subsets | $\in$ in set | $\forall$ for all | $\exists$ there exists | $\wedge$ and

11 Induction

Base Case $P(0)$. Induction Hypothesis, Inductive step $P(k+1)$ "claim to be true: $P(k)$

Strong Induction: assume $V(k)$ is true for $0 \le k \le n$

If $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then S has a smallest element

Well-ordering Principle – every non-empty set of natural #s in any subset of natural #s

$n > 0$, $n-1 \in \mathbb{N}$, $P(n-1)$ true $\to P(n)$ contradiction

12 Stable Marriage

man-optimal, woman-pessimal | woman-optimal = unstable

stable/unstable/rogue couple | pessimal woman = least preferred some (whatever) man paired/in stable pairing.

Improvement Lemma – If M proposes to W on the day, on every subsequent day she has someone on a string she likes as least as much as M.

Proof – Suppose jth day, $j > k$ W has some or $M^* < M$ on a string. On day $j-1$, she has M' on a string and liked at least as much as M. M' still proposes since she paired couple. So W has at least as much as M' on jth day, best choice best of good as M'. M' will choose over M^* – contradicts assumption of pairing lemma.

Lemma: The algorithm terminates w/ a pairing

Proof: Suppose man M left unpaired. Must have proposed to every woman on list. By Improvement lemma each woman has someone on a string. Thus terminal $\mathbb{Z}$ = n women for n men on a string, including M = n+1 men, contradiction.

Theorem: pairings produced is always stable

Proof – Show there no man M cause in rogue couple. Any couple (M, W) is in pairing. Suppose M prefers some woman W^* to W. Will show W^* prefers her partner to M. Argue that W^* prefers her partner M^* to M, (M, W^*) can be rogue couple. $W^* > W$ in M's list, must have proposed to her first, so W^* must have rejected him for someone she prefers. By Improvement Lemma, W^* likes her partner at least as much as M. Therefore, $M^* > M$ in woman's list, so (M, W^*) is rogue couple, ↯ pairing is stable.

Theorem: The pairing output by the stable Marriage Algorithm is male optimal

Proof: Suppose not male optimal. Assume kth day rejected is day k – M was rejected by W^* in favor of M^* who proposed. optimal woman = stable pairing $T = \{M + W^*, \ldots\}$ (M, W^*) = rogue couple. ⇒ W^* prefers M^* to M, since rejected M. On day k = day she rejected, M^* rejected W^* at least as much as optimal woman, at least as much as W^*. Therefore, (M^*, W^*) = rogue couple, ↯ not stable. Contradiction = assumption = male optimal.

Theorem: If a pairing is male optimal, it's woman pessimal

Proof: Let $T = \{\ldots (M, W) \ldots\}$ = male optimal. Suppose for sake of contradiction that stable pairing exists $S = \{\ldots (M^*, W) \ldots (M, W') \ldots\}$ s.t. $M^* < M$ for (M, W) = rogue couple in S. W prefers M > M^* since $M^* \downarrow$. M prefers W to partner W' in S, so W is partner in male optimal pairing T. Contradiction – male optimal = female pessimal

13 Mod

Theorem: If $a \equiv c \bmod m$ and $b \equiv d \bmod m$ and $a \cdot b = c \cdot d \bmod m$ Proof: $c = a + k \cdot m$ and $d = b + l \cdot m$, so $c \cdot d = a + k \cdot m \cdot b + l \cdot m = a \cdot b + (k+l) \cdot m$ $= a \cdot b = c \cdot d \bmod m$

$+ - \times$ = ok $\div$ = $x = y \bmod m$ = m divides $(x-y)$ = $x = y \bmod m$ e.g. 2, 9, 5 are congruent modulo 12

multiplicative inverse only exists if set is 1 = relatively prime

Theorem: Let m, x be positive integers, such that $\gcd(m, x) = 1$ then x has a multiplicative inverse (mod m) = unique solution for $ax \equiv 1 \bmod m$ = a = unique multiplicative inverse

Proof: Consider sequence of numbers $0, x, 2x \ldots (m-1)x$ = all distinct mod m. Only m distinct values mod m. $ax \equiv 1 \bmod m$ for $a(a \bmod m) = a$ = unique multiplicative inverse

Verify: $0x = bx \bmod m$ for 2 distinct values a, b in range $0 \le b \le a \le m-1$ $(a-b)x \equiv 0 \bmod m \Rightarrow (a-b)x = km$ for integer k. $x + m$ are relatively prime, so x cannot share divisors

$a - b$ = integer multiple of m, but $a - b$ is between 1 and $m-1$. $1 = \gcd(m, x)$ so $m + bx$

Theorem: Let x, y, q, r be natural numbers such $x = yq + r$ and $r < y$ then $\gcd(x, y) = \gcd(r, y)$

Proof: This is the same common divisor of x and y is also a common divisor of x and r and vice versa. Let d divide x and y, so there exist integers z and z' s.t. $zd = x$ and $z'd = y$ $z'd = y \Rightarrow r = x - yq = zd - z'dq = (z - z'q)d$ so d also divides r. Euclid's + extended euclid

14 Bijections + RSA

Bijections – $f: A \to B$ bijection = there is a unique $a \in A$ s.t. $f(a) = b$: 1. f is onto: every $b \in B$ has pairing at A

1. f is 1:1 – for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$

2. f is onto – for all $b \in B$ there exists $a \in A$ s.t. $f(a) = b$

Lemma: for a finite set A, $f: A \to A$ is bijection if and only if f has an inverse function $g: A \to A$ s.t. $\forall x \in A$ $g(f(x)) = x$ Proof: If $f(x) = f(x')$, then $x = g(f(x)) = g(f(x')) = x'$.

Since f is 1:1, must have |A| elements in image of f ⇒ onto. Proof: Let $N = pq$, p, q relatively prime $\varphi(N) = (p-1)(q-1)$. Multiplicity = (N, e), $\gcd(e, \varphi(N)) = 1$

★ RSA: $E(x) = x^e \bmod N$, $N = pq$, e relatively prime $\varphi(p-1)(q-1)$ $\{1, 2, \ldots (p-1)\}$ we have $a^{p-1} = 1 \bmod p$. $a^x \bmod p \equiv 1$ p = any #, x = factor of $p-1$, a = relatively prime

Fermat's Little Theorem: For any prime p and any $a \in \{1, 2, \ldots (p-1)\}$ $(p-1)! \equiv a \cdot p^{-1} \cdot (p-1)! \pmod p$ $\equiv -p - 1)!$

Proof: $f(x)$ is bijection. $(p-1)! \equiv a \cdot p^{-1} \cdot (p-1)! \pmod p$, we have $a(E(x)) = x \bmod N$ for every $x \in \{0, 1, \ldots N-1\}$ $\varphi(N) = |\{a \in \{0, 1, \ldots N-1\} : \gcd(a, N) = 1\}| = (p-1)(q-1)$ for integer b =

Theorem: modular definition of E and D, we have $(x^e)^d = x \bmod N$ for every $x \in \{0, 1, \ldots N-1\}$. By definition, $d = \text{Inv}(e, (p-1)(q-1))$, so $ed = 1 + b(p-1)(q-1)$ for integer b =

Proof: go back to the def $x^{ed} = x^{1+b(p-1)(q-1)} = x(x^{(p-1)(q-1)}) = x \cdot 1^b = x$ Test 1: x not coprime, p, q – use Fermat's Little Theorem to deduce $x^{p-1} = 1 \bmod p$. Then $x^{ed} = x^{1+b(p-1)(q-1)} = x$ Test 2: x is multiple of p, so clearly divisible by p. Also q = divisible by p and q, must be divisible by pq, $x^{ed} = x \bmod pq$

$(x^{p-1})^{b(q-1)} \equiv 1^{b(q-1)} \bmod p$ and have $x^{b(p-1)(q-1)} - 1 \equiv 0 \bmod p$. Test 3: x is multiple of q – clearly divisible by q. Also q = divisible by p and q, must be divisible by pq, $x^{ed} = x \bmod pq$

divisible by p, product of primes – $pq = N$ $\equiv 0 \bmod N$.

15 Polynomials

Property 1: A non-zero polynomial has at most d roots. Property 2: Given distinct points $(x_1, y_1) \ldots (x_d, y_d)$ there exists a polynomial of degree d with distinct points. Polynomial Interpolation (Lagrange) $\Delta_1(x) = \frac{(x-y)(x-z)}{(x_1-y)(x_1-z)}$, $P(x) = y_1\Delta_1(x) + y_2\Delta_2(x)$

polynomial $p(x)$ of degree d (mod m) d such coeff $p(x_i) = y_i$ $0 \le i \le d$

Proof of property 2: Find roots, $\forall i$: $f(x_i) = g(x_i) = 0$ mod m pts. Contradiction

Property 3: Claim: $\forall a \in S$ and a polynomial $p(x)$ w/ degree d, then $p(x) = (x-a)q(x)$ for polynomial w/ degree d-1 (Lemma 2: a polynomial w/ degree d w/ distinct roots $a_1 \ldots a_d$ can be written as $p(x) = (x-a_1) \ldots (x-a_d)$

Finite Fields: F_m, for $F(x_m)$ points, not poly – deg $|1$, $d|m$, $d-1 \mid x^m$, $d-1 \nmid x^{d+1}$, $x^{d-1} = 1 \bmod p$.

Secret sharing (mod p), $q > n, s$ (n = total # of people, s = secret). $f(0) = s$,

$\frac{1}{2} = 4$

$\gcd(7, 2) = 1$ $1 = 7 + 2(-3)$

$-3 \bmod 7 = 4$

$2^{43} \bmod 77$

$2^{43} \bmod 7 = (2^6)^7 \cdot 2 \bmod 7 = 2 \bmod 7$

$2^{43} \bmod 11 = 6^{10})^4 \cdot 2^3 \bmod 7 = 8 \bmod 7$

$7 \mid 2^{43} - 2 - 7n$ $2n + 7 = 11n + 4$

$11 \mid 2^{43} - 4 - 11n$ 30

$10^{25^{105}} \bmod 77 = 10^{25^{105}} \bmod 11 = 10^{25^{105}} \bmod 7 = 0$

$25^{105} \bmod 22 = 3 \cdot 11$, $10^{25^{105}} \bmod 6 = 0$

$25^{105} \equiv 1 \bmod 22$

$10^{25^{105}} \bmod 77 = 10^{25^{105}} \bmod 22$

$(10-2)^4 \bmod 77$

$(3-2)^4 \bmod 77$

$6^4 \bmod 77$

27