**A. i. LOGIC**

* proposition: can be T/F
* tautology: T for all values, e.g. $p⋁¬p$, $p\rightarrow q\leftrightarrow ¬q\rightarrow ¬p$
* contradiction: F for all val, e.g. $p⋀¬p$
* if neither of 2 above, contingency
* de Morgan’s laws: $¬∀xP(x)≡∃x¬P(x)$ ; $¬∃xP(x)≡∀x¬P(x)$
* modus ponens: $(p⋀(p\rightarrow q))\rightarrow q$
* modus tollens: $(¬q⋀(p\rightarrow q))\rightarrow ¬p$

**ii. PROOFS**

* direct$ (p\rightarrow q)$
* contrapositive ($p\rightarrow q≡¬q\rightarrow ¬p)$
* contradiction ($¬(p\rightarrow q)\rightarrow F$)
* non-constructive existence: all cases are true

**iii. SETS**

* subset: every elt of A is in B: $A⊆B$
* **Well-ordering property**: every nonempty subset of the set of positive integers has a least element
* A=B means $∀x(x\in A\leftrightarrow x\in B)$
* $A∪B=\{x :x\in A⋁x\in B\} $
* $A∩B=\{x :x\in A⋀x\in B\}$
* complement: $\overbar{A}=\{x :x\in U⋀x\notin A\}$
* difference: $A\B=\{x :x\in A⋀x\notin B\}$
* Cartesian pdt: $A×B=\{(a,b) :a\in A⋀b\in B\}$
* Power set: $P\left(A\right)=\{x:x⊆A\}$
* Empty set Ø contains no elements
* Ø$⊆$A, x$\notin $ Ø for arbitrary set A, elt x
* disjoint set: intersection is the empty set
* Russell’s paradox: A={x:x$\notin $x}
* set ID: existential for arbitrary elt🡪generalize. negating nested quant:

****

**B. i. FUNCTIONS**

* **fxn**: non-empty sets A&B, f:A🡪B assigns exactly 1 elt of B to ea. elt of A. A:domain, a$\in $A:preimage, B:codomain, b$\in $B:image
* inverse: assign elt of A to one of B s/t f(a)=b
* composed: lower level’s (e.g. g(x)) range$⊆$higher’s (f(x)) domains for f(g(x))
* must be 1-to-1. if no inverse, not 1-to-1 or onto
* **injective**=1-to-1. No y assigned twice. For every $a\_{1},a\_{2}\in A$, f(a1)=f(a2)🡪a1=a2
* **surjective**=onto. $∀(b\in B)(∃\left(a\in A\right):f\left(a\right)=b)$
* graph$⊆$AxB s/t f(a)=b for each ordered pair (a,b)
* sequence: “function from a subset of the set of integers to a set S. We use the notation an to denote the image of the integer n. We call an a term of the sequence.”

**ii. CARDINALITY**

* set of rational numbers is countably inﬁnite: snake method. List p/q s/t p+q=some integer, skip duplicates
* set of real numbers is not countable: decimal expansion, diagonalization arg
* lAl=lBl iff 1-to-1 correspondence bw the two sets
* countable set: either ﬁnite or has the same cardinality as the set of positive integers (1-to-1 rel)
* if A,B countable, so is union

**C. Number theory. i. DIVISION**

* all ints: a l b iff c=b/a
* division algorithm: there are unique integers q and r, with 0 ≤ r<d, such that a = dq+r (q=quotient, r=*positive* remainder)
* a ≡ b (mod m) iff $∃k\in Z$ : a = b+km
* addition and multiplication preserve ≡
* so a+bm≡(a+b) (mod m)
* “Closure” property: If a and b belong to Zm, then a+mb and a·mb belong to Zm.
* base conversion: div by base, successive quotients are digits from right to left
* mod exponentiation: conv. exp. to binary exp to make use of repeated squares

**ii. PRIMES**

* An integer p>1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.
* **Fundamental Theory of Arithmetic**: int>1 can be written uniquely as a prime or as the product of 2+ primes, where the prime factors are in order of nondecreasing size.
* If n is a composite integer, then n has a prime divisor less than or equal to √n

*pf: n=ab. If a>√n and b>√n, then ab >√n·√n = n: contradiction. So a ≤√n or b ≤√n*

* gcd(a,b): largest int “d” s.t. d l a and d l b

*The* ***gcd*** *of 2 ints ,not both zero, exists bc the set of common divisors of these integers is nonempty and ﬁnite.*

* lcm(a,b) = p1max(a1,b1)p2max(a2,b2) ···p n max(an,bn)

*The* ***lcm*** *exists bc the set of ints divisible by both a and b is nonempty (as ab belongs to this set), and every nonempty set of positive integers has a least element by WOP*

* ab= gcd(a,b)·lcm(a,b)
* ints a,b relatively prime if gcd(a,b)=1
* integers a1,a2,...,an are pairwise relatively prime if gcd(ai, aj) = 1 whenever 1≤i<j ≤ n.
* **Euclid’s lemma**: Let a = bq+r, a,b,q,r$\in $Z. Then gcd(a,b) = gcd(b,r).
* **Bezout’s theorem**: If a and b are positive integers, then there exist integers s and t such that gcd(a,b)= sa+tb.
* if a prime num divides a composite num, it also divides 1 of the composite’s factors
* ac≡bc(mod m)&gcd(c,m)=1🡪a≡b(mod m)
* for relatively prime ints a,m, the inverse a mod m exists and is unique: (sa≡1(mod m))

*Pf: gcd(a,m)=1=sa+tm. tm(mod m)=0, so 1=sa. s is inverse of a mod m. Unique: Suppose a,b both inv. Then xb ≡ 1 mod m 🡪 axb ≡ a mod m, but ax ≡ 1 mod m*

*🡪 axb ≡ b mod m. Hence a ≡ b mod m.*

* to solve linear congruence ax ≡ c (mod m), multiply both sides by inverse. to solve system, back substitution or the following:
* **Chinese Remainder Theorem**: for a system of linear congruences with relatively prime mods m1,m2…mn, the solution is a unique # m=m1m2…mn.

*Pf: let Mk=m/mk, k=1,2…n🡪gcd(mk,Mk)=1. Must have inverse yk: Mkyk=1(mod mk). Note x ≡ akMkyk ≡ ak (mod mk). Soln: x = a1M1y1 +a2M2y2 +···+anMnyn.*

* **Fermat’s Little Theorem**: If p is prime and p$∤$a, then a^(p−1) ≡ 1 (mod p). Also, for every integer a we have a^p ≡ a(mod p).

**RSA CRYPTOGRAPHY**

* RSA: n,e to encrypt. Decrypt: inverse; only reasonable time when p,q known
* (n,e) where n = pq (p,q lg primes), and exp e rel. prime to (p−1)(q −1).
* Encrypt with key (2537,13). 2537 = 43·59, gcd(e,(p−1)(q −1)) = gcd(13,42·58) = 1.
* Translate the letters into their numerical equivalents. If needed: add 0 so 2 dig, pad plaintext w dummy Xs
* Then group #s into blocks of 4 digits (because 2525 < 2537 < 252525).
* Encrypt each block using the mapping C = M^13 mod 2537. Repeated sq 🡪 1819^13 mod 2537 = 2081 and 1415^13 mod 2537 = 2182. The encrypted message is 2081 2182.
* Decryption key d is inv of e mod(p−1)(q −1) [exists bc gcd(e,(p−1)(q −1)) = 1.] by def of mod, de≡ 1 (mod (p−1)(q −1))🡪de= 1+k(p−1)(q −1) for some k. So:
* C^d ≡ (M^e)^d = M^de = M^(1+k(p−1)(q−1) (mod n)).
* By **FLT** [when gcd(M,p) = gcd(M,q) = 1] M^(p−1) ≡ 1 (mod p) & M^(q−1) ≡ 1 (mod q). Consequently, C^d ≡ M ·(M^(p−1))^k(q−1) ≡ M ·1 = M(mod p) and
* C^d ≡ M(M^(q−1))^k(p−1)≡M(mod q). Bc gcd(p,q) = 1, **CRT**🡪 C^d ≡ M(mod pq).

**PROOF BY INDUCTION**

* (P(1)∧∀k(P(k)→ P(k+1))) →∀nP(n), k$\in $Z^+

*Pf: Assume P(n) is false at least once. S =pos ints w P(n) false is nonempty. By WOP, S has a least elt; call it m. m>1🡪m−1 is a pos int. m−1 < m(least elt)🡪m-1*$\notin $ *S, so P(m−1) must be true. P(m−1) →P(m). Contradiction.*