

1(a) Determine whether 97 is prime, as efficiently as you can. State clearly any theorems that you use, and show your work.

Theorem: if n is composite, then it is divisible by a prime $\leq \sqrt{n}$.

Since $\sqrt{97} < \sqrt{100} = 10$, we only have to check the primes 2, 3, 5, 7.

- Clearly, 97 is not divisible by 2, 3, or 5.

- It is not divisible by 7:

$$97 \div 7 = 13 \frac{6}{7}$$

Hence 97 is prime.

(b) Determine the cardinality of each of these sets, with brief explanations:

- (i) the set of all finite strings of 0s and 1s
- (ii) the set of all functions from $\{1, 2, 3\}$ to $\{a, b, c, d\}$
- (iii) the set of all irrational numbers

(i) This set is countable and infinite. To list them all, first list strings of length 0, then strings of length 1, then strings of length 2, etc.

(ii) the cardinality is 4^3 .

(iii) This set is uncountable because \mathbb{R} is uncountable and \mathbb{Q} is countable. (If $\mathbb{R} - \mathbb{Q}$ were countable, then $\mathbb{R} = (\mathbb{R} - \mathbb{Q}) \cup \mathbb{Q}$, a union of two countable sets, and so \mathbb{R} would be countable.)

2(a) How many positive integers are there whose distinct prime factors are exactly 2, 3, 5, and 7, having 10 prime factors? (eg. $2 \cdot 3^4 \cdot 5^3 \cdot 7^2$)

We want positive integers w, x, y, z with $w+x+y+z=10$,
to get $2^w 3^x 5^y 7^z$. Such a 4-tuple is described by
three positions in the expression: $\underbrace{1+1+1+1+1}_w \underbrace{1+1}_x \underbrace{1+1+1+1}_y \underbrace{1+1}_z$

There are 9 positions, so the
number of ways of choosing them is

$$\boxed{\binom{9}{3}}$$

2(b) Write the number 1023 in base 4. (Show your work.)

$$\begin{aligned} 1023 &= 255 \cdot 4 + 3 \\ &= (63 \cdot 4 + 3) \cdot 4 + 3 \\ &= ((15 \cdot 4 + 3) \cdot 4 + 3) \cdot 4 + 3 \\ &= (((3 \cdot 4 + 3) \cdot 4 + 3) \cdot 4 + 3) \cdot 4 + 3 \\ &= 3 \cdot 4^4 + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 \end{aligned}$$

So, $\boxed{33333}$ in base 4.

$$\begin{aligned} \text{OR, } 1023 &= 1024 - 1 = 2^{10} - 1 = 4^5 - 1 \\ &= 100000 - 1 \quad \text{in base 4} \\ &= 33333 \end{aligned}$$

3. On a certain island, everyone is a knight or a knave. Knights always tell the truth and knaves always lie. A says "B is a knave." B says "the two of us are of opposite types." Let p be the proposition "A is a knight" and let q be the proposition "B is a knight."

(a) Write down two propositions (involving p and q) which express the information you have learned from the statements of A and B.

(b) Use truth tables for your propositions to determine what A and B are.

(a) Statement ①: $(p \wedge \neg q) \vee (\neg p \wedge q)$

or, equivalently, $p \oplus q$

Statement ②: $(q \wedge (p \oplus q)) \vee (\neg q \wedge (\neg(p \oplus q)))$

or, equivalently,

$(\neg q) \oplus (p \oplus q)$

(b)

p	q	$\neg p$	$\neg q$	$p \oplus q$	$(\neg q) \oplus (p \oplus q)$	① \wedge ②
T	T	F	F	F	F	F
T	F	F	T	T	F	F
F	T	T	F	T	T	T
F	F	T	T	F	T	F

The only way for ① and ② to both be true is if p is false, q is true.

So

A is a knave, B is a knight.

4(a) Show, by a combinatorial argument, that $\binom{2n}{2} = 2\binom{n}{2} + n^2$ for any $n \in \mathbb{Z}_+$.

LHS = # of 2-element subsets of a set of $2n$ elements.

Split the set into two sets $A \cup B$, each of size n .

there are 3 kinds of 2-element subsets: ① those in A , ② those in B , and ③ those with one elt. of A and one elt. of B .

The number of subsets of type ① is $\binom{n}{2}$.

The number of subsets of type ② is $\binom{n}{2}$.

The number of subsets of type ③ is n^2
(choose one from each)

So, # of 2-elt. subsets of $A \cup B$ is $2\binom{n}{2} + n^2$.

(b) Show that $\sum_{k=0}^n 2^k \binom{n}{k} = 3^n$.

Binomial theorem:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Taking $a=2$, $b=1$ we get

$$3^n = \sum_{k=0}^n \binom{n}{k} 2^k$$

5. Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions.

(a) Define what it means for f to be *injective* (one-to-one), *surjective* (onto), and *bijective*.

(b) Prove that if $g \circ f$ is surjective then so is g .

(c) If $g \circ f$ is a bijection, is f a bijection? Explain why or why not.

(a) f injective : $\forall a, b \in A, f(a) = f(b) \rightarrow a = b$

f surjective : $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$

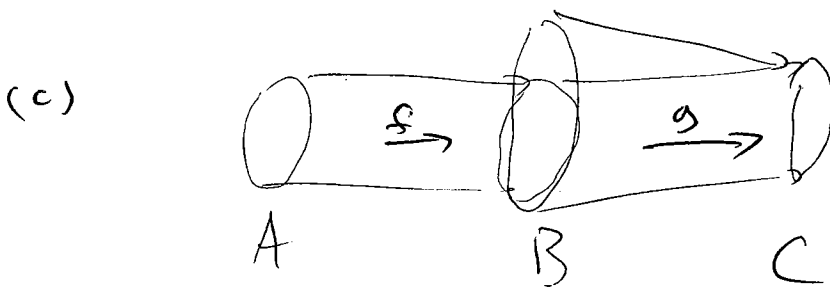
f bijective : injective and surjective.

(b) $g \circ f$ surjective. So, for any $c \in C$,

there is an $a \in A$ with $g(f(a)) = c$.

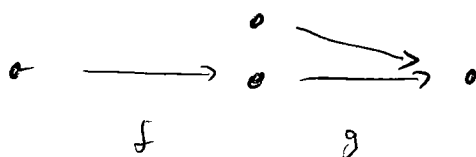
Writing $b = f(a)$, we have $g(b) = c$.

So for any $c \in C$, we found a $b \in B$ with $g(b) = c$. Hence g is surjective.



f need not be a bijection, because B could be larger than A and C .

eg. If A and C have one element each, and B has two elements, then f will not be a bijection.



6. Recall from the homework that if p is prime and $0 < k < p$ then p divides $\binom{p}{k}$.

(a) Give the precise definition of the statement " $l \equiv m \pmod{n}$."

(b) Using the fact above, prove that for any positive integers a and b and any prime p ,

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

(a) This means: $l - m$ is divisible by n .

(b) The LHS is

$$\begin{aligned} (a+b)^p &= \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} \\ &= b^p + \binom{p}{1} a b^{p-1} + \binom{p}{2} a^2 b^{p-2} + \dots + \binom{p}{p-2} a^{p-2} b^2 + \binom{p}{p-1} a^{p-1} b + a^p \end{aligned}$$

$$\text{So, } (a+b)^p - (a^p + b^p) = \binom{p}{1} a b^{p-1} + \dots + \binom{p}{p-1} a^{p-1} b$$

$$\left(= \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \right)$$

Each binomial coefficient on the RHS is divisible by p . Hence each term is divisible by p , so the RHS is divisible by p . \square