The Pigeonhole Principle

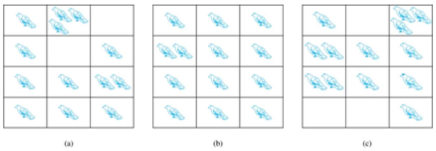
Section 6.2

Section Summary

- The Pigeonhole Principle
- The Generalized Pigeonhole Principle

The Pigeonhole Principle

- If a flock of 20 pigeons roosts in a set of 19 pigeonholes, one of the pigeonholes must have more than 1 pigeon.



Pigeonhole Principle: If k is a positive integer and $k + 1$ objects are placed into k boxes, then at least one box contains two or more objects.

Proof: We use a proof by contraposition. Suppose none of the k boxes has more than one object. Then the total number of objects would be at most k. This contradicts the statement that we have $k + 1$ objects.

◀

The Pigeonhole Principle

Corollary 1: A function *f* from a set with $k + 1$ elements to a set with k elements is not one-to-one.

Proof: Use the pigeonhole principle.

- Create a box for each element y in the codomain of f .
- Put in the box for y all of the elements x from the domain such that $f(x) = y$.
- Because there are $k + 1$ elements and only k boxes, at least one box has two or more elements.

Hence, *f* can't be one-to-one.

◄

Pigeonhole Principle

Example: Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

Example (*optional*): Show that for every integer n there is a multiple of n that has only 0s and 1s in its decimal expansion.

Solution: Let n be a positive integer. Consider the $n + 1$ integers $1, 11, 111, \ldots, 11\ldots1$ (where the last has $n + 1$ 1s). There are n possible remainders when an integer is divided by n. By the pigeonhole principle, when each of the $n + 1$ integers is divided by n, at least two must have the same remainder. Subtract the smaller from the larger and the result is a multiple of n that has only 0s and 1s in its decimal expansion.

Word Problem on Collisions

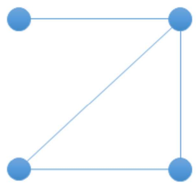
- **Example:** In a very dark room there is a wardrobe; it contains 200 **black** socks; 200 **blue** socks and 200 **green** socks. Somebody randomly picked N socks from there.
  - What is the smallest N that guarantees that there are at least two socks of the same color?
  - What is the smallest N that guarantees that there are at least two black socks or at least two blue socks?

(Refer to the worst-case running time of an algorithm.)

Pigeonhole Principle + Additional Reasoning

Example: Some country has N cities; some of them are connected by a two-way non-stop bus service between two cities.

Prove that there exist two cities that are endpoints to the same number of bus services.



The Generalized Pigeonhole Principle

The Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Proof: We use a proof by contraposition. Suppose that none of the boxes contains more than $\lceil N/k \rceil - 1$ objects. Then the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = N,$$

where the inequality $\lceil N/k \rceil < \lceil N/k \rceil + 1$ has been used. This is a contradiction because there are a total of n objects. ◀

Example: Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.

The Generalized Pigeonhole Principle

Example: **(a)** How many cards must be selected from a standard deck of 52 cards to guarantee that at least three cards of the same suit are chosen?

(b) How many must be selected to guarantee that at least three hearts are selected?

Solution: **(a)** We assume four boxes; one for each suit. Using the generalized pigeonhole principle, at least one box contains at least $\lceil N/4 \rceil$ cards. At least three cards of one suit are selected if $\lceil N/4 \rceil \geq 3$. The smallest integer N such that $\lceil N/4 \rceil \geq 3$ is $N = 2 \cdot 4 + 1 = 9$.

(b) A deck contains 13 hearts and 39 cards which are not hearts. So, if we select 41 cards, we may have 39 cards which are not hearts along with 2 hearts. However, when we select 42 cards, we must have at least three hearts. (Note that the generalized pigeonhole principle is not used here.)

Generalized Pigeonhole Principle

- **Example:** Assume that in the whole world there are more than 7 billion people having full body weight not exceeding 100 kilograms. (We do not know how these weights are assigned; what is their distribution, etc.)
  What number of people should necessarily have the same body weight? Everyone's weight is rounded to the closest milligram.

Pigeonhole Principle in Number Theory

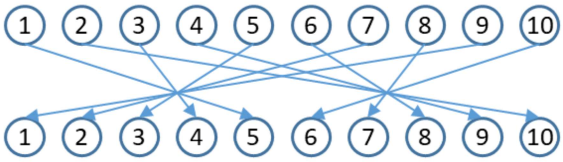
- **Example:** Prove that among any 7 full squares there are two that end with the same digit.
- **Solution:** Sort all full squares into bins (depending on their last digit):
(No full square can end with digit 2,3,7,8 – exhaustive search.)

- Since there are 7 items and 6 bins, at least two items will be in the same bin.

Existence of the Inverse Element

Statement: Let p be any prime number. For any $a \not\equiv 0 \pmod{p}$ there exists exactly one inverse element a^{-1} such that $a^{-1}a \equiv 1 \pmod{p}$.

Proof: First prove that function $f(x) = (a \cdot x \bmod p)$ is injective.



(Figure for $p = 11$, $a = 5$.)
$f\colon \{1, \dots, p-1\} \to \{1, \dots, p-1\}$

Indeed, assume that $a \cdot x_1 \bmod p \; = \; a \cdot x_2 \bmod p$. Rewrite this:

$$a \cdot x_1 \equiv a \cdot x_2 \pmod{p}; \quad a \cdot x_1 - a \cdot x_2 \equiv 0 \pmod{p};$$
$$a \cdot (x_1 - x_2) \equiv 0 \pmod{p}.$$

Since $a \not\equiv 0\ (mod\ p)$, we have $x_1 - x_2 \equiv 0 \pmod{p}$; $x_1 \equiv x_2 \pmod{p}$.

Pigeonhole Principle: Injective function between sets of the same size must be surjective (if some {1,...,p-1} do not have preimages; there must be collisions).
So, there must be some x^* such that $f(x^*) = 1$. This x^* is a^{-1}.

Chinese Remainder Theorem

Chinese Remainder Theorem: For any mutual primes p,q there exists unique solution for the system of congruences:

$$\begin{cases} x \equiv a \pmod{p}, \\ x \equiv b \pmod{q}. \end{cases}$$ The solution has form $x \equiv C \pmod{p \cdot q}$,

Example:

$$\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 6 \pmod{11}. \end{cases}$$

Solution:

$x \equiv 39 \pmod{55}$

	0	1	2	3	4	5	6	7	8	9	10
0	0		35	25	15	5			30	20	10
1	11	1		36	26	16	6			31	21
2	22	12	2		37	27	17	7			32
3	33	23	13	3		38	28	18	8		
4		34	24	14	4		39	29	19	9	

Chinese Remainder Theorem

Pigeonhole-based proof:
Every x from $\{0, \ldots, p \cdot q - 1\}$ maps to a pair (a, b)
where $a \in \{0, \ldots, p-1\}$, $b \in \{0, \ldots, q-1\}$ and $\begin{cases} x \equiv a \pmod{p}, \\ x \equiv b \pmod{q}. \end{cases}$

This mapping should be *injective* because p,q are mutual primes. But it is therefore also *surjective* (because $\{0, \ldots, p-1\} \times \{0, \ldots, q-1\}$ has the same size as $\{0, \ldots, p \cdot q - 1\}$.
Since it is surjective; each (a,b) has preimage C that maps to it. The congruence system is solvable; Chinese Remainder Theorem is proven. The proof is nonconstructive (no way to find preimage C).

(A constructive proof could use Blankinship's algorithm, etc.)