Pigeon-Hole Principle

Pigeon-Hole Principle

If m items are put into n boxes and $m > n$, then some boxes have more than one item. Since $m > n$, after filling up the n boxes we have still items left over which means some box has more than 1 item.

e.g. In a crowd of 367 people, at least two people have the same birthday.

Handshaking

From Wikipedia

Handshaking

If there are n people who can shake hands with one another (where $n > 1$), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people. As the 'boxes' correspond to number of hands shaken and each person can shake hands with anybody from 0 to $n - 1$ other people, this creates $n - 1$ possible boxes. This is because either the '0' or the '$n - 1$' box must be empty (if one person shakes hands with everybody (else), it's not possible to have another person who shakes hands with nobody; likewise, if one person shakes hands with nobody there cannot be a person who shakes hands with everybody else). This leaves n people to be placed in at most $n - 1$ non-empty boxes, guaranteeing duplication.

$a^k \equiv_n 1$, when gcd(a,n)=1

Theorem

If a is relatively prime to n then there exists $k > 0$ such that $k \leq n$ and $a^k \equiv_n 1$.

Proof

Assume a is relatively prime to n. Consider the remainders of

$$a, a^2, \ldots, a^{n+1}$$

when divided by n. There are $n+1$ elements in $\{a, a^2, \ldots, a^{n+1}\}$ and there can be only n remainders (from 0 to $n-1$). By the Pigeon-Hole Principle, there exists $i, j \in \{1..n+1)$ and $i \neq j$ (assume $i < j$) such that a^i and a^j have the same remainder, i.e. $a^i \equiv_n a^j$.

Since $i < j$, $j - i > 0$ and $j - i \leq n$ (since j is at most $n+1$ and i is at least 1). Since a is relatively prime to n , $a^{i-1} \equiv_n a^{j-1}$ (by cancellation). Continuing to cancel $a's$ on both sides we get (since $i < j$), $1 \equiv_n a^{j-i}$ i.e. $a^k \equiv_n 1$ where $k = j - i$.

Example

Let $a = 3$ and $n = 10$ then 3 and 10 are relatively prime. Find a k such that $3^k \equiv_{10} 1$.

k	1	2	3	4	5	6	7	8	9	10
$3^k mod\, 10$	3	9	7	1	3	9	7	1	3	9

We have $3^4 \equiv_{10} 1$.

Also $3^8 \equiv_{10} 1$.

Finding inverse using $a^k \equiv_n 1$

Finding inverse

Let $a \in \mathbb{Z}_n$. If a and n are relatively prime, there exists a k such that $0 < k \leq n$ and $a^k \equiv_n 1$.
Since $a^k = a * a^{k-1}$ and $a *_n a^{k-1} \equiv_n 1$ and so a^{k-1} is the inverse of a.

Since $gcd(3, 10) = 1$, we can find the inverse of 3.
From above, $3^4 \equiv_{10} 1$, $\therefore 3 * 3^3 \equiv_{10} 1$
From table above $3^3 \equiv_{10} 7$ $\therefore$ 7 is the inverse of 3.
Check: $3 * 7 = 21 \equiv_{10} 1$.