Event
A

Perform n - trials, independent

$$X_i = \begin{cases} 1 & \text{if } A \text{ occurs} \\ 0 & \text{otherwise} \end{cases}$$

$1 \le i \le n$

$\forall 1 \le i \le n \quad E[X_i] = 1 \cdot P(X_i = 1) + 0 \cdot P(X_i = 0)$

$= P(A) := \mu$

Relative frequency of A occuring in n - independent trials $=$ $\frac{\#\text{ of times A occurs in } n \text{ trials}}{n}$

$= \frac{\sum_{i=1}^{n} X_i}{n}$

$= \frac{S_n}{n}$

relative frequency of A $\frac{S_n}{n} \to \mu$ in Probability of A

Probability as $n \to \infty$

RSA - Algorithm

Rivest
Shamir ~ 1977
Adelman

Clifford
Cocks ~ 1973

Person
Khulani
"message"
M

Person
Sonal

: Create a one way function F

$e = F(M, \text{public key})$

Khulani
: Apply F on M

IND one
else can
invert M

: Sonal can "invert"
F to get M.
$M = G(e, \text{Private key})$

1(a) We need to show

$\sim$ is reflexive, symmetric & transitive.

(i) reflexive

let $a \in \mathbb{Z}$

as $n \mid 0$

$\Rightarrow n \mid a-a$

$\Rightarrow a \sim_n a$

(ii) symmetry

let $a, b \in \mathbb{Z}$ $a \sim_n b \Rightarrow n \mid a-b$

$\Rightarrow n \mid -(b-a)$

$\Rightarrow n \mid b-a$

$b \sim_n a$

(iii) transitive

let $a, b, c \in \mathbb{Z}$

$a \sim_n b$ & $b \sim_n c$

$n \mid a-b$ & $n \mid b-c$

$\Rightarrow n \mid (a-b)+(b-c)$

$\Rightarrow n \mid a-c$

$\Rightarrow a \sim_n c$ □

(ii) Let r_1, r_2 be given.

Let $z \in \mathbb{Z}$, and $z \in \bar{r}_1$, $z \in \bar{r}_2$

Then, $z = nk_1 + r_1$, $z = nk_2 + r_2$

$\therefore \quad nk_1 + r_1 = nk_2 + r_2$

We know $r_1, r_2 \in \{1, 2, \ldots, n-1\}$

$\Rightarrow n(k_1 - k_2) = r_2 - r_1$

As $r_1 < n$, $k_2 < n$ $\therefore r_2 - r_1 < n$

$\therefore r_2 - r_1 = 0 \Rightarrow r_1 = r_2$ Also $k_2 = k_1$

$\bar{r}_1 = \bar{r}_2$

$\therefore$ For r_1 and r_2 distinct,

$\bar{r}_1 \cap \bar{r}_2 = \phi$