RANDOM NUMBERS (from 1st lesson)

Informal: a number $m \in \mathbb{N}$ is random if for every program $P$ which outputs $m$, $P$ is longer than $m$.

Show that:

→ there are infinitely many random numbers.

→ the property of being random is undecidable.

Formal view:

→ program size $|P_e| = e$
→ $m \in \mathbb{N}$ is random if for all programs $e \in \mathbb{N}$ st. $P_e(m) = m$, it holds $e > m$.

(1) there are infinitely many random numbers.

Recall that each computable function is computed by infinitely many programs. Hence, for each $k \in \mathbb{N}$ there is $e_1 < e_2 < ... < e_k$ st. $P_{e_i} \neq \emptyset i = 1, \ldots, k$

$$|\{ P_{e_i}(0) \mid i \leq e_k \land P_{e_i}(0) \downarrow \}| \leq e_k - k$$

Hence, there are at least $k$ numbers $m \leq e_k$ which can’t be generated by programs $e < m$. 

→ these numbers are random.

Since this holds for every $k$, there are infinitely many random numbers.
(2) \( R = \{ m \mid m \text{ is random} \} \) is not recursive.

Assume \( R \) to be recursive, i.e.

\[
\chi_R(m) = \begin{cases} 
1 & \text{if } m \in R \\
0 & \text{otherwise}
\end{cases}
\]

Define

\[
g(m, x) = \text{least random number } > m \\
= \mu z, z \in R \text{ and } z > m \\
= m + 1 + \mu z, (m + 1 + z \in R) \\
= m + 1 + \mu z, (\chi_R(m + 1 + z) = 1)
\]

computable

by some there is \( s: \mathbb{N} \to \mathbb{N} \) total computable

s.t.

\[
g(m, x) = \varphi_{s(m)}(x)
\]

least random number > m

By 2nd recursion theorem there is \( m_0 \in \mathbb{N} \) \( \varphi_{m_0} = \varphi_{s(m_0)} \)

\[
\varphi_{m_0}(0) = \varphi_{s(m_0)}(0) = g(m_0, 0) = (\text{least random number } > m_0)
\]

hence \( m_0 \) generates a random number > \( m_0 \), contradiction!

\( \Rightarrow R \) not recursive.

Note \( \overline{R} \) is r.e.

\[
sc_{\overline{R}}(m) = \mu t, \bigvee_{e=0}^m sc(e, 0, m, t)
\]

\( \overline{R} \) is not r.e.

i.e. \( \{ \text{check if some program } e < m \text{ outputs } m \text{ on } 0 \} \)