1 Problem

Input: A PRNG engine that generates random integers uniformly distributed on $[0, n)$.
Output: A random integer y uniformly distributed on $[0, s)$, where $0 < s \le n$.

2 Rejection Sampling

2.1 Algorithm

```
uint Uniform(Prng, uint s)
    uint q = Prng.n / s      // integer division
    uint m = q * s
    while true
        uint x = Prng()      // Unif{0, ..., n-1}
        if x < m
            return x % s
```

2.2 Analysis

2.2.1 Notation

- $q = \lfloor n/s \rfloor$ and $m = qs$ (the largest multiple of s not exceeding n)
- Let $X_1, X_2, \dots$ be the *i.i.d.* outputs of successive PRNG calls, with

$$X_t \sim \mathrm{Unif}\{0, \dots, n-1\}.$$

- The (surely finite) stopping time

$$T = \min\{t : X_t < m\}.$$

- The algorithm returns

$$Y = X_T \bmod s.$$

2.2.2 Average Time Complexity

At each draw we have the acceptance event $A_t = \{X_t < m\}$ with

$$\mathbb{P}(A_t) = \frac{m}{n}.$$

Thus, T is geometric with success probability m/n, so

$$\mathbb{P}(T < \infty) = 1 \quad \text{and} \quad \mathbb{E}[T] = \frac{n}{m}.$$

This implies that T is finite, so the algorithm always terminate and is expected to draw n/m times from PRNG. Therefore, the average time complexity of the algorithm is

$$O\left(\frac{n}{m}\right) \cdot \Big(\text{the time complexity of } \texttt{Prng()}\Big),$$

and we can further claim that $O(n/m)$ is actually $O(1)$.

Proof. Since m is the largest multiple of s not exceeding n, we can write

$$n = m + r, \quad \text{where } 0 \leq r < s.$$

Then

$$\frac{n}{m} = \frac{m+r}{m} = 1 + \frac{r}{m} < 1 + \frac{s}{m} = 1 + \frac{1}{q} \leq 2$$

2.2.3 Correctness

Let $A = \{X_1 < m\}$ be the acceptance event of the first draw. Then for any $y \in \{0, \ldots, s-1\}$,

$$\mathbb{P}(Y = y) \;=\; \mathbb{P}(A)\,\mathbb{P}(y = X_1 \bmod s \mid A) + \mathbb{P}(A^c)\,\mathbb{P}(Y = y),$$

since A is the event that we accept immediately, otherwise we "restart" memorylessly.

Now we have $\mathbb{P}(A) = m/n = qs/n$ and, conditional on A, X_1 is uniform on $\{0, \ldots, m-1\}$, which has exactly q residues congruent to y mod s, hence

$$\mathbb{P}(y = X_1 \bmod s \mid A) = \frac{q}{m} = \frac{1}{s}.$$

Pluggin in we have

$$\mathbb{P}(Y = y) = \frac{qs}{n} \cdot \frac{1}{s} + \left(1 - \frac{qs}{n}\right)\mathbb{P}(Y = y)$$
$$\Rightarrow \mathbb{P}(Y = y) = \frac{1}{s}.$$