Cormen 31.7-3

Assume we have an efficient function D_A that decrypts 1% of messages randomly chosen from $\mathbb{Z}_n$.

```
Decrypt(C)        ▷ C = P_A(M) is the coded message that we want to decrypt
Repeat
      Repeat
            Z ← Random(0, n − 1)
      until gcd(Z, n) = 1        ▷ Z^{-1} exists (Corollary 31.26)
      M' ← D_A(P_A(Z) · C)
until P_A(M') ≡ P_A(Z) · C  (mod n)        ▷ M' is a correct decryption of P_A(Z) · C
return Z^{-1} M'
```

- If the algorithm terminates, it returns M:
  This is easy to prove.
- Expected # random choices ≈ 100:
  - On the average the inner loop is executed ≈ 1 time per execution of the outer loop:
    $$P(\gcd(Z,n)=1) = \frac{\phi(n)}{n} = \frac{(p-1)(q-1)}{pq} = \frac{pq-p-q+1}{pq} = 1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{pq}$$
    $$\approx 1, \text{ since } p,q > 10^{100}$$
  - On the average the outer loop is executed ≈ 100 times:
    In the inner loop we choose random numbers from $\mathbb{Z}_n$, until we find one that is in $\mathbb{Z}_n^*$. Thus, in the outer loop we apply D_A to $P_A(Z) \cdot C$, where Z is a number randomly chosen from $\mathbb{Z}_n^*$. If we could assume that $P_A(Z) \cdot C$ were a number randomly chosen from $\mathbb{Z}_n$, we would clearly be done. However, it is sufficient to assume that it is randomly chosen from $\mathbb{Z}_n^*$:

    $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ and
    $$\frac{|\mathbb{Z}_n - \mathbb{Z}_n^*|}{|\mathbb{Z}_n^*|} = \frac{n-\phi(n)}{n} = \frac{pq-(p-1)(q-1)}{pq} = \frac{q+p-1}{pq} < 10^{-100}.$$
    Thus, even if all numbers in $\mathbb{Z}_n - \mathbb{Z}_n^*$ are among those that D_A decrypts correctly, D_A still correctly decrypts $\approx 1\%$ of the numbers in $\mathbb{Z}_n^*$.

    Hence, since $P_A(Z) \cdot C = P_A(Z) \cdot P_A(M) \equiv P_A(ZM) \pmod{n}$, we just need to prove that
    $$Z \text{ randomly chosen from } \mathbb{Z}_n^* \Rightarrow P_A(ZM) \text{ randomly chosen from } \mathbb{Z}_n^*$$
    We prove this in two steps.
    * Z randomly chosen from $\mathbb{Z}_n^* \Rightarrow ZM$ randomly chosen from $\mathbb{Z}_n^*$:
      Assume that M is random. Then $P(\gcd(M,n)=1) \approx 1$.
      If $\gcd(M,n)=1$, then
      $$Z_1 M \equiv Z_2 M \pmod{n} \Rightarrow Z_1 \equiv Z_2 \pmod{n},$$
      i.e., $M\mathbb{Z}_n^* = \mathbb{Z}_n^*$. In other words, $f(Z) = ZM \bmod n$ is a one-to-one map from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$.
    * ZM randomly chosen from $\mathbb{Z}_n^* \Rightarrow P_A(ZM)$ randomly chosen from $\mathbb{Z}_n^*$:
      $P_A(ZM) = (ZM)^e \bmod n = Z^e M^e \bmod n$.
      If $\gcd(M,n)=1$, then for any $Z_1, Z_2 \in \mathbb{Z}_n^*$,
      $$Z_1^e M^e \equiv Z_2^e M^e \pmod{n} \Rightarrow (Z_1^{-1})^{e-1} Z_1^e M^e (M^{-1})^e \equiv (Z_2^{-1})^{e-1} Z_2^e M^e (M^{-1})^e \pmod{n}$$
      $$\Rightarrow Z_1 \equiv Z_2 \pmod{n}$$