On the divisibility of a random variable*

by

Marcel K. Goh (Montréal, Québec)

11 September 2020

If X is an integer-valued random variable and n is a positive integer, we might want to know the probability that n divides X. To this end, we will make use of the probability generating function

$$p(z) = \sum_{j=0}^{\infty} p_j z^j.$$

We have the following result:

Theorem A. *Let X be a nonnegative integer-valued random variable whose probability generating function $p(z)$ has radius of convergence $R > 1$. Let n be a positive integer and let $\zeta_1, \ldots, \zeta_n$ denote the nth roots of unity. The probability that n divides X is given by two equivalent formulas:*

$$\mathbf{P}\bigl\{X \equiv 0 \pmod{n}\bigr\} = \frac{1}{n}\sum_{k=1}^{n} p(\zeta_k) = \frac{1}{n}\sum_{k=1}^{n} \Re\, p(\zeta_k)$$

Proof. Let $p_j = \mathbf{P}\{X = j\}$ for all positive integers j. We are trying to compute the sum

$$p^* = p_0 + p_n + p_{2n} + \cdots.$$

Consider the generating function

$$f(z) = \biggl(1 + \frac{1}{z^n} + \frac{1}{z^{2n}} + \cdots\biggr) p(z).$$

For any multiple of kn of n, there is some term of the infinite sum that will pull p_{kn} into the constant term of $f(z)$. So it is clear that $[z^0]f(z) = p_0 + p_n + p_{2n} + \cdots = p^*$. We can rewrite $f(z)$ as

$$f(z) = \frac{p(z)}{1 - z^{-n}} = \frac{z^n p(z)}{z^n - 1}.$$

Letting $g(z) = f(z)/z$ and applying Cauchy's Integral Formula, the constant coefficient is given by

$$[z^0]f(z) = [z^{-1}]g(z) = \frac{1}{2\pi i}\oint g(z)\,dz,$$

where the path of integration is taken in the annulus of convergence. The function

$$g(z) = \frac{z^{n-1}p(z)}{z^n - 1}$$

has only n singularities on the unit circle: a pole of order 1 at each of the n roots of unity. So we may take our path of integration to be any positively-oriented loop around the origin that stays outside the closed unit disk and inside the disk $|z| < R$. By the Residue Theorem, this is the sum of the residues at each of the n poles, so we have

$$p^* = \frac{1}{2\pi i}\oint g(z)\,dz = \frac{1}{2\pi i}\cdot 2\pi i\bigl(\operatorname{Res}(g;\zeta_1) + \cdots + \operatorname{Res}(g;\zeta_n)\bigr).$$

* This is a generalisation of an assignment question given by Prof. Luc Devroye in his COMP 690 class, Fall 2020.

We let $g(z) = a(z)/b(z)$, and since $a(z) = z^{n-1}p(z)$ and $b(z) = z^n - 1$ are both holomorphic in neighbourhoods around each of the poles, for any pole ζ_i of g we have

$$\operatorname{Res}(g; \zeta_k) = \frac{a(\zeta_k)}{b'(\zeta_k)} = \frac{{\zeta_k}^{n-1} p(\zeta_k)}{n{\zeta_k}^{n-1}} = \frac{p(\zeta_k)}{n}.$$

Plugging the nth roots of unity into the formula, we have

$$p^* = \sum_{k=1}^{n} \operatorname{Res}(g; \zeta_k) = \sum_{k=1}^{n} \frac{p(\zeta_k)}{n}$$

Note if ζ_k is not real, then $\overline{\zeta_k}$ is also an nth root of unity. Using the identity $\Re z + \Re(\overline{z}) = (z + \overline{z})$, we find that

$$p^* = \frac{1}{n} \sum_{k=1}^{n} p(\zeta_k) = \frac{1}{n} \sum_{k=1}^{n} \Re\, p(\zeta_k),$$

assuring us that p^* is real and proving the theorem statement. ▮