SUMS OF RANDOM INTEGERS REDUCED MODULO m

By A. Dvoretzky and J. Wolfowitz

1. **Introduction.** Let

$$X_1, X_2, \cdots, X_n, \cdots \tag{1}$$

be an infinite sequence of independent random variables which assume *only integral values*. Put

$$S_n = X_1 + \cdots + X_n \qquad (n = 1, 2, \cdots), \tag{2}$$

and let m be any fixed integer greater than 1. Denote S_n reduced mod m by Y_n ; i.e., Y_n is a random variable which assumes only the values 0, 1, $\cdots$, $m - 1$ with the respective probabilities

$$P_n(j) = \text{Prob}\,\{S_n \equiv j \pmod m\} \qquad (j = 0, 1, \cdots, m - 1).$$

It is easily seen that under quite general assumptions Y_n is equidistributed in the limit; i.e.,

$$\lim_{n=\infty} P_n(j) = \frac{1}{m} \qquad (j = 0, 1, \cdots, m - 1). \tag{3}$$

In this paper we obtain necessary and sufficient conditions for the validity of (3) in terms of the distribution functions of (1). We also derive various sufficient conditions for (3), distinguish between essential and accidental equidistribution in the limit, and remark upon the rapidity of approach to equidistribution and some related problems.

The special case $m = 2$ has been considered, in a somewhat different setting, by H. B. Horton [1] who applied his results to obtain a method of generating "random numbers". Our results may also be used for the same purpose, that is, to construct a device for effectuating physically, so to speak, a random variable which assumes all integral values from 0 to $m - 1$ with the same probability $1/m$. Taking large m and employing a suitable transformation, it is possible to obtain a physical device for "generating" a random variable whose cumulative distribution function approximates a given one to any prescribed degree of accuracy.

Since this paper was written there has appeared a paper by Horton and Smith [2] dealing with the same subject. In it the authors, generalizing Horton's previous work [1], obtain sufficient conditions for the validity of (3). These are special cases of sufficient conditions which we deduce from the necessary and sufficient ones.

Received October 5, 1949; in revised form, November 19, 1949.