

# Re: sums of discrete uniform random variables

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-12/msg04722.html>

---

- *From:* Kira Yamato <[kirakun@xxxxxxxxxxxxxx](mailto:kirakun@xxxxxxxxxxxxxx)>
  - *Date:* Mon, 24 Dec 2007 03:23:15 -0500
- 

On 2007-12-24 02:54:50 -0500, quasi <[quasi@xxxxxxxx](mailto:quasi@xxxxxxxx)> said:

On Mon, 24 Dec 2007 02:38:04 -0500, quasi <[quasi@xxxxxxxx](mailto:quasi@xxxxxxxx)> wrote:

On Sun, 23 Dec 2007 23:35:04 -0800 (PST), Butch Malahide <[fred.galvin@xxxxxxxx](mailto:fred.galvin@xxxxxxxx)> wrote:

On Dec 24, 1:08 am, quasi <[qu...@xxxxxxxx](mailto:qu...@xxxxxxxx)> wrote:

Let  $X_1, X_2, X_3, \dots$  be independent, identically distributed random variables, each uniformly distributed on the set  $\{0, \dots, n-1\}$ . In other words, each  $X_i$  is uniformly distributed mod  $n$ .

Prove or disprove:

$(X_1 + \dots + X_k) \bmod m$  is uniformly distributed mod  $m$  iff  $m|n$ .

Do you really need all those assumptions? Wouldn't it be enough to assume that one of the variables, say  $X_1$ , is uniformly distributed mod  $m$ , and the rest are integer-valued variables with arbitrary distributions?

Sure — that's better, provided it's true, and it does seem like it should be true.

Actually, the generalization you suggested makes it easier to see

## Re: sums of discrete uniform random variables

what's going on.

Suppose  $X$  and  $Y$  are independent, integer-valued random variables and such that  $(X \bmod m)$  is uniformly distributed mod  $m$ . Then  $((X + Y) \bmod m)$  must also be uniformly distributed mod  $m$ . The proof is obvious, just by observing that for all  $a, b$  in  $\{0, \dots, m-1\}$ ,

$$P(((X + Y) \bmod m) = a) \mid (Y \bmod m) = b = 1/m$$

regardless of the value of  $b$ .

It follows that, for all  $a$  in  $\{0, \dots, m-1\}$ ,

$$P(((X + Y) \bmod m) = a) = 1/m$$

proving that  $((X + Y) \bmod m)$  is uniformly distributed, mod  $m$ .

I'll have to think about the converse.

Take  $k=1$ . If  $m$  does not divide  $n$ , then  $(X \bmod m)$  won't be uniformly distributed.

--

-kira

.