

Re: SF: Infinity proof

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/1188.html>

From: Proginoskes (proginoskes_at_email.msn.com)

Date: 04/18/05

Date: 17 Apr 2005 23:04:36 -0700

jstevh@msn.com wrote:

> [...]

> *As other posters have also now been talking about how it's*

> *impossible to randomly choose out of infinity.*

That is not what they're (and we're) saying, but rather it's impossible to randomly choose out of a countable infinity UNIFORMLY; i.e., so that any element has just as much of a chance as being picked as any other.

Random just means that it's impossible to know what the result is ahead of time.

(I)

For instance, you can pick a positive integer at random by choosing a real number R in the interval $[0,1]$ uniformly (which *can* be done), and then choosing the integer as follows:

(1) If R is in $(1/2,1]$ or 0, let $N = 1$.

(2) Otherwise, let N be the positive integer such that R is in $(1/2^N, 1/2^{(N-1)}]$.

The value of N is random, because you don't know what N will be ahead of time, but not all positive integers are equally likely to be chosen.

The number 3 is twice as likely to be chosen as 4, for instance.

With this distribution (that's the formal way of saying how likely each outcome is, when choosing at random), the probability of choosing a positive even number is $1/4 + 1/16 + 1/64 + \dots = 1/3$, even though there are just as many positive even integers as positive odd integers.

(II)

The normal way of handling probability concerning positive integers is to choose numbers the following way:

(1) If $N > k$, then the probability of choosing N is zero;

(2) Otherwise, the probability of choosing N is $1/k$.

This gives a probability distribution depending on k , which is uniform on $\{1,2,3,\dots,k\}$. (Each of the outcomes $1, 2, \dots, k$ is equally likely.) Then the probability of a certain property P is calculated and called p_k . Then the limit of p_k is taken.

Calculating probabilities with rational numbers can be handled similarly, once you enumerate (list) them in a particular order.

(III)

Getting back to your "50% claim" ...

The good news is: Yes, there is a probability distribution of the rational numbers where 50% of the time, your method of choosing factors results in a non-trivial rational factor of M . In fact you can increase 50% arbitrarily close to 100% (but never actually attaining 100%).

The bad news is: To find this probability distribution, you probably need to know the prime factors of M ahead of time.

> *The problem is solved with my work by human choice, [...]*

What exactly is "human choice"? If you can't define it, if it can't be formalized, then your paper doesn't belong in a mathematical journal. (Well, a mathematical journal with a good reputation, anyway.)

Does "human choice" involve knowing the factors of M ahead of time? If so, you've just gone in a circle; you need to factor M in order to use SF to factor M .

---- Christopher Heckman