Generating 'random' integers

Martin Griffiths
The University of Manchester, UK
<martin.griffiths@manchester.ac.uk>

One of my undergraduate students recently asked me whether it was possible to generate a random positive integer. After some thought, I realised that there were plenty of interesting mathematical ideas inherent in her question. So much so in fact, that I decided to organise a workshop, open both to undergraduates and postgraduates, in order to explore some of these ideas. This led to many lively discussions regarding the generation of arbitrarily large integers, and we considered both practical and theoretical aspects of this problem.

The purpose of the present article is to discuss and distil the mathematics that came out of just this one short session, and to highlight some of the educational benefits to be gained from running such workshops. It was apparent that the students were genuinely intrigued by the wealth of fascinating material that evolved from such an apparently innocent question. In fact, I have since given an informal talk on this very theme to some that were not involved in the workshop, with the result that several of them wished to follow it up.

The material presented here is aimed at undergraduates and bright students in Years 11 and 12. Although our journey starts with a distinctly statistical flavour, we soon find ourselves venturing into the realms of pure mathematics. Indeed, we will encounter aspects of probability, random variables, analysis, special functions, Fourier series and more. For students or teachers who are unfamiliar with some of the more advanced mathematical ideas discussed here, nothing is essentially lost by skipping the odd paragraph on a first reading. It is hoped, however, that readers will be inspired to undertake further study in these areas.

We also consider the teaching and learning that took place in this workshop within the context of the *Australian Senior Secondary Mathematics Curriculum*, a draft consultation version of which appeared on the website (ACARA, 2010). It was proposed that this curriculum should comprise four courses: Essential Mathematics, General Mathematics, Mathematical Methods and Specialist Mathematics. Each of these course focuses on a pathway meeting the educational needs of some particular group of students.

What do we mean by a "random integer"?

Let us first answer this question somewhat informally with respect to a finite set of integers. If a coin is tossed into the air then, ignoring the possibility for it to land on its edge, the outcome would be either a head or a tail. We might assign the integer 1 to heads and 2 to tails, so that each toss would result in a 1 or a 2. If these outcomes are equally likely then the coin is said to be fair, with each toss resulting in a random integer from the set {1,2}. More generally, when the word "random" is associated with some probabilistic experiment it tends to imply that all of the outcomes are equally likely to occur.

We now apply, via a specific example, a little more formality to the notion of a 'random integer'. On rolling a fair tetrahedral die many times we would expect the proportions of ones, twos, threes and fours that occur each to tend to $\frac{1}{4}$ as $n \to \infty$. This may be expressed as follows. With n_k denoting the number of times a k has occurred after n rolls of the die, we would expect that

$$\lim_{n\to\infty} \frac{n_k}{n} = \frac{1}{4} \tag{1}$$

for $k = 1,2,3,4$. This is known as the *law of averages*, and is certainly not trivial to prove (see Grimmett & Stirzaker, 2001, p. 31). To be a little more rigorous, we might say that $\frac{n_k}{n}$ converges to $\frac{1}{4}$ as $n \to \infty$ in the sense that, for any $\varepsilon > 0$,

$$P\left(\frac{1}{4} - \varepsilon \le \frac{n_k}{n} \le \frac{1}{4} + \varepsilon\right) \to 1 \text{ as } n \to \infty \tag{2}$$

Let us try to unravel what the above mathematical statement is actually saying. First, it is worth pointing out what (2) is *not* saying. It does not imply, for example, that for every possible sequence comprising ones, twos, threes and fours the proportion of ones tends to $\frac{1}{4}$ as $n \to \infty$. Take the sequence 1, 1, 1, 1, 1, … for example! However, (2) does tell us that for any fixed number $\varepsilon > 0$, however close to 0 it is, if we roll the dice for long enough then we can ensure that the probability of $\frac{n_k}{n}$ being within ε of $\frac{1}{4}$ is as close to 1 as we like. Incidentally, the underlying probability distribution here is known as *discrete uniform*.

At this point it is worth mentioning a common misconception amongst undergraduate students with regard to this limiting process. Some believe that as n increases then each of n_1, n_2, n_3 and n_4 should get closer and closer together. This, however, is not the case. It is certainly possible for each of these frequencies to get further apart as n increases, while still satisfying (1). Probability is to be studied in the Essential Mathematics course (ACARA, 2010), and students are expected to appreciate the notion of relative frequency, perform simulations and even apply probability to simple queuing problems. Furthermore, both discrete and continuous random variables appear in Mathematical Methods.

For the probabilistic experiments discussed above there were only a finite number of possible outcomes. What happens when we try to extend this idea of 'equally likely events' to situations whereby there are an infinite (albeit countable) number of possible outcomes? Suppose that N is a discrete random variable with the property that $P(N = n) > 0$ for each positive integer

n. It is clear that, in order for the sum

$$\sum_{n=1}^{\infty} \mathrm{P}(N = n)$$

to converge, we must have $\mathrm{P}(N = n) \to 0$ as $n \to \infty$. Thus, there exists no $c > 0$ such that $\mathrm{P}(N = n) = c$ for each n. In other words, we cannot construct a mass function for N such that each positive integer is equally likely to occur. Therefore, in answer to my student's question, it would appear that it is not possible to generate a random integer. So we can all pack up and go home? Not likely! The answer raises yet more questions; ones that may be used as a springboard for the exploration of some fascinating areas of mathematics.

Generating positive integers

A well-known example of a distribution taking non-zero probabilities on all of the positive integers is the geometric distribution. If, for example, we define X to be the number of rolls of our tetrahedral die required to obtain the first appearance of a 3, then

$$X \sim \mathrm{Geo}\left(\tfrac{1}{4}\right)$$

The mass function of X is given by

$$\mathrm{P}(X = n) = \frac{1}{4}\left(\frac{3}{4}\right)^{n-1}$$

This is because, in order for the first appearance of a 3 to occur on the nth roll, it must have been the case that each of the first $n - 1$ rolls resulted in numbers other than 3. Then, assuming that the outcomes on each roll were independent, the formula for $\mathrm{P}(X = n)$ follows. In connection with this, geometric series are covered in both the General and the Specialist Mathematics courses (ACARA, 2010).

The process of rolling the die until a 3 appears could in theory be used to generate a positive integer, although we would need to be prepared to wait a very long time! Given any period of time, say 10 years for sake of argument, there is a chance, however small that chance might be, that we will not have rolled a 3 by the end of that time period, even if we rolled the die every waking moment. Of course, further practical constraints come into play here. If we did ever have to roll the die for such a lengthy period, it would have become extremely worn and might no longer be fair.

How about getting a computer to simulate this experiment? Setting up such a simulation would certainly be very straightforward. However, even though the computer can 'roll' the die many thousands of times faster than we can, there is still no guarantee that a 3 will have appeared within 10 years (or within any other time period for that matter). This brings us onto one further point; computers possess *pseudo-random number generators*. These are algorithms for obtaining sequences of numbers that pass at least some of the established statistical tests for randomness. Students might be interested in finding out about such tests. Indeed, they could go on to consider whether or not numbers generated by a computer may ever be regarded as truly random;

this could have implications for the simulations. It is worth visiting the Wikipedia website (2010b) in this regard.

Another way to generate positive integers is by way of the random variable U, possessing the *continuous uniform* distribution with probability density function $f(u)$ defined by

$$f(u) = \begin{cases} 1 & 0 < u \leq 1 \\ 0 & \text{otherwise} \end{cases}$$

We then set $M = \left\lfloor \frac{1}{U} \right\rfloor$, where $\lfloor x \rfloor$ denotes the *floor function*, giving the largest integer less than or equal to x (thus, for example $\lfloor x \rfloor = 3$ and $\lfloor 7 \rfloor = 7$). From this the mass function of M may be obtained as

$$\mathrm{P}(M = m) = \frac{1}{m} - \frac{1}{m+1} = \frac{1}{m(m+1)}$$

This of course presupposes that our random number generator is able to provide us with numbers in the interval (0,1) to an arbitrary degree of accuracy. Thus, with regard to generating integers, it would appear that the issue is not now one of time, but of accuracy. For example, in order to generate the number 1 000 000, $\frac{1}{U}$ would have to be between 1 000 000 and 1 000 001. This requires U to be specified to at least seven places of decimals, which of course poses no problems whatsoever. However, to cater for the possibility of generating much larger integers, far greater levels of accuracy are required. We can write programmes to generate numbers in (0,1) to ever-greater levels of accuracy, but this will be at the expense of time; it seems we are back to square one!

Making some comparisons

Returning to theoretical considerations, we might next dream up ways of comparing how well two particular random variables, N_1 and N_2 say, are able to 'approximate' or 'mimic' the behaviour of some aspect of a uniform distribution on $\{1,2,\ldots,n\}$ as n increases without limit. To this end, suppose that D_m is a discrete uniform random variable on the first m positive integers, so that its mass function is given by $\mathrm{P}(D_m = d) = \frac{1}{m}$ for d = 1,2,…,m, and $\mathrm{P}(D_m = d) = 0$ otherwise. Note, for example, that one particular property of D_m is that $\mathrm{P}(D_m \text{ is a square}) \to 0$ as $m \to \infty$. On the basis of this, the calculation of $\mathrm{P}(N_1 \text{ is a square})$ and $\mathrm{P}(N_2 \text{ is a square})$ might, in some sense at least, allow us to make comparisons with regard to how 'uniform' these distributions are. Let us follow this line of enquiry for the moment.

From our previous definition of M, the probability that it is a square is given by

$$\mathrm{P}(M \text{ is a square}) = \sum_{m=1}^{\infty} \frac{1}{m^2(m^2+1)} = \sum_{m=1}^{\infty} \frac{1}{m^2} - \sum_{m=1}^{\infty} \frac{1}{m^2+1} \qquad (3)$$

At this point we may choose to adopt either a numerical or a theoretical approach to calculating this probability. The former might allow students to exercise their programming skills or to develop ingenious methods of approximation, while the latter would give them the opportunity to explore

more advanced mathematical territory. We pursue here the analytic route; some may wish to skip the following paragraph on a first reading and then come back to it after having done a little research in this area.

It is well-known that the first sum on the right of (3) is equal to $\frac{\pi^2}{6}$. For a proof of this see Apostol (1976, p. 266) or visit Chapman's website (2009), where no less than fourteen of proofs of this result are to be found. Let us therefore concentrate on the second sum. It is possible to obtain the following *Fourier series* for $\cos \alpha x$:

$$\cos \alpha x = \frac{\sin \alpha\pi}{\alpha\pi} + \frac{2\alpha \sin \alpha\pi}{\pi} \sum_{m=1}^{\infty} \frac{(-1)^m \cos mx}{\alpha^2 - m^2}$$

For those not familiar with such series, they allow us to decompose any periodic function into an infinite sum of sines and cosines, and are utilised in areas of applied mathematics and physics such as signal processing and acoustics. Students might like to explore the Wikipedia website (2010a) to found out more about the mathematical properties and applications of Fourier series. This would allow them to see the trigonometric functions encountered in Mathematical Methods (ACARA, 2010) in a rather more challenging setting. On putting $\alpha = i$ and $x = \pi$ we have

$$\cos i\pi = \frac{\sin i\pi}{i\pi} + \frac{2i \sin i\pi}{\pi} \sum_{m=1}^{\infty} \frac{1}{-1 - m^2}$$

which rearranges to give

$$\sum_{m=1}^{\infty} \frac{1}{m^2 + 1} = \tfrac{1}{2}(\pi \coth \pi - 1)$$

On combining the above results it follows that

$$\mathrm{P}(M \text{ is a square}) = \frac{1}{6}\left(\pi^2 - 3\pi \coth \pi + 3\right) \approx 0.568$$

As an alternative to this, we could agree to disregard the first k positive integers in order to diminish the effect of the initial high concentration of squares amongst the integers. Use can then be made of the continuous uniform random variable V with probability density function given by

$$f(v) = \begin{cases} \dfrac{1}{a} & 0 < v \leq a \\ 0 & \text{otherwise} \end{cases}$$

where

$$a = 1 - \sum_{m=1}^{k} \frac{1}{m(m+1)}$$

On redefining M as $\left\lfloor \frac{1}{V} \right\rfloor$ we would then have

$$\mathrm{P}(M \text{ is a square}) = \frac{1}{a} \sum_{k=\lceil \sqrt{k+1} \rceil}^{\infty} \frac{1}{m^2(m^2+1)}$$

where $\lceil x \rceil$ is the *ceiling function*, giving the smallest integer greater or equal to x. Numerical calculations give, for example, $\mathrm{P}(X \text{ is a square}) \approx 0.079$ when $k = 10$.

Let us next consider a general geometric random variable X ~ Geo(p). To this end,

$$\mathrm{P}(X \text{ is a square}) = \sum_{n=1}^{\infty} p(1-p)^{n^2-1} = \frac{p}{2(1-p)}\left\{\theta(1-p)-1\right\}$$

where $\theta(x)$ is the *theta function* given by

$$\theta(x) = 1 + 2\sum_{n=1}^{\infty} x^{n^2}$$

It can be shown that $\mathrm{P}(X \text{ is a square}) \to 1$ as $p \to 1$ and $\mathrm{P}(X \text{ is a square}) \to 0$ as $p \to 0$, which is as we would expect intuitively. The theta function can be implemented using Mathematica, a sophisticated piece of software published by Wolfram (2007). For example $\mathrm{P}(X \text{ is a square}) \approx 0.384$ when $p = \frac{1}{4}$ while $\mathrm{P}(X \text{ is a square}) \approx 0.762$ when $p = \frac{3}{4}$. It should be noted that $\theta(x)$ is related to elliptic functions, and, as a consequence, is associated with some rather advanced mathematics; see, for example, Hardy and Wright (2008) or Rose (1994). It is fascinating how our simple initial question has led on to functions that were studied by some of the greatest mathematicians of the nineteenth and twentieth centuries.

This investigation also gives students the chance to encounter the 'innocent-looking' (more on this shortly) random variable Y defined, for $y = 1,2,3,\ldots$, via the mass function

$$\mathrm{P}(Y = y) = \frac{6}{\pi^2 y^2} \tag{4}$$

noting that our earlier observation

$$\sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6}$$

does indeed imply that (4) is a genuine mass function. We have

$$\mathrm{P}(Y \text{ is a square}) = \frac{6}{\pi^2}\sum_{y=1}^{\infty} \frac{1}{\left(y^2\right)^2} = \frac{6}{\pi^2}\sum_{y=1}^{\infty} \frac{1}{y^4}$$

Since, from Apostol (1976, p. 266) once more,

$$\sum_{y=1}^{\infty} \frac{1}{y^4} = \frac{\pi^4}{90}$$

it is the case that

$$\mathrm{P}(Y \text{ is a square}) = \frac{\pi^2}{15} \approx 0.658$$

From the foregoing discussion, it would seem that, provided the value of its parameter p is small, a geometric distribution fares rather well compared to the other distributions. Of course, some might argue that the method of comparison we have been using thus far is rather arbitrary. Furthermore, it would be very easy to 'manufacture' a mass function for N looking distinctly non-uniform yet for which $\mathrm{P}(N \text{ is a square})$ is as close to 0 as we like. Are we thus able to identify a less arbitrary aspect of the behaviour of D_m as $m \to \infty$? A fairly obvious candidate would be the fact that $\mathrm{E}(D_m)$, the expectation of D_m, tends to infinity as $m \to \infty$, but surely there cannot be a mass function with the ability to mimic this property? Oh yes there can! Let us return, as promised,

to the innocent-looking random variable Y. The interesting thing here is that

$$\mathrm{E}(Y) = \frac{6}{\pi^2} \sum_{y=1}^{\infty} \frac{y}{y^2} = \frac{6}{\pi^2} \sum_{y=1}^{\infty} \frac{1}{y}$$

which shows, by virtue of the fact that the series on the right diverges, that $\mathrm{E}(Y)$ does not have a finite mean. Incidentally, there are several ways of showing that the series

$$\sum_{y=1}^{\infty} \frac{1}{y}$$

diverges, none of which would be beyond able students from Years 11 or 12; see Knuth (1968, p. 74), for example.

This fact that Y does not possess a finite mean might initially seem somewhat counterintuitive, and certainly makes an interesting point for discussion. One way of looking at this is as follows. Suppose that we had a way of generating integers by way of this distribution, and a sample of size n was obtained. Let $\bar{Y}(n)$ denote the mean of this sample. Then, for any positive integer N you care to choose, $\mathrm{P}(\bar{Y}(n) > N) \to 1$ as $n \to \infty$. This of course raises some interesting questions: How may we generate integers via this probability distribution? Is it indeed possible?

Let us now compare the random variables X and Y in this respect. Although X has the property that $\mathrm{E}(X) \to \infty$ as $p \to \infty$, it is the case that $\mathrm{E}(X)$ is finite for any particular value of p. In this sense at least, Y might be regarded as being far more successful at copying the limiting behaviour of $\mathrm{E}(D_m)$.

Running the workshop

This was a voluntary session, and took place one afternoon. Twenty-two students attended—an ideal number for this sort of activity. My aims were for each member of the class to have the opportunity to:

- work collaboratively;
- make decisions about how they might proceed;
- venture into areas of mathematics with which they were unfamiliar;
- carry out some independent exploration and research.

In order to facilitate the above, the students worked in groups initially, with each group possessing both undergraduates and undergraduates.

After a brief introduction outlining some of the ideas discussed in the second section of this article, the students were given the freedom to proceed in any manner they saw fit. From this point I acted as more of a guide than a teacher, steering groups or individuals back to more fruitful lines of enquiry if it was evident that their current train of thought was not leading anywhere, or making suggestions if they had reached an apparent impasse, but trying to keep out of the way as much as possible. I also ensured that computers with mathematical software and internet access were available.

If I felt that a group had a particularly promising idea then I would ask them to share their findings with the rest of the class. In order to avoid continually disrupting the flow of the session, however, I would sometimes rather ask

an individual to circulate amongst the other groups to explain their current line of enquiry. We concluded the workshop with a plenary activity, pulling together, and trying to make some sort of sense of, the wealth of mathematical ideas that were generated. At one point this even turned into a healthy debate, with some contesting an assertion posited by one of the groups.

Final thoughts

The distilled version of what went on in the workshop described in this article was of course just one of a plethora of ways in which the session might have proceeded. However, I have found that, whatever the outcome, running workshops such as these can have numerous educational benefits. Mathematical exploration is encouraged, which in turn aids the development of technique, problem-solving ability and knowledge. A setting is created within which productive mathematical discussion and collaboration is able to take place; possibly in the form of peer teaching both within and between the groups. In addition, since practical, theoretical and computational work arises in such a natural manner from this activity, there is scope for students to encounter a wide variety of learning experiences. Indeed, the theme of mathematical investigation pervades much of the Essential Mathematics course (ACARA, 2010).

Furthermore, the workshop allows students to consider, a little more deeply, the mathematics associated with various distributions they may already be familiar with. Ambitious students might next like to look at other distributions in the light of the ideas discussed here. A comprehensive list of both discrete and continuous distributions can be found in (Grimmett & Stirzaker, 2001).

In the Secondary National Strategy (2007) guidance document for schools in the United Kingdom, a *rich task* is described as one that:

- is accessible and extendable;
- allows learners to make decisions;
- involves learners in testing, proving, explaining, reflecting and interpreting;
- promotes discussion and communications;
- encourages originality and invention;
- encourages 'what if' questions;
- is enjoyable and contains the opportunity for surprise.

It would certainly seem that our workshop activity satisfies these criteria to a large extent. Indeed, there is no reason whatsoever why such tasks should not also be part of a university curriculum. They provide alternative modes of learning to those experienced in lectures or even tutorials. In the workshop environment, the freedom to explore means that a student's learning experience tends to be rather more holistic than in the more traditional settings. Furthermore, mathematical discovery is initiated by the students; something that simply cannot be replicated in a lecture theatre.

If the reader is interested in running their own workshops then see also

(Griffiths, 2009; 2010a; 2010b). The ideas presented in these papers certainly have the potential to be developed into rich tasks for undergraduate students.

References

Apsostol, T. M. (1976). *Introduction to analytic number theory*. New York, NY: Springer.

Australian Curriculum, Assessment and Reporting Authority. (ACARA). (2010). *Developing the Australian Curriculum*. Retrieved 30 November 2010 from http://www.australiancurriculum.edu.au

Chapman, R. (2003). *Evaluating* $\zeta(2)$. Retrieved 10 December 2010 from http://www.secam-local.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf

Griffiths, M. (2009). The immortal ant and the expanding balloon. *Teaching Mathematics and its Applications, 28*(3), 150–158.

Griffiths, M. (2010a). Maximizing a probability: A student workshop on an application of continuous distributions. *Journal of Statistics Education, 18*(2), 1–17.

Griffiths, M. (2010b). Thematic mathematics: the combinatorics of prime factorisations. *Teaching Mathematics and its Applications, 29*(1), 25–40.

Grimmett, G., & Stirzaker, D. (2001). *Probability and random processes*. Oxford, UK: Oxford University Press.

Hardy, G. H., & Wright, E. M. (2008). *An introduction to the theory of numbers* (6th ed.). Oxford, UK: Oxford University Press.

Knuth, D. (1968). *The art of computer programming* (Vol. 1). Reading, MA: Addison-Wesley.

National Centre for Excellence in the Teaching of Mathematics. (2007). *Rich tasks*. Retrieved 7 December 2010 from http://www.ncetm.org.uk/mathemapedia/Rich+Tasks

Rose, H. E. (1994). *A course in number theory* (2nd ed.). Oxford, UK: Oxford University Press.

Secondary National Strategy. (2007). *Mathematics at Key Stage 4: Developing your scheme of work*. Reading, UK: DfES.

Wikipedia contributors. (2010a). *Fourier series: Wikipedia, The Free Encyclopedia*. Retrieved 12 November 2010 from http://en.wikipedia.org/wiki/Fourier_series

Wikipedia contributors. (2010b). *Pseudorandom number generator: Wikipedia, The Free Encyclopedia*. Retrieved 8 November 2010 from http://en.wikipedia.org/wiki/Pseudorandom_number_generator

Wolfram Research Team. (2007). *Mathematica 6*. Champaign, IL: Wolfram.