Random Number Generators

Ishaan Patkar (working with Tong Miao)

What does it mean to be random?

"Random" is an overused word. In everyday use, "random" most often means "arbitrary," for instance: "pick a random number" usually means "pick an arbitrary number." When it is not used in this sense, the word is instead used to express uncertainty in the outcome of an event; for instance: "that game involves randomness." For a word that is used as commonly as "randomness" is, oddly, there is little understanding of what it means.

On the surface, randomness does not seem to be particularly very important. For a long time, its only purpose for humanity was to entertain in the form of games. But the beginning of the study of probability in mathematics in the 19th century brought a new use of the word random: "randomly choosing a marble from a bag." It is in this probabilistic sense of the word that randomness has its most important use.

Mathematics — and science to a certain extent — has thus given randomness a new meaning, but neither mathematicians, nor scientists, have been able to come up with a satisfactory definition of what randomness means. Adding to the controversy is quantum physics, which claims that the universe is fundamentally random. But we cannot go on with a discussion of randomness without some understanding of what random means, so a definition will be presented, though it may not by satisfactory enough for higher mathematics. Statisticians have debated over the properties that a sequence of random numbers have, but have not been able to come up with a good definition. Thus, we take a different approach here:

Definition. A *random event* is an event which has more than one possible outcome, and the probabilities of each outcome are fixed.

In other words, the probability of each outcome of a random event, no matter how many times it occurs, is always the same. Note also that a random event must have more than one outcome. If an event has exactly one possible outcome, we call it a *deterministic* event.

Definition. A *deterministic event* is an event what has exactly one outcome.

In other words, a deterministic event is, well, determined — there is exactly one outcome. Like randomness, determinism shows up in many unexpected places. For instance, classical pre-quantum physicists believed that there existed a certain set of rules under which the universe moved from state to state; that is, they believed the universe was deterministic, and science was the way to understand how the universe operated. This belief was one of the reasons why quantum physics was difficult to accept — in the words of Albert Einstein, ”God does not play dice with the universe.”

Another really important place where determinism shows up is computers (and, by extension, the human brain). A computer must be totally and completely predictable or else it is broken. Thus, a computer is deterministic by definition.

This, in fact, proves that computers cannot generate true randomness by themselves because an event cannot be both deterministic and random, and every event run on a computer must be deterministic. This is why all random number generators (RNGs) for computers are actually *pseudorandom* number generators (PRNGs). There are true random number generators available for computers, such as the service offered by random.org or by fourmilab.ch/hotbits, but all such RNGs use external sources of randomness.

But why would we want randomness on a computer? Well, the advent of both computers and the study of randomness have created some uses for it. The following is a list of some of these uses:

Simulation. Randomness is necessary to simulate any event that uses any degree of randomness.

Statistical Sampling. Related to simulation, but not quite the same is the use of randomness in statistical sampling. Statistics shows that a random sample of a data set can act as a representative of the set, and so a source of randomness can aid in data analysis.

Cryptography Modern cryptography relies on a scheme called asymmetric encryption, which is a type of cipher which uses two keys: a public key, and a private key. The public key is used to encrypt messages, which only the private key can decode. This allows the private key to be kept secret, whereas the public key can be distributed freely. However, an important part of the generation of these ciphers is factoring large numbers which must be chosen as randomly as possible to provide the most security.

Computer Programming Algorithms that incorporate some randomness are often faster than their deterministic counterparts. For instance, the most common algorithm that checks if a number is prime, the Miller-Rabin Test, incorporates randomness and is faster than its deterministic counterpart.

Calculation Many expressions are difficult to calculate even for a computer. Techniques like the Monte Carlo Method can be used to approximate these numbers using a source of randomness. For instance, given a random sequence of numbers in $[0, 1)$, we can approximate π by plotting each pair onto the unit square. The probability that a point will be in the quarter circle is $\frac{\pi}{4}$ by geometric probability. So, counting the number of points within radius 1 of the origin, and dividing that by the total number of points should give us an approximation of $\frac{\pi}{4}$. (This technique can also be used as an intuitive statistic to judging how random a sequence is.)

Recreation One important use of randomness on computers is in the form of games, which have always used some degree of randomness to be unpredictable, and therefore fun.

Games on computers naturally use randomness in a similar way. Likewise, procedural generation also uses randomness to create unpredictable results.

Random Numbers

Numbers are the obvious choice for generating randomness on computers, since computers fundamentally deal with numbers. But what does a "random number" mean? Once again, we are faced with the vague definition of the concept of randomness. However, extending the above definition to numbers, we have the following definition:

Definition. A *random number* is a number which is chosen by a random event.

So, for instance, a random number might be chosen such that $\mathrm{P}(0) = \frac{1}{2}$ and $\mathrm{P}(1) = \frac{1}{2}$. We might interpret flipping a coin as a series of random numbers in this sense. Now, obviously, a random number by itself is not very useful. A sequence of random numbers is more useful, and, just for clarity:

Definition. A *sequence of random numbers* is a sequence of numbers, each of which were chosen by the same random event.

However, it is not very practical to write a new random number generator for every random event. Therefore:

Theorem. *Let E be an event with a finite number of outcomes $O_1, O_2, \ldots, O_n$, and let $P(O_i)$ be the probability that O_i is occurring, with $P(O_i)$ being rational. Then, there exists some integer q such that for every O_i k such that $P(O_i) = \frac{k}{q}$ for some integer k.*

Proof. This is a fairly simple theorem to prove, and we can construct a q and a k for all i. Suppose $\mathrm{P}(O_i) = \frac{a_i}{b_i}$ where a_i and b_i are integers. Then let $m = \mathrm{lcm}(b_1, b_2, b_3, \ldots, b_n)$. We then have:

$$\mathrm{P}(O_i) = \frac{a_i \frac{m}{b_i}}{m}.$$

Since $b_i \,|\, m$, $a_i \frac{m}{b_i}$ is an integer, so we are done. □

This theorem thus suggests that we have every random number be uniformly distributed. That is, the probability of each number being selected should be equal. Do note, however, that we can technically use any event E_n with n outcomes, since we can construct the uniform distribution out of E_n and then use that to construct any event. However, the uniform distribution is also the most conventient here. Thus, unless otherwise specified, we will assume that we will generate random numbers, and sequences of random numbers, from the uniform distribution.

Generating Random Numbers: The Linear Congruential Generator

In this paper, we will focus mostly on the Linear Congruential Method (LCM) of generating random numbers on computers. (Do note that most of what is shown here was first shown in *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* by Donald Knuth, which is recommended to the reader for further reading).

Before we begin, we will first assume that the reader is familiar with basic number theory and modular arithmetic. Furthermore, we will use the notation $a \equiv b \pmod{m}$ to denote modular equivalence, whereas $a \bmod m$, without parenthesis, will refer to the operation of taking the remainder when a is divided by m. Formally:

Definition. Let $r = a \bmod m$ if $a \equiv r \pmod{m}$ and $0 \leq r < m$.

Note that it follows that $a \bmod m = b \bmod m \iff a \equiv b \pmod{m}$, meaning that this operation is more or less identical to modular congruence.

Now, the Linear Congruential Generator (LCG) is actually very simple. We define a Linear Congruential Sequence (LCS) to be the sequence generated by the list (x_0, a, c, m) where m is the modulus, $0 \leq x_0 < m$ is the seed, $0 \leq a < m$ is the multiplier, and $0 \leq c < m$ is the increment. We can then generate the LCS $(x_0, x_1, x_2, \ldots)$ by following this simple recursion:

$$x_n = (ax_{n-1} + c) \bmod m\,. \tag{1}$$

Now, the first natural step would be to find a closed form for x_n. We will use the notation sequence (x_0, a, c, m) to refer to the LCS defined with seed x_0, multiplier a, increment c, and modulus m.

Theorem 1. *If x_n and x_k are the nth and kth terms of the LCS (x_0, a, c, m), respectively, then:*

$$x_n = \left(a^{n-k}x_k + \frac{a^{n-k}-1}{a-1}c\right) \bmod m\,. \tag{2}$$

(Here, if $e < 0$, then $b^e = (b^{-1})^{-e}$, where b^{-1} is the multiplicative modular inverse of $b \bmod m$.

Proof. Choose some k. We will prove this by induction over n.

Base case, $n = k$. Then:

$$\left(a^{n-k}x_k + \frac{a^{n-k}-1}{a-1}c\right) \bmod m = \left(a^0 x_k + \frac{a^0-1}{a-1}c\right) \bmod m = (x_k) \bmod m = x_k$$

Suppose now that Equation 2 holds for $n = i$. We will then prove that it holds for $n = i+1$. Since $x_{i+1} = (ax_i + c) \bmod m$, we have $x_{i+1} \equiv ax_i + c \pmod{m}$, and $0 \leq x_{i+1} < m$. Likewise, since $x_i = \left(a^{i-k}x_k + \frac{a^{i-k}-1}{a-1}c\right) \bmod m$, $x_i \equiv a^{i-k}x_k + \frac{a^{i-k}-1}{a-1}c \pmod{m}$ and $0 \leq x_i < m$. Therefore:

$$\begin{aligned}
x_{i+1} &\equiv ax_i + c \pmod{m} \\
&\equiv a\left(a^{i-k}x_k + \frac{a^{i-k}-1}{a-1}c\right) + c \pmod{m} \\
&\equiv a^{i-k+1}x_k + \frac{a^{i-k+1}-a}{a-1}c + c \pmod{m} \\
&\equiv a^{i-k+1}x_k + \frac{a^{i-k+1}-a+a-1}{a-1}c \pmod{m} \\
&\equiv a^{i-k+1}x_k + \frac{a^{i-k+1}-1}{a-1}c \pmod{m}.
\end{aligned}$$

Since $0 \leq x_{i+1} < m$, $x_{i+1} = \left(a^{i-k+1}x_k + \frac{a^{i-k+1}-1}{a-1}c\right) \bmod m$. This completes our induction. □

From this theorem, a simple closed form follows:

$$x_n = \left(a^n x_0 + \frac{a^n - 1}{a - 1}c\right) \bmod m\,. \tag{3}$$

Now, the first question that comes to mind when analyzing an LCS is how many numbers will it produce? And are these numbers in a uniform distribution? It turns out that every LCS is actually periodic. Take the first $m+1$ terms of an LCS with modulus m: $(x_0, x_1, x_2, \ldots, x_m)$. There are m possible values for each x_k, which means that by the Pigeonhole Principle, there exists some x_i and x_j such that $x_i = x_j$. Then we have $x_{i+1} = x_{j+1}, x_{i+2} = x_{j+2}, \ldots$, or in general, $x_{i+k} = x_{j+k}$ for every k. Note that it is not necessary that x_0 be repeated, for instance:

$$(1, 8, 3, 8, 3, \ldots)$$

is the LCS given by $(1, 5, 8, 10)$, and x_0 does not repeat.

In fact, some variation on this argument can show that most random number generators have a period. But what does the period do to a sequence of random numbers? Suppose we have a sequence of integers in (not necessarily an LCS) $(x_1, x_2, x_3, \ldots)$ where $\lambda + k$ is the minimum number such that $x_{\lambda+k} = x_k$. Then we have $x_i = x_{i+\lambda}$ for all $i \geq k$. If we use numbers past $x_{\lambda+k}$, we will begin to repeat numbers that are already used, and in the same order, meaning that the numbers are easily predictable, and so not random enough. In addition, note that since $x_{\lambda+k}$ is the smallest number the repeats, $(x_1, x_2, \ldots, x_{\lambda+k-1})$ is a sequence of distinct numbers.

Suppose that the generator for this sequence can potentially produce integers in the range $[0, m)$. Then, as $\lambda + k$ approaches m, the sequence approaches a uniform distribution, and the number of useable integers increases. This means that to create the best generator, we want the larges $\lambda + k$.

This idea also applies to the LCG. There exists a generator (x_0, a, c, m) with period m for every m: the generator $(0, 1, 1, m)$ which produces the sequence $(0, 1, 2, \ldots)$. However, this is a very predictable sequence, and so not very random. It would be better if we knew exactly which choices of (x_0, a, c, m) produces m distinct integers.

Notice also that in this example, $k = 0$. Is this necessary for the LCG to produce m distinct integers?

Theorem. *If (x_0, a, c, m) is a LCS with period λ, and a is relatively prime to m, then $x_0 = x_\lambda$.*

Proof. Suppose $k + \lambda$ is the least integer such that $x_{k+\lambda} = x_k$, for some k. Then, by Equation

3 we have:

$$\begin{aligned}
x_{k+\lambda} &= x_k \\
\left(a^{k+\lambda}x_0 + \frac{a^{k+\lambda}-1}{a-1}c\right) \bmod m &= \left(a^k x_0 + \frac{a^k-1}{a-1}c\right) \bmod m \\
a^{k+\lambda}x_0 + \frac{a^{k+\lambda}-1}{a-1}c &\equiv a^k x_0 + \frac{a^k-1}{a-1}c \pmod m \\
(a^{k+\lambda}-a^k)x_0 + \frac{(a^{k+\lambda}-1)-(a^k-1)}{a-1}c &\equiv 0 \pmod m \\
a^k(a^\lambda-1)x_0 + \frac{a^k(a^\lambda-1)}{a-1}c &\equiv 0 \pmod m \\
a^k\left((a^\lambda-1)x_0 + \frac{a^\lambda-1}{a-1}c\right) &\equiv 0 \pmod m.
\end{aligned}$$

Since a and m are relatively prime, there exists a multiplicative inverse of a modulo m. Therefore:

$$\begin{aligned}
(a^\lambda-1)x_0 + \frac{a^\lambda-1}{a-1}c &\equiv 0 \pmod m \\
a^\lambda x_0 + \frac{a^\lambda-1}{a-1}c &\equiv x_0 \pmod m \\
\left(a^\lambda x_0 + \frac{a^\lambda-1}{a-1}c\right) \bmod m &= x_0 \\
x_\lambda &= x_0.
\end{aligned}$$

Therefore, x_0 repeats itself, and so $k = 0$. □

Now, notice that if $k \neq 0$, then $\gcd(a, m) = r > 1$. This means that, for $n > 0$:

$$\begin{aligned}
x_n &= \left(a^n x_0 + \frac{a^n-1}{a-1}c\right) \bmod m \\
x_n &\equiv a^n x_0 + \frac{a^n-1}{a-1}c \bmod m \\
x_n &= a^n x_0 + \frac{a^n-1}{a-1}c + qm,
\end{aligned}$$

for some integer q. Thus:

$$\begin{aligned}
x_n &= a^n x_0 + \frac{a^n-1}{a-1}c + qm \\
&= a^n x_0 + \frac{(a^n-a)+(a-1)}{a-1}c + qm \\
&= a^n x_0 + \frac{a^n-a}{a-1}c + c + qm \\
x_n - c &= a^n x_0 + a\frac{a^{n-1}-1}{a-1}c + qm.
\end{aligned}$$

Note that since $n > 1$, $a-1 \mid a^{n-1}-1$. Therefore, we have $r = \gcd(a,m) \mid a^n x_0 + a\frac{a^{n-1}-1}{a-1}c + qm = x_n - c$. Thus, $x_n \equiv c \pmod{r}$, meaning that $x_n = pr + c$ for some p. Since $0 \leq x_n < m$, the possible values for x_n are then $\{c, r+c, 2r+c, \ldots, (\frac{m}{r}-1)r+c\}$. Therefore, if an LCG produces all m possible integers, we must have $k = 0$ and so the period must be m.

The logical question is, what are the (x_0, a, c, m) such that the period length will be m? To begin investigating this question, we need a few important results.

Theorem 2 (Fermat's Little Theorem)**.** *If p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let $S = \{a \bmod m\,, (2a) \bmod m\,, \ldots, ((p-1)a) \bmod m\,\}$ and let $T = \{1, 2, 3, \ldots, p-1\}$. We will prove that $S = T$. Since a is not a multiple of p, $ka \not\equiv 0 \pmod{p}$ for all $1 \leq k \leq p-1$, since p is prime. Therefore, $(ka) \bmod p \neq 0$ meaning that $(ka) \bmod p \in T$. So $S \subseteq T$.

Now, we will show that there exists some i for every j such that $(ia) \bmod p = j$. Since a is relatively prime to p, there exists a multiplicative inverse of a, a^{-1}, so $j \equiv (ja^{-1})a \pmod{p}$. Therefore, $j = ((ja^{-1})a) \bmod p$, meaning that $T \subseteq S$. Thus, $S = T$.

Therefore, we have $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$. So, $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Since $p \nmid (p-1)!$ and as p is prime, $(p-1)!$ is relatively prime to p, meaning that $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem 3. *Let p be a prime and n a positive integer such that if $p = 2$, then $n > 1$. Then if $a \equiv 1 \pmod{p^n}$ and $a \not\equiv 1 \pmod{p^{n+1}}$ then $a^p \equiv 1 \pmod{p^{n+1}}$ and $a \not\equiv 1 \pmod{p^{n+2}}$.*

Proof. Since $a \equiv 1 \pmod{p^n}$, we have $a = 1 + kp^n$ for some integer k. We have $a \not\equiv 1 \pmod{p^{n+1}}$, so $p \nmid k$. Therefore:

$$\begin{aligned}
a^p &= (1+kp^n)^p \pmod{p} \\
&= 1 + \binom{p}{1}kp^n + \binom{p}{2}k^2p^{2n} + \cdots + \binom{p}{p-1}k^{p-1}p^{(p-1)n} + \binom{p}{p}k^p p^{pn} \\
&= 1 + \sum_{i=1}^{p-1}\binom{p}{i}k^i p^{in} + k^p p^{pn} \\
&= 1 + p^{n+1}\sum_{i=1}^{p-1}\frac{\binom{p}{i}}{p}k^i p^{(i-1)n} + k^p p^{pn}.
\end{aligned}$$

Now, notice that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, and, for $1 \leq i \leq p-1$, $p \nmid i!$ and $p \nmid (p-i)!$. Therefore, as $p \mid p!$, we have $p \mid \frac{p!}{i!(p-i)!} = \binom{p}{i}$. Furthermore, as p is prime, $p \geq 2$, so $pn \geq 2n$. Since $n \geq 1$, $pn \geq 2n \geq n+1$. Thus, $p^{n+1} \mid k^p p^{pn}$. Therefore:

$$a^p = 1 + p^{n+1}\left(\sum_{i=1}^{p-1}\frac{\binom{p}{i}}{p}k^i p^{(i-1)n} + k^p p^{(p-1)n-1}\right)$$

so $a^p \equiv 1 \pmod{p^{n+1}}$. On the other hand:

$$\begin{aligned} a^p &= 1 + p^{n+1}\left(\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} k^i p^{(i-1)n} + k^p p^{(p-1)n-1}\right) \\ &= 1 + p^{n+1}\left(1 + \sum_{i=2}^{p-1} \frac{\binom{p}{i}}{p} k^i p^{(i-1)n} + k^p p^{(p-1)n-1}\right) \\ &= 1 + kp^{n+1} + p^{n+2}\left(\sum_{i=2}^{p-1} \frac{\binom{p}{i}}{p} k^i p^{(i-1)n-1} + k^p p^{(p-1)n-2}\right). \end{aligned}$$

Since $p > 2$, $p - 1 > 1$ and as $n \geq 1$, $(p-1)n > 1$. Thus, $(p-1)n \geq 2$ meaning that $(p-1)n - 2 \geq 0$. Likewise, the summation only contains integers, so we have $a^p \equiv 1 + kp^{n+1} \pmod{p^{n+1}}$. Since $k \nmid p$, we have $a^p \equiv 1 + kp^{n+1} \not\equiv 1 \pmod{p^{n+1}}$.

If $p = 2$, then $a^p = a^2 = 1 + k2^{n+1} + k^2 2^{2n}$. Since $p = 2$, we have $n > 1$ or $n \geq 2$. So, $2n \geq n + 2$, and $2^{n+2} \mid 2^{2n}$. Thus, $a^2 = 1 + k2^{n+1} + 2^{n+2}(k^2 2^{n-2})$, meaning that $a^2 \equiv 1 + k2^{n+1} \not\equiv 1 \pmod{2^{n+2}}$. □

Note that a combination of these two theorems gives us Euler's Theorem. However, it is not useful for studying LCGs, so the proof will not be presented here.

With these two preliminary results out of the way, we can return to studying the periods of LCGs. First, let us consider the periods of a single sequence.

Theorem 4 (Due to Knuth)**.** *If λ is the period of the LCS $(x_0, a, c, m_1 m_2)$ then if λ_1 and λ_2 are the periods of $(x_0 \bmod m_1, a \bmod m_1, c \bmod m_1, m_1)$ and $(x_0 \bmod m_2, a \bmod m_2, c \bmod m_2, m_2)$, respectively, then $\lambda = \operatorname{lcm}(\lambda_1, \lambda_2)$.*

Proof. Suppose $(x_0, x_1, x_2, \ldots)$ is the sequence generated by $(x_0, a, c, m_1 m_2)$, $(y_0, y_1, y_2, \ldots)$ the sequence generated by $(x_0 \bmod m_1, a \bmod m_1, c \bmod m_1, m_1)$, and $(z_0, z_1, z_2, \ldots)$ the sequence generated by $(x_0 \bmod m_2, a \bmod m_2, c \bmod m_2, m_2)$. Notice that then:

$$\begin{aligned} y_n &= \left((a \bmod m_1)^n (x_0 \bmod m_1) + \frac{(a \bmod m_1)^n - 1}{a \bmod m_1 - 1} c\right) \bmod m_1 \\ y_n &\equiv (a \bmod m_1)^n (x_0 \bmod m_1) + \frac{(a \bmod m_1)^n - 1}{a \bmod m_1 - 1} c \pmod{m_1} \\ &\equiv a^n x_0 + \frac{a^n - 1}{a - 1} c \pmod{m_1} \\ &\equiv x_n \pmod{m_1}. \end{aligned}$$

Since $0 \leq y_n < m_1$, we then have $y_n = x_n \bmod m_1$. By the same process, $z_n = x_n \bmod m_2$. Therefore, since $x_n = x_{n+\lambda}$ for all nonnegative integers n, then $y_n = y_{n+\lambda}$ and $z_n = z_{n+\lambda}$ for all nonnegative integers n. We will now prove that $\lambda_1 \mid n$ and $\lambda_2 \mid n$.

Suppose that $\lambda_1 \nmid \lambda$. Then let $\lambda = d\lambda_1 + r$ where $0 \leq r < \lambda_1$. We then have $y_n = y_{n+\lambda} = y_{n+d\lambda_1+r} = y_{n+r}$ since λ_1 is the period, for all n. But this means that $y_n = y_{n+r}$ for all n, meaning that the sequence repeates every r. However, $r < \lambda_1$, which would then mean that λ_1 is not the length of the minimum period. Therefore, $\lambda_1 \mid \lambda$. By the same steps, we can show that $\lambda_2 \mid \lambda$, meaning that $\operatorname{lcm}(\lambda_1, \lambda_2) \mid \lambda$, meaning that $\lambda \geq \operatorname{lcm}(\lambda_1, \lambda_2)$.

Now we will show that the sequence $(x_0, x_1, x_2, \ldots)$ repeats over $\operatorname{lcm}(\lambda_1, \lambda_2) = \lambda'$. Since $\lambda_1 \mid \lambda'$ and $\lambda_2 \mid \lambda'$, we have $y_n = y_{n+\lambda'}$ and $z_n = z_{n+\lambda'}$ for all nonnegative integers n. This means that $x_n \bmod m_1 = x_{n+\lambda'} \bmod m_1$, so $x_n \equiv x_{n+\lambda'} \pmod{m_1}$, and likewise, $z_n = z_{n+\lambda'} \implies x_n \bmod m_2 = x_{n+\lambda'} \bmod m_2 \implies x_n \equiv x_{n'_\lambda} \pmod{m_2}$. Thus, $m_1 \mid x_{n+\lambda'} - x_n$ and $m_2 \mid x_{n+\lambda'} - x_n$. Since m_1 and m_2 are relatively prime, this means $m_1 m_2 \mid x_{n+\lambda'} - x_n$, meaning that $x_{n+\lambda'} \equiv x_n \pmod{m_1 m_2}$ and so $x_{n+\lambda'} = x_n$ since both are in the range $[0, m_1 m_2)$.

Therefore, since the period must be at least $\lambda' = \operatorname{lcm}(\lambda_1, \lambda_2)$ and since the sequence repeats over λ', λ' is the period of the sequence $(x_0, x_1, x_2, \ldots)$. □

This theorem gives us a tool which we can use to ensure that the period is of a certain length. Let λ is the period of a sequence generated by (x_0, a, c, m). We can then break up any modulus m into relatively prime parts by using its prime factorization; that is, $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$. If λ_i is the period of the sequence $(x_0 \bmod p_i^{e_i}, a \bmod p_i^{e_i}, c \bmod p_i^{e_i}, p_i^{e_i})$ for all $1 \leq i \leq n$, then $\lambda = \operatorname{lcm}(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n)$. Note that $\lambda \leq \lambda_1 \lambda_2 \lambda_3 \cdots \lambda_n$, with equality occurring iff each λ_i is relatively prime. Furthermore, note that $\lambda_i \leq p_i^{e_i}$, meaning that $\lambda_1 \lambda_2 \lambda_3 \cdots \lambda_n \leq p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} = m$ with equality occurring iff $\lambda_i = p_i^{e_i}$. In other words, $\lambda = m$ iff $\lambda_i = p_i^{e_i}$, which ensures that each λ_i is relatively prime. Now we must find some criteria for which the sequence (x_0, a, c, p^n) for some prime p has period p^n.

Theorem 5 (Due to Knuth)**.** *The sequence $(x_0, x_1, x_2, \ldots)$ generated by (x_0, a, c, p^n) has period p^n if and only if p^n and c are relatively prime and $a \equiv 1 \pmod{p}$ or $a \equiv 1 \pmod{4}$ if $p = 2$ and $n > 1$.*

Proof. $\implies$ Suppose the sequence has period p^n. Then, as the first p^n elements of the sequence must be distinct (or else the period will be less than p^n), there must be some integer i, $0 \leq i < p^n$ such that $x_i = 0$. By Equation 2 we can write every element x_{k+i} in terms of x_i as follows:

$$x_{k+i} = \left(a^k x_i + \frac{a^k - 1}{a - 1} c\right) \bmod p^n$$
$$x_{k+i} \equiv a^k x_i + \frac{a^k - 1}{a - 1} c \pmod{p^n}.$$

Since $x_i = 0$, this simplifies to:

$$x_{k+i} \equiv \frac{a^k - 1}{a - 1} c \pmod{p^n}.$$

Since the period is p^n, there exists some k such that $x_{k+i} = 1$. Then:

$$1 \equiv \frac{a^k - 1}{a - 1} c \pmod{p^n},$$

meaning that c has a multiplicative inverse, and so c is relatively prime to p^n. Now, noting that since p^n is the period, we have:

$$\frac{a^{p^n} - 1}{a - 1} c \equiv x_{i+p^n} = x_i = 0 \pmod{p^n}$$

Multiplying both sides by $(a-1)$ we get $a^{p^n}-1 \equiv 0 \pmod{p^n}$ or $a^{p^n} \equiv 1 \pmod{p^n}$. So, $a^{p^n-1} \equiv a^{-1} \pmod{p}$, the multiplicative inverse of a modulo p. As $p-1 \mid p^n-1$, by Fermat's Little Theorem:

$$a^{-1} \equiv a^{p^n-1} \equiv (a^{p-1})^{\frac{p^n-1}{p-1}} \equiv 1^{\frac{p^n-1}{p-1}} \equiv 1 \pmod{p}$$

Thus, multiplying by a, we have $a \equiv 1 \pmod{p}$.

Now, if $p = 2$ and $n > 1$, we need to additionally prove that $a \equiv 1 \pmod{4}$. We have $a \equiv 1 \pmod{2}$, so assume now that that $a \equiv 3 \pmod{4}$. Then either $a \equiv 3 \pmod{8}$ or $a \equiv 7 \pmod{8}$, but either way, $a^2 \equiv 1 \pmod{2^3}$. By the repeated use of Theorem 3 we have $a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$, or $2^{n+1} \mid a^{2^{n-1}} - 1$.

Now, suppose $a^{2^{n-1}} - 1 = 2^{n+1}y$ for some y, and $a - 1 = 2z$. Since $a \equiv 3 \pmod{4}$, $a - 1 \equiv 2 \pmod{4}$, meaning that 2 is the highest power of 2 that divides $a - 1$. Thus, z is odd. Now, dividing, we have:

$$\frac{a^{2^{n-1}}-1}{a-1} = \frac{y}{z}2^n.$$

Since $a - 1 \mid a^{2^{n-1}} - 1$, $\frac{y}{z}2^n$ is an integer. As z is odd, we must have $z \mid y$, meaning that $\frac{y}{z}$ is an integer. Therefore:

$$\begin{aligned}
\frac{a^{2^{n-1}}-1}{a-1} &\equiv 0 \pmod{2^n} \\
\frac{a^{2^{n-1}}-1}{a-1}c &\equiv 0 \pmod{2^n} \\
(a^{2^{n-1}}-1)x_k + \frac{a^{2^{n-1}}-1}{a-1}c &\equiv 0 \pmod{2^n},
\end{aligned}$$

since $a^{2^{n-1}} - 1 \equiv 0 \pmod{2^{n+1}}$ means that $2^n \mid a^{2^{n-1}} - 1$. This is true for any x_k, so:

$$\begin{aligned}
a^{2^{n-1}}x_k + \frac{a^{2^{n-1}}-1}{a-1}c &\equiv 0 \pmod{2^n} \\
a^{2^{n-1}}x_k + \frac{a^{2^{n-1}}-1}{a-1}c &\equiv x_k \pmod{2^n} \\
x_{k+2^{n-1}} &\equiv x_k \pmod{2^n},
\end{aligned}$$

meaning that the sequence has period $n-1$, not n. This is impossible, so $a \equiv 1 \pmod{4}$.

$\Longleftarrow$ We will combine the cases of $p > 2$ and $p = 2$. Suppose $a \equiv 1 \pmod{p^i}$, and $a \not\equiv 1 \pmod{p^{i+1}}$. We have $i > 0$ by the conditions, or $i > 1$ if $p = 2$. By Theorem 3, we then have $a^{p^n} \equiv 1 \pmod{p^{n+i}}$ (if $p = 2$, $i > 1$). Therefore, $a^{p^n} - 1 = yp^{n+i}$ for some integer y, and likewise, $a - 1 = zp^i$ for some integer z as $a \equiv 1 \pmod{p^i}$. Since $a \not\equiv 1 \pmod{p^{i+1}}$, $p \nmid z$. Thus:

$$\frac{a^{p^n}-1}{a-1} = \frac{y}{z}p^n.$$

Since $a - 1 \mid a^{p^n} - 1$, $\frac{y}{z}p^n$ is an integer. Since $p \nmid z$, we must have $z \mid y$, so $\frac{y}{z}$ is an integer. Therefore,

$$\frac{a^{p^n}-1}{a-1} \equiv 0 \pmod{p^n}$$

Multiplying both sides by $a-1$, we have $a^{p^n} \equiv 1 \pmod{p^n}$. Therefore, for every x_k, we have:

$$\begin{aligned} x_{k+p^n} &= \left(a^{p^n} x_k + \frac{a^{p^n}-1}{a-1}c\right) \bmod p^n \\ x_{k+p^n} &\equiv a^{p^n} x_k + \frac{a^{p^n}-1}{a-1}c \pmod{p^n} \\ &\equiv x_k \pmod{p^n} \end{aligned}$$

since $a^{p^n} \equiv 1 \pmod{p^n}$ and $\frac{a^{p^n}-1}{a-1} \equiv 0 \pmod{p^n}$. Now, suppose the sequence has period λ. Since the sequence repeats every p^n elements, we have $\lambda \,|\, p^n$ (by the technique discussed in the proof of the last theorem). As $\lambda \,|\, p^n$, $\lambda = p^j$ for some integer j. Assume now that $j < n$.

Since $a \equiv 1 \pmod{p^i}$ and $a \not\equiv 1 \pmod{p^i}$, by Theorem 3, $a^{p^j} \equiv 1 \pmod{p^j}$ and $a^{p^j} \not\equiv 1 \pmod{p^{i+j+1}}$. This means that $p^j \mid \frac{a^{p^j}-1}{a-1}$ and $p^{j+1} \nmid \frac{a^{p^j}-1}{a-1}$. Since $p^j = \lambda$ is the period, for every k:

$$x_k = x_{k+p^j} = \left(a^{p^j} x_k + \frac{a^{p^j}-1}{a-1}c\right) \bmod p^n$$

by Equation 3. Therefore:

$$\begin{aligned} x^k &\equiv a^{p^j} x_k + \frac{a^{p^j}-1}{a-1}c \pmod{p^n} \\ 0 &\equiv (a^{p^j}-1)x_k + \frac{a^{p^j}-1}{a-1}c \pmod{p^n}. \end{aligned}$$

Therefore, for some integer r:

$$(a^{p^j}-1)x_k + \frac{a^{p^j}-1}{a-1}c = rp^n.$$

Simplifying:

$$\begin{aligned} (a^{p^j}-1)x_k + \frac{a^{p^j}-1}{a-1}c &= rp^n \\ \left(\frac{a^{p^j}-1}{a-1}\right)((a-1)x_k + c) &= rp^n. \end{aligned}$$

Note that $p^j \mid \frac{a^{p^j}-1}{a-1}$ and $p^{j+1} \nmid \frac{a^{p^j}-1}{a-1}$. Thus, let $\frac{a^{p^j}-1}{a-1} = sp^j$, with $p \nmid s$. We then have:

$$sp^j((a-1)x_k + c) = rp^n.$$

As $p \nmid s$, $s \,|\, r$, so $\frac{r}{s}$ is an integer. Thus:

$$(a-1)x_k + c = \frac{r}{s}p^{n-j}.$$

Therefore, we have:

$$(a-1)x_k + c \equiv 0 \pmod{p^{n-j}}$$

since $n > j$, or

$$(a-1)x_k \equiv -c \pmod{p^{n-j}}.$$

Now, if $\gcd(a-1, p) > 1$, then $p \mid a-1$, meaning that $p \mid c$. However, $\gcd(p, c) = 1$, so $\gcd(a-1, p) = 1$ as well. But we have $a \equiv 1 \pmod{p}$ meaning that $p \mid a-1$, so this is impossible as well. Therefore, we cannot have $j < n$. Since $p^j \mid p^n$, we have $j \leq n$, meaning that $j = n$, and the period, λ of the sequence is p^n. □

Now, every $p_i^{e_i}$ in the prime factorization of m must satisfy this theorem. So if $m = p_1^{e1} p_2^{e2} p_3^{e3} \cdots p_n^{e_n}$ then $a \equiv 1 \pmod{p_i}$ for every integer $1 \leq i \leq n$, $a \equiv 1 \pmod{p_i}$. Additionally, if $2 \mid m$ and has a power of at least 2; that is, if $4 \mid m$, we must have $a \equiv 1 \pmod{4}$. Finally, we must have $\gcd(c, p_i^{e_i}) = 1$ for every integer $1 \leq i \leq n$, meaning that $p_i \nmid c$ and so $gcd(m, c) = 1$. These conditions thus give the following theorem:

Theorem 6. *An LCG (x_0, a, c, m) has a period of m if and only if, for every prime p $p \mid m \implies p \mid a-1$, $4 \mid m \implies 4 \mid a-1$, and c is relatively prime to m.*

Now, the theory behind LCGs and how random a sequence they produce goes far beyond what is presented here. The reader is recommended to read Chapter 3 of *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* by Donald Knuth for more about LCGs, including a test specifically for these types of generators called the spectral test, which involves an n-dimensional analysis of the generator.

While it is interesting to analyze such sequences, LCGs have less practical use today than perhaps was seen when Knuth was writing his book. The theorems presented here thus probably are more of interest to the mathematician than the computer programmer.