Number theory

Elementary number theory and its applications, 2ed, K. Rosen. Addison-Wesley, 1988.

Definition Let m be a positive integer. If a and b are integers, we say that *a is congruent to b modulo m* if $m \mid (a-b)$, denoted by $a \equiv b \pmod{m}$.

Definition. The integers a and b are called *relatively prime* if a and b have greatest common divisor $(a,b) = 1$.

Definition . Let n be a positive integer. *The Euler phi-function* $\phi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Euler's theorem. If m is a positive integer and a is an integer with $(a,m) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{m}$.

Definition. Let a and m be relatively prime positive integers. Then the least positive integer x such that $a^{x} \equiv 1 \pmod{m}$ is called *the order of a modulo m* denoted by $\mathrm{ord}_m\, a$.

Example Find the order of 2 modulo 7.
$2^1 = 2 \pmod{7}$, $2^2 = 4 \pmod{7}$, $2^3 = 1 \pmod{7}$.
Therefore $\mathrm{ord}_7\, 2 = 3$.

Definition . If r and n are relatively prime integers with $n > 0$ and if $\mathrm{ord}_n\, r = \phi(n)$, then r is called a *primitive root modulo n*.

<u>Theorem</u> 1 If $\text{ord}_m\, a = t$ and if u is a positive integer, then

$$\text{ord}_m\,(a^u) = t / (t,u)$$

<u>Corollary</u> 1 Let r be a primitive root modulo m where m is an integer $m > 1$. Then r^u is a primitive root modulo m if and only if $(u, \phi(n)) = 1$.

Proof By Theorem 1 we know that

$$\text{ord}_m\, r^u = \text{ord}_m\, r / (u, \text{ord}_m\, r) = \phi(m) / (u, \phi(m)).$$

Consequently, $\text{ord}_m\, r^u = \phi(m)$, and r^u is a primitive root modulo m, if and only if $(u, \phi(m)) = 1$.

<u>Pseudo – Random Numbers</u>

- Middle square method

John von Neumann (invent game theory, first computer, atomic bomb)
6139
37687321
6873

- Linear congruential method

$$x_{n+1} \equiv ax_n + c \pmod{m}, \quad 0 \le x_{n+1} < m$$

$m > 0$, $2 \le a \le m$, $0 \le c \le m$, $0 \le x_0 \le m$.

<u>Theorem</u> The terms of the sequence generated by the linear congruential method are given by

$$x_k \equiv a^k x_0 + c(a^k - 1) / (a - 1) \pmod{m}, \quad 0 \le x_k < m.$$

Proof by mathematical induction. for $k = 1$, the formula is obviously true, since $x_1 \equiv ax_0 + c \pmod{m}$, $0 \le x_1 < m$. Assume that the formula is valid for the k th term, so that

$$x_k \equiv a^k x_0 + c(a^k - 1) / (a -1) \pmod{m}, 0 \le x_k < m.$$

since

$$x_{k+1} \equiv a x_k + c \pmod{m}, 0 \le x_{k+1} < m.$$

we have

$$\begin{aligned} x_{k+1} &\equiv a(a^k x_0 + c(a^k -1)/(a-1)) + c \\ &\equiv a^{k+1} x_0 + c(a(a^{k-1})/(a-1) + 1 \\ &\equiv a^{k+1} x_0 + c(a^{k+1} - 1)/(a-1) \pmod{m} \end{aligned}$$

which is the correct formula for the (k+1)th term. This demonstrates that the formula is correct for all positive integers k.

The period length of a linear congruential pseudo-random number generator is the maximum length of the sequence obtained without repetition.

Theorem The linear congruential generator produces a sequence of period length m if and only if $(c,m) =1$, $a \equiv 1 \pmod{p}$ for all primes p dividing m, and $a \equiv 1 \pmod{4}$ if $4 \mid m$.

For the proof see D. E. Knuth, "The art of computer programming" vol 2, "seminumerical algorithms", 2nd ed Addison Wesley, 1981. pp. 9-20.

A special case where $c = 0$ is called *multiplicative congruential method.*

$$x_{n+1} \equiv a x_n \pmod{m}, \ 0 < x_{n+1} < m.$$

or

$$x_n \equiv a^n x_0 \pmod{m}, \quad 0 < x_{n+1} < m.$$

For many applications, the generator is used with the modulus m equal to the Mersenne prime $M_{31} = 2^{31} - 1$. When the modulus m is prime, the maximum period length is m -1, and this is obtained when a is a primitive root of m. To find a primitive root of M_{31} that can be used with the good results, we first demonstrate that 7 is a primitive root of M_{31}

<u>Theorem</u> The integer 7 is a primitive root of $M_{31} = 2^{31} - 1$.

Proof To show that 7 is a primitive root of M_{31}, it is sufficient to show that

$$7^{(M_{31} - 1)/q} \not\equiv 1 \pmod{M_{31}}$$

for all prime divisors q of M_{31} -1. With this information we can conclude that $\text{ord}_{M_{31}} 7 = M_{31} - 1$. To find factorization of M_{31} -1, we note that

$$\begin{aligned} M_{31} - 1 &= 2^{31} - 2 = 2(2^{30} - 1) = 2(2^{15} - 1)(2^{15} + 1) \\ &= 2(2^5-1)(2^{10}+2^5+1)(2^5+1)(2^{10}-2^5+1) \\ &= 2.3^2.7.11.31.151.331 \end{aligned}$$

if we show that

$$7^{(M_{31} - 1)/q} \not\equiv 1 \pmod{M_{31}}$$

for q = 2,3,7,11,31,151,331, then we know that 7 is a primitive root of M_{31} = 2147483647. Since

$$7^{(M_{31} - 1)/2} \equiv 2147483546 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/3} \equiv 1513477735 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/7} \equiv 120536285 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/11} \equiv 1969212174 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/31} \equiv 512 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/151} \equiv 535044134 \not\equiv 1 \pmod{M_{31}}$$
$$7^{(M_{31} - 1)/331} \equiv 1761885083 \not\equiv 1 \pmod{M_{31}}$$

we see that 7 is a primitive root of M_{31}.

In practice we do not want to use the primitive root 7 as the generator, since the first few integers generated are small. We find a larger primitive root using Corollary 1. We take a power of 7 where the exponent is relatively prime to $M_{31} - 1$. For instance, since $(5,M_{31}) = 1$, Corollary 1 tells us that $7^5 = 16807$ is also a primitive root. Since $(13,M_{31} -1) = 1$, another possibility is to use $7^{13} \equiv 252246292 \pmod{M_{31}}$ as the multiplier.

Choice of modulus

Let w be the computer's word size, or 2^e on an e-bit binary computer. Use $m = w \pm 1$.

Why not $m = w$?

When $m = w$ the right-hand digits of x_n are much less random than the left-hand digits. If d is a divisor of m, and if

$$y_n = x_n \bmod d$$

we can easily show that

$$y_{n+1} = (a\, y_n + c) \bmod d$$

for $x_{n+1} = a\, x_n + c - qm$ for some integer q, and taking both sides mod d cause the quantity qm to drop out when d is a factor of m.

This shows that the low-order form a congruential sequence that has a period of length d or less.

Other methods

Linear congruential method can be generalized to, say, a quadratic congruential method

$$x_{n+1} = (d\, x^2_n + a\, x_n + c) \bmod m$$

additive number generator (Mitchell and Moore 1958)

$$x_n = (x_{n-24} + x_{n-55}) \bmod m \quad n \geq 55$$

the least significant bits "$x_n \bmod 2$" have a period of length $2^{55} - 1$. Therefore the generator must have a period at least this long.

<u>Chi-square test</u>

We can say how probable or improbable certain types of events are.

The difference between observed Y_s and expected np_s

$$V = (Y_2 - np_2)^2 + (Y_3 - np_3)^2 + \ldots + (Y_{12} - np_{12})^2$$

What is the probability what V is this high using true dice?

Suppose that every observation can fall into one of k categories. We take n *independent* observations. Let p_s be the probability that each observation falls into category s, and let Y_s be the number of observations that actually do fall into category s.

Weighted by the prob. of occurrence np_s

$$V = \sum_{1 \leq s \leq k} \frac{(Y_s - np_s)^2}{np_s}$$

Expanding $(Y_s - np_s)^2 = Y_2 - 2np_s Y_s + n^2 p_s^2$ and

$Y_1 + Y_2 + \ldots Y_k = n$

$p_1 + p_2 + \ldots p_k = 1$

$$V = \frac{1}{n} \sum_{1 \leq s \leq k} \left(\frac{Y_s^2}{p_s} \right) - n$$

$v = k - 1$ the number of degree of freedom is $k - 1$.

Chi-square distribution table says "The quantity V will be less than or equal to x with approximate probability p, if n is large enough".

How large should n be? Rule of thumb is $np_s \geq 5$

Range of V	Indication
0-1 %, 99-100 %	Reject X
1-5 %, 95-99 %	Suspect ?
5-10 %, 90-95 %	Almost reject +

Example five Chi-square test on three data of four generators.

	B			C			D			F	
		+								X	X
			+						?	?	X
?						+	+		X	X	X
+				X	+				X	X	?
									X	X	X

B : $x_0 = 0$, $a = 3141592653$, $c = 2718281829$, $m = 2^{35}$
C : $x_0 = 0$, $a = 2^7 + 1$, $c = 1$, $m = 2^{35}$
D : $x_0 = 47194118$, $a = 23$, $c = 0$, $m = 10^8 + 1$
F : $x_0 = 314159265$, $a = 2^{18} + 1$, $c = 1$, $m = 2^{35}$

Conclusion, B and D are satisfactory, C is on the borderline, F is unsatisfactory.