e random sequences?bw about: "an unpredictable sequence where all numbers qual frequency?"uential method is a simple method used by Java: $X_0 = arbitrary seed$ $X_i = (aX_{i-1} + c) \mod m, i > 0$ indom sequences.is wrong with 0, 0, 0, 0, anyway? Can't that occur election?large power of 2. sults, want $a \equiv 5 \mod 8$, and a, c, m with no common				
 able, a 'tray' random sequence is difficult (i.e., slow) r (or human) to produce. Must have some nondeterministic reaction leads of producing random reaction leads of nonder (random one-time values used soperations). b) dent is of his message.) b) genes c) genes c) dent end on the sequence is a sequence that satisfies cartain reprefet. message.) b) genes c) genes c) dent used is useful for reproduce. That is had or predict. message. b) genes c) genes c) dent is a sequence is that is had or predict. message. b) genes c) dent is a sequence is that is had or predict. message. b) genes c) dent is a sequence is that is had or predict. message. b) genes c) dent is a sequence is that is had or predict. message. b) genes c) dent is a sequence is that is had or predict. message. b) genes c) dent is a sequence is that is had or predict. message. b) genes d) dent is a sequence is that is had or predict. message. b) genes d) dent is a sequence is that is had or predict. message. b) genes d) dent is a sequence is that and is generator: sequences like 0, 1, 3, 7, 1, 2, 7, 1, 4, e) this is why Jone deent give you the raw 4B bits. d) dent is a "Rondom Sequence"? message. b) dent is a "Rondom Sequence"? message. b) dent is a menode in a sequence. that is a menode is a simple method used by Jow. Mather is a menode in 0, 0, 0, 0, onywey? Con't that occur is a some indent is a simple method used by Jow. Mather is a simple indent is a simple method used by Jow. Mather is a simple indent is a simple of a length of sequence before and reaconable potency (necesure certain dependencies at X, 1, 2, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1,? the menode is a simple method used by Jow. Mather is a some of a length of sequence before and reaconable potency (necesure certain dependencies at X, 1, 2, 2, 2, 2, 2, 2, 3, 4, 4, 0, 1,				
thms ar (or human) to produce. Must have some nondeterministic course:	Why Random Sequences?	Pseudo-Random Sequences	What Can Go Wrong (I)?	
modes keys and names (random one-time values used songe unique). theread only a sequence that satisfies actual oper ties, even if deterministic (as is useful for reproductivity). theread only a sequence that satisfies actual oper ties, even if deterministic (as is useful for reproductivity). theread only a sequence that satisfies actual oper ties, even if deterministic (as is useful for reproductivity). the (32) (4300)17.1; (11) and (3) (31, 7, 12, 7, 14,, 14) and (24) mod (8) (31, 7, 12, 7, 14,, 14) and (8) (31, 7, 12, 7, 14,, 14) and (24) (er (or human) to produce. Must have some nondeterministic rce. Can use:	course, in a state of sin. JOHN VON NEUMANN (1951)	
 streams of random bits (e.g., stream ciphers encrypt yx yxoring perpoducible streams of pseudo-random bits (s.g., cryptography) we need sequence that is hard or a predict. Sum of therministic is subsulf for expreducibility). e.g., cryptography) we need sequence that is hard or a predict. Sum of the transition of the that hard one sequence is that random sequences (probably) pass. Iook at lengths of runs: increasing or decreasing contiguous s. y. statistical criteria to be used are quite involved. For funct, volume 2. What Is a "Random Sequence"? a sequence where all numbers occur with equal frequency? b, A.,? w boat: "an unpredictable sequence where all numbers quite involved. For funct, volume 2. w boat: "an unpredictable sequence where all numbers accur with equal frequency?" b, A.,? w boat: "an unpredictable sequence where all numbers quite involved. Sequences?" b) La sequence?" b) La sequence?" b) La sequence?? c) La Le La sequence where all numbers occur with equal frequency?? c) L, L, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1,? tis wrong with 0, 0, 0, 0, anyway? Can't that occur blection? tis wrong with 0, 0, 0, 0, anyway? Can't that occur blection? tis wrong with 0, 0, 0, 0, anyway? Can't that occur blection? to "a to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable pattern" and pass certain section? to "a to "actionable patte		etween keystrokes or incoming internet message.	erns. E.g., just using lower 3 bits of X_i in Java's 48-bit	
 c. games c. games c. games c. cost Leever #35 n Numbers (Chapter 11) random sequences? dow at englance dow at englance	streams of random bits (e.g., stream ciphers encrypt y xor'ing reproducible streams of pseudo-random bits	operties, even if deterministic (as is useful for reproducibility). e.g., cryptography) we need sequence that is <i>hard</i> or	$= (5(X_{i-1} \bmod 8) + 3) \bmod 8$	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	e, games	pm sequence: deterministic sequence that passes some statistical tests that random sequences (probably) pass.	$0, 1, 3, 7, 1, 2, 7, 1, 4, \dots$	
CS61B Lecture #35What Is a "Random Sequence"? a sequence where all numbers occur with equal frequency"? $3, 4,?$ erating Pseudo-Random Sequences as you might think. mplex jumbling methods can give rise to bad sequences. use inform numbers? $0, 1, 1, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1, ?$ t is wrong with $0, 0, 0, 0,$ anyway? Can't that occur lection?erating Pseudo-Random Sequences as you might think. mplex jumbling methods can give rise to bad sequences. $x_0 = arbitrary seed$ $X_i = (aX_{i-1} + c) \mod m, i > 0$ t is wrong with $0, 0, 0, 0,$ anyway? Can't that occur lection?erating Pseudo-Random Sequences as you might think. mplex jumbling methods can give rise to bad sequences. $x_0 = arbitrary seed$ $X_i = (aX_{i-1} + c) \mod m, i > 0$ targe power of 2. uits, want $a \equiv 5 \mod 8$, and a, c, m with no common nerator with a period of m (length of sequence before nd reasonable potency (measures certain dependencies art X_i) t s of a to "have no obvious pattern" and pass certain see Knuth). $= 25214033017, c = 11, m = 216, to compute 48-bitpm numbers. It's good enough for many purposes, but$		s. ly, statistical criteria to be used are quite involved. For		
a sequence where all numbers occur with equal frequency"?as you might think.m Numbers (Chapter 11) $3, 4, \dots$?random sequences?w about: "an unpredictable sequence where all numbersndom sequences?w about: "an unpredictable sequence where all numbersndom sequences. $0, 1, 1, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1, \dots$?ne. 1 ibrary classes and methods.utations.t is wrong with 0, 0, 0, 0, anyway? Can't that occurutations. $a = 5 \mod 8$, and a, c, m with no commonnerator with a period of m (length of sequence before and reasonable potency (measures certain dependencies $a = X_{i,j}$)t is wrong with 0, 0, 0, 0, anyway? Can't that occurutations.	1:45 2021 C561B: Lecture #35 2	38:45 2021 C561B: Lecture #35 4	38:45 2021 C5618: Lecture #35 6	
Numbers (Chapter 11)3, 4,?mplex jumbling methods can give rise to bad sequences.a indom sequences?w about: "an unpredictable sequence where all numbers qual frequency?" $x_0 = arbitrary seed$ $X_i = (aX_{i-1} + c) \mod m, i > 0$ ne.a library classes and methods.large power of 2.untations.sult: "an unpredictable sequence before ind reasonable potency (measures certain dependencies ent X_i.)sult. method is a simple method sequence before ind reasonable potency (measures certain dependencies ent X_i.)t is wrong with 0, 0, 0, 0, anyway? Can't that occur lection?sults, want $a \equiv 5 \mod 8$, and a, c, m with no common increator with a period of m (length of sequence before ind reasonable potency (measures certain dependencies ent X_i.)t is or "have no obvious pattern" and pass certain see Knuth). $= 25214903917$, $c = 11$, $m = 2^{48}$, to compute 48-bit pm numbers. It's good enough for many purposes, but	CS61B Lecture #35	What Is a "Random Sequence"?	verating Pseudo-Random Sequences	
m Numbers (Chapter 11)3, 4,?mplex jumbling methods can give rise to bad sequences.indom sequences?w about: "an unpredictable sequence where all numbersuntial method is a simple method used by Java:indom sequences. $0, 1, 1, 2, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1,?$ is wrong with 0, 0, 0, 0, anyway? Can't that occurine.a library classes and methods.is wrong with 0, 0, 0, 0, anyway? Can't that occuriarge power of 2.utations.sults, want $a \equiv 5 \mod 8$, and a, c, m with no commonincreator with a period of m (length of sequence before ind reasonable potency (measures certain dependencies ent X _i .)is of a to "have no obvious pattern" and pass certain is good enough for many purposes, but		a sequence where all numbers occur with equal frequency"?	as vou might think.	
$= 25214903917$, $c = 11$, $m = 2^{48}$, to compute 48-bit pm numbers. It's good enough for many purposes, but	random sequences? ndom sequences"? m sequences. ne. a library classes and methods.	w about: "an unpredictable sequence where all numbers qual frequency?" 0, 1, 1, 2, 2, 2, 2, 2, 3, 4, 4, 0, 1, 1, 1,? It is wrong with 0, 0, 0, 0,anyway? Can't that occur	uential method is a simple method used by Java: $X_0 = arbitrary seed$ $X_i = (aX_{i-1} + c) \mod m, i > 0$ large power of 2. sults, want $a \equiv 5 \mod 8$, and a, c, m with no common merator with a period of m (length of sequence before and reasonable potency (measures certain dependencies ent X_i .) ts of a to "have no obvious pattern" and pass certain	
38:45 2021 C561B: Lecture #35 1 38:45 2021 C561B: Lecture #35 3 38:45 2021 C561B: Lecture #35 5	8:452021 C5410-1 article #95 1	38/45 2021 C5619-1 artum #35 2	= 25214903917 , $c = 11$, $m = 2^{48}$, to compute 48-bit om numbers. It's good enough for many purposes, but aphically secure.	

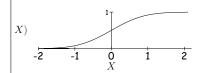
Additive Generators erator: $X_n = \begin{cases} arbitary value, & n < 55\\ (X_{n-24} + X_{n-55}) \mod 2^e, & n \ge 55 \end{cases}$ es than 24 and 55 possible. period of $2^f(2^{55} - 1)$, for some $f < e$. mentation with circular buffer: 55; *31) % 55]; // Why +31 (55-24) instead of -24? /* modulo 2^{32} */ . 54] is initialized to some "random" initial seed values.	aphic Pseudo-Random Number Generator Example good block cipher—an encryption algorithm that encrypts bits (not just one byte at a time as for Enigma). AES is rovide a key, K , and an initialization value I . udo-random number is now $E(K, I + j)$, where $E(x, y)$ is on of message y using key x .	<pre>by the set of the</pre>
What Can Go Wrong (II)? ds to bad correlations. s IBM generator RANDU: $c = 0$, $a = 65539$, $m = 2^{31}$. U is used to make 3D points: $(X_i/S, X_{i+1}/S, X_{i+2}/S)$, es to a unit cube, be arranged in parallel planes with voids between. So ts" won't ever get near many points in the cube:	 phic Pseudo-Random Number Generators form of linear congruential generators means that one inture values after seeing relatively few outputs. ou want unpredictable output (think on-line games involving domly generated keys for encrypting your web traffic.) <i>phic pseudo-random number generator (CPRNG)</i> has the nat ts of a sequence, no polynomial-time algorithm can guess pit with better than 50% accuracy. current state of the generator, it is also infeasible to ct the bits it generated in getting to that state. 	Adjusting Range and Distribution Equence of numbers, X_i , from above methods in range ⁴⁸ , how to get uniform random integers in range 0 to easy: use top k bits of next X_i (bottom k bits not as be careful of slight biases at the ends. For example, if $X_i/(2^{48}/n)$ using all integer division, and if $(2^{48}/n)$ gets n, then you can get n as a result (which you don't want). fix that by computing $(2^{48}/(n-1))$ instead, the probability -1 will be wrong.

CS61B: Lecture #35 7

eneralizing: Other Distributions

have some desired probability distribution function, and random numbers that are distributed according to that How can we do this?

normal distribution:



desired probability distribution. $P(Y \leq X)$ is the hat random variable Y is < X.

38:45 2021	
------------	--

38:45 2021

CS61B: Lecture #35 14

CS61B: Lecture #35 13

Java Classes

(): random double in [0..1).

til.Random: a random number generator with constructors: herator with "random" seed (based on time).) generator with given starting value (reproducible).

random integer

nt in range [0..n). andom 64-bit integer. (), nextFloat(), nextDouble() Next random values of other types. h() normal distribution with mean 0 and standard deviation rve"). .shuffle(L, R) for list L and Random R permutes Ling R).

38:45 2021

38:45 2021

CS61B: Lecture #35 16

CS61B: Lecture #35 15

38:45 2021

Random Selection

que would allow us to select N items from list:

L and return sublist of K>=0 randomly	
elements of L, using R as random source. */	
(List L, int k, Random R) {	
i = L.size(); i+k > L.size(); i -= 1)	
ement i-1 of L with element	
tInt(i) of L;	
<pre>sublist(L.size()-k, L.size());</pre>	

efficient for selecting random sequence of K distinct **m** [0..N), with $K \ll N$.

CS61B: Lecture #35 18

Arbitrary Bounds

rbitrary range of integers (L to U)?

```
m float, x in range 0 \le x < d, compute
```

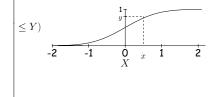
nextInt(1<<24) / (1<<24);

ple a bit more complicated: need two integers to get

and = ((long) nextInt(1<<26) << 27) + (long) nextInt(1<<27); * bigRand / (1L << 53);</pre>

eralizing: Other Distributions (II)

e y uniformly between 0 and 1, and the corresponding x ed according to P.



Shuffling				
a random permutation of b technique for sorting N N random numbers ch to one of the list elem ist using random numbers a bit better:	-element lis ents			
<pre>>(List L, Random R) { i = L.size(); i > 0; : elements i-1 and R.ne;</pre>		L;		
0 1 2 3 4 5 4 2 3 4 2 3 3 A 2 2 3 3	Swap items $3 \iff 3$	0 1 2 3 4 5 A 3 3 2 2 A 3 2 4		
1♣ 3♡ 3♣ A♡ 2♡ 2♣	$2 \Longleftrightarrow 0$	20 30 A A A0 3 2		
1♣ 3♡ 2♡ A♡ 3♣ 2♣ 38:45 2021	$1 \Longleftrightarrow 0$	3 (2 (2) A (3) 3 (2) CS61B: Lecture #35 17		

rnative Selection Algorit	hm (Floyd)		
	Example		
ence of K distinct integers O<=K<=N. */			
lect(int N, int K, Random R)			
ger> S = new ArrayList<>();	5 4 [4] 6 2 [2, 4]		
I-K; i < N; i += 1) {	7 5 [5, 2, 4]		
s in S are < i ndInt(i+1); // 0 <= s <= i < N	8 5 [5, 8, 2, 4] 9 4 [5, 8, 2, 4, 9]		
<pre>set(j) for some j) value i (which can't be there</pre>	<pre>selectRandomIntegers(10, 5, R)</pre>		
ter the s (i.e., at a random ther than the front)			
i);			
random value s (which can't be			
<pre>ret) at front s);</pre>			
38:45 2021	CS61B: Lecture #35 19		