Random() Adventures in Minecrosoftcraft

A cautionary tale


MINECRAFT
MOJANG

Pseudo-random number generators

rand(), Random(), ...

Java, C, C++ – LCG

Ruby, Python – Mersenne Twister

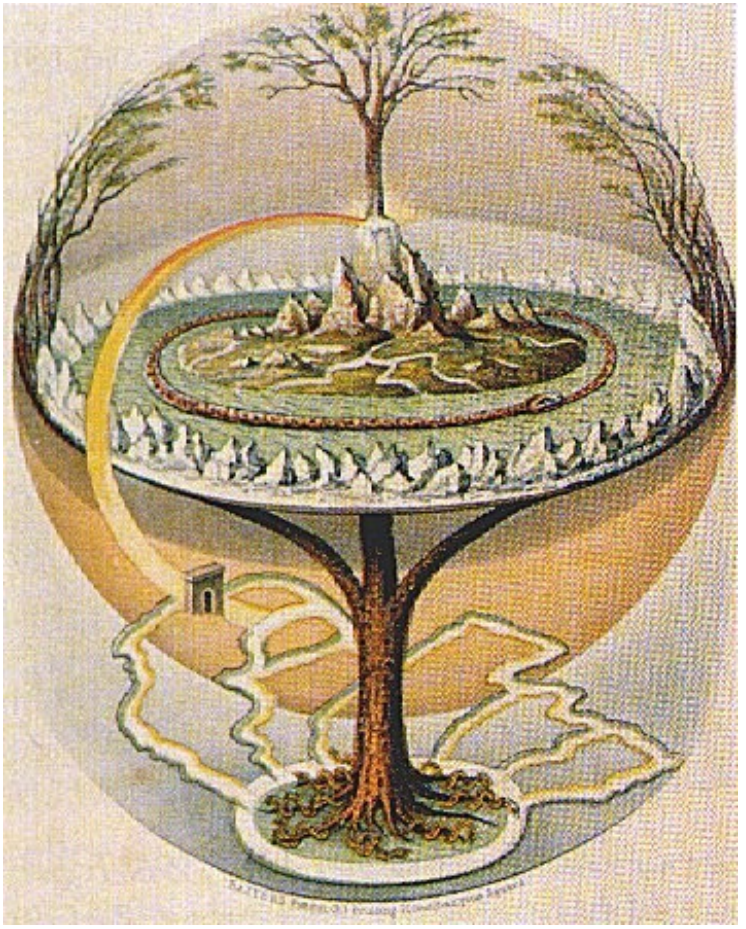
Would you trust a Random() stranger?

java.util.Random

$$state := (state * 25214903917) + 11 \bmod 2^{48}$$

1000111100101111001111001110110101000001010001000

The world grows from a seed

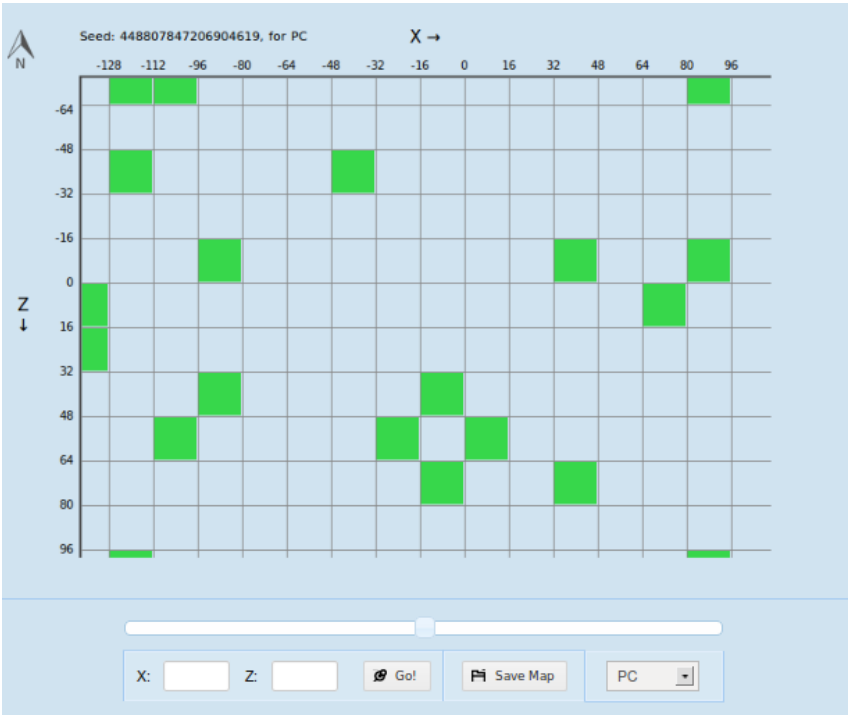


Yggdrasil

Oluf Olufsen Bagge, 1847

Slimes

© Mojang AB, CC-A-NC



chunkbase.com/apps/slime-finder/

```
Random rnd = new Random(seed +
                        (long) (xPosition * xPosition * 0x4c1906) +
                        (long) (xPosition * 0x5ac0db) +
                        (long) (zPosition * zPosition) * 0x4307a7L +
                        (long) (zPosition * 0x5f24f) ^ 0x3ad8025f);
return rnd.nextInt() % 10 == 0;
```

Complicated looking, She'll be right.

Collect known places where slimes appear

Search for seeds where they appear in those spots

```
for (seed = 0; seed < (1 << 64); seed++) {
     boolean match = true;
     for (positionValue in knownAppearedPositions) {
          Random rnd = new Random(seed + positionValue ^ 0x3ad8025f);
          match = match && (rnd.nextInt() == 10);
     }
     if (match) ...
}
```

~ 1800 years

Septimius Severus

© Raymond Ostertag
CC-A-SA

Empress Jingū

java.util.Random

$$state := (state * 25214903917) + 11 \bmod 2^{48}$$

```
for (seed = 0; seed < (1 << 48); seed++) {
     boolean match = true;
     for (positionValue in knownAppearedPositions) {
          Random rnd = new Random(seed + positionValue ^ 0x3ad8025f);
          match = match && (rnd.nextInt() == 10);
     }
     if (match) ...
}
```

~ 10 days

32	+	65	=	97
132	+	765	=	897
1932	+	8765	=	10697

32	x	65	=	2080
132	x	765	=	100980
1932	x	8765	=	16933980

In LCGs we return the **top** bits of the state
Because the bottom bit does this:

0101010101010101

mod 2^{48} mucks with decimal

$2^{48} = 281474976710656$

All multiples of 10 are even

11000010101111000000111001000110001010101
0101001

1100001010111000000111001000110001010101
0101001

18 bits

~ 4 ms

Work out possibilities for lower 18 bits

Only look at 48-bit seeds which end with these

Narrowing down...

30 confirmed spots where slimes appear
… only one possibility for lower 18 bits
8 possibilities for lower 48 bits

~3 seconds to search possibilities

random.nextLong()

48 bit state means only 2^{48} outputs

Only actually 2^{48} possible “random” seeds.

9 likely seeds

random.nextLong()

48 bit state means only 2^{48} outputs

Only actually 2^{48} possible “random” seeds.

9 likely seeds

Don't trust a Random() stranger

Even if they give you a free ride

https://github.com/pruby/slime-seed