

# The `lcg` package

Erich Janka – Das Vollpreiskind  
janka@utanet.at

2008/09/10 (v1.2)

## Abstract

This Package contains macros to generate (pseudo) random numbers with L<sup>A</sup>T<sub>E</sub>X by a simple linear congruential generator. The user can specify a range of integers containing the generated random numbers.

To pass options to the package, the  $\langle key \rangle = \langle value \rangle$  scheme of the `keyval` package is used.

If no options are specified, random numbers will be generated in the interval from 1 to  $2^{31} - 1$  (= 2147483647). Let  $S$  be the smallest and  $L$  the largest number of the specified range, then the following inequalities must hold because of limitations of L<sup>A</sup>T<sub>E</sub>X:

$$-2^{31} + 1 \leq S \leq L \leq 2^{31} - 1 \quad \text{and} \quad L - S \leq 2^{31} - 2$$

The generated random numbers will be stored in a L<sup>A</sup>T<sub>E</sub>X counter definable by the user.

## 1 User Interface

The `lcg` package is loaded with

```
\usepackage[list of options]{lcg}.
```

The optional Argument is a comma separated list of entries of the kind  $\langle key \rangle = \langle value \rangle$  or  $\langle key \rangle$ . In the second case the key will be set to a standard value. For example the line

```
\usepackage[first=10, last=20]{lcg}
```

loads the package and generates the L<sup>A</sup>T<sub>E</sub>X counter `rand` which will hold pseudo random numbers from 10 to 20. All available keys and their standard values are introduced below.

**\rand** Each call of the command `\rand` will write a new random number to the counter provided by the user with the key  $\langle counter \rangle$  or to the standard counter of this package—`rand`. Now it's possible to do whatever can be done with counters. The command evokes a linear congruential random number generator described below.

`\reinitrand` The command `\reinitrand[list of options]` has one optional argument which is identical to the argument of `\usepackage`, i. e. the same keys in the comma separated list are allowed. The effect is that specified keys will be set and all others will be reset to their standard values.

`\chgrand` The syntax of the command `\chgrand` is identical to `\reinitrand`. The difference is that `\chgrand` will set the specified keys but won't effect any other key.

## 1.1 The Options

This section deals with the list of all available keys and their standard values.

**counter** This key sets the name of the L<sup>A</sup>T<sub>E</sub>X counter where the random numbers will be stored. If the counter already exists (maybe somebody likes random page numbers), L<sup>A</sup>T<sub>E</sub>X will prompt a warning and will use it. If the counter doesn't exist, it will be defined by this package and set to 0.

**Standard value:** rand

**first** This key sets the left boarder of the range within random numbers will be generated. Its value can be any number from  $-2^{31} + 1$  to  $2^{31} - 1$ , as long as it is not greater than the value of the key *last* and the difference to the value of *last* doesn't exceed  $2^{31} - 2$ .

**Standard value:** 1

**last** This key sets the right boarder of the range within random numbers will be generated. Its value can be any number from  $-2^{31} + 1$  to  $2^{31} - 1$ , as long as it is not less than the value of the key *first* and the difference to the value of *first* doesn't exceed  $2^{31} - 2$ .

**Standard value:**  $2^{31} - 1$

**seed** The value of this key is the starting value for the algorithm generating the random numbers and must be within the range 1 to  $2^{31} - 1$ . If the value is smaller than 1, the random number generator will be initialized with the time, the page number and the actual line of the file. This key allows reproduction of the sequences of random numbers.

**Standard value:** 0

**quiet** When using the `lcg` package it sends some lines of information to the screen and the `log`-file:

- The name of the counter holding the generated random numbers
- The lower bound of the range of random numbers
- The upper bound of the range of random numbers
- The initial value of the random number generator

To suppress this output this key can be used. If the value starts with the letter *y*, *Y*, *j* or *J* there will be no output whereas words beginning with the letters *n* or *N* won't suppress it.

**Standard value:** *y*

## 2 Example

This documentation loaded the package with:

```
\usepackage[first=10, last=20]{lcg}
```

The lines

```
\rand\arabic{rand} \rand\arabic{rand} \rand\arabic{rand}
\rand\arabic{rand} \rand\arabic{rand} \rand\arabic{rand}
\rand\arabic{rand} \rand\arabic{rand} \rand\arabic{rand}
```

generate these numbers (all between 10 and 20): 20 19 15 12 18 17 16 20 17

Now the counter `die` should simulate a die and hold random numbers from 1 to 6. In addition it is demonstrated how to switch off the output to the screen and to the log-file. This can be achieved with one of the following lines:

```
\reinitrand[last=6, counter=die, quiet]
```

After that, the numbers 3 1 2 5 2 6. are a product of:

```
\rand\arabic{die} \rand\arabic{die} \rand\arabic{die}
\rand\arabic{die} \rand\arabic{die} \rand\arabic{die}
```

As one can see, the key `\first` has been reset to 1.

The following lines will change the range to  $-6$  to  $+6$  without modifying any other option:

```
\chgrand[first=-6]
```

Here the numbers 0 4 -4 3 -5 6 are stored in a user defined counter and brought to paper by:

```
\rand\arabic{die} \rand\arabic{die} \rand\arabic{die}
\rand\arabic{die} \rand\arabic{die} \rand\arabic{die}
```

At last, random numbers between 1 and 12 will be generated and stored in the standard counter `rand`. The seed will be set to 1234. There will also be a warning because the name of the counter is set to `rand` which was already defined when calling the package:

```
\reinitrand[last=12, seed=1234]
```

```
\rand\Roman{rand} \rand\Roman{rand} \rand\Roman{rand}
```

These lines produce: XI V VII. When using other formats than `arabic` for printing, the desired numbers might not appear on the screen because these formats don't support the full range of  $2^{31} - 1$ .

### 3 The Linear Congruential Generator

The linear congruential generator used produces a sequence of numbers  $I_j$  in the range from 1 to  $m$  by following rule:

$$I_{j+1} = aI_j \bmod m$$

where  $I_0$  is set to a arbitrary starting value (called “seed”). The quality of this generator depends on the choice of the parameters  $a$  and  $m$ . Another problem is that when implementing the algorithm as above, the multiplication might leave the range  $\text{\LaTeX}$  can deal with. The solution is Schrage’s method [W. PRESS et al. *Numerical Recipes in C*. 2nd edition. Cambridge University Press 1992] which allows to perform the multiplications without leaving the given range. This is done by introducing two variables  $r$  and  $q$ :

$$m = aq + r \quad \text{with} \quad q = \lfloor m/a \rfloor \quad \text{and} \quad r = m \bmod a$$

where  $\lfloor \cdot \rfloor$  denotes the integer part of the argument. If  $z$  is an integer and  $0 \leq r < q$  and  $0 < z < m - 1$ , then the following (in)equalities hold:

$$\begin{aligned} 0 &\leq a \cdot (z \bmod q) \leq m - 1 \\ 0 &\leq \lfloor m/a \rfloor \leq m - 1 \\ az \bmod m &= \begin{cases} a \cdot (z \bmod q) - \lfloor z/q \rfloor & \text{if the term is } \leq 0 \\ a \cdot (z \bmod q) - \lfloor z/q \rfloor + m & \text{otherwise} \end{cases} \end{aligned}$$

To exploit the whole possible range and guarantee good performance,  $a$  and  $m$  are set as follows:  $a = 7^5 = 16807$  and  $m = 2^{31} - 1 = 2147483647$  and this gives  $q = 127773$  and  $r = 2836$ .

### 4 The Code

#### 4.1 Checking for possible conflicts

The following lines check if the commands provided by this package are already defined:

```
1 \ifundefined{rand}{}
2     {\PackageWarning{lcg}{Command ‘rand’ already defined}}
3 \ifundefined{r@ndcountername}{}
4     {\PackageWarning{lcg}{Command ‘r@ndcountername’
5         already defined}}
```

Checking internal commands:

```
6 \ifundefined{r@nd}{}
7     {\PackageWarning{lcg}{Command ‘r@nd’ already defined}}
8 \ifundefined{initr@nd}{}
9     {\PackageWarning{lcg}{Command ‘initr@nd’ already defined}}
10 \ifundefined{cutr@nger@nd}{}
```

```

11     {\PackageWarning{lcg}{Command 'cutr@nger@nd' already defined}}
12 \@ifundefined{@derr@nd}{
13     {\PackageWarning{lcg}{Command '@derr@nd' already defined}}
14 \@ifundefined{ProcessOptionsWithKVr@nd}{
15     {\PackageWarning{lcg}{Command 'ProcessOptionsWithKVr@nd'
16     already defined}}%
17 \@ifundefined{qui@t}{
18     {\PackageWarning{lcg}{Command 'qui@t' already defined}}
19 \@ifundefined{firstlett@r@nd}{
20     {\PackageWarning{lcg}{Command 'firstlett@r@nd' already defined}}
21

```

Checking the used counters:

```

22 \@ifundefined{c@f@rst}{
23     {\PackageWarning{lcg}{Counter 'f@rst' already defined}}
24 \@ifundefined{c@l@st}{
25     {\PackageWarning{lcg}{Counter 'l@st' already defined}}
26 \@ifundefined{c@cr@nd}{
27     {\PackageWarning{lcg}{Counter 'cr@nd' already defined}}
28 \@ifundefined{f@rst}{
29     {\PackageWarning{lcg}{Existing command 'f@rst' conflicts
30     with counter 'f@rst'}}
31 \@ifundefined{l@st}{
32     {\PackageWarning{lcg}{Existing command 'l@st' conflicts
33     with counter 'l@st'}}
34 \@ifundefined{cr@nd}{
35     {\PackageWarning{lcg}{Existing command 'cr@nd' conflicts
36     with counter 'cr@nd'}}

```

## 4.2 Macros for (re)initialization

**init** Set starting values for the parameters and counters to standard values or according to the provides keys

```

37 \def\initr@nd{%
38     \def\r@ndcount@rname{rand}%
39     \newcount \f@rst
40     \newcount \l@st
41     \newcount \cr@nd
42     \pr@keys@r@nd%
43     \ProcessOptionsWithKVr@nd{Init}%
44     \p@stkeys@r@nd%
45     \@utputr@nd%
46 } % end of \def\initr@nd

```

**reinit** Sets the provided keys and resets all other options.

```

47 \def\reinitr@nd{\@ifnextchar[\@reinitr@nd{\@reinitr@nd[]}}%
48 \def\@reinitr@nd[#1]{%
49     \pr@keys@r@nd%
50     \setkeys{Init}{#1}%

```

```

51 \p@stkeysr@nd%
52 \@putr@nd%
53 }% end of \def\reinitrand

```

**chgrand** Sets the provided keys and doesn't change any other option.

```

54 \def\chgrand{\@ifnextchar[\@chgr@nd{\@chgr@nd[]}]
55 \def\@chgr@nd[#1]{%
56 \@tempcnta = \z@
57 \@tempcntb = \z@
58 \setkeys{Init}{#1}%
59 \p@stkeysr@nd%
60 \@putr@nd%
61 } % end of \def\chgrand

```

### 4.3 The keys

**use keys** The following lines are from the `geometry` package written by HIDEO UMEKI (who borrowed it from the `hyperref` package written by SEBASTIAN RAHTZ). It enables the usage of the  $\langle key \rangle = \langle value \rangle$  scheme of the `keyval` package.

```

62 \def\ProcessOptionsWithKVr@nd#1{%
63 \let\@tempa\@empty
64 \@for\CurrentOption:=\@classoptionslist\do{%
65 \ifundefined{KV@#1@\CurrentOption}%
66 {}{\edef\@tempa{\@tempa,\CurrentOption,}}
67 \edef\@tempa{%
68 \noexpand\setkeys{#1}{\@tempa\@optionlist{\@currname.\@currxt}}}
69 \@tempa
70 \AtEndOfPackage{\let\@unprocessedoptions\relax}}

```

**first**

```
71 \define@key{Init}{first}[1]{\f@rst = #1}
```

**last**

```
72 \define@key{Init}{last}[2147483647]{\l@st = #1}
```

**counter**

```
73 \define@key{Init}{counter}[rand]{\def\r@ndcountername{#1}}
```

**seed**

```

74 \define@key{Init}{seed}[\z@]{% seed for random number generator
75 \ifnum #1 < \z@%
76 \PackageWarning{lcg}{Seed should be > 0 --
77 Seed will be initialized with the actual time}%
78 \cr@nd = \z@%
79 \else%
80 \cr@nd = #1
81 \typeout{Random number generator initialized to #1}%
82 \fi%
83 }

```

quiet

```
84 \define@key{Init}{quiet}[y]{
85   \def\qui@t{\expandafter\firstletter\end #1\delimiter}
86   \if \qui@t y% nothing to do
87   \else\if\qui@t Y \def\qui@t{y}
88   \else\if\qui@t j \def\qui@t{y}
89   \else\if\qui@t J \def\qui@t{y}
90   \else\if\qui@t n \def\qui@t{n}
91   \else\if\qui@t N \def\qui@t{n}
92   \else
93     \PackageWarning{lcg}{Value of key <quiet> must be <y> or <n>}
94     \def\qui@t{y}
95   \fi\fi\fi\fi\fi\fi
96 }
```

#### 4.4 Macros called by other macros

**pr@keys** The command `\pr@keysr@nd` is used to define and initialize all parameters (counters) needed by this package (before the keys are evaluated). Random numbers will be generated from `f@rst` to `f@rst + l@st - 1`, `cr@nd` will hold the random numbers (full range: 1 to  $2^{31} - 1$ ) and `rand` will hold the random numbers (user defined range). The counters are also initialized to standard values. If the counter `cr@nd` equals zero, the seed will be initialized according to the actual time by the command `\r@nd`:

```
97 \def\pr@keysr@nd{%
98   \f@rst = \@ne           % 1
99   \l@st = 2147483647     % 2147483647
100  \cr@nd = \z@           % 0
101  \@tempcnta = \z@
102  \@tempcntb = \z@
103  \def\r@ndcountername{rand}%
104  \def\qui@t{n}
105 } % end of newcommand\def\pr@keysr@nd
```

**p@stkeys** The command `\p@stkeysr@nd` is executed after the keys are evaluated as last step of the initialization. The setting of the counter `l@st` depends on whether the key `<last>` is set or not. and the counter (user defined or standard name) is created.

```
106 \def\p@stkeysr@nd{%
107   \@rderr@nd%           last < first -> swap
108   \cutr@nger@nd%       range too big -> cut
109   \@ifundefined{c@\r@ndcountername}{\newcounter{\r@ndcountername}}%
110   {%
111     \PackageWarning{lcg}{Using an already existing
112       counter \r@ndcountername}%
113   }%
114   \setcounter{\r@ndcountername}{0}%
115 } % end of \def\p@stkeysr@nd
```

**firstletter** This macro is used to determine the first letter of the value of the key *quiet*.

```
116 \def\firstlett@nd#1#2\delimiter{#1}
```

**@output** Output to log-file/screen

```
117 \def\@output@nd{%
118   \if \qui@t y% do nothing
119   \else
120     \typeout{Smallest possible random number: \the\f@rst}%
121     \typeout{Largest possible random number: \the\l@st}%
122     \typeout{The pseudo random numbers will be stored
123     in the LaTeX counter '\r@ndcountname'}%
124   \fi
125 }
```

**@order** If the value of the key *last* is less than the value of *first*, they will be exchanged.

```
126 \def\@order@nd{%
127   \ifnum \l@st < \f@rst%
128     \PackageWarning{lcg}{Key 'last' less than key 'first'
129     -- swapped}%
130     \@tempc@nta = \f@rst
131     \f@rst = \l@st
132     \l@st = \@tempc@nta
133   \fi%
134 }% end of \def\@order@nd
```

**cutr@nge** If the given range of random numbers exceeds the possibilities of L<sup>A</sup>T<sub>E</sub>X (the limit is  $2^{31} - 1$ ), then the value of the T<sub>E</sub>X-counter *@tempc@nta* will be less than zero and the right border will be adjusted.

```
135 \def\cutr@nge@nd{%
136   \ifnum \l@st < \z@ \else
137     \@tempc@ntb = -2147483646 % -2^31 + 2
138     \@tempc@nta = \f@rst
139     \advance \@tempc@ntb \l@st
140     \multiply \@tempc@ntb \m@ne
141     \advance \@tempc@nta \@tempc@ntb
142     \ifnum \@tempc@nta < \z@%
143       \PackageWarning{lcg}{Range contains too many numbers
144       -- right border reset to largest possible value}%
145       \advance \l@st \@tempc@nta
146     \fi%
147     \fi%
148 }% end of \checkr@nge
```

## 4.5 Macros for random number generation

**rand** The command `\rand` calls the internal command `\r@nd` which stores *s* random number (full range) within the counter *cr@nd*. If the condition

$$cr@nd \leq (l@st - f@rst + 1) \cdot \frac{2^{31} - 1}{l@st - f@rst + 1}$$



holds, `cr@nd` will be transformed to the given range:

$$f@rst + cr@nd - (l@st - f@rst + 1) \cdot \frac{cr@nd}{l@st - f@rst + 1}$$

and the result stored in the corresponding counter and otherwise `\rand` calls itself till the condition is satisfied. It's important to notice that the result of the division of two integers is again an integer (the fraction part is lost)!

```

149 \def\rand{%
150   \r@nd%
151   \@tempcnta
152   \@tempcntb
153   \@tempcnta = \f@rst
154   \@tempcntb = \l@st
155   \multiply \@tempcnta \m@ne
156   \advance \@tempcntb \@tempcnta
157   \advance \@tempcntb \@ne           %l@st-f@rst+1
158   \@tempcnta = 2147483647
159   \divide \@tempcnta \@tempcntb
160   \multiply \@tempcnta \@tempcntb
161   \ifnum \cr@nd > \@tempcnta
162     \rand%
163   \else
164     \setcounter{\r@ndcountername}{\cr@nd}%
165     \@tempcnta = \cr@nd
166     \divide \@tempcnta \@tempcntb
167     \multiply \@tempcnta \@tempcntb
168     \multiply \@tempcnta \m@ne
169     \addtocounter{\r@ndcountername}{\@tempcnta}%
170     \addtocounter{\r@ndcountername}{\f@rst}%
171   \fi
172 } % end of \rand

```

`r@nd` The command `\r@nd` generates pseudo random numbers within the range 1 to  $2^{31} - 1$  Schrage's method and stores them in the counter `cr@nd`:

```

173 \def\r@nd{%
174   \ifnum \cr@nd < \@ne%           then ... initialize generator
175     \cr@nd = \the\time
176     \advance \cr@nd \inputlineno
177     \multiply \cr@nd \thepage
178     \advance \cr@nd \the\year
179     \multiply \cr@nd \the\month
180     \multiply \cr@nd \the\day
181     \advance \cr@nd \inputlineno
182     \if \qui@t y%
183     \else
184       \typeout{Random number generator initialized to \the\cr@nd}%
185     \fi
186   \r@nd%

```

```

187 \else                                     % else ... generate new number
188   \@tempcnta = \cr@nd
189   \divide \@tempcnta 127773               % \@tempcnta = floor(z/q)
190   \@tempcntb = \@tempcnta                % \@tempcntb = floor(z/q)
191   \multiply \@tempcnta -2836             % \@tempcnta = -r*floor(z/q)
192   \multiply \@tempcntb -127773          % \@tempcntb = -q*floor(z/q)
193   \advance \cr@nd \@tempcntb           % cr@nd = z mod q
194   \multiply \cr@nd 16807                 % cr@nd = a * (z mod q)
195   \advance \cr@nd \@tempcnta           % cr@nd = a*z mod m
196   \ifnum \cr@nd < \z@%
197     \advance \cr@nd 2147483647 % cr@nd = (a*z mod m) > 0
198   \fi
199 \fi
200 }%           end of \r@nd

```

## 4.6 Initialization

```

201 \initr@nd      % initialize the package

```