# Chapter 3. Random Walks on Groups

## A. Examples

A fair number of real world problems lead to random walks on groups. This section contains examples. It is followed by more explicit mathematical formulations and computations.

### 1. Random walk on the circle and random number generation

Think of $Z_p$ (the integers mod $p$) as $p$ points wrapped around a discrete circle. The simplest random walk is a particle that moves left or right, each with probability $\frac{1}{2}$. We can ask: how many steps does it take the particle to reach a given site? How many steps does it take the particle to hit every site? After how many steps is the distribution of the particle close to random? In Section C, we show that the answer to all of these questions is about $p^2$.

A class of related problems arises in computer generation of pseudo random numbers based on the recurrence $X_{k+1} = aX_k + b (\text{mod } p)$ where $p$ is a fixed number (often $2^{32}$ or the prime $2^{31} - 1$) and $a$ and $b$ are chosen so that the sequence $X_0 = 0$, $X_1$, $X_2, \ldots,$ has properties resembling a random sequence. An extensive discussion of these matters is in Knuth (1981).

Of course, the sequence $X_k$ is deterministic and exhibits many regular aspects. To increase randomness several different generators may be combined or "shuffled." One way of shuffling is based on the recurrence $X_{k+1} = a_k X_k + b_k$ (mod $p$) where $(a_k, b_k)$ might be the output of another generator or might be the result of a "true random" source as produced by electrical or radioactive noise. We will study how a small amount of randomness for $a$ and $b$ spreads out to randomness for the sequence $X_k$.

If $a_k \equiv 1$ and $b_k$ takes values $\pm 1$ with probability $\frac{1}{2}$, we have a simple random walk. If $a_k \neq 1$ is fixed but nonrandom, the resulting process can be analyzed by using Fourier analysis on $Z_p$. In Section C we show that if $a_k \equiv 2$, then about $\log p \log\log p$ steps are enough to force the distribution of $X_k$ to be close to uniform (with $b_k$ taking values $0$, $\pm 1$ uniformly). This is a great deal faster than the $p^2$ steps required when $a_k \equiv 1$. If $a_k \equiv 3$, then $\log p$ steps are enough.

What if $a_k$ is random? Then it is natural to study the problem as a random walk on $A_p$ - the affine group mod $p$. This is the set of pairs $(a, b)$ with $a, b \in Z_p$, $a \neq 0$, $gcd(a, p) = 1$. Multiplication is defined by

$$(a, b)(c, d) = (ac,\ ad + b).$$

Some results are in Example 4 of Section C, but many simple variants are unsolved.