1026-11-191 **Par Kurlberg***, Department of Mathematics, KTH, 10044 Stockholm, Sweden, and **Carl Pomerance**, Department of Mathematics, Dartmouth College, Hanover, NH 03755-3551. *On the period of the linear congruential and power generators.*

Given coprime integers b and n, let ord(b,n) be the multiplicative order of b modulo n. The length of the periods of some popular pseuderandom number generators (the power generator, the linear congruential generato, and the Blum-Blum-Shub generator) turns out to be related to ord(b,n) for apropriately chosen b and n. (Note that the case n=p, where p is prime is related to Artin's primitive root conjecture.) We will give lower bounds on ord(b,n) for b fixed and n ranging over certain subsets of the integers, e.g., the set of primes, the set of "RSA moduli" (i.e., products of two primes), the full set of integers, and the images of these sets under the Carmichael lambda function. Assuming the generalized Riemann hypothesis, we can show that the order is essentially maximal for almost all n in the above mentioned subsets. We can also give weaker unconditional bounds. The lower bounds in the case of RSA moduli shows that certain "cycling attacks" on the RSA crypto system are ineffective. (Received February 26, 2007)