Monte Carlo Methods for Index Computation (mod p) By J. M. Pollard Abstract. We describe some novel methods to compute the index of any integer relative to a given primitive root of a prime p. Our first method avoids the use of stored tables and apparently requires 0(p) operations. Our second algorithm, which may be regarded as a method of catching kangaroos, is applicable when the index is known to lie in a certain interval; it requires 0(w) operations for an interval of width w, but does not have complete certainty of success. It has several possible areas of application, including the factorization of integers. 1. A Rho Method for Index Computation. The concept of a random mapping of a finite set is used by Knuth [1, pp. 7-8] to explain the behavior of a type of random number generator. A sequence obtained by iterating such a function in a set of p elements is 'rho-shaped' with a tail and cycle which are random variables with expectation close to (1) VW/8) - 0.6267 Vp, (as shown first in [2], [3]). Recently [4], we proposed that this theory be applied to recurrence relations such as (2) x/+1 = x2±l (modp), and showed how a very simple factorization method results, in which a prime factor p of a number can be found in only 0(p'A) operations. The method has been further discussed by Guy [5] and Devitt [6], who have found it suitable for use in programmable calculators. We now suggest that the same theory can be applied to sequences such as x0 = 1, [0< x,.< x? > (mod p) for < ^p < x,. < ^p V jP <x¡

< xt < p. The idea of this definition, which can be varied in many ways, is that the three possibilities are chosen in a 'random' manner, and the resulting sequence is sufficiently 'complicated' to be regarded as a random mapping; in addition, all the Xj axe easily expressible in terms of q and r. As a consequence, we can give an Received May 1, 1977; revised November 18, 1977. AMS (MOS) subject classifications (1970). Primary 10-04, 10A10, 12C99. Key words and phrases. Indices, primitive roots, finite fields.   algorithm to compute the index of q in 0(p) operations, and with a very small storage requirement. The method is an alternative to the following method of D. Shanks (see [7, pp. 9, 575-576]). Put m = [\fp] + 1, and rewrite the equation q=ram + b (mod p), (0 < a, b < m) as qr~b = ram (mod p). To solve this, compute the sets qr~b and ram (mod p), and find a common member by sorting both sets (the idea has other applications [8], [9]). The method is of order p^log p and requires storage 0(pVl). The main interest of our method, which may be slightly faster, is that it shows that such storage is unnecessary. We are not aware of any particular need for such index calculations, but believe that the ideas may have other applications (such as those described in the last section). Diffie and Hellman [10] conjecture, and hope, that the estimate 0(p'/2) is the best possible (for a general prime). But there is some possibility of obtaining a more powerful method from the ideas of Western and Miller, to which Miller [11] has recently drawn attention; we sketch a possible approach. We generate the sequence rl (mod p) and (for r > p) try to find numbers which factor entirely into primes below some limit (as Brillhart and Morrison [12] do with their Ö,)—or perhaps primes whose epacts [4], [5] are below some limit, the factoring being by our method mentioned earlier. After a sufficient number of successes, we compute the indices of these primes as the solution of a set of linear equations (mod p - 1). Then, to obtain the index of an arbitrary q, we need only find one number qr' (mod p) which factors into this set of primes. Continuing the description of our method based on (3), we define sequences (a¡) and (b¡) such that (4) x,. = qahbi (mod p). Thus, we set a0 = 0 and aj+, = a¡ + 1, 2a¡, or a¡ (mod p - 1), according to the three cases in (3); similarly, we put bQ = 0 and bi+x = b¡, 2b¡ or b¡ + 1 (mod p - 1). We introduce an idea of R. W. Floyd [1, p. 4] which was used in [4] ; we will have xt = x2/. just when / is a positive multiple of the cycle length and not less than the tail length. The least

such i has been named the epact [5]. For a true random mapping, it has expectation close to V(7TSp/288)^1.0308Vp", and we conjectured [4] that this holds also for sequences of type (2). For (3), we believe that the constant may be different, but not by much. Thus, a calculation on 50 primes near 104 gave a mean value for e(p)/pVi of 1.08. The individual epacts are quite variable, some being as large as 3y/p~, as they are for the epacts associated with (2) for which Guy [5] conjectures that max e(p) ~(x lnx),/2 as x —* °°. p n1 '3, by a version of Fermat's method [1], [5]. Let n = pc7, where M

< n/M, and let (a, n) = 1 ; then the equation a2x=an + i (modn), has a solution with 2nh < 2x < M + n/M, namely x = xh(p + q). We can find the solution (or fail to find it) in 0((n/M)Vl) steps and hence factor n (sometimes). In calling this method the Square Root Sieve we are assuming that it is possible to introduce some degree of sieving [13], [14], without losing the advantage of the square root. Certainly some improvement, at least, is possible; thus [5], if n = 11 (mod 12), thenx = 0 or 6 (mod 12) according as n = -1 or 3 (mod 8), and we can easily make use of such a restriction on x to a single residue class. 924 J. M. POLLARD We have not been able to experiment with this method. We remark that it likes best a number composed of two nearly equal prime factors, which the rho method [4] likes worst. Acknowledgements. I am grateful to Professor Donald E. Knuth for some comments and references, and to the referee for his criticisms; also to the editors of Scientific American for some timely information about kangaroos and cryptography (August 1977). Added in Proof. We understand that our lambda method is already known to conjurors as 'Kruskal's principle' (see Scientific American, February 1978). We doubt if they use a more sophisticated version, with two herds of kangaroos each confined to a residue class, with which we have obtained the factorization: 272 - 3 = 83 x 131 x 294971519 x 1472414939. Mathematics Department Plessey Telecommunications Research Taplow Court, Maidenhead Berkshire, England 1. D. E. KN