MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 155–172

On Factorisation, with a Suggested New Approach

By J. C. P. Miller

To my friend of several decades, D. H. Lehmer

Abstract. This paper gives a brief survey of methods based mainly on Fermat's Theorem, for testing and establishing primality of large integers. It gives an extension of the Fermat-Lucas-Lehmer Theorems which allows us to establish primality, or to factorise composites, in cases where the Carmichael λ-exponent is known (or a multiple or submultiple of it, by a moderate factor). The main part of the paper is concerned with describing a method for determining the λ-exponent in cases where the Fermat test is *not* satisfied. This method is a variation of A. E. Western's method for finding indices and primitive roots, based on congruences $N = a + b$, where N is the number whose exponent is required, and both a and b are A_k-numbers, that is, having no factor larger than p_k, the kth prime. The most onerous problem lies in the finding of a sufficient number of congruences (at least k) and in the choice of a suitable value of k. The determination of the approximate number of A_k-splittings available is considered, to allow an estimate of the amount of labour (human or electronic) needed to be made.

The final suggestion, rather inconclusive, is that the method has possibilities worth exploring further and may be as economical, after development, as existing methods, and possibly more so when N is large.

1. The proof of primality, or the factorisation, of large integers has been a subject of major interest to mathematicians and others for centuries. It always remains a difficult problem because any method that becomes available is always pushed speedily to its limits.

The straightforward method for deciding both versions of the problem completely is to use the fact that the number N is either a prime, or has a factor not exceeding $\sqrt{N}$. We may therefore try to divide N by each prime up to $\sqrt{N}$; this eventually solves the problem in a number of operations of maximum order $\sqrt{N}$ – slightly less if a list of primes is available. If we have no list of primes we can try by using all odd numbers, possibly excluding those which themselves have an obvious small factor. However the number of operations is still basically of order $\sqrt{N}$.

There are other methods, for example involving quadratic forms $N = Ax^2 + By^2$, x, y integers, that depend on trials with a similar number of operations.

Such methods, with number of operations of basic order $\sqrt{N}$, although this may, in a particular case of actual factorisation, turn out to be a considerable overestimate,

Received August 15, 1974.

AMS (MOS) subject classifications (1970). Primary 10A10, 10A25; Secondary 10–04.

Key words and phrases. Factorisation of integers, indices, exponents.

do, in fact, need the full number of operations when proof of primality is the final result. They are considered as virtually useless for all except small numbers, or for removing small factors, even with a fast computer. The practical limit is perhaps about 10^{10}—this estimate may be useful for comparison. In fact a method of order $\sqrt{N}$ is hardly regarded as a method at all.

2. For proof of primality—the worst case for methods of basic order $\sqrt{N}$—we have a much faster alternative in most cases. This is the use of Fermat's Theorem, which states that:

If N is prime, then

$$N | a^{N-1} - 1 \tag{2.1}$$

for all a not divisible by N. Alternatively:

If N is prime, then

$$N | a^{N} - a \tag{2.2}$$

for all a.

If (2.1) is satisfied for a particular base a, prime to N, we shall say that N satisfies a Fermat Test for base a, or that it satisfies the F_a-test.

Unfortunately, as it stands, satisfaction by N of either of these test relations is not enough to prove primality, since the direct converse of Fermat's Theorem is not true. Exceptional integers, N, composite, but satisfying (2.1) or (2.2), exist and are of two kinds:

(i) *Poulet Numbers.* A number N is defined to be a *Poulet number* if it is composite, but satisfies an F_a-test for some a, prime to N. The name is chosen because Poulet (1928) produced the first substantial list of P_2-numbers, although Sarrus seems the first to have reported one in 1819, according to Lehmer (1936). Although Poulet's list was confined to base 2, it seems reasonable to extend the name to composite numbers satisfying an F_a-test, and to call them P_a-numbers, with the general name P-numbers for composite numbers satisfying an F-test for at least one, but not all, bases.

(ii) *Carmichael Numbers.* A number N is defined to be a *Carmichael number* if it is composite but satisfies

$$N | a^{N} - a \quad \text{for } \textit{all } a.$$

We see that if $(N, a) = 1$, then $N | a^{N-1} - 1$.

Carmichael numbers must have at least three factors, Poulet numbers may have only two. Either may have a larger number of factors.

3. By Fermat's Theorem it is clear that if $N \nmid a^{N-1} - 1$ for some a prime to N, then N is composite. However if, conversely, $N | a^{N-1} - 1$ then, although N is probably prime, and with high probability, we cannot be sure that it is not a Poulet or a Carmichael number. We need an extended test.

Now, there exists a *least exponent* ξ for given N, a with $(a, N) = 1$, such that $N|a^{\xi} - 1$, and, if N satisfies the F_a-test (2.1), then clearly $\xi|N - 1$. Also, if N is prime, we know that there exists a base g, such that $N|g^{N-1} - 1$ with $N - 1$ at the *least* exponent, i.e., there exists a *primitive root* $a = g$ for N. In fact, there are several primitive roots, an individual set for each prime N.

There exists also a least exponent ξ for $N, a, (a, N) = 1$, when N is composite. If $N = p_1p_2$, a product of two distinct primes, then

$$\xi|\mathrm{LCM}(p_1 - 1, p_2 - 1)$$

and, generally, if $N = \Pi_{i=1}^{h} p_i^{\delta_i}$, $\delta_i \geqslant 1$, and $M = \Pi_{i=1}^{h} p_i$ then

$$\xi|\mathrm{LCM}(N/M, p_1 - 1, p_2 - 1, \cdots, p_h - 1) = \lambda(N).$$

Here $\lambda(N)$ is Carmichael's λ-function or λ-exponent, except that for $p_1 = 2, \delta_1 = 2$, an extra factor 2 is needed; this does not concern us, since we always have odd N. Note that ξ depends on a, though $\lambda(N)$ does not. See Carmichael (1914, p. 52).

A Poulet number or P_a-number occurs when $\xi(a)|N - 1$, and a Carmichael number occurs when $\lambda(N)|N - 1$.

When N is composite, we see that $\lambda(N)$ is always less than $N - 1$. Thus if we can show that N satisfies (2.1) for some a, and $N - 1$ is the least exponent, N must be prime, that is, N is prime if we can find a prime to N such that $N|a^{N-1} - 1$ and $N \nmid a^{(N-1)/p_i} - 1$ for every $p_i|N$. This is the theorem of Lucas; see Lehmer (1936).

4. Lehmer (1933), (1939) analyses the Lucas theorem more closely in his Theorem A (1933) and Theorem 1 (1939). We do not quote these, but instead combine and extend them to cover λ-exponents, and submultiples of λ-exponents, as well.

THEOREM. *If* N *has* λ*-exponent* $\lambda(N)$, *and* $q^{\alpha} \| \lambda(N)$, q *prime*, $\alpha \geqslant 1$, *and if, further,* $N|X_\beta$, $\beta < \alpha$, *but* $N \nmid X_{\beta-1}$ *where* $X_\beta = a^{Y_\beta} - 1$, $Y_\beta = \lambda(N)/q^{\alpha-\beta}$, *then either*

(a) $(N, X_\beta) = 1$, *and each prime factor of* N *is of the form* $kq^\beta + 1$;

or (b) $(N, X_\beta) \neq 1$, *and is a proper factor of* N.

The proof is simple, for $Y_\beta = qY_{\beta-1}$, and so

$$X_\beta = a^{Y_\beta} - 1 = (a^{Y_{\beta-1}} - 1)\left(\sum_{0}^{q-1} a^{kY_{\beta-1}}\right)$$

and each prime factor of N, which divides X_β, must divide one or other of the factors on the right. In case (a) N divides the second factor, and the exponent for each of its prime factors has q^β as an essential component, whence the first conclusion. In case (b) at least one, but *not all*, of the factors of N divide $X_{\beta-1}$

so that

$$(N, X_{\beta-1})|N \quad \text{with} \quad 1 < (N, X_{\beta-1}) < N.$$

We note particularly that if we test several prime factors $q = q_i$ of $\lambda(N)$, we can use individual $a = a_i$ for each; this is important for the *complete* factorisation of N.

COROLLARY. Selfridge (see Brillhart and Selfridge (1967)) gives a theorem: *Let N be an odd integer > 1. If $N - 1 = \Pi q_i^{\alpha_i}$, q_i prime, and if for each q_i there exists an a_i for which $a_i^{N-1} \equiv 1 \pmod N$, but $a_i^{(N-1)/q_i} \not\equiv 1 \pmod N$, then N is prime.*

The Selfridge theorem is just equivalent to a demonstration that $N - 1$ is the least exponent for some primitive root g. This is a if all $a_i = a$, otherwise it is unknown. We are, however, mainly interested in factorisation in this paper, and can adapt the test, instead, to *find* the least exponent ξ for any given a for which (2.1) is found to hold. In this case we know that $\xi|N - 1$, and we wish to know which factors of the exponent

$$N - 1 = 2^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$$

may be omitted, and still leave $N|a^{\xi'} - 1$ where

$$\xi' = 2^{\beta'_1} q_2^{\beta'_2} \cdots q_k^{\beta'_k} .$$

The exponent ξ is achieved when no single β_i, i.e., min β'_i can be reduced without destroying divisibility by N.

5. We now discuss details and economics of this process:

First we consider as a unit process the evaluation of $a^n \pmod N$. We write $n = \Sigma_{i=0}^{\kappa} \gamma_i 2^i$, $\gamma_i = 0$ or 1, a binary digit. Starting with $r_0 = 1$, we evaluate

$$r_{i+1} = a^{\gamma_i} r_i^2 \qquad \pmod N.$$

The number of digits in each multiplication is set by N; we suppose this has H digits, or that it is an h-length machine number, where machine numbers have l digits and $h \geqslant H/l > h - 1$. Evaluation of r_{i+1} involves two multiplications, and two divisions for remainder (mod N). At first sight we are concerned with $2H$ digit or $2h$-length products, but by interweaving multilength multiplication and division processes we can manage with $h + 1$ length calculations (virtually h length for h not small). Also if $\gamma_i = 0$ (as it will be in about half the cases) there is only one multiplication and division per step. Each step involves h-length or H-digit calculations, i.e., $O(\log_2 N)^2$ of work. The number of steps is κ, which is $O(\log_2 n)$. Thus a unit process costs $O(\log_2 N)^2 \log_2 n$.

Now suppose that we are testing a^X (mod N), where

$$X = 2^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$$

where we know that $a^X \equiv 1$ (mod N), and need the least ξ such that $a^\xi \equiv 1$ (mod N). Clearly $\xi | X$. We need to evaluate a^X (mod N) with each separate factor $q_i^{\alpha_i}$ of X used last, in order to find how many factors q_i, say $q_i^{\beta_i}$, are necessary to give 1 (mod N) when all other factors needed are present.

Consider, for illustration, eight factors, A = 2^{α_1}, B = $q_2^{\alpha_2}$, C, D, E, F, G, H = $q_8^{\alpha_8}$ with X = ABCDEFGH. We can develop X and a^X by using factors ordered as in the following scheme, in which arrows indicate actual calculations

$$\begin{tikzcd}
{} \arrow[r] & \mathrm{A} \arrow[r] & \mathrm{B} \arrow[r] & \mathrm{C} \arrow[r] & \mathrm{D} \arrow[r] \arrow[ddr] & \mathrm{E} \arrow[r] & \mathrm{F} \arrow[r] \arrow[dr] & \mathrm{G} \arrow[r] & \mathrm{H} \\
 & & & & & & & \mathrm{H} \arrow[r] & \mathrm{G} \\
 & & & & & \mathrm{G} \arrow[r] & \mathrm{H} \arrow[r] \arrow[dr] & \mathrm{E} \arrow[r] & \mathrm{F} \\
 & & & & & & & \mathrm{F} \arrow[r] & \mathrm{E} \\
{} \arrow[r] & \mathrm{E} \arrow[r] & \mathrm{F} \arrow[r] & \mathrm{G} \arrow[r] & \mathrm{H} \arrow[r] \arrow[ddr] & \mathrm{A} \arrow[r] & \mathrm{B} \arrow[r] \arrow[dr] & \mathrm{C} \arrow[r] & \mathrm{D} \\
 & & & & & & & \mathrm{D} \arrow[r] & \mathrm{C} \\
 & & & & & \mathrm{C} \arrow[r] & \mathrm{D} \arrow[r] \arrow[dr] & \mathrm{A} \arrow[r] & \mathrm{B} \\
 & & & & & & & \mathrm{B} \arrow[r] & \mathrm{A}
\end{tikzcd}$$

It will be seen that each letter is used exactly four times, i.e., $(1 + \log_2 \nu)$ times, where ν is the number of distinct prime factors, and is, as here, a power 2^λ. Each pair of factors AB, CD, EF, GH comes individually to the right, and is individually inverted. To allow for $\nu = 2^\lambda + \mu$, we take 2μ of the factors as pairs $S_1 S_2$, and, when any such pair (treated as a whole unit until then) comes to the right, it is inverted, giving two extra units in the count. Thus $2^\lambda - \mu$ letters occur $\lambda + 1$ times and 2μ letters occur $\lambda + 2$ times, for $\mu < 2^\lambda$.

We are, however, less interested in the number of such operations, than in the total work. From above estimates, this is

$$\sum_S \lambda' (\log_2 N)^2 \log_2 S, \qquad S = \mathrm{A, B, C, D, E, F, G, H},$$

with $\lambda' = \lambda + 1$ or λ, λ = integer next greater then $\log_2 \nu$. This is near $\log_2 \nu \times (\log_2 N)^2 \log_2 X$ since X is the product of all the S. Thus the cost of the operation is $O((\log_2 N)^2 \log_2 X \log_2 \nu)$ or essentially $(\log_2 N)^3$ since X is usually $O(N)$, and $\log_2 \nu$ very small.

In individual practical cases we can improve things a little further, by splitting X into two parts nearly as equal as possible, and doing the same for each part as we progress in the separation into distinct factors. In this way we may have individual prime powers at more than two levels of splitting, but we shall have long factors at lower levels used less often, and shorter easy factors used more often.

6. We now indicate how the processes outlined above may be used for factorisation, as well as for proof of primality.

To test a number N:

1. Choose a base a, and test whether N is F_a.

If not, N is composite; ⟶ 6.

If N is F_a, then it may be prime, or a Fermat or a Carmichael number; ⟶ 2.

2. Choose another base b, prime to a, and test if N is F_b.

If not, N is composite; ⟶ 6.

This second test is not likely to succeed as well if N is a Fermat number, but will do so if it is a Carmichael number or a prime, If then, N is F_b (not ruling out the possibility that it is also a P_b-number); ⟶ 3.

3. By a method such as that described in Section 5, determine least exponents ξ_a, ξ_b for bases a and b.

If either exponent, or their LCM is $N-1$, then N is prime; ⟶ 5.

If $\mathrm{LCM}(\xi_a, \xi_b)$ is large, i.e., $N-1$ is a small multiple thereof, then N is probably prime; ⟶ 4.

If LCM is small; ⟶ 6.

4. Try other bases c, d. It is best, but not essential to have a, b, c, d, coprime in pairs. Try until $\mathrm{LCM}(\xi_a, \xi_b, \xi_c, \xi_d) = N-1$; this would prove that N is prime; ⟶ 5.

If the LCM remains persistently $<N-1$ (for a Carmichael number it will remain much smaller) we must attempt factorisation; ⟶ 6.

5. N *is prime.*

6. N is composite, certainly or very probably. *We attempt factorisation.*

To do this there are many methods. We propose a new approach. This is to use the exponent $\lambda(N)$ defined in Section 3.

If one or more F-tests have succeeded we may know enough to achieve factorisation. If not, we must attempt to find the exponent, an outstanding problem in number theory of great difficulty in general. We first consider, in Sections 7 and 8, how to use the exponent when it is known. Then, from Section 9 onward, we consider a possible strategy for finding $\lambda(N)$.

7. Factorisation of N, When its Greatest Exponent X for any Base a is Known. We shall confine ourselves to the case where N is square-free. If this is not the case, suppose that

$$N = \prod_{i=1}^{n} p_i^{\delta_i} \quad \text{and} \quad M = \prod_{i=1}^{n} p_i .$$

Then we know that

$$\lambda(N) = \mathrm{LCM}(N/M,\ p_1 - 1, p_2 - 1, \cdots, p_n - 1).$$

We are assuming further that N has no small factors (which are easy to find and remove) so that $p_1 \neq 2$. In fact we shall assume that N/M and $\mathrm{LCM}(p_1 - 1, p_2 - 1, \cdots, p_h - 1) = Y$ are coprime. It is always best to test for small factors before starting a major computing operation. Thus

$$\lambda(N) = \frac{N}{M} Y = \prod_{i=1}^{n} p_i^{\delta_i - 1}\ Y,$$

$$P = (N,\ \lambda(N)) = N/M, \qquad M = N/P,$$

Next

$$Q = (M,\ \lambda(N)) = \prod_{\delta_i > 1} p_i .$$

So M/Q is a square-free product of primes occurring only once in N.

We then proceed with P/Q replacing P, again isolating square-free factors; thus $R = (P/Q,\ Q)$ and Q/R gives the product of primes occurring exactly squared in N. Continue thus until N is completely analysed into sets of factors appearing with equal degree, still to be separated.

We may now assume that $N = \Pi_{i=1}^{h} p_i$, a product of odd primes and $\lambda(N) = \mathrm{LCM}(p_1 - 1, p_2 - 1, \cdots, p_h - 1)$, with $(\lambda(N), N) = 1$.

Write $\lambda(N) = 2^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots q_k^{\beta_k}$. The prime $q_1 = 2$ is certainly present, as it occurs in every $p_i - 1$. Suppose that

$$q_j^{\beta_j} \,\|\, p_i - 1; \qquad q_j^{\beta_j} \nmid p_{i'} - 1, \qquad i' \neq i,$$

and consider $\xi' = \lambda(N)/q_j$: Then

$$p_{i'} - 1 \mid \lambda(N)/q_j, \qquad i' \neq i; \qquad p_i - 1 \nmid \lambda(N)/q_j,$$

since the last factor q_j is needed only for $p_i - 1$. So there does exist a base a such that

$$a^{\xi} \equiv 1 \quad (\mathrm{mod}\ p_{i'}),\ i' \neq i,$$
$$a^{\xi} \not\equiv 1 \quad (\mathrm{mod}\ p_i).$$

So if $r_\xi \equiv a^\xi$ (mod N) then $p_{i'} \mid r_\xi - 1, i' \neq i, p_i \nmid r_\xi - 1$ and we must have $p_i = N/(N,\ r_\xi - 1)$ and p_i is isolated. Other factors may be similarly isolated.

8. As an example consider $N = 12999\ 63601$. This is a Carmichael number and we shall assume that we know that $\lambda(N) = 3600$. We seek the factors.

We take $a = 2$ and use factors of

$$\lambda(N) = 3600 = 5^2 \cdot 3^2 \cdot 2^4$$

with the initial order as indicated, to evaluate $r_i = a^i \pmod N$.

$a = 2$				$a = 3$			
i	r_i	i	r_i	i	r_i	i	r_i
1	2	50	1320 52923	1	3	50	− 2042 75117
5	32	100	1363 82527	5	243	100	1190 31680
25	335 54432	300	1	25	− 2876 58409	300	2338 63525
75	− 2078 20991			75	− 238 79532	900	1
225	2164 80201	12	4096	225	− 2143 17200		
450	86 59209	60	259 78648	450	86 59209		
900	1	300	1	900	1		

Values are given for $i = 5, 5^2, 3 \cdot 5^2, 3^2 \cdot 5^2, 2 \cdot 3^2 \cdot 5^2, 2^2 \cdot 3^2 \cdot 5^2$. The last gives $r_{900} = 1$. So 2^2 only, and not 2^4, is needed. We test $(r_{450} - 1, N) =$ 1082401; the other factor of N is 1201, which can be seen to be prime.

Now alter the order of the factors (second column-pair above). This shows $r_{300} = 1$, so the second factor 3 is not needed. Now we check $(r_{100} - 1, N) =$ 1082401–again!

To complete our evaluation of the exponent ξ for $a = 2$ we must test r_{12} and r_{60} (see above); we see then that $\xi = 300$ and that $(r_{60} - 1, N) = 1$, which is no help.

We now try $a = 3$ (last two column-pairs above) and find

$$(r_{300} - 1, N) = 721801, \qquad N/721801 = 1801$$

from this, without testing further residues, we find $N = 601 \cdot 1201 \cdot 1801$. These are all prime–which has to be checked!

This example has been streamlined and left incomplete. It has been given in order to exhibit the use of penultimate residues.

In general the order in which factors are used in developing a^X is not of prime importance. It may, however be worthwhile to suggest that if, for any reason, it is suspected that $\xi \ll N$, it is perhaps worthwhile to start with factors of $N - 1$ (if $\xi | N - 1$, i.e. if N is F_a) in ascending order, since it is then likely that some of the large factors may not be needed at all. Thus, in our example if we had started on factors of $N - 1 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 13 \cdot 47 \cdot 197$ in that order, we should not have needed to use the last three at all.

Most cases should yield to treatment of this sort, once the value of $\lambda(N)$ is known. It should also be fairly simple if at least one or two ξ_a are known that are not much less than $\lambda(N)$. The difficult case is where just one ξ_a is known, much less than $\lambda(N)$, and nothing else. Thus, for example $2^{101} - 1$ is composite, so that both factors and their product have $\xi_2 = 101$, but it is very hard to find ξ_a for any other a, and unless we do, we cannot separate the factors by the method outlined above.

This brings us to the major problem of this paper: How does one find $\lambda(N)$ when it does *not* divide $N - 1$?

9. A. E. Western (Western and Miller, 1968) has devised a method for determining indices and primitive roots for modulus a prime, and has found it feasible, even easy, for use with primes up to at least 10^7. It can readily be extended to composite moduli, and provides the value of $\lambda(N)$ directly, or maybe a moderate multiple of $\lambda(N)$.

For every N, there exists $\lambda(N)$, the Carmichael exponent. This exponent divides the Euler function $\phi(n)$, and is equal to it only when N is of the form p^α or $2p^\alpha$, where p is prime. It may be noted that every prime factor of $\phi(N)$ and so of $\phi(N)/\lambda(N)$ is a divisor of $\lambda(N)$, i.e., $\phi(N)$ contains all and only primes that are factors of $\lambda(N)$ possibly to a higher power, maybe much higher, than in $\lambda(N)$.

For each a prime to N, there is a least exponent ξ_a such that $a^{\xi_a} = 1$ (mod N), where $\xi_a | \lambda(N)$. There exist values of a such that $\xi_a = \lambda(N)$, these are Carmichael's *primitive* λ-*roots*. If $a = g$ is such a primitive λ-root, then g^i, $i = 0(1)\lambda$, generates, modulo N, $\lambda(N)$ distinct residues $r_i < N$ and prime to N, i.e. $\lambda(N)$ members of the group of $\phi(N)$ such residues. This is the complete group only if $N = p^\alpha$ or $2p^\alpha$; the group is then cyclic. Otherwise the group needs more than one generator. In this case the first generator, as we may call it, can be chosen to be a primitive λ-root, with exponent $\lambda(N)$. The other generators will all have exponent *dividing* $\lambda(N)$; that is, $\lambda(N)$ is a period for every generator.

For a cyclic group, with a single generator g we may use its exponent i as the index of the corresponding r_i and write $i = \operatorname{ind}_g r_i$ (mod $N - 1$), since $g^{N-1} = 1$, and $\operatorname{ind}_g g^{N-1} = \operatorname{ind}_g 1 = 0$. In this way as in Western and Miller (1968), a system of indices may be used for calculation.

For groups with several generators, the system can be extended. Each residue r can be expressed as $g_1^{i_1} h_2^{i_2} h_3^{i_3} \cdots$ where g_1 is a primitive λ-root, and $h_2, h_3, \cdots$ the remaining generators. Then ind r is the vector $(i_1, i_2, i_3, \cdots)$, and we know that $\lambda(N) \cdot \operatorname{ind} r = 0$ (mod $\lambda(N)$) in all cases. In practice, we have to *find* the least multiplier X, for which $X \operatorname{ind} r = 0$ (mod $\lambda(N)$), or any small multiple of it.

10. To achieve this, when $\lambda(N)$ is unknown, we work with indices in the manner devised by Western. We write

$$cN = a + b \tag{10.1}$$

which is equivalent to

$$\text{ind } a \equiv \text{ind}(-b) \pmod{\lambda(N)}. \tag{10.2}$$

The pairs (a, b) are very numerous; we need $M + \delta$ relations involving M primes, so we need to find those which are products of small primes only. For example, with primes to 37, we have 13 indices to deal with (we must include that of -1), so we need 13 identities involving these indices. The extra δ relations (δ a small integer) may be needed to allow for redundancies. We want $M = 1$, of course, but such a relation is too hard to find directly. It is much easier to find relations with large M (e.g., $M = 10000$), but then it is troublesome to reduce them. Western used basically $m = 12$ to 15, with an extra 20 primes or so used sparingly, i.e.,only one to a relation. For present day needs with a computer, I estimate that we may need $M = 200$ to 300.

We can reduce the relations found to the form

$$X_q \text{ ind } q \equiv 0 \pmod{\lambda(N)} \tag{10.3}$$

by direct elimination. Then X_q contains all factors of $\lambda(N)$ not in ind q (in practice only the primitive element g_1 of the index is important for our purpose). We need, then, some q such that ind q is prime to $\lambda(N)$. With $M = 13$ we have twelve primes, 2 to 37, to work with, and can reduce to form (10.3) for each of them. From these, we should be able to obtain, collectively, the complete value of $\lambda(N)$. We should certainly be able to get enough values of ξ_q to complete the factorisation of N as in Sections 7, 8.

A way of achieving all this is exhibited in full detail in the Introduction to Western and Miller (1968). It is true that there it was known that $\lambda(N) = N - 1$, but this plays no part in the finding and reduction of congruences. The final stages, of course, diverge.

Examples. One or two small illustrations of indices with more than one generator may be helpful.

(i) $N = 91 = 7 \times 13$ $\phi(N) = 6 \times 12 = 72$ $\lambda(N) = \text{LCM}(6, 12) = 12$

a	1	2	3	5	6	10	11	12 ···	27	29 ···	34
ξ_a	1	12	6	12	12	6	12	6 ···	2	3 ···	4

etc.

We find that $2^\alpha 3^\beta$, $0 \leqslant \alpha \leqslant 11$, $0 \leqslant \beta \leqslant 5$, represents all residues. A list is given of indices for primes less than N.

q	α	β	q	α	β	q	α	β	q	α	β	q	α	β	q	α	β
1	0	0	11	3	4	29	8	2	43	10	4	61	0	5	79	8	4
2	1	0	17	2	3	31	1	5	47	11	1	67	9	4	83	9	3
3	0	1	19	9	5	37	7	0	53	4	2	71	1	4	89	7	3
5	5	1	23	10	0	41	5	5	59	11	3	73	7	5			

(ii) $N = 105 = 3 \times 5 \times 7$ $\phi(N) = 2 \times 4 \times 6 = 48$ $\lambda(N) = \text{LCM}(2, 4, 6) = 12$

a	−1	1	2	4	8	11	13	16	17	19	22	23	26	29	31	32	34
ξ_a	2	1	12	6	4	6	4	3	12	6	4	12	6	2	6	12	2

etc.

We find that $2^\alpha 29^\beta(-1)^\gamma$ or $2^\alpha 29^\beta 34^\gamma$ each cover all residues.

(iii) For $N = 150$, $\phi(N) = 40$, $\lambda(N) = 20$, we find $13^\alpha(-1)^\beta$ will serve.
For $N = 210$, $\phi(N) = 48$, $\lambda(N) = 12$, we find $17^\alpha 29^\beta(-1)^\gamma$ will serve.

11. We come now to the main problem: How do we obtain enough relations (10.1) to cover all the factors involved in all our pairs (a, b)?

There are clearly numerous relations available; the problem is to pick out those where all factors are small. Western has described quite fully the way he tackled this problem for his particular purpose in Western and Miller (1968), and it is recommended that this account be studied.

A new version will be suggested in this paper, where we expect to have much larger numbers N to deal with, though no actual large example will be exhibited; nor indeed has one ever been attempted, for it seems that the scale envisaged cannot be feasibly tackled without an automatic computer–no computer program has yet been compiled for such a job.

We start with a simple example, to illustrate processes:

Consider factorisation of $N = 91$ (we have to ignore deliberately values of a and b that are not prime to 91). We seek $a = -b \pmod N$, with all factors of a, b small; we use $-1, 2, 3, 5, 11$ (five in all) and need five relations–we make it six in case a redundancy turns up–a frequent occurrence. We find

		Index coefficients					
$N=91$		-1	2	3	5	11	*Equation no.*
$96\equiv 5$	$2^5 3\equiv 5$	•	5	1	-1	•	1
$90\equiv -1$	$2\cdot 3^2 5\equiv -1$	1	1	2	1	•	2
$88\equiv -3$	$2^3 11\equiv -3$	1	3	-1	•	1	3
$81\equiv -10$	$3^4\equiv -2.5$	1	-1	4	-1	•	4
$80\equiv -11$	$2^4 5\equiv -11$	1	4	•	1	-1	5
$75\equiv -16$	$3\cdot 5^2\equiv -2^4$	1	-4	1	2	•	6

Thus equation 6 is $\operatorname{ind}(-1) - 4 \operatorname{ind} 2 + \operatorname{ind} 3 + 2 \operatorname{ind} 5 = 0$. This can be written as $\mathbf{Ai} = \mathbf{A}(i_{-1} i_2 i_3 i_5 i_{11})^T = \mathbf{0}$, where $\mathbf{A}$ is the 6×5 matrix of coefficients, and $\mathbf{i}$ is a vector (or matrix, if more than one generator is involved) of indices $\operatorname{ind} p = i_p$. Further relations in the elimination process are:

$7=3+5$	$(0\ \ 7\ \ -1\ \ 1\ \ 0)\mathbf{i}\equiv\mathbf{0}$	
$8=1+2$	$(1\ \ 6\ \ 3\ \ 0\ \ 0)\mathbf{i}\equiv\mathbf{0}$	
$9=1-4$	$(1\ \ 6\ \ -3\ \ 0\ \ 0)\mathbf{i}\equiv\mathbf{0}$	
$10=2\times 1+6$	$(1\ \ 6\ \ 3\ \ 0\ \ 0)\mathbf{i}\equiv\mathbf{0}$	This is 8
$11=1+7$	$(0\ \ 12\ \ 0\ \ 0\ \ 0)\mathbf{i}\equiv\mathbf{0}$	This is 8 + 9
$12=8-9$	$(0\ \ 0\ \ 6\ \ 0\ \ 0)\mathbf{i}\equiv\mathbf{0}$	

Note that $\operatorname{ind}(-1)$ is needed only modulo 2, but others must be calculated more carefully. Also

$$13 = 3 \times 5 \quad (1 \quad 0 \qquad 0 \quad 3 \quad 0)\, i \equiv 0 \ \text{using } 11$$

$$14 = 2 \times 3 \quad (1 \quad 6 \quad -2 \quad 0 \quad 2)\, i \equiv (0 \quad 0 \quad 1 \quad 0 \quad 2)\, i \equiv 0 \ \text{using } 9$$

Thus $\xi_2 | 12$, $\xi_3 | 6$, and $\xi_5 | 12$, and in all probability $\lambda(91) = 12$. This is easily verified, for $2^{12} - 1 = 4095 = 3^2 5 \cdot \mathbf{91}$; also

$$2^6 - 1 = 63 = 3^2 \cdot 7 \ \text{ and } \ 2^6 + 1 = 65 = 5 \cdot \mathbf{13}$$

and $12 | \lambda$. We note that the factors of 91 are split.

Likewise

$$3^6 - 1 = 728 = 2^3 \cdot \mathbf{91}, \quad 3^3 - 1 = 26 = 2 \cdot \mathbf{13}, \quad 3^6 = 1 = 28 = 2^2 \cdot 7$$

and factors of 91 are again split.

On the other hand $2^4 - 1 = 15$, $2^8 + 2^4 + 1 = \mathbf{91}$, so the exponent factor 3 is needed for *both* factors of N. Further, $5^6 - 1 = 2^2 3^2 \cdot 7 \cdot 31$, and $5^6 + 1 = 2 \cdot \mathbf{13} \cdot 601$, and factors of N are again split.

12. Western uses extensive tables of A_n-numbers for various n. Here an A_n-number is composite with no factor exceeding the nth prime p_n. They suffice for finding partitions $a + b = N$ for the numbers with which he had to deal. However, his tables, extensive as they are, are not adequate for dealing with much larger N, nor are they immediately ready for use on a computer, which will certainly be needed for large N.

I now wish to propose an approach which has not been tested fully, indeed hardly at all. Nevertheless I hope it may be a first approximation to a method that might be developed during actual experiment and use; there are several available degrees of freedom.

The main time-consuming process is that of testing members of a partition, a and b, to pick out A_n-numbers for a moderately low value of n. Each test is quite reasonably limited–only n primes p_r, $r \leqslant n$, for some moderate value of n have to be tried, then *either* a (or b) is completely factorised, *or* we know it is *not* an A_n-number. But failures to find an A_n-number are frequent, and successes relatively rare. Nevertheless we need only a moderate number of successes, in fact n, plus a small surplus, to anticipate redundant relations, which occur early in a small, but not negligible number of cases. We also note that no small factor can occur in both a and b, and that the presence of small factors greatly increases the probability of absence of large ones greater than p_n.

The last remark suggests, then, that one element of the pair, say a, be manufactured, as can easily be done, without the presence of the smaller primes, $2, 3, 5, \cdots, 29$, for example, and subtracted from the nearest multiple cN of N; the difference b must then be tested for factors $2, 3, \cdots, p_n$.

Western describes his experiences in this process of testing for small factors and advises $c = 1$ as giving the best results. Certainly any factor of c cannot occur in b without being in a as well, which means it could be cancelled. Nevertheless, since we are making up our values of a, it is worth looking near several values of cN, in the hope of finding a very small value of b,–such a small value may compensate for the loss of one small prime as a possible factor of b. Experience is needed.

The suggested approach is then:

(i) Manufacture numbers a from primes p_k with $k \geqslant m$, e.g., $p_m = 31$, $m = 11$, in the example below. Also $k \leqslant n$; we used $p_n = 73$ below, but retained a few more in the search, and kept what were needed. Then all primes p_n, $n < 11$, are exclusively available as factors of b (except for factors of c), and also other factors not used in a. The probability of success in obtaining an A_n-number depends substantially on the size of the smallest primes available as factors.

We may make a table of numbers for a by

(a) Making a first list of primes p_m to p_n, and beyond.

(b) Develop a second list of products of two primes, by cross-multiplying the first list with itself and sorting.

(c) Repeat the process to get a list of numbers with three factors–or maybe go directly to four factors.

Continue until numbers of order $\sqrt{N}$, starting less than $\sqrt{N}$, are obtained, to give a relatively permanent and rather big stock.

(d) Finally combine two of the final lists to give a list for immediate use, of numbers near N, and near $2N$, and $3N$, etc.

Details need experiment and investigation; for example it may be better for very big numbers, to combine three lists near $N^{1/3}$.

The magnitude of the task suggested also needs investigation.

(ii) The next step is to obtain from the final combination of lists, a number a near cN and hence $b = cN - a$, and test this for factors $\leqslant p_n$. Discard if a residual factor remains. It may however be useful (a) not to decide the value of p_n too soon, and (b) to record relations involving a *single* extra factor in a range not greatly exceeding p_n, in the hope of repetition, and so elimination, later.

(iii) When $n + \epsilon$ successful relations involving two A_n-numbers have been found, carry out the reduction of the index relations, to get those involving just one index. This will give $\lambda(N)$, or maybe a super- or sub-multiple adequate for the final factorisation process.

13. A particular case is now described, to give a preliminary idea of the method and work involved.

Take

$$N = 50059, \quad p_m = p_{11} = 31, \quad p_n = 109, \text{ later } 73.$$

The two-factor list contains 64 numbers, from $31^2 = 961$ to $59^2 = 3481$. The three-factor list has 112 numbers from $31^3 = 29791$ to $37^2 79 = 108151$. This covers N and $2N$.

Near 50059, there are 29 numbers in the list giving b between -14502 and $+18420$ inclusive; of these 10 have maximum factor $\leqslant 73$. Near 2×50059 there are 55 numbers giving b between -14961 and $+8033$; of these 13 have largest factor from 53 to 83 and 19 from 53 to 109.

Thus we have 23 relations for the 21 primes to 73, or 22 if we include -1. We hope this is enough. The relations used are (mod 50059) and in descending order of largest prime:

$$31 \cdot 43 \cdot 71 + 3 \cdot 5^2 73 = 0$$
$$31 \cdot 43 \cdot 73 + 53^2 = 0$$
$$31^2 41 + 2 \cdot 73^2 = 0$$
$$37^2 67 + 5 \cdot 23 \cdot 73 = 0$$
$$31 \cdot 47 \cdot 67 + 3 \cdot 7^2 17 = 0$$
$$37 \cdot 41 \cdot 67 = 3^2 13^2$$
$$37 \cdot 43 \cdot 67 = 11 \cdot 19 \cdot 31$$
$$37 \cdot 41 \cdot 61 + 3 \cdot 7 \cdot 19^2 = 0$$
$$31 \cdot 53 \cdot 61 = 3 \cdot 5 \cdot 7$$
$$41 \cdot 47 \cdot 53 = 3 \cdot 11 \cdot 61$$
$$41 \cdot 43 \cdot 61 = 3^3 5^2 11$$
$$31 \cdot 53^2 + 13 \cdot 17 \cdot 59 = 0$$
$$31^2 53 = 2 \cdot 19 \cdot 23$$
$$41^2 53 + 3^2 5^2 7^2 = 0$$
$$31 \cdot 37 \cdot 47 = 2 \cdot 5^2 7 \cdot 11$$
$$47^3 = 3 \cdot 5 \cdot 13 \cdot 19$$
$$31^2 43 + 2^5 3 \cdot 7 \cdot 13 = 0$$
$$31 \cdot 37 \cdot 43 + 2 \cdot 3^2 41 = 0$$
$$31 \cdot 43^2 = 2^2 3 \cdot 5 \cdot 11^2$$
$$37 \cdot 43^2 = 2 \cdot 3 \cdot 7 \cdot 19 \cdot 23$$
$$31 \cdot 41^2 = 2^2 3^3 19$$
$$37 \cdot 41^2 = 2 \cdot 3 \cdot 7 \cdot 17^2$$
$$37^3 = 2 \cdot 3^3 11$$

The reduction of the equations is not shown; it is straightforward as in the example in Western and Miller (1968), though tedious–it would not be so on a computer! To estimate work involved, it is relevant to note that, using care to keep coefficients small, the first double-figure coefficient, 10, came when the largest prime involved was 31 (in equation 55). The coefficient first exceeds 50 when six primes, to $p = 13$, are left (equation 87). It is 60 when four primes are left (equation 104), 307 when three are left (equation 130), 553 when two are left, and finally reaches $99008 \times \text{ind}\, 2 = 0$. In fact $N = 113 \cdot 443$, and $\lambda(N) = 24752$. Possibly a more careful reduction would produce this.

The main comment here is that large coefficients come only in the last few stages. The reduction is thus relatively easy numerically, and mostly single length, even for larger N.

14. One problem remains. What is the probability that a number a is an A_n-number, with all factors $\leqslant p_n$? This depends, of course, on which of the first n primes are actually available, and not otherwise excluded.

In Western and Miller (1968) there are given, in Table 6, extensive counts $f_n(x)$ of A_n-numbers not greater than x. We may use this function to give an estimate of the probability that a "random" x is an A_n-number. Then, assuming that we need k such numbers of size up to this, we can estimate the number of trials we need in finding them. In fact we need k numbers with probability $f_k(x)/x$ of success in finding each, if we use primes up to p_k, to give relations for an elimination scheme. The approximate number of trials needed then is $kx/f_k(x)$.

The table of $f_k(x)$ allows a thorough study of this function, which represents an amount of labour in some appropriate unit. We give below a typical set of values, for $x = 10^6$.

$x = 10^6$. Values of $kx/f_k(x)$

k	p_k	kx/f	k	p_k	kx/f	k	p_k	kx/f
1	2	50000	20	71	381	40	173	319.6
2	3	14085				41	179	319.6
3	5	5917	30	113	328.3	42	181	319.6
4	7	3142	31	127	326.5	43	191	319.9
5	11	2056	32	131	324.9	44	193	320.2
6	13	1461	33	137	323.6	45	197	320.4
7	17	1133	34	139	322.4	46	199	320.7
8	19	914	35	149	321.6	47	211	321.2
9	23	772	36	151	320.9	48	223	322.0
10	29	680	37	157	320.4	49	227	322.7
11	31	608	38	163	320.0	50	229	323.4
12	37	557	39	167	319.7	51	233	324.1

This shows that for a given limit (here 10^6) there is an optimum value of k, for which the total number of trials needed for k equations is a minimum, here 320.

There follows a table giving minimum kx/f, with corresponding k and p_k, for $x = 10^{3(1)8}$; the last two are values for $n = 51$, where they are still decreasing with k; we try to estimate better values.

Minimum values of $kn/f_k(x)$

x	k	p_k	kx/f	x	k	p_k	kx/f
10^3	8	19	24	10^7	>51	>233	<697
10^4	13	41	61	10^8	>51	>233	<1625
10^5	24	89	143		Estimates		
10^6	41	179	320	10^7	65	313	(670)
$2 \cdot 10^6$	47	211	403	10^8	100	499	(1500)

The ratios of kx/f as x increases tenfold seem to be diminishing towards 2. Thus a 10-fold increase in x corresponds to a 2-fold increase in the amount of work. This perhaps suggests a power of x, between $x^{1/3}$ and $x^{1/4}$.

The size of x, compared with N, depends on our success in finding values of a near cN; one hopes to light on values such that b is near $N^{\frac{1}{2}}$ or maybe rather larger, with some regularity. We can then test only these, and the number of them needed is then represented by $x = N^{\frac{1}{2}}$, which means perhaps $N^{1/6}$ trials. But much more work is needed both on actual trials and on estimating their number for numbers N of various representative trials.

15. For further trials using $f_k(x)$, we cannot rely on extended actual counts, but may instead make use of an approximate expansion derived as indicated below:

The function $f_n(x)$ satisfies the recurrence relation

$$f_n(x) = f_{n-1}(x) + f_n(x/p_n)$$

since every A_n-number in the count either has p_n as a factor, which can be divided out, leaving a smaller A_n-number, or p_n is not a factor, which means we have an A_{n-1}-number.

We can express the condition for an A_n-number in another way. An A_n-number counted in $f_n(x)$ is of the form

$$p_1^{\xi_1} p_2^{\xi_2} \cdots p_n^{\xi_n} \leqslant x$$

or, taking logarithms (to any base) it is a solution of the linear Diophantine inequality

$$l_1\xi_1 + l_2\xi_2 + \cdots + l_n\xi_n \leqslant \log x = y$$

where l_i is written for $\log p_i$. If we call the number of such solutions $\phi_n(y)$, then $f_n(x) = \phi_n(y)$ and the recurrence relation becomes

$$\phi_n(y) = \phi_{n-1}(y) + \phi_n(y - l_n).$$

This is a form of difference equation in y, and we may expect at least an approximate solution in the form of a polynomial in y.

Incidentally, the results may be expected to be independent of any particular interpretation or values of the constants l_i.

G. H. Hardy (1940, pp. 69ff) has proved that

$$\phi_2(y) = \frac{y^2}{2l_1l_2} + \frac{1}{2}\left(\frac{1}{l_1} + \frac{1}{l_2}\right) y + o\left(\frac{y}{\log y}\right)$$

from which we may deduce

$$\phi_n(y) = \chi_n(y) + o(y^{n-1}/\log y)$$

where

$$n!\, l_1l_2 \cdots l_n\chi_n(y) = y^n + ½n(l_1 + l_2 + \cdots + l_n)y^{n-1}.$$

The error term has been the subject of as yet unpublished investigations by Western and myself, with help from N. G. R. Sanders, R. M. Needham, and C. T. T. Scofield at the Cambridge University Mathematical Laboratory, to quite high limits; it seems considerably more restricted than suggested above.

We were encouraged to proceed further, and write (to condense two stages of investigation) $L(n) = \Pi_{i=1}^{n} l_i$, $S(n) = \Sigma_{i=1}^{n} l_i$,

$$Y = Y(n) = y + \tfrac{1}{2}S(n), \qquad \Phi_n(Y(n)) = \phi_n(y),$$

and to assume

$$n!\, L(n)\Phi_n(Y(n)) = \gamma_0(n)Y^n(n) + \frac{1}{3}\binom{n}{2}\gamma_2(n)Y^{n-2}(n) + \frac{1}{5}\binom{n}{4}\gamma_4(n)Y^{n-4}(n) + \cdots.$$

The difference equation becomes

$$\Phi_n(Y(n)) - \Phi_n(Y(n) - l_n) = \{\Phi_{n-1}(Y(n-1))\}/nl_n$$

or

$$\Phi_n\left(Y(n-1) + \frac{1}{2}l_n\right) - \Phi_n\left(Y(n-1) - \frac{1}{2}l_n\right) = \{\Phi_{n-1}(Y(n-1))\}/nl_n.$$

From this, by expanding in powers of $Y(n-1)$ and equating coefficients, and then solving the resulting difference equations, with initial condition $\phi_0(Y) = 1$ for all y, we obtain

$$\begin{aligned} n!\, L(n)\Phi_n(Y) = Y^n &- \frac{1}{3}\binom{n}{2}S_2^*(n)\, Y^{n-2} + \frac{1}{15}\binom{n}{4}(5S_2^{*2} + 2S_4^*)Y^{n-4} \\ &- \frac{1}{63}\binom{n}{6}(35S_2^{*3} + 42S_2^*S_4^* + 16S_6^*)Y^{n-6} \\ &+ \frac{1}{135}\binom{n}{8}(175S_2^{*4} + 420S_2^{*2}S_4^* + 320S_2^*S_6^* + 84S_4^{*2} + 144S_8^*)Y^{n-8} \\ &+ \cdots + \text{error} \end{aligned}$$

with $S_{2r}^* = \Sigma_{i=1}^n(\tfrac{1}{2}l_i)^{2r}$ and $Y(n) = Y$.

The error for $\Phi_3(Y)$ and for $\Phi_4(Y)$ has been studied, as was that in $\Phi_2(Y)$, and remains small—a few units only—for as far as is likely to be needed for a long time.

It is hoped to write a fuller account of the error investigations at a future time. Two further papers may help in the study of approximations to $f_n(x)$; these are N. G. de Bruijn (1951) and D. G. Hazlewood (1973).

16. The net result of this discussion is that there seems to be some hope that a method of factorisation might be devised, needing effort of order CN^α for a number N, with α maybe less than ¼. This may be too optimistic, but it seems worth trying for. The original hope was for an effort of order $C(\log N)^\beta$, with β bounded, perhaps by 5 or so. It seems that C might be rather large. The variety of choice available in selecting the partition $a + b = cN$ seems encouragingly large and unexplored. To sum up, the method seems worth further experiment.

It is worth remarking that the process will readily provide, with little further work, primitive roots and indices for the prime factors found for N, since congruences modulo N are also congruences modulo P if $P|N$.

Western found the method the best he could devise for finding primitive roots and indices, working by hand, with desk machines. J. S. Fenton (unpublished) has produced a computer program to carry out the process as used by Western, for primes in the region of 50000 to 100000, i.e.,in the range to give an extension to Western and Miller (1968). This program works well, though the extension of published tables has not yet been carried out.

New ideas and new recruits into this field would be welcome.

7 de Freville Avenue
Cambridge
Cambridgeshire CB4 IHN, England

J. BRILLHART & J. L. SELFRIDGE 1967, "Some factorizations of $2^n \pm 1$ and related results," *Math. Comp.*, v. 21, 1967, pp. 87–96; Corrigendum, *ibid.*, v. 21, 1967, p. 751. MR **37** #131.

N. G. DE BRUIJN 1951, "On the number of positive integers $\leqslant x$ and free of prime factors $> y$," *Nederl. Akad. Wetensch. Proc. Ser. A,* v. 54, 1951, pp. 50–60. MR **13**, 724.

R. CARMICHAEL 1914, *The Theory of Numbers.*

G. H. HARDY 1940, *Ramanujan*, Cambridge Univ. Press, Cambridge. MR **3**, 71.

D. G. HAZLEWOOD 1973, *Bull. London Math. Soc.*, v. 5, 1973, pp. 159–163.

D. H. LEHMER 1933, "Some new factorizations of $2^n \pm 1$," *Bull. Amer. Math. Soc.*, v. 39, 1933, pp. 105–108.

→ D. H. LEHMER 1936, *Amer. Math. Monthly*, v. 43, 1936, pp. 347–354.

D. H. LEHMER 1939, "A factorization theorem applied to a test for primality," *Bull. Amer. Math. Soc.*, v. 45, 1939, pp. 132–137.

P. POULET 1928, *Sphinx-Oedipe*, 23, 1928.

A. E. WESTERN & J. C. P. MILLER 1968, *Tables of Indices and Primitive Roots*, Roy. Soc. Math. Tables, vol. 9, Cambridge Univ. Press, London. MR **39** #7792.