XiV

This is combined with the congruence ending with ind p, mentioned above, and integrated is moved to the right-hand side; the remaining steps follow as above.

Cases occasionally occur where g is composite but has more than two prime factors or includes a repeated prime factor; these are dealt with in a similar manner.

The values of ind p_2 , ind p_3 , ..., ind p_n are then calculated in succession. The values of the residue-indices

$$v_r = (\text{ind } p_r, P - 1) \quad (r = 1, 2, ..., n)$$

are finally found; this completes the calculations for P.

The reader is recommended to read the worked out example given below in Part IV, \$17, which will make the process above described more intelligible.

In the remainder of this introduction, the indices are sometimes expressed in the form in which they were obtained during the original hand computations, namely as

$$x + \epsilon \lambda$$

where

$$-\frac{1}{2}\lambda < x \leqslant \frac{1}{2}\lambda$$
 $\epsilon = 0$ or I

This may be written as x or $x\lambda$, but $x + \lambda$ will be used in this introduction, except in §17.4. In the tables each index is given as a positive integer between 0 and P.

In Table 1 either g, or -g' if g' < g, is chosen as the primitive root to which the indices refer. In Tables 2 to 4, $P \equiv 1 \pmod{4}$ always, and g = g'.

PART II. INVESTIGATIONS ON PRIMES FOR WHICH THE LEAST q-IC NON-RESIDUE IS RELATIVELY LARGE

8. General remarks

In §5 it was shown that for a prescribed modulus P there exists a p_s for each prime q such that $q \nmid \text{ind } p_s$, and that this $p_s < \sqrt{P} + 1$. This provides an upper bound for n, the number of primes to be used in forming A_n -numbers, if success is to be guaranteed. This bound, given by $p_n \ge p_s$, is too large to be practical. It is thus of interest to examine the special cases, q = 2, q = 3, etc., to obtain better upper bounds for n in terms of P. In fact, the following paragraphs exhibit short tables which give the least primes $P_q(m)$ for which all primes up to p_m are q-ic residues, so that n = m in all cases where $P < P_q(m)$.

The results show that, for primes $P < 36.10^6$ the value of n that suffices for each $q \le 17$ is as follows:

Cases where q > 17 are dealt with in § 16 and Table 7.

9. The case of q = 2

Let P(n), P'(n), written for $P_2(n)$ and $P'_2(n)$, denote the smallest primes, P, of the forms 8k - 1 and 8k + 1 respectively which are such that all the primes $p_1, p_2, ..., p_n$ are quadratic residues (mod P).

Using the law of quadratic reciprocity, the values to n=14 listed in the following table were found. These values were checked, and the list extended to n=16 by means of a program constructed by J. Lindley for EDSAC 2. It is interesting that, for each $n \le 13$, $P_n < P'_n$, but for n=14 to 16, $P_n > P'_n$.

n	p_n	P(n)	P'(n)	
I	2	7	17	
2	3	23	73	
3	5	71	241	
4	7	311	1009	
4 5 6	II	479	2689	
6	13	1559	8089	
7	17	5711	33049	
7 8	19	10559	53881	
9	23	18191	87481	
10	29	31391	4 83289	
II	31	3 66791	5 15761	
12	37	3 66791	10 83289	
13	41	3 66791	38 18929	
14	43	40 80359	38 18929	
15	47	125 37719	92 57329	
16	53	307 06079	220 00801	
1	444	aivos	7723	2224

We may note also that Lehmer 1954 gives

$$P'(17) = P'(18) = 48473881$$
 $P'(19) = 175244281$ $P'(20) = P'(21) = 427733329$ and $P'(22) = 898716289$

10. The case of q = 3

In this section $P(n) = P_3(n)$ denotes the smallest prime P such that $p_1, p_2, ..., p_n$ are cubic residues (mod P).

Here 3|P-1, and it is known that P can be expressed in the quadratic form

$$P = \frac{1}{4}(L^2 + 27M^2)$$

Cunningham (1927, pages 128, 132) has given criteria in terms of L and M, showing for each prime \leq 47 when it is a cubic residue modulo P. These are derived from Gauss's law of cubic reciprocity.

When 2 is a cubic residue, 2|L and consequently 2|M, and when 3 is a cubic residue, 3|M. Hence, putting L=2l and M=6m, both 2 and 3 are cubic residues when

$$P = l^2 + 243m^2$$

The cases m=1, l=2 or 4 make P composite, whilst l=8, m=1 gives $P_2=307$. When 5 is a cubic residue, 5|l or 5|m, and the case l=20, m=1 gives $P_3=643$. When 7 is a cubic residue, 7|l or 7|m, and there are now four cases to be considered:

(1)
$$5.7|m$$
 $P = j^2 + 3(315k)^2$
(2) $7|l \text{ and } 5|m$ $P = (7j)^2 + 3(45k)^2$
(3) $5|l \text{ and } 7|m$ $P = (5j)^2 + 3(63k)^2$
(4) $5.7|l$ $P = (35j)^2 + 3(9k)^2$

Cases (1) and (3) give no $P < 10^4$, and case (2) gives P > 6075. Case (4) for j = 1 and k = 4 gives $P_4 = 5113$.

The next stage is to list all values of j and k satisfying the criteria for 11 and 13 for $P < 10^8$, to calculate the corresponding values of P, to exclude composite values of P, and to list the remaining values of P in order of magnitude, and then to apply the criteria for 17, 19, 23, 29, 31, 37 and 41. The calculations are too long to be given in full; the results were checked to 36.10⁶ on EDSAC 2 by means of a program compiled by P. Becker. They are, including the values given above:

n	p_n	$P_3(n)$	n	p_n	$P_3(n)$
2	3	307	8	19	3 60007
3	5	643	9	23	47 755 ⁶ 9
4	7	5113	10	29	103 18249
5	11	21787	II	31	103 18249
6	13	39199	12	37	651 39031
7	17	3 60007	13	41	> 108
					The same of the sa

II. The case of q = 5

This is treated fully as the criteria developed (by A. E. W.) do not seem to have been published previously. In this section we are concerned with primes P such that $p_1, p_2, ..., p_n$ are residues of 5th powers, and 5|P-1.

.5225

11.1. Notation and preliminary theory

Let $\zeta = \exp \frac{2}{5}i\pi$ be a primitive 5th root of unity, satisfying the equation

It is known that the class-number of the field of ζ , called $k(\zeta)$, is 1, and that η_0 is the fundamental unit (see Smith 1894, pages 95 and 99).

$$\eta_0 = \frac{1}{2}(-1 + \sqrt{5})$$

$$\pi = \pi(\zeta) = a_0 \zeta + a_1 \zeta^2 + a_2 \zeta^4 + a_3 \zeta^3$$

Let

denote a prime factor of P. Its conjugates are

$$\pi_1 = s\pi = \pi(\zeta^2)$$
 $\pi_2 = s^2\pi = \pi(\zeta^{-1})$ $\pi_3 = s^3\pi = \pi(\zeta^{-2})$

Here s is the substitution ($\zeta:\zeta^2$); the application of s permutes the coefficients of π cyclically. Also $\phi=\pi\pi_2 \quad \text{and} \quad \phi_1=\pi_1\pi_3$

are factors of P of the form $x + y\sqrt{5}$. Then

$$P = \phi \phi_1 = \pi \pi_1 \pi_2 \pi_3$$

The multiplication of π by any unit, say $\zeta^x \eta_0^y$, gives an associated form of π ; in order to select one of the infinite number of associated forms, x is so chosen as to make π semi-primary, that is to satisfy $\pi(\zeta) \equiv \pi(1) \pmod{\omega^2}$

11.8. The case of r = 13. Here

$$(13|\pi) = (\pi|13) \equiv \pi^{\frac{1}{3}(13^4-1)} = \pi^{34(13^3-1)} \equiv (\pi_2 \pi^{-1})^{34} \pmod{13}$$
 (11.81)

and the congruence

$$\gamma^{17} \equiv 1 \pmod{13} \tag{11.82}$$

(11.83)

must be solved.

The cube of (11.82) is

$$\gamma^{51} \equiv 1 \pmod{13}$$

So

$$\gamma \equiv \gamma^{52} = (\gamma^{13})^4 \pmod{13}$$

Now by (11.32)

$$\gamma^{13} \equiv \gamma_3 \pmod{13}$$

so that

$$\gamma \equiv \gamma_3^4 \pmod{13}$$

and, applying s, we have
$$\gamma_1 \equiv \gamma^4$$
 $\gamma_2 \equiv \gamma_1^4 \equiv \gamma^{16} \pmod{13}$

and finally If we write

$$\gamma \gamma_2 \equiv \gamma^{17} \equiv I \pmod{13}$$

$$\gamma = a + b\zeta + c\zeta^2 + d\zeta^3$$

and seek a solution γ' of

$$\gamma \gamma_2 \equiv 1 \pmod{13}$$

we find by trial that a solution with $b \equiv 0$ is

$$a \equiv -5$$
 $b \equiv 0$ $c \equiv 2$ $d \equiv 6 \pmod{13}$

This gives, however,

$$\gamma_3'\gamma'^4\equiv\zeta^4$$

so that $\gamma = \zeta^{-2}\gamma'$ is one solution of (11.82). The 17 solutions of (11.82) are thus

 $\gamma, \gamma_k, \gamma_k^2, \gamma_k^3$ and γ_k^6 (k = 0, 1, 2, 3) $\gamma = 2 + 6\zeta - 5\zeta^3$ (11.84)

where

The test for $(13|\pi) = 1$ is then

$$\pi_2 \equiv \pm M\pi \pmod{13}$$

where M is one of the 17 solutions (11.84).

Alternatively, as there are few cases for which this test is needed, it is simpler to use the following test, (11.85) $\pi_1 \pi_2^4 \equiv + \pi_2 \pi^4 \pmod{13}$

which is readily obtained from (11.81), for

$$\pi^{17} = \pi^{13}\pi^4 \equiv \pi_3\pi^4$$

12. Results for q = 5

Here $P(n) = P_5(n)$ is the least prime for which $p_1, p_2, ..., p_n$ are residues of 5th powers. The values of P(n) for n = 1, 2, and 3 are found by examining Cunningham, Woodall & Creak 1922 a (pages 1, 3, and 22).

A list was then made of all values of a_0 , a_1 , a_2 , and a_3 satisfying the inequalities proved in §11.2, and the congruential conditions proved in §§11.4 and 11.5. The corresponding values of A, B, and P were then calculated, the cases where P was composite deleted, and the rest arranged in order of magnitude of P. The remaining conditions given in §§11.6 to 11.8 were then applied, and the values of P(4) and P(5) found, and the fact that $P(6) > 2.10^6$.

As a check, and to extend the search, a program was constructed by D. Fairburn, then a student at the University Mathematical Laboratory, Cambridge, and run on EDSAC 1.

This tested each prime 5n + 1 for $p_1, p_2, ...$ as quintic residues, until one failed; every such prime from 2.10⁶ to 5.10⁶ was tested in this way, and the values of P(6) and P(7) emerged, and the fact that $P(8) > 5.10^6$. A similar program was compiled by P. Becker for EDSAC 2, and run to 36.10^6 , thus modifying the last inequality to $P(8) > 36.10^6$.

The complete list obtained is

n	p_n	$P_5(n)$
I	2	151
2	3	431
3	5	6581
4	7	67651
5 6	II	2 41981
6	13	2 0 81921
7	. 17	33 95921
8	19	> 360 00000
		~2210

13. The cases of q = 7, 11, 13, 17

In this section $P_k(n)$ means the least prime of which $p_1, p_2, ..., p_n$ are residues of kth powers (k = 7, 11, 13, 17).

It is possible to obtain inequalities in the case of k = 7 similar to those of §11.2, and tests for r being a residue of a 7th power (mod P) similar to those of §11. It was, however, found impracticable to proceed further with this method.

From Cunningham, Woodall & Creak 1922a (pages 3 and 19) we derive $P_7(1)$ and

 $P_7(2)$ and Table 1 in the present work shows that $P_7(3) > 50000$.

By calculation of $2^{(P-1)/14}$ (mod P) for all $P \equiv 1 \pmod{7}$ between 5.10⁴ and 10⁵, a list was made of all primes P for which 2 is a residue of a 7th power; then by calculation of $3^{(P-1)/14}$ (mod P), those P for which 3 is also a residue of a 7th power were found; then by calculation of $5^{(P-1)/14}$ (mod P), those P for which 5 is also a residue of a 7th power were found. This gave $P_7(3)$ and showed that $P_7(4) > 10^5$.

Finally, as for quintic residues, an extended search on EDSAC I was made with another program compiled by D. Fairburn (this extended to 5.106), and P. Becker's program for EDSAC 2 was used to check these results and to extend the search to

36.106; P(6) emerged.

The complete list obtained is

		• •			
VIII *	n	p_n	$P_{7}(n)$		
4.47	1	. 2	631		
- in \$ 11.2.2	2	3	553 ¹		
value of a	3	5	72661		27
977 T = T2	4	7	8 65957		7201
	5	II	23 75059		
XX X	6	13	323 53609		
	7	17	> 360 00000	,	wam 9
				,	wan a

Programs for EDSAC 1 and 2 were also made by D. Fairburn and P. Becker for testing primes p_n as residues of 11th, 13th, and 17th powers; these were run on the machines for P > 10000, and earlier values were extracted from Cunningham, Woodall & Creak 1922a.

Results are of course rather few, and are listed below.

n	p_n	$P_{11}(n)$	$P_{13}(n)$	$P_{17}(n)$
I	2	331	4421	1429
2	3	39139	44851	6563
3	5	2 53243	11 94961	14 58601
4	7	43 97207	23 67691	> 360 00000
5	II	215 87171	> 360 00000	
6	13	> 360 00000		
		12-	28	

14. Previous tables

Mention should also be made of previous tables of residue-indices. Kraitchik 1924 (Table I) gives residue-indices of 2 for P < 300000. This table contains many errors. It has all been checked; errors for P < 100000 are listed in Lehmer 1941, in which other tables are also listed: the range 100000 < P < 300000 has been recomputed, partly by F. Gruenberger on an IBM card-programmed calculator, and partly by means of a program prepared by D. B. Gillies, and used on the Elliott 401 computer belonging to the N.R.D.C., which was also used to extend the table. The checking was completed by R. H. Merson, on the Pegasus machine at R.A.E., Farnborough.

Kraitchik 1924 (Table IV) gives a primitive root and indices of primes not exceeding 100 for prime moduli P < 10000. Cunningham, Woodall & Creak (1922a, b) give least primitive roots, g and -g', and residue-indices of 2, 3, 5, 6, 7, 10, 11, 12 for $P \le 25409$. These were extended and tables made for other bases by means of Gillies's program on the Elliott 401 computer, and later by means of a program prepared by M. J. Ecclestone for EDSAC 2. These tables give all residue-indices with base 2 up to P = 1048571, with bases 3(primes)47 for P to 10000000, and also for bases 6(composite)50, excluding exact powers, to the same limit.

These tables were useful in determining values of $P_{p_r}(n)$. From the list for base 2, primes P were extracted, mainly by W. Barrett, for which the residue-index has a factor $p \ge 7$. Then the list for base 3 was examined to see if the corresponding ν has the same factor p_r ; if so the list for base 5 was examined, and so on. This provided a valuable check on results obtained by other methods, and was a vital link during the preparation of the EDSAC 1 program; it brought to light an obscure error in the original version.

Part III. Enumeration of A_n -numbers

15. Recurrence relations

Denote by $f_r(x)$ the number of A_r -numbers a_r such that $0 < a_r \le x$.

Theorem 3.
$$f_r(x) = f_{r-1}(x) + f_r(x/p_r)$$
 (15.1)

This is obvious since, if a_r contains p_r as a factor, a_r/p_r is an A_r -number, while if a_r is prime to p_r it is an A_{r-1} -number.

28. The maxima of g, the least positive primitive root

Let G(x) denote max g(P), $P \le x$, and restricted as indicated in each table below. From Tables 1 to 4 we extract the results tabulated.

G(x) for unrestricted P

P	P-I	G	P	P-1	G	
7	2.3	3	5881	$2^3 \cdot 3 \cdot 5 \cdot 7^2$	31	
23	2.11	5	36721	$2^4 \cdot 3^3 \cdot 5 \cdot 17$	37	
41	$2^3.5$	6	55441	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	38	*
71	2.5.7	7	71761	$2^4.3.5.13.23$	44	
191	2.5.19	19	110881	$2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	69	
409	$2^3.3.17$	21	760321	$2^9.3^3.5.11$	73	
2161	$2^4 \cdot 3^3 \cdot 5$	23				2279
	~ .	-				

This list is complete for P < 2000000, as has been verified by R. H. Merson on a Pegasus computer, and with the help of a program by M. J. Ecclestone for EDSAC 2. Table 1 shows that for $10^3 < P < 5.10^4$, we have

 $P \equiv 3 \pmod{8}$ $P \equiv 5 \pmod{8}$ $P \equiv 7 \pmod{8}$ G_7 \boldsymbol{P} \boldsymbol{P} \boldsymbol{P} G_5 8011 14 1021 9439 22 19843 10559 23 19 1597 6581 26 23 12391 21757 24181 29 17 15791 26701 31 22 31391

Thus, G for $P \equiv 3$, 5 or 7 (mod 8) is less than G for $P \equiv 1 \pmod{8}$ for all values of P between 10³ and 5.10⁴. It seems therefore to be probable that G for unrestricted primes exceeding 5.10⁴ will be found among primes congruent to 1 (mod 8).

Table 1 also shows that G for $P \equiv 1 \pmod{8} \equiv -1 \pmod{3}$ is less than G for $P \equiv 1 \pmod{24}$: G for the former set is 15, for P = 8681.

Lastly, consider the primes $P \equiv 1 \pmod{24}$ with respect to their residue modulo 5. Table 1 shows that G for $P \equiv \pm 2 \pmod{5}$ is less than G for $P \equiv \pm 1 \pmod{5}$ for all values of P between 10³ and 5.10⁴; for the former set G = 19 for P = 5113. Again Tables 1 and 2 show that for $P \equiv 1 \pmod{24}$ and $-1 \pmod{5}$, that is for $P \equiv 49 \pmod{120}$ G is less than it is for $P \equiv 1 \pmod{120}$ for all values of P between 10³ and 10⁵ with one exception, namely G = 31 for P = 23209, which is equal to G for $5881 \le P < 36721$ when $P \equiv 1 \pmod{120}$.

Conjecture B. From these facts, it seems probable that max g for $P > 5.10^4$ will be found in general among primes $P \equiv 1 \pmod{120}$.

These results are to be expected, for if $P \equiv 1 \pmod{8}$, and q is any odd prime factor of P - 1, q is a quadratic residue modulo P; so if $P \equiv 1 \pmod{24}$, not only are 2 and 3 quadratic residues and therefore also 6, but there is also the possibility that 5 may be

2230

either a quadratic residue or a cubic residue. On the other hand if P = -1(8), either 3|P-1, in which case 3 is not a quadratic residue, or $3\nmid P-1$, in which case there is no question of cubic residues.

29. The maxima of h, the least positive prime primitive root

Denote by H(x) the max h(P), $P \le x$. Tables 1 to 4 give the following values for H.

P	P- 1	H	P	P-1	H
3 7 23 41 109 191	2 2.3 2.11 2 ³ .5 2.59 2.5.19	2 3 5 7 11 19	271 2791 11971 31771 190321	$2.3^{3}.5$ $2.3^{2}.5.31$ $2.3^{2}.5.7.19$ $2.3^{2}.5.353$ $2^{4}.3.5.13.61$	43 53 79 107 149

It is interesting that all these values of P exceeding 4r and less than 5.10^4 are congruent to $-1 \pmod{4}$. The last case in this list is the only one in which h > 107, in Tables 2 to 4; that no entry is omitted has been demonstrated by R. H. Merson.

30. Conjectures as to the order of magnitude of G and H

The following tables give the values of $G/\ln P$, $G/(\ln P)^2$, $G/(\ln P)^3$, and of $H/\ln P$, $H/(\ln P)^2$ and $H/(\ln P)^3$. The logarithms are to base e.

Conjecture C
$$G = O\{(\ln P)^3\}$$
 and
$$H = O\{(\ln P)^3\}$$

All that has been proved about the order of G is Vinogradoff's theorem (Landau 1927, page 178) that $g(P) = O(p^{\frac{1}{2} + \delta})$

for every $\delta > 0$.

\cdot P	$rac{G}{\ln P}$	$\frac{G}{(\ln P)^2}$	$\frac{G}{(\ln P)^3}$
3	1.8	1·66	1.508
7 23	1·5	0.79	0.407
- 4I	r·6	0·51 0·44	0·162 0·117
71	1.6	0.39	0.090
409	3.6	0.69	0.131
2161	3·5 3·0	0·58 0·39	0·097 0·051
5881	3.6	0.41	0.047
36721	3.2	0.33	0.032
Triese zes 71761	3·5 3·9	o·32 o·35	0·029 0·031
110881	5.9	0.21	0.031
760321	5.4	0.40	0.029

INTRODUCTION

P	$\frac{H}{\ln P}$	$\frac{H}{(\ln P)^2}$	$\frac{H}{(\ln P)^3}$
P 3 7 23 41 109 191 271 2791 11971	1.8 1.5 1.6 1.9 2.3 3.6 7.7 6.7 8.4	1.66 0.79 0.51 0.51 0.50 0.69 1.37 0.84 0.90	0.407 0.162 0.137 0.107 0.131 0.245 0.106
31771 190321	10.3	I.OI I.OO	o·096 o·083

PART VI. DESCRIPTION OF THE TABLES WITH HINTS ON THE USE OF THE MAIN TABLES I TO 4

31. Contents of Tables 1 to 8

Tables I to 4 are similar. For each prime P there are listed: (i) The complete factorization of P-I. (ii) g, the least positive primitive root, g', where -g' is the least negative primitive root, and h, the least positive prime primitive root: g' is given in Table I only, in other tables g'=g always. (iii) For each of several numbers a there is given the index, ind a, such that

$$g^{\operatorname{ind} a} \equiv a \pmod{P}$$

and on the right of the index, the residue-index ν given by

$$\nu = (P - 1, \text{ind } a)$$

which is such that

$$a^{(P-1)/\nu} \equiv \operatorname{r} \pmod{P}$$

and $(P-1)/\nu$ is the least index with this property.

The particular integers a in the tables are as follows:

Tables I, 2 a = 2, 3, 5, 6, 7, 10, 11, 12, 13, 17, 19, 23, 29, 31, 37

Table 3 a = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37

Table 4 a = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Table I covers all values of P to 50021; Table 2 extends the range to all values of $P \equiv I \pmod{24}$ less than 100000; Table 3 to all values of $P \equiv I$ or 49 (mod 120) less than 250000; and Table 4 to all values of $P \equiv I \pmod{120}$ less than 1000000.

Indices for values of a not in the tables can be found from the basic relations

$$\operatorname{ind} a \equiv \operatorname{ind} b \pmod{P-1}$$
 if $a \equiv b \pmod{P}$

$$\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{P - 1}$$

and indices for higher prime values of a can be found readily by the method described in § 18. However, Table 5 lists those indices for 37 in Tables 1 to 3, and those indices <math>47 in Table 4, in cases where <math>h is large.

Table 6 gives counts of A_n -numbers, that is of numbers with their largest prime factor $\leq p_n$, for various upper limits N. In fact for each N there is a list for

$$p_n = 2 \text{ (primes) } 233, \text{ or } n = 1 \text{ (1) } 51$$

of counts of numbers with largest prime factor at most p_n . The values of N are

$$N = 10^3 \left(10^3\right) 2.10^4 \left(10^4\right) 2.10^5 \left(2.10^4\right) 10^6 \left(10^5\right) 2.10^6 \left(2.10^5\right) 10^7 \left(10^6\right) 2.10^7 \left(2.10^6\right) 5.10^7 \left(5.10^6\right) 10^8$$

Table 7 gives the results of the application of Theorem 4, see § 16.

Table 8 lists counts of primitive roots and compares these counts with estimates based on the conjectures of Part V, §§23, 24.

32. Use of the tables of indices with examples

The main use of the major Tables 1 to 4 is similar to that of the Canon Arithmeticus of Jacobi 1839. This well-known work gives, for each prime P, or prime power P^{α} , less than 1000, a complete table of indices, with respect to some primitive root G, for all $a \leq P - 1$, or for all $a \leq P^{\alpha} - 1$ and prime to P, and also a complete inverse table of residues $G^n \pmod{P}$ for n = 1(1)P - 1, or of $G^n \pmod{P^{\alpha}}$ for $n = 1(1)\phi(P^{\alpha})$. The primitive root, G, used is not always the least, but may be another convenient one, such as 10.

These tables have been completely revised and extended by W. Patz in Jacobi 1956. Here the least positive primitive root, g, is always used, and tables are also given for modulus $2P^{\alpha} < 1000$, as well as for modulus P^{α} , while two further tables are given for each prime modulus P. These last give for each index x the indices of $g^{x} + 1$ and of $g^{x} - 1$, and correspond to addition and subtraction logarithms for ordinary numbers, in the same way that ordinary indices play the part of logarithms.

The tables now given here are, like those of Kraitchik 1924, much more restricted in what they give for each P; they give only the indices for a few small numbers, almost all primes. Kraitchik's list extends to $p_n = 97$, ours only to $p_n = 37$ or 47. Nevertheless, by use of ingenuity and some quite simple devices, and a little extra work, it is possible to achieve results nearly as easily as by use of Jacobi's *Canon*. The range of P is, of course, enormously extended both in Kraitchik 1924 (to P < 10000) and in our tables.

We shall use an example to illustrate, albeit inadequately, some of these devices. *Example*. Obtain the solutions, if any, to the congruences

(i)
$$x^4 \equiv 95 \pmod{4933}$$
 (ii) $x^{15} \equiv 97 \pmod{4933}$

(i) From the tables on page 26 for P = 4933

$$\operatorname{ind} 95 \equiv \operatorname{ind} 5 + \operatorname{ind} 19$$

$$\equiv 3385 + 1709$$

$$\equiv 162$$

$$(\operatorname{mod} 4932)$$

But 162 + 4932k cannot be a multiple of 4; thus (i) has no solution.

(ii) Here

$$97.51 \equiv 14 \pmod{4933}$$

so that

$$ind 97 \equiv ind 2 + ind 7 - ind 3 - ind 17$$

 $\equiv 1 + 4401 - 1800 - 1951$
 $\equiv 651$ (mod 4932)

Now 651 + 4932k is a multiple of 15 when k = 2 + 5m.

Hence

$$\operatorname{ind} x \equiv \frac{651 + 4932k}{15} \pmod{4932}$$

$$= 701, 2345 \text{ or } 3989 \text{ for } k = 2, 7, \text{ or } 12$$

The solutions required are thus

$$x = 2^{701}$$
, 2^{2345} or 2^{3989} (mod 4933)

These values of x have now to be simplified.

We may, with a desk machine available, compute the residues directly by involution, mainly squaring. Thus

$$2^{21} = 2097152 \equiv 627 = a$$

$$2^{43} = 2a^{2} = 786258 \equiv 1911 = b$$

$$2^{87} = 2b^{2} = 7303842 \equiv 3002 = c$$

$$2^{175} = 2c^{2} = 18024008 \equiv -1174 = d$$

$$2^{350} = d^{2} = 1378276 \equiv 1969 = e$$

$$x_{1} = 2^{701} = 2e^{2} = 7753922 \equiv 4179$$

$$\equiv -754$$
(mod 4933)

which gives the first solution.

We may, however, use the table on page 26 to provide short cuts, thus

or

$$2^{4237} \equiv 2^{-695} \equiv 13$$

$$2^{695} \equiv \frac{1}{13} \equiv \frac{1 + 2 \cdot 4933}{13}$$

$$\equiv 759$$

$$2^{701} \equiv 64 \cdot 759$$

$$\equiv -754$$
(mod 4933)

and

(To find 1/13, note that $4933 \equiv 6 \pmod{13}$ and $1+2.6 \equiv 0 \pmod{13}$, hence 1+2.4933 is a multiple of 13.)

Again, for the second solution, with $\lambda = \frac{1}{2}(P - 1)$ as in (2.3),

$$2345 \equiv -121 + \lambda \pmod{4932}$$

Hence

$$2^{2345} \equiv -2^{-121} \pmod{4933}$$

Now

$$ind 11 + ind 5 \equiv 1444 + 3385 \equiv -103 \pmod{4932}$$

and so

$$2^{2345} \equiv -2^{-18}.55 \pmod{4933}$$

Again ind
$$7 - \text{ind } 17 \equiv 4401 - 1951 \equiv -16 + \lambda \pmod{4932}$$

so that
$$-2^{-16} \equiv \frac{7}{17} \equiv \frac{7 - 8.4933}{17} \pmod{4933}$$

$$\equiv -2321$$
and
$$2^{2345} \equiv 55 \cdot (-2321) \cdot \frac{1}{4}$$

$$\equiv -4330/4 \equiv -2165/2$$

$$\equiv 2768/2$$
and
$$x_2 \equiv 1384$$
 (mod 4933)

This is a little longer than for the first solution, though it is all 'pencil and paper' work, whereas the involution method needs a desk machine. Possibly it is better to combine both methods, first supplementing the printed table by some extra entries. For example, with g = 2, as here, the first ten powers made be assumed known, and used directly. Also, by direct multiplication

$$2^{20} \equiv -2153 \qquad 2^{70} \equiv +1123$$

$$2^{30} \equiv +379 \qquad 2^{80} \equiv +563$$

$$2^{40} \equiv -1611 \qquad 2^{90} \equiv -649$$

$$2^{50} \equiv -2042 \qquad 2^{100} \equiv +1379$$

$$2^{60} \equiv +584 \qquad 2^{200} \equiv +2436$$
(mod 4933)

Then, from page 26,

$$2 \text{ ind } 29 + \text{ ind } 7 \equiv 7722 + 4401$$

 $\equiv 12123$
 $\equiv +2259$ (mod 4932)

and

$$2^{2345} \equiv 841.7.2^{86}$$

$$\equiv 841.7.563.64$$

$$x_2 \equiv 1384$$
(mod 4933)

Lastly

$$3989 \equiv -943 \equiv 1444 - 2383 - 4 \pmod{4932}$$

and so

$$\begin{array}{l}
\mathbf{z}^{3989} \equiv \mathbf{I} \cdot \frac{1}{23} \cdot \frac{1}{16} \\
 \equiv \frac{\mathbf{I} \cdot \mathbf{I} - 4933}{23} \cdot \frac{\mathbf{I}}{16} \\
 \equiv -2\mathbf{I} \cdot 4/16 \\
 \equiv (-107 - 4933)/8 \\
 x_3 \equiv -630
\end{array}$$
(mod 4933)

Alternatively

$$2^{-943} \equiv 2^{-1022} \cdot 2^{79}$$

$$\equiv -11 \cdot 2^{70} \cdot 2^{9}$$

$$\equiv -11 \cdot 1123 \cdot 512$$

$$\equiv -630$$
(mod 4933)

from the auxiliary table made for the second solution.

To check the results is simpler. We have

$$x_{1}: \quad \text{ind} - 754 \equiv \lambda + \text{ind} \ 2 + \text{ind} \ 13 + \text{ind} \ 29$$

$$\equiv 701$$

$$x_{2}: \quad \text{ind} \ 1384 \equiv 3 \text{ ind} \ 2 + \text{ind} \ 173 \quad (\text{mod} \ 4932)$$
But
$$29 \cdot 173 = 5017 \equiv 84 \quad (\text{mod} \ 4933)$$
so
$$\text{ind} \ 173 \equiv 2 \text{ ind} \ 2 + \text{ind} \ 3 + \text{ind} \ 7 - \text{ind} \ 29$$
and
$$\text{ind} \ 1384 \equiv 5 \text{ ind} \ 2 + \text{ind} \ 3 + \text{ind} \ 7 - \text{ind} \ 29$$

$$\equiv 2345$$

$$x_{3}: \quad \text{ind} - 630 \equiv \lambda + \text{ind} \ 2 + 2 \text{ ind} \ 3 + \text{ind} \ 5 + \text{ind} \ 7$$

$$\equiv 3989$$

$$(\text{mod} \ 4932)$$

In each case 15 ind x = 651, as it should.

Alternatively, we may check directly by computing, for example, x_1^{15} (mod 4933). We find

$$(-754)^{3} \equiv 1837$$

$$1837^{2} \equiv 397$$

$$397^{2} \equiv -247$$

$$-247.1837 \equiv 97$$
(mod 4933)

This example has been treated at length to illustrate the kind of short cuts that can be devised.

PART VII. THE CHECKING OF THE PROOFS

33. Many tables in Number-Theory, by reason of relatively unsystematic entries, cannot be differenced, and are correspondingly difficult to render free from error. Tables 1 to 4 in this volume were set up in type from printer's copy prepared from punched cards. These cards were punched from the original manuscript in order to cope with a major change of layout decided on for printing, which meant that the original manuscript was not in the best form for the printer.

Since the cards were punched it was decided to prepare a program for an automatic computer, which could read these cards and check that each value of $g^{\text{ind }a}$ did in fact reduce modulo P to a. A further change in plan rendered the original manuscript even more remote from the printed work, so that, in fact, the cards already punched were further processed when producing printer's copy, and it was eventually decided to punch a further set of cards from the first proofs from the printer, and to check these by automatic computer. This was done on the ACE at the National Physical Laboratory, and formed the ultimate check of all stages of preparation of the tables.

It seems worthwhile to record these stages in some detail:

(i) The original calculations were made and checked by hand or desk machines by A.E.W. and collaborators. The results were all finally expressed in the form described at the end of §7 in Part I.

(ii) These calculations were transcribed by A.E.W. on to the manuscript sheets originally intended for the printer.