397.

SPECIMEN TABLE $M \equiv a^\alpha b^\beta$ (MOD. N) FOR ANY PRIME OR COMPOSITE MODULUS.

[From the *Quarterly Journal of Pure and Applied Mathematics*, vol. IX. (1868), pp. 95—96 and plate.]

If N be a prime number, and a one of its primitive roots, then any number M prime to N, or what is the same thing, any number in the series $1, 2, \ldots N-1$, may be exhibited in the form $M \equiv a^\alpha$ (Mod. N); where α is said to be the index of M in regard to the particular root a. Jacobi's *Canon Arithmeticus* (Berlin, 1839), contains a series of tables, giving the indices of the numbers $1, 2, 3 \ldots N-1$ for every prime number N less than 1000, and giving conversely for each such prime number the numbers M which correspond to the indices $\alpha = 1, 2, \ldots (N-1)$ (*Tabulæ Numerorum ad Indices datos pertinentium et Indicum Numero dato correspondentium*). A similar theory applies, it is well known, to the composite numbers; the only difference is, that in order to exhibit for a given composite number N the different numbers less than N and prime to it, we require not a single root a, but two or more roots $a, b, \ldots$ and that in terms of these we have $M = a^\alpha b^\beta \ldots$ (Mod. N). For each root a there is an index A (or say the Indicator of the root), such that $a^A \equiv 1$ (Mod. N), A being the least index for which this equation is satisfied; and the indices $a, b, \ldots$ extend from 1 to $A, B, \ldots$ respectively; the number of different combinations or the product $AB\ldots$, being precisely equal to $\phi(N)$, the number of integers less than N and prime to it. The least common multiple of $A, B\ldots$, is termed the Maximum Indicator, and representing it by I, then for any number M not prime to N, we have $M^I \equiv 1$ (Mod. N), a theorem made use of by Cauchy for the solution of indeterminate equations of the first order. Thus $N = 20$, the roots may be taken to be 3, 11; the corresponding exponents are 4, 2 (viz. $3^4 \equiv 1$ (Mod. 20) $11^2 \equiv 1$ (Mod. 20)), and the product of these is 8, the number of integers less than 20 and prime to it; the series [*go to p.* 86]

s.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
OTS		1	2	3	2	5	3	3, 5	2	3	2	5, 7	6	3	2, 11	3, 7	10	5	10	3, 11	2, 13	7	10	5, 7, 13	2	7	2	3, 13	10	7, 11
D.		1	2	2	4	2	6	2, 2	6	4	10	2, 2	12	6	4, 2	4, 2	16	6	18	4, 2	6, 2	10	22	2, 2, 2	20	12	18	6, 2	28	4, 2
I.		1	2	2	4	2	6	2	6	4	10	2	12	6	4	4	16	6	18	4	6	10	22	2	20	12	18	6	28	4
	0	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8
	1	0	0	0	0	0	0	0, 0	0	0	0	0, 0	0	0	0, 0	0, 0	0	0	0	0, 0	0, 0	0	0	0, 0, 0	0	0	0	0, 0	0	0, 0
		2	1		1		2		1		1		5		1, 0		10		17		1, 0		8		1		1		11	
			3	1	3		1	1, 0		1	8		8	1		1, 0	11		5	1, 0		4	20		7	8		1, 0	27	
				4	2		4		2		2		10		2, 0		4		16		2, 0		16		2		2		22	
					5	1	5	0, 1	5		4	1, 0	9	5		1, 1	7	1	2		1, 1	2	15	1, 0, 0		3	5	2, 1	18	
						6	3				9		1				5		4				6		8				10	
							7	1, 1	4	3	7	0, 1	7		1, 1	0, 1	9	2	12	3, 0		1	21	0, 1, 0	5	1	16		20	1, 0
								8	3		3		3		3, 0		14		15		3, 0		2		3		3		5	
									9	2	6		4	2		2, 0	6		10	2, 0		8	18		14	4		2, 0	26	
										10	5		2				1		1		2, 1		1				6		1	
											11	1, 1	11	4	0, 1	3, 0	13	5	6	0, 1	5, 0		3	1, 1, 0	16	5	13	1, 1	23	0, 1
												12	6				15		3				14		9				21	
													13	3	3, 1	3, 1	12	4	13	1, 1	0, 1	3	12	0, 0, 1	19		8	0, 1	2	3, 0
														14	2, 1		3		11				7		6		14		3	
															15	2, 1	2		7			6	13			11		3, 1	17	
																16	8		14		4, 0		10		4		4		16	
																	17	3	8	3, 1	5, 1	7	17	1, 0, 1	13	10	15	4, 1	7	1, 1
																		18	9				4		15				9	
																			19	2, 1	4, 1	9	5	0, 1, 1	8	7	12	5, 0	15	
																				20	3, 1		9				7		12	2, 0
																					21	5	19		12	9			19	
																						22	11		17		14		6	
																							23	1, 1, 1	11	2	11	5, 1	24	3, 1
																								24	10				4	
																									25	6	10	4, 0	8	
																										26	9		13	
																											27	3, 0	25	
																												28	14	
																													29	2, 1
																														30

31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	
17	3, 15	2, 10	3	2, 6	5, 19	5	3	2, 14	3, 11, 21	6	5, 13	28	3, 21	2, 26	5	10	5, 7, 17	3	3	
30	8, 2	10, 2	16	12, 2	6, 2	36	18	12, 2	4, 2, 2	40	6, 2	42	10, 2	12, 2	22	46	4, 2, 2	42	20	
30	8	10	16	12	6	36	18	12	4	40	6	42	10	12	22	46	4	42	20	
30	16	20	16	24	12	36	18	24	16	40	12	42	20	24	22	46	16	42	20	
0	0, 0	0, 0	0	0, 0	0, 0	0	0	0, 0	0, 0, 0	0	0, 0	0	0, 0	0, 0	0	0	0, 0, 0	0	0	1
12		1, 0		1, 0		11		1, 0		26		39		1, 0		30		26		2
13	1, 0		1	11, 0		34	1		1, 0, 0	15		17	1, 0		16	18		1	1	3
24		2, 0		2, 0		22		2, 0		12		36		2, 0		14		10		4
20	7, 1	9, 1	5		1, 0	1	4	9, 0		22	1, 0	5	8, 0		1	17	1, 0, 0	29		5
25				0, 1		9				1		14				2		27		6
4	2, 1	2, 1	11		2, 1	28	6	11, 1	3, 0, 1	39		7	9, 1	1, 1	19	38	0, 1, 0		15	7
6		3, 0		3, 0		33		3, 0		38		33		3, 0		44		36		8
26	2, 0		2	10, 0		32	2		2, 0, 0	30		34	2, 0		10	36		2	2	9
2		0, 1				12		10, 0		8		2				1		13		10
29	7, 0		7	8, 0	5, 1	6	12	7, 0	0, 1, 0	3	5, 1	6		4, 1	9	27	3, 1, 0	40	8	11
7				1, 1		20				27		11				32		11		12
23	1, 1	6, 1	4	3, 1	4, 0	13	17		1, 1, 1	31	0, 1	40	2, 1	11, 1	14	3	3, 0, 1	33	17	13
16		3, 1				3		0, 1		25		4		2, 1		22				14
3	0, 1		6			35	5			37		22	9, 0		17	35		30		15
18		4, 0		4, 0		8		4, 0		24		30		4, 0		28		20		16
1	4, 0	9, 0		5, 1	3, 0	5	16	2, 1		33	5, 0	16	8, 1	9, 0	7	42	0, 0, 1	25	19	17
8				11, 0		7				16		31				20		28		18
22	5, 0	8, 1	14	10, 1	0, 1	25		5, 1	2, 1, 0	9	4, 1	29	1, 1	6, 0	15	29	1, 1, 1	35	14	19
14		1, 1				23		11, 0		34		41				31		39		20
17	3, 1		12			26	7		0, 0, 1	14		24	0, 1		13	10			16	21
11				9, 0		17		8, 0		29		3		5, 1		11		24		22
21	6, 1	5, 1	15	7, 0	1, 1	21	14	10, 1	1, 0, 1	36	1, 1	20	5, 0	11, 0		39	0, 1, 1	38	13	23
19				2, 1		31				13		8				16		37		24
10	6, 0	8, 0	10		2, 0	2	8	6, 0		4	2, 0	10	6, 0		2	34	2, 0, 0	16		25
5		7, 1		4, 1		24				17		37		0, 1		33		17		26
9	3, 0		3	9, 1		30	3		3, 0, 0	5		9	3, 0		4	8		3	3	27
28		4, 1				14		1, 1		11		1		3, 1		6				28
27	5, 1	7, 0	13	6, 0	5, 0	15	11	4, 1	2, 0, 1	7	3, 1	25	4, 1	10, 1	18	43	3, 0, 0	18	6	29
15						10				23		19				19		14		30
31	4, 1	6, 0	9	8, 1	4, 1	27	15	9, 1	0, 1, 1	28	2, 1	32	7, 0	8, 0	6	5	2, 1, 0	7	4	31
	32	5, 0		5, 0		19		5, 0		10		27		5, 0		12		4		32
		33	8	7, 1		4	13		1, 1, 0	18		23			3	45		41	9	33
			34	6, 1		16		3, 1		19		13		10, 0		26		9		34
				35	31	29	10	8, 1		21		12	7, 1		20	9	1, 1, 0			35
					36	18				2		28				4		12		36
						37	9	7, 1	3, 1, 1	32	4, 0	35	4, 0	9, 1	21	24	1, 0, 1	32	7	37
							38	6, 1		35		26		7, 0		13		19		38
								39	2, 1, 1	6		15	3, 1		8	21		34	18	39
									40	20		38				15		23		40
										41	3, 0	18	6, 1	8, 1	12	25	2, 0, 1	15	12	41
											42	21				40				42
												43	5, 1	7, 1	5	37	3, 1, 1	6	5	43
													44	6, 1		41		8		44
														45	11	7		31		45
															46			22		46
																47	2, 1, 1	5	11	47
																	48	21		48
																		49	10	49
																			50	50

[*from p.* 83] of these is in fact 1, 3, 7, 9, 11, 13, 17, 19, each of which is expressible in the required form, viz. $1 \equiv 3^0 . 11^0$, $3 \equiv 3^1 . 11^0$, $7 = 3^3 . 11^0$, &c. (Mod. 20): the maximum indicator is 4; viz. $1^4 \equiv 1$, $3^4 \equiv 1$, $7^4 \equiv 1$, &c. (Mod. 20).

The table pp. 84, 85 gives the Indices for the numbers less than N and prime to it, for all values of N from 1 to 50; the arrangement may be seen at a glance; of the five lines which form a heading, the first contains the numbers N; the second the root or roots belonging to each number N, the third the indicators of these roots, the fourth the maximum indicator, the fifth the number $\phi(N)$. The remaining lines contain the index or indices of each of the ϕN numbers M less than N and prime to it, the number corresponding to such index or indices, being placed outside in the same horizontal line. For example, 30 has the roots 7, 11, indices 4, 2 respectively; the Maximum Indicator is 4, and the number of integers less than 30 and prime to it is 8; taking any such number, say 17, the indices are 1, 1, that is, we have $17 = 7^1 . 11^1$ (Mod. 30).

The foregoing corresponds to the *Tabulæ Indicum Numero dato correspondentium* of Jacobi; on account of multiplicity of roots there does not appear to be any mode of forming a single table corresponding to the *Tabulæ Numerorum ad Indices datos pertinentium;* and there would be no adequate advantage in forming for each number N a separate table in some such form as

$N = 20$.

Roots 3	11	Nos.
0	0	1
0	1	11
1	0	3
1	1	13
2	0	9
2	1	19
3	0	7
3	1	17

which I have written down in the form of a table of single entry; for although (whenever, as in the present case, the number of roots is only two) it might have been better exhibited as a table of double entry, when the number of roots is three or more it could not of course be exhibited as a table of corresponding multiple entry.