On the Number of Solutions of Certain Trinomial Congruences

By Jacqueline Wells and Joseph Muskat

1. In the course of his extensive investigations into Fermat's Last Theorem, H. S. Vandiver considered the number of solutions (x, y) of

$$1 + ax^c \equiv by^e \pmod{p},$$

where $ce + 1 = p$, a prime, and $xy \not\equiv 0 \pmod{p}$.

If $ab \not\equiv 0 \pmod{p}$, the following is an equivalent formulation: Let g be a primitive root of p. Then determine, for i and j fixed, $0 \leqq i \leqq c - 1$, $0 \leqq j \leqq e - 1$, the number of pairs (r, s), $0 \leqq r \leqq e - 1$, $0 \leqq s \leqq c - 1$, for which the congruence

$$1 + g^{i+cr} \equiv g^{j+es} \pmod{p} \tag{1}$$

is solvable. The number of solutions (r, s) will be denoted by $[i, j]_{ce}$, or simply by $[i, j]$, if c and e are fixed.

$$\sum_{j=0}^{e-1} [i, j]_{ce} = \begin{cases} e - 1, & e \text{ even}, \quad i = 0, \\ e - 1, & e \text{ odd}, \quad i = c/2, \\ e, & \text{otherwise} \end{cases} \tag{2}$$

[2]

It follows from (2) that $[i, j]_{ce} \leqq e$.

For a fixed e and p, let N_k denote the number of the ce-pairs (i, j) for which $[i, j]_{ce} = k$.

Given a fixed i for which

$$\sum_{j=0}^{e-1} [i, j]_{ce} = e,$$

then the integers $[i, 0]$, $[i, 1]$, $[i, 2]$, $\cdots$, $[i, e - 2]$, $[i, e - 1]$ form a *partition* of e. The partition $e\,0\,0 \cdots 0\,0$, where, for a fixed i, there is one j such that $[i, j] = e$, and, for all other j, $[i, j] = 0$, enters into a criterion for Fermat's Last Theorem [3, Theorem 2].

Erna H. Pearson computed the values of the $[i, j]$ for several values of e and p. A list of the cases she considered can be found in [2, p. 1284]. During 1954 and 1955, Emma Lehmer, J. L. Selfridge, and C. A. Nicol, with the aid of the SWAC digital computer, computed the values of $[i, j]$ for $e = 5, 7$, $p < 1024$; $e = 11$, $p < 800$; $e = 13$, $p < 600$; and e prime, $17 \leqq e < 256$, $p < 512$. For each p, the N_k, $k = 0, 1, \cdots, e$, were determined, and the occurrences of each of the partitions of e were tallied [1].

In [1], it was suggested that the values of the N_k and the occurrences of the various partitions deviated significantly from what was "expected." To probe this situation, we undertook to calculate the $[i, j]$, the values of the N_k, and the occurrences of the various partitions for $e = 5, 7, 9, 11$, and 13, $p < 18{,}000$. We leave to the end a brief description of the program.

Received September 25, 1964. This research was sponsored in part by the National Science Foundation, under Research Grants G11309 and GP-2091.

2. We assumed the following probability model: Given e objects, each is to be put independently into one of e cells. (We neglect the fact that ours is a sampling without replacement situation.) Then the probability that a given cell contains exactly k objects is given by the binomial distribution as

$$\binom{e}{k}\left(\frac{1}{e}\right)^k\left(\frac{e-1}{e}\right)^{e-k}.$$

In the problem considered here, the objects are the e solutions of (1) with i fixed. The cells are the values $0, 1, \cdots, e-1$ which j may take.

Table 1 shows, for $e = 5$, the expected and the observed occurrences of the N_k, $k = 0, 1, \cdots, 5$.

For each value of e in the study, the primes $p \equiv 1 \pmod{e}$, arranged in ascending order, were subdivided into several groups. Within each group, the values of $N_k/(p-1)$, for each $k, 0 \leqq k \leqq e$, were sorted from low to high and every nth value, where n depended upon e, was recorded. For $e = 5$, the first six primes were omitted and the remaining 505 in the study were divided into five *groups* of 101 each. In Table 2, every nth value of $N_0/(p-1)$, $n = 1, 21, 41, 61, 81, 101$, is recorded for each of the five groups.

Tables 1 and 2, being typical of the tables generated in this study, suggest that this probability model approximates the actual situation quite well. Table 2 and similar tables indicate that, as p increases, the approximation improves. The full set of tables can be found in [4].

3. In [1] the occurrences of the various partitions of e among the solutions of (1) for fixed i were tabulated. According to the probability model outlined in Section 2,

TABLE 1

	Proportion expected	Proportion observed	Occurrences
N_0	.32768	.32761	1,419,388
N_1	.40960	.40979	1,775,443
N_2	.20480	.20472	886,952
N_3	.05120	.05115	221,602
N_4	.00640	.00642	27,818
N_5	.00032	.00030	1,317
Totals	1.00000	.99999	4,332,520

TABLE 2

Distribution of $N_0/(p-1)$, $e = 5$, Within Groups

Group	Range of p	1st	21st	41st	61st	81st	101st
1	131–3061	.31391	.32432	.32660	.32791	.32983	.33906
2	3121–6451	.31974	.32588	.32696	.32800	.32919	.33534
3	6481–10111	.32460	.32597	.32719	.32805	.32881	.33463
4	10141–14221	.32434	.32652	.32733	.32783	.32883	.33055
5	14251–17981	.32522	.32688	.32744	.32796	.32852	.33126

the number of ways of obtaining a particular partition can be calculated as the product of the number P_1 of permutations of the numbers in the partition times the number P_2 of permutations of the values of j in one of the P_1 permutations of the partition.

$$P_1 = e!/t_0!\, t_1!\, t_2! \cdots t_e!\,,$$

where t_n is the number of occurrences of n in the partition.

Let s_j denote the number of j's in a *particular* permutation. Then

$$P_2 = e!/s_0!\, s_1!\, s_2! \cdots s_{e-1}!\,.$$

Since the probability model has e^e equally likely outcomes, the probability of a given permutation is given by

$$P_1P_2/e^e.$$

As an illustration, consider, for $e = 5$, the partition 3 1 1 0 0. This means that, for a fixed value of i, P_1 expresses the number of arrangements of the j's so that there is one j for which $[i, j] = 3$, there are two j's for which $[i, j] = 1$, and for the other two j's, $[i, j] = 0$.

$$P_1 = 5!/2!\cdot 2!\cdot 0!\cdot 1!\cdot 0! = 30.$$

One of these thirty arrangements is $[i, 2] = 3$, $[i, 1] = [i, 4] = 1$, $[i, 0] = [i, 3] = 0$. For this case, P_2 expresses the number of arrangements of the five solutions of (1) so that three of them correspond to $j = 2$, and one each to $j = 1$ and $j = 4$.

$$P_2 = 5!/0!\cdot 1!\cdot 3!\cdot 0!\cdot 1! = 20.$$

Clearly, the value of P_2 is the same for each of the thirty arrangements. Thus, the probability that a given set of solutions forms the partition 3 1 1 0 0 is

$$30\cdot 20/5^5 = 600/3125 = 0.192.$$

(Note that the denominator of P_2 can be obtained by affixing "factorial" symbols to all the numbers in the representation of the partition and forming the product.)

The observed and expected occurrences of the various partitions for $e = 5$ and $e = 7$ are shown in Tables 3 and 4.

TABLE 3

Partitions, $e = 5$

Partition	Proportion expected	Proportion observed	Occurrences	First occurrence
5 0 0 0 0	.0016	.001521	1,317	521
4 1 0 0 0	.0320	.032102	27,800	71
3 2 0 0 0	.0640	.063968	55,396	41
3 1 1 0 0	.1920	.191925	166,206	31
2 2 1 0 0	.2880	.287345	248,839	31
2 1 1 1 0	.3840	.384966	333,378	11
1 1 1 1 1	.0384	.038173	33,058	31
Totals	1.0000	1.000000	865,994	

TABLE 4
Partitions, e = 7

Partition	Proportion expected	Proportion observed	Occurrences	First occurrence
7 0 0 0 0 0 0	.000008	.000007	3	9829
6 1 0 0 0 0 0	.000357	.000363	150	617
5 2 0 0 0 0 0	.001071	.001013	419	659
5 1 1 0 0 0 0	.005355	.005349	2,213	239
4 3 0 0 0 0 0	.001785	.001769	732	421
4 2 1 0 0 0 0	.026775	.026445	10,941	71
4 1 1 1 0 0 0	.035699	.035593	14,726	113
3 3 1 0 0 0 0	.017850	.017881	7,398	127
3 2 2 0 0 0 0	.026775	.026338	10,897	379
3 2 1 1 0 0 0	.214196	.214878	88,902	43
3 1 1 1 1 0 0	.107098	.106963	44,254	29
2 2 2 1 0 0 0	.107098	.107913	44,647	113
2 2 1 1 1 0 0	.321295	.320731	132,697	29
2 1 1 1 1 1 0	.128518	.128484	53,158	29
1 1 1 1 1 1 1	.006120	.006275	2,569	421
Totals	1.000000	1.000002	413,733	

The probability that a partition is the partition $e\,0\,0\cdots 0\,0$ is $1/e^{e-1}$. The deviations mentioned at the end of Section 1 were apparently due to overlooking P_2 in computing expected occurrences.

4. The solutions of (1) were obtained on the University of Pittsburgh's IBM 7070 computer. The program differed in several respects from the program for the SWAC computer described in [1], as a much larger memory was available.

For $e = 5, 7, 9, 11$, and 13, cards containing primes $p \equiv 1 \pmod e$ and the least primitive root g of p were available from a previous study. Mr. Dale Isner of the staff of the University of Pittsburgh's Computation Center supplied a program which generated a list of the partitions of p.

A modified index table was generated as follows:
For each p, g, g^2, g^3, $\cdots$, g^k, $\cdots$, $g^{(p-1)/2}$, reduced modulo p, were generated. If $n \equiv g^k \pmod p$, $0 < n < p$, then k, reduced modulo e, was stored in cell IND + $\min\{n, p - n\}$.

The values of g^{i+rc}, reduced modulo p, were then generated. For each i having e values of $g^{i+rc} \not\equiv -1 \pmod p$, consider $m \equiv g^{i+rc} \pmod p$, $0 < m < p - 1$. If $m < (p - 1)/2$, the number (value of j) in cell IND + m + 1 was found and stored in a list of solutions. If $m \geqq (p - 1)/2$, the number in cell IND + p − m − 1 was stored in the solution list, as for e odd,

$$\operatorname{ind}(m + 1) \equiv \operatorname{ind}(p - m - 1) \pmod e.$$

For each i, the solution list was analyzed to determine the appropriate partition, and the relevant counters were tallied.

The results of the main program have been deposited in the UMT file. For each e, $e = 5, 7, 9, 11$, and 13, the primes $p \equiv 1 \pmod e$, $p < 18{,}000$, are listed, with

the values of N_k, $0 \leqq k \leqq e$, and the number of occurrences of the various partitions of e into which the solutions are grouped.

Pennsylvania State University
McKeesport, Pennsylvania

University of Pittsburgh
Pittsburgh, Pennsylvania

1. EMMA LEHMER & H. S. VANDIVER, "On the computation of the number of solutions of certain trinomial congruences," *J. Assoc. Comput. Mach.*, v. 4, 1957, pp. 505–510. MR **20** #428.
2. E. H. PEARSON & H. S. VANDIVER, "On a new problem concerning trinomial congruences involving rational integers," *Proc. Nat. Acad. Sci. U.S.A.*, v. 39, 1953, pp. 1278–1285. MR **15**, 684.
3. H. S. VANDIVER, "New types of trinomial congruence criteria applying to Fermat's Last Theorem," *Proc. Nat. Acad. Sci. U.S.A.*, v. 40, 1954, pp. 248–252. MR **15**, 778.
4. JACQUELINE WELLS, *Studies on the Number of Solutions of a Trinomial Congruence*, M. S. Thesis, University of Pittsburgh, Pittsburgh, Pa., 1964.

Tables of Values of Three Infinite Integrals

By Chih-Bing Ling and Hsien-Chueh Wu

Sometime ago, the senior author [1] evaluated the following two integrals to five decimal places for integral values of m and p up to 15 and 8, respectively.

$$I(m, p) = \frac{p^{m+1}}{2^p(m!)} \int_0^\infty \frac{x^m\,dx}{\sinh^p x} \qquad (m \geqq p \geqq 1)$$

(1)

$$J(m, p) = \frac{p^{m+1}}{2^p(m!)} \int_0^\infty \frac{x^m\,dx}{\cosh^p x} \qquad (m \geqq 0, p \geqq 1)$$

Two particular integrals $I(m, m)$ and $I(m, m-1)$ were further evaluated by Nelson and the senior author [2] to seven decimal places for $m = 1(1)40$. Nelson also evaluated these two integrals for the same range of values of m to 12D and 18D, respectively, in two papers [3], [4].

In the present paper, the two preceding integrals will be evaluated to 8D for m and p up to 25 and 12, respectively. The same method of evaluation will be used. The various sums of inverse powers required in the computation were tabulated to 32D by Glaisher [5], [6], and also appear in two well-known mathematical tables [7], [8]. The results are shown in Tables 1 and 2. Table 3 shows the factor $2^p(m!)/p^{m+1}$, also to 8D.

In addition, the following integral will also be evaluated to 8D for the same range of values of m and p.

$$S(m, p) = \int_0^\infty \frac{\sin^m x}{x^p}\,dx \qquad (m \geqq p \geqq 1). \tag{2}$$

The integers m and p are restricted as indicated, and $S(2m, 1)$ is to be excluded on account of its divergence. This last integral occurs in certain branches of mathematical physics, and on that account it was thought desirable to include a table of its values.

Received January 11, 1965.