√ Sey AMM 41 (1934) Please enter → 2016

of square matrices of order n of the form given below constitutes a field, where the n independent arguments $x_1, x_2, \cdots, x_n$, of the generic matrix, range over the rational field. The element in the rth row and sth column is defined as x_{s-r} (for $r<s$), as px_{n-r+1} (for $s=1$), as $px_{n-r+s}+qx_{n-r+s-1}$ (for $r\geqq s>1$).

3709. *Proposed by E. B. Escott, Oak Park, Ill.*

Determine the values of A in the trinomial

$$x^{12}+Ax^6y^6+y^{12}$$

so that it will have two polynomial factors of the sixth degree with rational coefficients.

3710. *Proposed by Harry Langman, Brooklyn, N.Y.*

If the C's represent binomial coefficients, show that

$$\begin{vmatrix} C_2^2 & C_3^3 & C_4^4 & \cdots & C_{n-1}^{n-1} & C_n^n & C_{n+1}^{n+1} \\ -(n-1) & C_2^3 & C_3^4 & \cdots & C_{n-2}^{n-1} & C_{n-1}^n & C_n^{n+1} \\ 0 & -(n-2) & C_2^4 & \cdots & C_{n-3}^{n-1} & C_{n-2}^n & C_{n-1}^{n+1} \\ 0 & 0 & -(n-3) & \cdots & C_{n-4}^{n-1} & C_{n-3}^n & C_{n-2}^{n+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & -2 & C_2^n & C_3^{n+1} \\ 0 & 0 & 0 & \cdots & 0 & -1 & C_2^{n+1} \end{vmatrix} = (n!)^2.$$

SOLUTIONS

272 [1917, 427], *Proposed by C. C. Yen, Tangshan, North China.*

How many integers prime to n are there in each of the sets:

(a) $1\cdot 2,\quad 2\cdot 3,\quad 3\cdot 4, \cdots, n(n+1);$

(b) $1\cdot 2\cdot 3,\quad 2\cdot 3\cdot 4,\quad 3\cdot 4\cdot 5, \cdots, n(n+1)(n+2);$

(c) $\dfrac{1\cdot 2}{2}, \dfrac{2\cdot 3}{2}, \dfrac{3\cdot 4}{2}, \cdots, \dfrac{n(n+1)}{2};$

(d) $\dfrac{1\cdot 2\cdot 3}{6}, \dfrac{2\cdot 3\cdot 4}{6}, \dfrac{3\cdot 4\cdot 5}{6}, \cdots, \dfrac{n(n+1)(n+2)}{6}$?

Solution by E. P. Starke, Rutgers University.

This problem in exactly this form is given in *Theory of Numbers* by Carmichael (1914), page 36.

Let the numbers of set (a) be represented by

$$a_j, \quad j=1, 2, 3, \cdots, n.$$

The necessary and sufficient condition that a_j be divisible by a prime, p, is

$$j \equiv p - 1 \text{ or } p \bmod p.$$

Hence, if a_j is prime to p, we must have

$$j \equiv 1, 2, \cdots, p - 2 \bmod p.$$

Let n be represented as $p_1^{r_1}p_2^{r_2}p_3^{r_3} \cdots p_s^{r_s}$, where the p's are the distinct prime factors of n. If a_j is prime to n, j must satisfy a set of s congruences,

$$j \equiv c_i \bmod p_i, \quad i = 1, 2, \cdots, s, \tag{1a}$$

where c_i has a value selected from the set

$$1, 2, \cdots, p_i - 2.$$

There are $(p_1-2)(p_2-2) \cdots (p_s-2)$ distinct systems of congruences (1a), whose solutions, if less than n, give suitable values of j.

By the "Chinese Remainder Theorem" there exists for each such system a unique solution $j \leqq p_1p_2 \cdots p_s$. Hence there are in all $(p_1-2)(p_2-2) \cdots (p_s-2)$ distinct values of j, $1 \leqq j \leqq p_1p_2 \cdots p_s$, for which a_j is prime to n.

The numbers from 1 to n inclusive divide up into $n/p_1p_2 \cdots p_s$ sets such that each number in any set is congruent, mod $p_1p_2 \cdots p_s$, to one of the numbers from 1 to $p_1p_2 \cdots p_s$ and conversely. The total number of values of j, and hence the number of integers in set (a) prime to n, is then $(p_1-2)(p_2-2) \cdots (p_s-2)$ times $n/p_1p_2 \cdots p_s$, which reduces immediately to

$$n(1 - 2/p_1)(1 - 2/p_2) \cdots (1 - 2/p_s).$$

Following the same line of argument, we have for set (b) the condition that a_j be divisible by p is

$$j \equiv p - 2 \text{ or } p - 1 \text{ or } p \bmod p.$$

So then congruences (1a) become here

$$j \equiv c_i \bmod p_i, \quad i = 1, 2, \cdots, s, \tag{1b}$$

where c_i now has a value selected from the set $1, 2, \cdots, p-3$. Continuing as for set (a), we find the number of integers in the set (b) prime to n is

$$n(1 - 3/p_1)(1 - 3/p_2) \cdots (1 - 3/p_s).$$

The solution for set (c) when n is any odd number, is the same as for set (a). But if n is even, 2 will divide a_j if and only if $j \equiv 3$ or 4 mod 4. That is, for a_j to be prime to n, j must satisfy, besides congruences (1a), the following,

$$j \equiv 1 \text{ or } 2 \bmod 4. \tag{1c}$$

Now suppose 4 is a factor of n. Then congruence $(1c)$ behaves with respect to n in the same way as the other congruences $(1a)$, so that the number of integers a_j in set (c) prime to n is given by

$$n(1 - 2/4)(1 - 2/p_1)(1 - 2/p_2) \cdots (1 - 2/p_s),$$

where $p_1, p_2, \cdots, p_s$ are the distinct odd prime factors of n.

But if $n=2m$, m odd, for a_j to be prime to n, j must be an integer less than $2p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ which satisfies the congruences (1a) and (1c). The Chinese Remainder Theorem gives us the number of values of j between 1 and $4p_1p_2\cdots p_s$ for which a_j is prime to n, but as $n=2p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ is not divisible by $4p_1p_2\cdots p_s$ the rest of the previous arguments cannot be followed here.

We may show, however, that the number of integers prime to $2m$ (for $1\leqq j\leqq 2m$) is the same as the number of integers prime to m (for $1\leqq j\leqq m$). Let us put

$$k = 2m - j - 1. \tag{2}$$

Relation (2) establishes a one-to-one correspondence between the set of subscripts $1\leqq j\leqq m-2$ and the set $m+1\leqq k\leqq 2m-2$. Also, since $a_k=2m^2-(2j+1)m+a_j$, we have a one-to-one correspondence between the integers in the two sets a_j and a_k which are prime to m. Let us now separate into two classes the integers prime to m in each set:

(A)	$j\equiv 1$ or 2 mod 4	(A′)	$k\equiv 1$ or 2 mod 4
(B)	$j\equiv 3$ or 4 mod 4	(B′)	$k\equiv 3$ or 4 mod 4.

To integers in class (A) correspond those in (B'); to the integers in (B) correspond those in (A'), since relation (2) implies $j+k\equiv 1$ mod 4. Thus the number of terms prime to $2m$ is the number of integers in (A) and (A′), which is the same as the number of integers in (A) and (B).

We have then the results for set (c):

$$\text{If } n \text{ is odd,}\quad n(1-2/p_1)(1-2/p_2)\cdots(1-2/p_s);$$
$$\text{If } n \text{ is even,}\quad n(1-2/p_1)(1-2/p_2)\cdots(1-2/p_s)/2,$$

where $p_1, p_2, \cdots, p_s$ are the distinct odd prime factors of n.

The solution for set (d) when n is any number prime to 6, is the same as for set (b). Since a_j is odd only when j is $1, 5, 9, \cdots$, it follows that when 2 is a factor of n, we must include with the congruences (1b) the following,

$$j \equiv 1 \bmod 4. \tag{1d}$$

Similarly 3 is not a divisor of a_j unless the numerator contains a multiple of 9. Hence if 3 is a factor of n we must include also the condition,

$$j \equiv 1, 2, \cdots, 6 \bmod 9. \tag{1d′}$$

The cases where n is divisible by 4 but not 3, by 9 but not 2, or by both 4 and 9, are easily disposed of by the same arguments used in earlier cases. We have, the number of integers in the set (d) prime to n is

$$n(1-3/4)(1-3/9)(1-3/p_1)(1-3/p_2)\cdots(1-3/p_s),$$

where only those factors are to be included which correspond to the distinct prime factors of n, in the three cases above.

2016

Suppose however $n=2m$, or $3m$, or $6m$, where m is prime to 6. a_j will be prime to n if besides the congruences (1b) j satisfies (1d), or (1d'), or both, respectively. Unfortunately there seems to be no formula or simple set of formulae which will give the number of solutions for $1 \leqq j \leqq n$ of these congruences.

Formulae for certain special cases are simple enough to be of some interest. Let $\psi(n)$ represent the number of integers of set (d) which are prime to n.

I. By an extension of the method used under (c), we can show that $\psi(2m)=\frac{1}{2}\psi(m)$, where m is prime to 6.

II. $\psi(3p)$, where p is a prime greater than 3, will equal $2p-4$, $2p-5$, $2p-6$, $2p-7$ according as p is congruent, mod 9, to 8, 1 or 5, 2 or 4, 7 respectively.

A table follows, showing the values of $\psi(n)$ for the values of n from 1 to 109.

	0	1	2	3	4	5	6	7	8	9
0		1	1	3	1	2	2	4	2	6
1	1	8	2	10	2	5	4	14	3	16
2	2	7	4	20	4	10	5	18	4	26
3	2	28	8	16	7	8	6	34	8	20
4	4	38	3	40	8	12	10	44	8	28
5	5	30	10	50	9	16	8	33	13	56
6	5	58	14	24	16	20	8	64	14	41
7	4	68	12	70	17	19	16	32	10	76
8	8	54	19	80	6	28	20	52	16	86
9	6	40	20	56	22	32	16	94	14	48
10	10	98	13	100	20	17	25	104	18	106

2016

read across

Type 3

Proofs for the two special cases above may be derived as follows.

I. Suppose a_{j_1} prime to m, $j_1<2m$. It is easy to verify that $a_{j_i}-a_{j_1}$, $i=2, 3, 4$, is divisible by m for $j_2=m-2-j_1$, $j_3=m+j_1$, $j_4=2m-2-j_1=m+j_2$; so that each a_{j_i} is also prime to m. Since m is odd, we see that one and only one of the $j_i \equiv 1$ mod 4. Call this one j_1. For every a_{j_1} there are three a_{j_i} for which $j \not\equiv 1$ mod 4. Hence the a_j separate into four sets containing $\frac{1}{2}\psi(m)$ integers each, and such that all integers in the first set satisfy $j\equiv 1$ mod 4. There are then $\frac{1}{2}\psi(m)$ integers a_j (for $j \leqq 2m$) prime to $2m$.

II. Place the numbers $1 \leqq j \leqq 3p$ in three rows of p columns each. Consider the values of j for which a_j is prime to $3p$. By (1b) the last three columns give no such values of j. The additional values of j to be excluded by (1d') are easily reckoned as soon as we know the residue of p mod 9.

Similar special results are easily obtained for $3p^2$, for $3p^3$, etc. The results for $3p_1p_2 \cdots$ depend upon the possible combinations of residues mod 9 of $p_1, p_2, \cdots$. The results for $6p$, $6p^2$, etc. depend upon the twelve possible residues of p mod 36. Results for $6p_1p_2 \cdots$ depend upon the possible combinations of residues mod 36 of $p_1, p_2, \cdots$.