

Divisibility Properties of Some Number Arrays¹

Marko Razpet

Institute of Mathematics, Physics and Mechanics
University of Ljubljana
Jadranska 19
61000 Ljubljana, YUGOSLAVIA

Abstract. For all nonnegative integers i, j let $q(i, j)$ denote the number of all lattice paths in the plain from $(0, 0)$ to (i, j) with steps $(1, 0)$, $(0, 1)$, and $(1, 1)$. In this paper it is proved that

$$q(i_n p^n + \dots + i_0, j_n p^n + \dots + j_0) \equiv q(i_n, j_n) \dots q(i_0, j_0) \pmod{p}$$

where p is an odd prime and $0 \leq i_k < p$, $0 \leq j_k < p$. This relation implies a remarkable pattern to the divisibility of the array of numbers $q(i, j)$.

1. Motivation.

Suppose that each square of the chessboard is represented by an ordered pair (i, j) of nonnegative integers. The chessboard is infinitely large in the sense that the coordinates i and j can be arbitrary nonnegative integers. The starting position of the king is the point $(0, 0)$. Suppose that on such a chessboard the king can move in three directions only:

$$(i, j) \rightarrow (i + 1, j), (i, j) \rightarrow (i, j + 1), (i, j) \rightarrow (i + 1, j + 1) \quad (1)$$

Let $q(i, j)$ denote the number of all different paths in which the king can reach the point (i, j) . We will solve the following problems (compare [1, 2, 3, 7]):

- 1 In how many ways can the king reach the square (i, j) in exactly k moves?
- 2 In how many ways can the king reach the square (i, j) in general? (find the number $q(i, j)$).
- 3 Display the divisibility properties of numbers $q(i, j)$.

2. Recurrence relations.

Let $M(i, j, k)$ denote the number of all different ways in which the king can move from the square $(0, 0)$ to the square (i, j) in exactly k steps of the form (1). If we put $m = \max\{i, j\}$ then the following relations are clear: $M(i, j, k) = M(j, i, k)$, $q(i, j) = q(j, i)$, $M(i, 0, k) = \delta_{ik}$ and $q(i, j) = \sum_{k=m}^{i+j} M(i, j, k)$.

¹This work was supported in part by the Research Council of Slovenia, Yugoslavia.

If $k < m$ or $k > i + j$ then $M(i, j, k) = 0$, where δ_{ik} denotes the Kronecker delta. An easy combinatorial argument gives the following recurrence formulas:

$$M(i, j, k) = M(i-1, j, k-1) + M(i, j-1, k-1) + M(i-1, j-1, k-1) \quad (2)$$

$$q(i, j) = q(i-1, j) + q(i, j-1) + q(i-1, j-1) \quad (3)$$

for $i \geq 1, j \geq 1, k \geq 1$. For each nonnegative integer i we introduce the generating function $G_i(x) = \sum_{j=0}^{\infty} q(i, j)x^j$ and from (3) we get (see [1] for details)

$$G_i(x) = (1+x)^i(1-x)^{-i-1}. \quad (4)$$

The generating function $G(x, y)$ in two formal variables x, y of the numbers $q(i, j)$ is defined by

$$G(x, y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} q(i, j)x^i y^j \quad (5)$$

and from (4) we get

$$G(x, y) = \frac{1}{1-x-y-xy}. \quad (6)$$

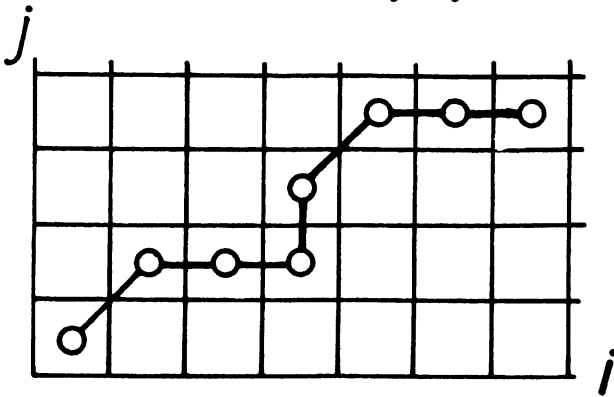


Figure 1
A path of the king

If we use the same indexing scheme also for array of numbers $M(i, j, k)$ then we can construct step by step from the relation (2) the tables for $M(i, j, k)$:

$$M(i, j, 2) : \begin{pmatrix} 1 & 2 & 1 \\ & 2 & 2 \\ & & 1 \end{pmatrix} \quad M(i, j, 3) : \begin{pmatrix} 1 & 3 & 3 & 1 \\ & 3 & 6 & 3 \\ & & 3 & 3 \\ & & & 1 \end{pmatrix}.$$

In the same manner we obtain the table for the numbers $q(i, j)$:

1	9	41	129	321
1	7	25	63	129
1	5	13	25	41
1	3	5	7	9
1	1	1	1	1

Explicit formulas for $M(i, j)$ and $q(i, j)$ can be derived, for instance, by means of the formal power series and the umbral calculus (see, for example, [4, 6, 8]), but we give a simple combinatorial proof.

Therefore we adopt the convention: if n, m are integers then $\binom{n}{m} = 0$ for $0 < n < m$ or for $n > 0, m < 0$.

The king must arrive from $(0, 0)$ at (i, j) in k moves, namely in $i + j - k$ diagonal steps, in $i - (i + j - k) = k - j$ horizontal, and in $j - (i + j - k) = k - i$ vertical steps. Therefore we obtain

$$M(i, j, k) = \frac{k!}{(i + j - k)!(k - j)!(k - i)!} = \binom{k}{i} \binom{i}{k - j}. \quad (7)$$

Since $q(i, j) = \sum_{k=m}^{i+j} M(i, j, k)$ we have an explicit formula for $q(i, j)$:

$$q(i, j) = \sum_{k=m}^{i+j} \binom{k}{i} \binom{i}{k - j}. \quad (8)$$

Formulas (7) and (8) give solutions of Problem 1 and 2 presented at the beginning. By a simple summation-index manipulation we get from (8) an attractive formula:

$$q(i, j) = \sum_{k=0}^{\mu} \binom{i}{k} \binom{i + j - k}{i} = \sum_{k=m}^{i+j} \binom{k}{i} \binom{i}{i + j - k},$$

where $m = \max\{i, j\}$ as before and $\mu = \min\{i, j\}$.

Remark: If a, b, c are natural numbers, then we can find also the number of colored paths $x(i, j; a, b, c)$, where the king marks each horizontal, vertical, and diagonal step, choosing respectively any one of a colors, b colors, and c colors (cf. [1]). By the same combinatorial argument as by derivation of (3) we get the recurrence relation

$$x(i, j; a, b, c) = ax(i - 1, j; a, b, c) + bx(i, j - 1; a, b, c) + cx(i - 1, j - 1; a, b, c) \quad (9)$$

for $i \geq 1, j \geq 1$ and similarly as (7) the explicit formula

$$x(i, j; a, b, c) = \sum_{k=m}^{i+j} \binom{k}{i} \binom{i}{k - j} a^{k-j} b^{k-i} c^{i+j-k}. \quad (10)$$

It is clear that $q(i, j) = x(i, j; 1, 1, 1)$, moreover the solution of the difference equation (9) is given by (10) which can be derived also for arbitrary positive numbers a, b, c by using formal power series (see, for example, [1]).

3. The numbers $q(i, j)$ modulo p .

Here the divisibility properties of the numbers $q(i, j)$ are studied. Since $q(i, j)$ are odd numbers, some interesting results can be obtained for moduli $p > 2$. We suppose that p here is always an odd prime. The array of $q(i, j)$ with the boundary conditions $q(0, j) = q(i, 0) = 1$ can be produced very quickly from the recurrence formula (3). For $p = 3$ we have the array of remainders of dividing $q(i, j)$ by 3 for $0 \leq i \leq 17, 0 \leq j \leq 17$:

1	2	1	1	2	1	1	2	1	0	0	0	0	0	0	0	0	0
1	0	2	1	0	2	1	0	2	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	2	1	2	1	2	1	2	1	0	0	0	0	0	0	0	0	0
1	0	2	2	0	1	1	0	2	0	0	0	0	0	0	0	0	0
1	1	1	2	2	2	1	1	1	0	0	0	0	0	0	0	0	0
1	2	1	0	0	0	2	1	2	0	0	0	0	0	0	0	0	0
1	0	2	0	0	0	2	0	1	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	2	2	2	0	0	0	0	0	0	0	0	0
1	2	1	2	1	2	1	2	1	1	2	1	2	1	2	1	2	1
1	0	2	2	0	1	1	0	2	1	0	2	2	0	1	1	0	2
1	1	1	2	2	2	1	1	1	1	1	2	2	2	1	1	1	1
1	2	1	0	0	0	2	1	2	1	2	1	0	0	0	2	1	2
1	0	2	0	0	0	2	0	1	1	0	2	0	0	0	2	0	1
1	1	1	0	0	0	2	2	2	1	1	1	0	0	0	2	2	2
1	2	1	1	2	1	1	2	1	1	2	1	1	2	1	1	2	1
1	0	2	1	0	2	1	0	2	1	0	2	1	0	2	1	0	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Denote by $q(i, j)_p$ the numbers $q(i, j)$ modulo p and introduce for $p = 3$ the matrix

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \end{bmatrix}.$$

The standard tensor (Kronecker product) in Z_3 , where Z denotes the ring of integers, gives

$$A \otimes A = \begin{bmatrix} 1A & 2A & 1A \\ 1A & 0A & 2A \\ 1A & 1A & 1A \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 1 & 2 & 2 & 2 & 2 & 1 & 1 \\ 1 & 2 & 1 & 0 & 0 & 0 & 2 & 1 & 2 \\ 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

This is exactly the array of $q(i, j)_3$ for $0 \leq i \leq 8, 0 \leq j \leq 8$. In the same way we construct $A \otimes A \otimes A, A \otimes A \otimes A \otimes A, \dots$ and we get the arrays $q(i, j)_3$ for $0 \leq i \leq 3^k - 1, 0 \leq j \leq 3^k - 1$ for $k = 3, 4, \dots$ respectively. We shall generalize this construction for an arbitrary odd prime p .

Theorem 1. *Let p be an odd prime. Then the following relations hold over Z_p :*

1. $q(p, i) = 1, 0 \leq i < p$;
2. $q(p-1, i) + q(p-1, i-1) = 0, 1 \leq i < p$;
3. $\sum_{k=0}^{p-1} q(k, j) = 0, 0 \leq j < p-1$;
4. $\sum_{k=0}^{p-1} q(k, p-1) = 1$.

Proof: During the proof we always calculate in Z_p .

1. We need the fact that

$$\binom{p+k}{i} = \binom{k}{i}$$

for each prime p and each nonnegative integer $i, i < p$, (see, for example, [9]). Suppose that $0 \leq i < p$, where p is an odd prime. Because of (8) we have

$$q(p, i) = \sum_{k=p}^{i+p} \binom{k}{i} \binom{i}{k-p} = \sum_{k=0}^i \binom{p+k}{i} \binom{i}{k} = \sum_{k=0}^i \binom{k}{i} \binom{i}{k} = 1.$$

2. From the recurrence formula (3) we obtain for $1 \leq i < p$:

$$q(p, i) = q(p, i-1) + q(p-1, i) + q(p-1, i-1).$$

The assertion 1 implies $q(p, i) = 1$ and $q(p, i-1) = 1$. Thus $q(p-1, i) + q(p-1, i-1) = 0$.

3. Denote by S_j the sum

$$\sum_{k=0}^{p-1} q(k, j), \quad 0 \leq j \leq p-2.$$

From the recursion formula for $q(i, j)$ we get by an easy calculation the relation

$$S_j + S_{j-1} = S_j - S_{j-1}.$$

This relation implies $2S_{j-1} = 0$ and finally

$$S_0 = S_1 = S_2 = \dots = S_{p-2} = 0.$$

4. Since p is an odd prime, we have

$$q(0, p-1) + q(1, p-1) + q(2, p-1) + \dots + q(p-2, p-1) + q(p-1, p-1) \\ = 1 + (q(1, p-1) + q(2, p-1)) + \dots + (q(p-2, p-1) + q(p-1, p-1)) = 1$$

because of 2. ■

The consequence of this theorem is the following form of the array of $q(i, j)_p$ for $0 \leq i < p$, $0 \leq j < p$:

$$\begin{array}{cccccc} 1 & p-1 & 1 & p-1 & \dots & 1 \\ 1 & \star & \star & \star & \dots & p-1 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & 3 & \star & \star & \dots & p-1 \\ 1 & 1 & 1 & 1 & \dots & 1 \end{array} .$$

By a fixed prime p the whole array of $q(i, j)_p$ is determined. Note that we choose always $0 \leq q(i, j)_p < p$. The origin for the subscripts i, j is at the lower left corner. We introduce the matrix A with the entries a_{ij} by

$$a_{ij} = q(p-1-i, j)_p \tag{11}$$

for $0 \leq i < p$, $0 \leq j < p$.

Theorem 2. For every odd prime p the following assertions hold in Z_p :

1. $\sum_{k=0}^{p-1} a_{ik} = \sum_{k=0}^{p-1} a_{kj} = 0$, $1 \leq i \leq p-2$, $0 \leq j \leq p-2$;
2. $\sum_{k=0}^{p-1} a_{0k} = 1$, $\sum_{k=0}^{p-1} a_{k, p-1} = 1$;
3. $A^2 = I$, where I denotes the unit matrix.

Proof:

1. Assertions 1 and 2 are direct consequences of Theorem 1. It is easy to prove that over Z_p $q(i, j) = q(i, p+j) = q(i, 2p+j) = \dots$. If $B = A^2$ then for $0 \leq i < p$, $0 \leq j < p$

$$b_{ij} = \sum_{k=0}^{p-1} a_{ik} a_{kj} = \sum_{k=0}^{p-1} q(p-1-i, k) q(p-1-k, j).$$

For integers u and v using (4) we derive in the sense of formal power series

$$\begin{aligned} (1+x)^{u+v} (1-x)^{-u-v-2} &= (1-x)^{-1} \sum_{k=0}^{\infty} q(u+v, k) x^k \\ &= \sum_{j=0}^{\infty} \sum_{k=0}^j q(u, k) q(v, j-k) x^j \\ &= \sum_{j=0}^{\infty} \sum_{k=0}^j q(u+v, k) x^j. \end{aligned}$$

Thus

$$\sum_{k=0}^j q(u, k)q(v, j-k) = \sum_{k=0}^j q(u+v, k)$$

for every integer j . The substitution $j = p-1$, $u = p-1-i$, $v = j$ for $0 \leq i < p$, $0 \leq j < p$ yields

$$\sum_{k=0}^{p-1} q(p-1-i, k)q(j, p-1-k) = \sum_{k=0}^{p-1} q(p-1-i+j, k) = \delta_{ij}$$

using Theorem 1. It follows that $b_{ij} = \delta_{ij}$ or equivalently $B = I$. ■

For each odd prime p the minimal polynomial of A over Z_p , is $p(\lambda) = \lambda^2 - 1 = \lambda^2 + p - 1$.

Theorem 3. For each odd prime p the following relation holds for every pair of nonnegative integers i, j :

$$q(i, j) \equiv q(i_n, j_n)q(i_{n-1}, j_{n-1}) \dots q(i_0, j_0) \pmod{p}, \quad (12)$$

where $i = i_n p^n + i_{n-1} p^{n-1} + \dots + i_0$, $j = j_n p^n + j_{n-1} p^{n-1} + \dots + j_0$, $0 \leq i_k < p$, $0 \leq j_k < p$.

Proof: We write $i = ap+b$, $j = cp+d$, where a, c are quotients and b, d remainders of dividing i, j by p respectively. Since $0 \leq b < p$, $0 \leq d < p$ the numbers $q(b, d)$ are elements of the matrix A . We will prove that in this case over Z_p $q(i, j) = q(a, c)q(b, d)$. Since in the field Z_p $(a+b)^p = a^p + b^p$, then $(f(x, y) + g(x, y))^p = f(x, y)^p + g(x, y)^p$ for any two formal power series $f(x, y), g(x, y)$ with coefficients in Z_p .

For $i = 0, 1, \dots, p-1$ we introduce the polynomials $S_i(x)$ by

$$S_i(x) = \sum_{j=0}^{p-1} q(i, j) x^j;$$

specially, from this definition we get

$$S_0(x) = 1 + x + x^2 + \dots + x^{p-2} + x^{p-1}$$

and from Assertion 2 of Theorem 1

$$S_{p-1}(x) = 1 - x + x^2 - \dots - x^{p-2} + x^{p-1}.$$

From (3) we get for $1 \leq i \leq p-1$ a new recurrence formula

$$(1-x)S_i(x) = (1+x)S_{i-1}(x).$$

Introducing the sum $S(x, y)$ by

$$S(x, y) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} q(i, j) x^i y^j$$

we see that

$$S(x, y) = \sum_{i=0}^{p-1} S_i(y) x^i$$

and an easy calculation gives

$$S(x, y) = S_0(y) + \frac{x(1+y)}{1-y} S(x, y) - \frac{x^p(1+y^p)}{1-y}.$$

Over the field Z_p we finally get

$$S(x, y) = \sum_{k=0}^{p-1} (x + y + xy)^k.$$

From the generating function (5) we find that

$$\begin{aligned} \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} q(i, j) x^i y^j &= \sum_{n=0}^{\infty} (x + y + xy)^n = \sum_{j=0}^{\infty} \sum_{k=0}^{p-1} (x + y + xy)^{jp+k} \\ &= \sum_{j=0}^{\infty} \sum_{k=0}^{p-1} (x^p + y^p + x^p y^p)^j (x + y + xy)^k \\ &= \sum_{d=0}^{\infty} \sum_{c=0}^{\infty} q(a, c) x^{cp} y^{pc} \sum_{b=0}^{p-1} \sum_{d=0}^{p-1} q(b, d) x^b y^d. \end{aligned}$$

Equating coefficients of $x^i y^j$ shows that if $i = ap + b$ and $j = cp + d$ then in Z_p $q(i, j) = q(a, c)q(b, d)$. By induction we finally obtain the relation (12). ■

This theorem implies that all information about the numbers $q(i, j)_p$ lies in the matrix A given by (11). Denote by $A^{(1)}, A^{(2)}, A^{(3)}, \dots$ the matrices $A, A \otimes A, A \otimes A \otimes A, \dots$ respectively. They are square-matrices of orders p, p^2, p^3, \dots respectively and their entries are $q(i, j)_p$ determined from (12). In particular, for $p = 7$, we obtain:

$$A = A^{(1)} = \begin{bmatrix} 1 & 6 & 1 & 6 & 1 & 6 & 1 \\ 1 & 4 & 5 & 0 & 2 & 3 & 6 \\ 1 & 2 & 6 & 3 & 6 & 2 & 1 \\ 1 & 0 & 4 & 0 & 3 & 0 & 6 \\ 1 & 5 & 6 & 4 & 6 & 5 & 1 \\ 1 & 3 & 5 & 0 & 2 & 4 & 6 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad A^{(2)} = \begin{bmatrix} 1A & 6A & 1A & 6A & 1A & 6A & 1A \\ 1A & 4A & 5A & 0A & 2A & 3A & 6A \\ 1A & 2A & 6A & 3A & 6A & 2A & 1A \\ 1A & 0A & 4A & 0A & 3A & 0A & 6A \\ 1A & 5A & 6A & 4A & 6A & 5A & 1A \\ 1A & 3A & 5A & 0A & 2A & 4A & 6A \\ 1A & 1A & 1A & 1A & 1A & 1A & 1A \end{bmatrix}.$$

We introduce in $A^{(2)}$ over Z_p the indexing of the blocks $B(i, j)$ as follows: $B(i, j) = q(i, j)A$. For $B(i, j)$ the same rule as for the numbers $q(i, j)$ is valid:

$$B(i, j) = B(i - 1, j) + B(i, j - 1) + B(i - 1, j - 1), \quad i \geq 1, j \geq 1,$$

with the boundary conditions $B(0, j) = B(i, 0) = A$. This can be generalized for the matrices $A^{(k)}$ for $k \geq 2$. We say that the array of $q(i, j)_p$, is *self-similar*. If we mark black the points (i, j) for which $q(i, j)_p = 0$ (or equivalently $q(i, j)$ is divisible by p) we obtain pictures of a remarkable design. The picture was constructed by a computer for $0 \leq i \leq 175, 0 \leq j \leq 175$. For small p each point can be coloured differently according with the number $q(i, j)_p$. The obtained picture displays the divisibility properties of the numbers $q(i, j)$.

Let $z(k, p), k = 1, 2, \dots$ denote the number of zeros in the matrix $A^{(k)}$ for a given odd prime p .

Theorem 4. *For every odd prime p and $k \geq 1$ the number $z(k, p)$ of all zero entries of the matrix $A^{(k)}$ is given by the formula*

$$z(k, p) = p^{2k} - [p^2 - z(1, p)]^k. \quad (13)$$

Proof: Since $A^{(k+1)} = A \otimes A^{(k)}$ over Z_p we obtain a simple recurrence formula

$$z(k + 1, p) = z(k, p)[p^2 - z(1, p)] + z(1, p)p^{2k}$$

and by induction we verify now (13) very easily.

For $p = 7$ we get $z(1, 7) = 5, z(2, 7) = 465$. Theorem 7 says that $A^2 = I$, moreover, we can prove that over Z_p in general

$$[A^{(k)}]^2 = I$$

for all $k \geq 0$. Specially, $[A^{(2)}]^2 = (A \otimes A)(A \otimes A) = A^2 \otimes A^2 = I \otimes I = I$. ■

The author found the ideas for the study of number array modulo a prime in [9, 10].

Acknowledgement.

The author would like to thank Professor Tomaž Pisanski for his help in preparing this paper.

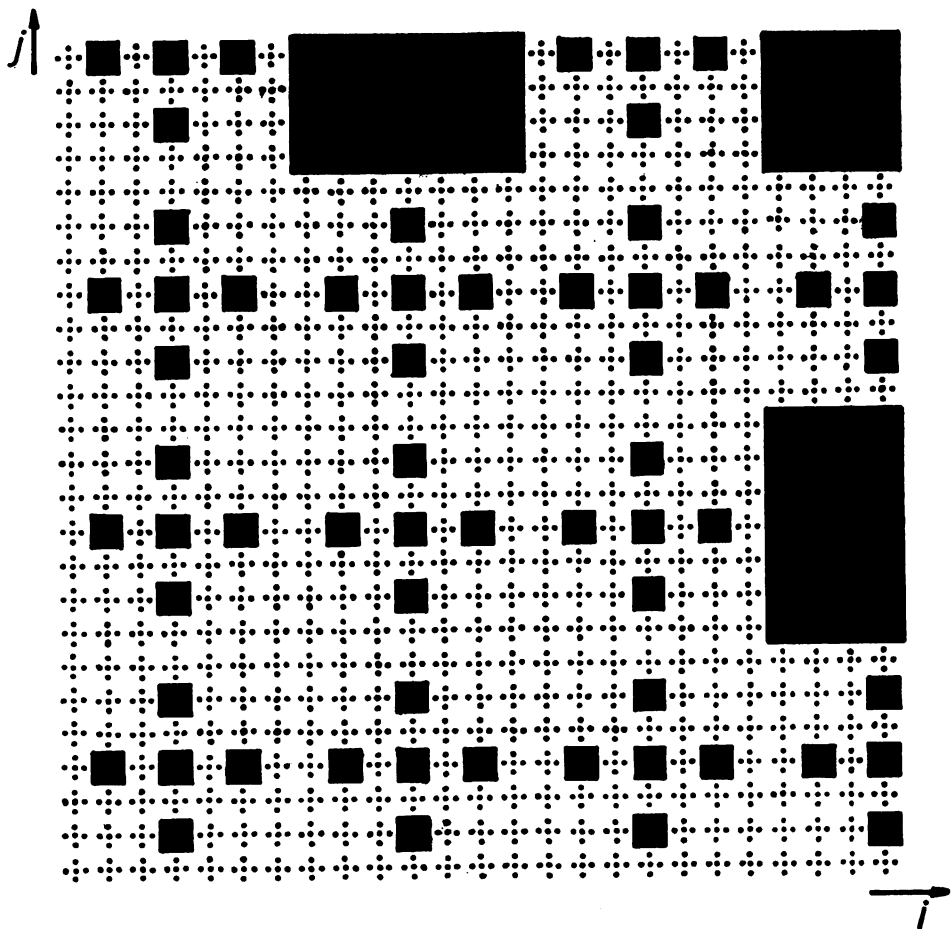


Figure 2
 The pattern to the divisibility of numbers $q(i, j)$ by $p = 7$

References

1. R.D. Fray, D.P. Roselle, *Weighted lattice paths*, Pacific J. Math. **37** (1971), 85-96.
2. I.M. Gessel, *A factorization for formal Laurent series and lattice path enumeration*, J. Comb. Theory (Ser. A) **28** (1980), 321-337.
3. J.S. Lew, *Polynomial enumeration of multidimensional lattices*, Math. System Theory **12** (1979), 253-270.
4. I. Niven, *Formal power series*, Amer. Math. Monthly **76** (1969), 871-889.
5. M. Razpet, *An application of the umbral calculus*, J. Math. Anal. Appl. (to appear).
6. J. Riordan, "Combinatorial Identities", Wiley, New York, 1968.
7. D.G. Rogers, *A Schröder triangle: three combinatorial problems*, in "Combinatorial Identities", Wiley, New York, 1969.
8. S. Roman, "The Umbral Calculus", Academic Press, Orlando, Florida, 1984.
9. M. Sved, *Divisibility — with visibility*, The Math. Intelligencer **10** (1988), 56-64.
10. S. Wolfram, *Geometry of binomial coefficients*, Amer. Math. Monthly **91** (1984), 566-571.