Now let k run over all even integers and put $i = k/2$. Then (13) yields $|M^k_{k/2}| \to 1$, and since $M_1^2 \supset M_2^4 \supset M_3^6 \supset \dots$, it follows that

$$|M^k_{k/2}| = 1$$

for every k. This means that for $l = as^{k/2}$ ($k = 2, 4, 6, \dots$) and for almost every a a required sequence $\{q_{n_\nu}\}$ does exist.

Application. In [2] it was proved that for almost every a the inequalities $|qa-p| < 1/t$, $|q| < ct$ (p, q integers) cannot be solved simultaneously for every $t > 1$ with an *odd* q, however large constant c is chosen. For this proof it is essential that for almost every a the sequence $\{q_n\}$ should contain a subsequence $\{q_{\nu_n}\}$ consisting of even numbers and such that $\lim\limits_n (q_{\nu_n+1}/q_{\nu_n}) = \infty$. Replacing this proposition by Theorem 2 we can obtain without further modification of arguments the following generalization of the result in [2]:

For almost every a, every $c > 0$ and every integer l the inequalities $|qa-p| < 1/t$ and $|q| < ct$ are not simultaneously solvable for arbitrary $t > 1$ if it is required that q should not be divisible by l.

It may be observed that the theorem of Duffin and Schaeffer and the estimation of the number of primes in arithmetical progressions enable us to prove that for almost every a the sequence $\{q_n\}$ contains primes belonging to any progression $b + na$ ($n = 1, 2, \dots$) with $(a, b) = 1$.

References

[1] R. J. Duffin and A. C. Schaeffer, *Khintchine's problem in metric diophantine approximation*, Duke Math. J. 8 (1941), p. 243-255.

[2] S. Hartman, *A feature of Dirichlet's approximation theorem*, Acta Arithmetica 5 (1959), p. 261-263.

[3] O. de Vries, *Metrische onderzoekingen van diophantische benaderings-problemen in het niet-lacunaire geval* (thesis), Amsterdam 1955.

MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCE
INSTITUTE OF MATHEMATICAL RESEARCH OF THE HUNGARIAN ACADEMY OF SCIENCE

Reçu par la Rédaction le 14. 1. 1960

ACTA ARITHMETICA
VI (1960)

On a generalization of Wilson's theorem

by

B. GYIRES (Debrecen, Hungary)

1. In the present paper we denote by printed Latin capitals quadratic matrices of order n, and by written Latin capitals quadratic matrices of order nr. In particular, E and O will denote the unit matrix and the zero matrix of order n, respectively, whereas $\mathcal{E}$ will be the unit matrix of order nr. $\langle A_1, \dots, A_r \rangle$ stands for a hypermatrix of order nr, built from matrices of order n, in which all elements outside the matrices in the main diagonal are zero matrices, and the hth element of the main diagonal is A_h. We shall call this matrix a diagonal-matrix, whereas the (evidently regular) matrix

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \cdot & \cdot & \cdot\,\cdot\,\cdot & \cdot \\ \lambda_1^{r-1} & \lambda_2^{r-1} & \dots & \lambda_r^{r-1} \end{bmatrix} . \tag{1}$$

built from the pairwise different numbers

$$\lambda_1, \lambda_2, \dots, \lambda_r \tag{2}$$

will be called the Vandermonde-matrix generated by the elements (2). The direct product of the matrix E with the matrix (1) is also regular, since by the well-known theorem on determinants of Kronecker the determinant of the direct product is the nth power of the determinant of the matrix (2).

A quadratic matrix whose elements are rational integers will be called *regular with respect to the module p* (p a prime), if its determinant is not divisible by p. By Cramer's rule for linear systems of congruences any matrix regular mod$p$ has an inverse in the sense that there exists a matrix, such that the product of multiplying by it the original martix will be congruent mod$p$ with the unit matrix. If the elements (2) are rational integers incongruent mod$p$, then it follows from the product representation of the Vandermonde-determinant that the matrix (1), and thus—again by the above mentioned theorem of Kronecker—also the direct product of the matrix E and the matrix (1), is regular $\bmod p$.

2. The theorem whose consequences we are going to investigate in the present paper is the following:

Theorem 1. *If the coefficients of the polynomial*

$$f(z) = a_0 + a_1 z + \ldots + a_{r-1} z^{r-1} + z^r \tag{3}$$

are rational integers, and if the roots

$$\eta_1, \eta_2, \ldots, \eta_r \tag{4}$$

of the equation $f(z) = 0$ *all have multiplicity* 1 *and the congruence* $f(z) \equiv 0 \pmod{p}$, *where* p *is a prime, has* $\bmod p$ *exactly as many incongruous solutions*

$$\alpha_1, \alpha_2, \ldots, \alpha_r \tag{5}$$

as its degree, then if we form with the matrices

$$A_0, A_1, \ldots, A_{r-1}, \tag{6}$$

having arbitrary rational integers as elements, the matrix polynomial

$$M(z) = A_0 + A_1 z + \ldots + A_{r-1} z^{r-1}, \tag{7}$$

we obtain the congruence

$$\mathcal{V}\mathcal{M}\mathcal{V}^{-1} \equiv \mathcal{W}\mathcal{N}\mathcal{W}^{-1} \pmod{p}, \tag{8}$$

where

$$\mathcal{M} = \langle M(\eta_1), \ldots, M(\eta_r)\rangle, \tag{9}$$

$$\mathcal{N} = \langle M(\alpha_1), \ldots, M(\alpha_r)\rangle, \tag{10}$$

$\mathcal{V}$ *resp.* $\mathcal{W}$ *is the direct product of the matrix* E *with the Vandermonde-matrix generated by the elements* (4) *resp.* (5), $\mathcal{V}^{-1}$ *is the ordinary inverse of* $\mathcal{V}$, *and* $\mathcal{W}^{-1} \equiv (\operatorname{Det} \mathcal{W})^{p-2}$ *adj.* $\mathcal{W} \pmod{p}$ *the inverse* $\bmod p$ *of* $\mathcal{W}$.

It is easy to see that there exists a polynomial (3) satisfying the conditions of Theorem 1. Indeed, let

$$f(z) = z^r - a \tag{11}$$

be a polynomial of degree r, with the rational integer a satisfying the conditions

$$r \mid p-1, \qquad a^{(p-1)/r} \equiv 1 \pmod{p}, \tag{12}$$

then—as is well known from elementary number theory—the binomial congruence $f(z) \equiv 0 \pmod{p}$ has r incongruent solutions, and on the other hand the roots of the equation $f(z) = 0$ are all of multiplicity 1.

Before proving Theorem 1, we shall consider some of its consequences.

If we go over to determinants on both sides of (8), then taking into account (9) and (10) we get the following

Theorem 2. *Under the conditions of Theorem* 1 *the congruence*

$$\operatorname{Det} M(\alpha_1) \ldots \operatorname{Det} M(\alpha_r) \equiv \operatorname{Det} M(\eta_1) \ldots \operatorname{Det} M(\eta_r) \pmod{p} \tag{13}$$

holds.

If polynomial (3) is equal to polynomial (11) satisfying condition (12), and if $n = 1$, i. e. (7) is a polynomial with rational integer coefficients and $M(z) = z$, then by virtue of (13) we get

$$\alpha_1 \alpha_2 \ldots \alpha_r \equiv (-1)^{r-1} a \pmod{p}. \tag{14}$$

If we do not rely upon congruence (13), then we can assert even more than (14).

Indeed, let p be an odd prime number, a a natural number, m one of the numbers p^a and $2p^a$, and $\varphi(m) = c$. If a is a rational integer and $r|c$, $a^{c/r} \equiv 1 \pmod{m}$, then—as is known—the congruence

$$z^r - a \equiv 0 \pmod{m}$$

has r incongruent solutions. If these are denoted by $\alpha_1, \ldots, \alpha_r$, then from the congruence

$$z^r - a \equiv (z - \alpha_1) \ldots (z - \alpha_r) \pmod{m}$$

we get by the substitution $z = 0$ congruence (14), where r must be now taken in the above-mentioned more general sense.

If $r = c = \varphi(m)$, then the congruence $a^{c/r} \equiv 1 \pmod{m}$ is fulfilled automatically and so by (14)

$$\alpha_1 \ldots \alpha_{\varphi(m)} \equiv (-1)^{\varphi(m)-1} \pmod{m},$$

where $\alpha_1, \ldots, \alpha_{\varphi(m)}$ are the elements of the reduced remainder system of m. Of course, this latter congruence is true for any natural m.

Now let again $n = 1$ and let polynomial (3) again be equal to polynomial (11) satisfying condition (12). If we still have $r = p-1$, then (13) says that

$$M(1)\, M(2) \ldots M(p-1) \equiv M(\omega_1)\, M(\omega_2) \ldots M(\omega_{p-1}) \pmod{p}, \tag{15}$$

where $\omega_1, \ldots, \omega_{p-1}$ are the $(p-1)$-th roots of unity. This is the theorem the proving of which was proposed by the author as a probem in the Schweitzer mathematical contest of 1951. ([2], problem 10.)

If we put $r = p-1$ in (14) or $M(z) = z$ in (15), we receive in both cases Wilson's congruence. Thus theorem (2) can be considered as a generalization—through congruence (14) or (15)—of Wilson's theorem, whereas Theorem 1 as expressed by (8) is a matrix generalization of the congruence of Wilson.

3. Now as regards the proof of Theorem 1, it follows almost trivially from the theorem we shall give below.

Let us suppose that the coefficients of the polynomial (3) belong to a field $\mathfrak{K}$ and that the number of distinct zeros in $\mathfrak{K}$ of this polynomial is equal to its degree. Let the zeros be the quantities under (2). Since the matrix (1) is, by the assumptions made for the generating numbers (2), regular in the field $\mathfrak{K}$, the direct product $\mathcal{U}$ of the matrix E with (1) is also regular, and so there exists in $\mathfrak{K}$ an inverse $\mathcal{U}^{-1}$ of $\mathcal{U}$. For the matrix polynomial (7) we also make the assumption that its coefficients are matrices consisting of elements belonging to $\mathfrak{K}$. After these preparations, the above-mentioned theorem can be formulated in the following way:

In order that the matrix $\mathcal{A}$ of order nr and with elemets from the field $\mathfrak{K}$ be carried over by the transformation $\mathcal{U}$ into the diagonal matrix $\mathcal{M} = \langle M(\lambda_1), \dots, M(\lambda_r)\rangle$, i. e. in order that the relation

$$\mathcal{A} = \mathcal{U}\mathcal{M}\mathcal{U}^{-1} \tag{16}$$

may hold, it is necessary and sufficient that the matrix be interchangeable with the matrix

$$\mathcal{G} = \begin{bmatrix} 0 & E & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & E & 0 & \dots & 0 & 0 \\ & \ddots & \ddots & & & & \\ & & \ddots & \ddots & & & \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ 0 & 0 & 0 & 0 & \dots & 0 & E \\ -a_0E & -a_1E & -a_2E & -a_3E & \dots & -a_{r-2}E & -a_{r-1}E \end{bmatrix}.$$

If, on the other hand,

$$\mathcal{A}_k = \langle A_k, \dots, A_k\rangle \qquad (k = 0, 1, \dots, r-1),$$

then the totality of the matrices of order nr and with elements from $\mathfrak{K}$ which are interchangeable with $\mathcal{G}$ is given by

$$\mathcal{A} = \mathcal{A}_0 + \mathcal{A}_1\mathcal{G} + \mathcal{A}_2\mathcal{G}^2 + \dots + \mathcal{A}_{r-1}\mathcal{G}^{r-1}, \tag{17}$$

provided the matrices (6) determining (17) run, independently of each other, through the totality of quadratic matrices of order n with elements from $\mathfrak{K}$.

For the case of $\mathfrak{K}$ being the complex field, this theorem was formulated and proved by J. Wellstein ([3], p. 7). His proof, however, can be transferred word for word also to this more general case.

Now if $\mathfrak{K}$ is the series of remainders belonging to the prime p and if the polynomial (3) satisfies the conditions of Theorem 1, and if, moreover, in the field of complex numbers we use the ordinary equality sign and in the field formed by the remainders belonging to p we use the sign of congruence to denote equality, then by the theorem of Wellstein quoted above we have for the matrices (17) in accordance with (16) the congruence

$$\mathcal{A} = \mathcal{V}\mathcal{M}\mathcal{V}^{-1} \equiv \mathcal{W}\mathcal{N}\mathcal{W}^{-1} \pmod{p}, \tag{18}$$

where the meaning of the symbols after the equality sign has been explained in connection with Theorem 1. (18), however, is identical with the expression (8).

Going over to determinants, we get from (18) the form

$$\operatorname{Det}\mathcal{M}(a_1)\dots\operatorname{Det}\mathcal{M}(a_r) \equiv \operatorname{Det}\mathcal{A} \pmod{p}$$

of the congruence expressed in Theorem 2. If we impose here the same restrictions which were used in passing from (13) to (15), we obtain a congruence known already to G. Rados. This congruence has been formulated and proved by Rados in connection with the proof of the so called König-Rados theorem in number theory ([1], p. 300).

4. If in (6) we have $r = p-1$ and $n = 1$, then the matrices (17) are—as is well known—cyclic matrices. Now, in order that the congruence

$$A_0 + A_1z + \dots + A_{p-2}z^{p-2} \equiv 0 \pmod{p}, \qquad A_0 \not\equiv 0 \pmod{p}$$

may have $p-k-1$ incongruent solutions, it is necessary and sufficient by the theorem of König-Rados mentioned under 3 that the rank mod p of the cyclic matrix $\mathcal{C}$ formed of the elements (6) be equal to k. On the other hand, by a special case of a theorem of Rédei-Turán ([5], p. 224) the validity of the congruences

$$\mathcal{P}_{p-1} \equiv \dots \equiv \mathcal{P}_{k+1} \equiv 0 \pmod{p}, \qquad \mathcal{P}_k \not\equiv 0 \pmod{p} \tag{19}$$

is also a necessary and sufficient condition, provided

$$\text{Det}(\mathcal{C}-z\mathcal{E}) = \sum_{j=0}^{p-1} (-1)^j \mathcal{P}_j z^{p-j-1}, \tag{20}$$

where thus $\mathcal{P}_j$ is the sum of the jth principal minors of the matrix $\mathcal{C}$. A confrontation of these two criteria gives—as they remark l. c.—the following

Theorem 3. *In order that the rank* mod$p$ *of the cyclic matrix* $\mathcal{C}$ *be equal to* k, *the validity of the congruences* (19) *is necessary and sufficient.*

Rédei and Turán postulated l. c. a direct proof of this theorem. In what follows we give such a proof of this theorem, based on our previous result, with the aid of the following theorem:

If $\mathcal{B}$ *is a quadratic matrix of order* m *defined over the field* $\mathfrak{K}$ *and the equation*

$$\text{Det}(\mathcal{B}-z\mathcal{E}) = 0 \tag{21}$$

has $z = \lambda$ *as a root of multiplicity* $m-k$ *contained in* $\mathfrak{K}$, *with respect to which the elementary divisors in* $\mathfrak{K}$ *of the matrix* $\mathcal{B}$ *are linear, then the rank of the matrix*

$$\mathcal{B}-\lambda\mathcal{E} \tag{22}$$

is equal to k. *The converse also holds: If* λ *is a root contained in* $\mathfrak{K}$ *of* (21), *for which the rank of* (22) *is* k *and the elementary divisors with respect to* λ *contained in* $\mathfrak{K}$ *of* $\mathcal{B}$ *are linear, then* λ *is a root of multiplicity* $m-k$ *of* (21).

This theorem is well known for the case where $\mathfrak{K}$ is the field of complex numbers ([4], p. 189). However, it can be proved also in this general case in exactly the same manner as for complex numbers. In this respect it suffices to point out that the concept of rank, as well as the multiplicity of the zeros of a polynomial, can be defined also in an arbitrary field.

Let $m = p-1$ and let $\mathcal{B}$ be equal to the cyclic matrix $\mathcal{C}$. If the remainder system of the prime p is taken to be the field $\mathfrak{K}$, then by (18) the matrix $\mathcal{C}$ has in this field $\mathfrak{K}$ $p-1$ eigenvalues, and also by (18) the elementary divisors in $\mathfrak{K}$ belonging to these eigenvalues are linear. If we still take into account that $\lambda \equiv 0 \pmod{p}$ is a zero of multiplicity $p-k-1$ mod$p$ of (20) if and only if (19) holds, then the proof of Theorem 3 becomes an immediate consequence of the theorem just quoted.

References

[1] G. Raussnitz, *A felsőbbfokú kongruenciák elméletéhez,* Math. Termtud. Értesitö I (1882-83), p. 296-308.

[2] T. Szele, *Az 1951. évi Schweitzer Miklós matematikai verseny,* Matematikai Lapok, Budapest, III. évf. (1952), p. 243-272.

[3] J. Wellstein, *Lösung der Aufgabe 89. I,* Jber. Deutsche Math. Verein. 42 (1932), p. 7-9.

[4] R. Zurmühl, *Matrizen,* Berlin (Göttingen), Heidelberg 1950.

[5] L. Rédei and P. Turán, *Zur Theorie der algebraischen Gleichungen über endlichen Körpern,* Acta Arith. 5 (1959), 223-225.

Reçu par la Rédaction le 25. 1. 1960