On the extension of Fermat's theorem to matrices of order *n*

By J. B. Marshall.

(*Received* 17*th April*, 1939. *Read* 5*th May*, 1939.)

It is proposed to establish, by elementary methods, a theorem for matrices analogous to Fermat's Theorem in the Theory of Numbers. In Jordan's *Traité des Substitutions* (Paris, 1870) pp. 127, 128, the order of any given linear substitution or matrix A with reference to any prime number p is determined, but the result given depends on the particular characteristic equation satisfied by the matrix A, and a general result applicable to all matrices of n rows and n columns does not seem to have been published hitherto.

(1) Fermat's Theorem in the Theory of Numbers is as follows:—

If p is a prime number and N is prime to p, then $N^{p-1} - 1$ is divisible by p, i.e. $N^{p-1} \equiv 1 \pmod{p}$.

To extend this to matrices we have to answer this question:—If p is a prime number, and A is a matrix of order n with integral elements, such that $|A|$ is prime to p, what is the smallest value of q which will always satisfy the congruence $A^q \equiv I \pmod{p}$? Here I is the unit matrix, and the notation means (as in Turnbull and Aitken, *Theory of Canonical Matrices* (London, 1932), 22) that every element of the matrix $(A^q - I)$ is either zero or a multiple of p. Hence A^q must be of the form

$$\begin{pmatrix} pa_{11}+1 & pa_{12} & pa_{13} \; \ldots \\ pa_{21} & pa_{22}+1 & pa_{23} \; \ldots \\ pa_{31} & \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \end{pmatrix}.$$

On expanding the determinant of this matrix, we get $|A^q| = 1 +$ a multiple of p, *i.e.* $|A^q| \equiv 1 \pmod{p}$. If $|A| \equiv 0 \pmod{p}$, then $|A^q| \equiv 0 \pmod{p}$, and therefore no relation of the form $A^q \equiv I \pmod{p}$ can exist.

(2) If $A = pB + C$, then $A^2 = p^2 B^2 + p(BC + CB) + C^2$, so that $A^2 \equiv C^2 \pmod{p}$. Similarly $A^q \equiv C^q \pmod{p}$ and thus we need consider only those matrices whose elements are all taken from the numbers $0, 1, 2 \ldots\ldots (p-1)$, since any matrix with integral elements can be put in the form $pB + C$ where C is such a matrix.

https://doi.org/10.1017/S0013091500024536 Published online by Cambridge University Press

(3) *The set of matrices of order n, whose elements are all taken from the numbers* 0, 1, 2 .... $(p-1)$, *and which are such that their determinants are prime to p, form a finite congruent group.* The unit matrix is the "identical" member of the group. The product of any two members of the set is congruent (mod p) with some member of the set. Every member has its reciprocal. In symbols, if A and B are any two members of the set, there exist members C and D such that $AB \equiv C$ (mod p) and $AD \equiv I$ (mod p). These properties are sufficient to establish that the set of matrices form a group.

The order of this group is $(p^n-1)(p^n-p)(p^n-p^2)\ldots\ldots(p^n-p^{n-1})$. This is established in Burnside's *Theory of Groups* (Cambridge 1911), § 83, and may also be proved from first principles by the following elementary method:—

Let u_r be the vector given by the rth row of the matrix. Then the n elements of u_1 may each consist of any of the p numbers 0, 1, 2 .... $(p-1)$, except that they may not all be zero since this would make the matrix singular. There are therefore p^n-1 ways of selecting this vector. When u_1 has been selected, u_2 may be any of the p^n possible vectors except those which are congruent with $k_1 u_1$ (mod p) $\{k_1 = 0, 1, 2 \ldots\ldots (p-1)\}$, since any of these vectors will make all the minor determinants formed from the first two rows congruent with 0 (mod p) and therefore the matrix will be singular (mod p), and this will not be the case if u_1 and u_2 are linearly independent. There are therefore p^n-p ways of selecting u_2. Similarly u_3 may be any of the p^n possible vectors except those which are congruent with $k_1 u_1 + k_2 u_2$ (mod p) $\{k_1 = 0, 1, \ldots\ldots (p-1) . k_2 = 0, 1 \ldots\ldots (p-1)\}$ and the numbers of ways of selecting u_3 is therefore $p^n - p^2$. The same argument applies to all the other rows, and the total number of matrices, *i.e.* the order of the group, is therefore as stated above.

By an elementary proposition in the Theory of Groups the number q which we are seeking must be a submultiple of the order of the group.

(4) By the Cayley-Hamilton Theorem (Turnbull and Aitken, page 43) every matrix of order n satisfies an identity of the form

$$A^n - p_1 A^{n-1} + p_2 A^{n-2} \ldots\ldots \pm p_n I = 0$$

where $p_n = |A|$. Removing or adding multiples of p this reduces to the congruence $A^n + \lambda_1 A^{n-1} + \lambda_2 A^{n-2} + \ldots\ldots + \lambda_{n-1} A + \mu I \equiv 0$ (mod p) where $\lambda_r = 0, 1, 2 \ldots\ldots (p-1)$, $\mu = 1, 2 \ldots\ldots (p-1)$. Now if $(x^n + \lambda_1 x^{n-1} + \lambda_2 x^{n-2} + \ldots\ldots + \lambda_{n-1} x + \mu)$ is a factor (mod p) of

https://doi.org/10.1017/S0013091500024536 Published online by Cambridge University Press

$(x^q - 1)$, the above congruence must give $A^q - I \equiv 0 \pmod{p}$, and hence if q is such that $(x^n + \lambda_1 x^{n-1} + \lambda_2 x^{n-2} + \ldots . + \mu)$ is a factor (mod p) of $x^q - 1$, no matter what values are given to the λ's and μ, then $A^q - I \equiv 0 \pmod{p}$ will be true for all matrices of order n with integral elements.

(5) By Fermat's Theorem we know that $(x+a)\{a=1, 2 \ldots . (p-1)\}$ is a factor (mod p) of $x^{p-1} - 1$. Hence $(x+a_1)(x+a_2)\{a_1 = 1, 2, \ldots . (p-1)$, $a_2 = 1, 2, \ldots . (p-1)$, $a_1 \neq a_2\}$ must be a factor (mod p) of $x^{p-1} - 1$. Hence $(p - 1)$ must be a submultiple of the value of q for $n = 2$.

Consider next the cases where the expression $x^2 + \lambda_1 x + \mu$ is irreducible (mod p), *i.e.* cannot be factorised. This introduces the conception of a *Galois Field.*

Let $F(x)$ be an arbitrary rational integral function with integral coefficients, and let $P(x)$ be a rational integral function of degree n irreducible *modulo* p (p being a prime number). If we divide $F(x)$ by $P(x)$ we obtain a quotient $Q(x)$ and a remainder which can be written in the form $f(x) + p\,.\,q(x)$ where $f(x)$ is of the form $f(x) \equiv a_0 + a_1 x + \ldots . + a_{n-1} x^{n-1}$, each a_i belonging to the series $0, 1, 2, \ldots . (p-1)$. Then $F(x) \equiv f(x) + p\,.\,q(x) + P(x)\,.\,Q(x)$.

Then $f(x)$ is called the *residue* of $F(x)$, moduli p and $P(x)$, and we write $F(x) \equiv f(x)$ (modd p, $P(x)$). Since each of the n a's may take p values, there are p^n possible residues. These residues form a field, called a *Galois Field*, of order p^n. [L. E. Dickson, *Linear Groups* (Leipzig, 1901), § 6.]

[*Note.* If $P(x)$ is reducible (mod p), or if p is not a prime, the residues do not form a field, since at least two non-zero residues can be found whose product is 0 (modd p, $P(x)$).]

(6) Let $P(x)$ be the irreducible (mod p) function $x^n + \lambda_1 x^{n-1} + \ldots . + \mu$, and let $F(x)$ be x^r, so that

$$x^r \equiv f(x) + p\,.\,q(x) + (\mu + \lambda_{n-1}x + \ldots + \lambda_1 x^{n-1} + x^n)(b_0 + b_1 x + \ldots + b_{r-n} x^{r-n}).$$

Then $f(x)$ cannot be zero. For, if so, we get from the above identity, since μ is prime to p, first that $b_0 \equiv 0 \pmod{p}$ and hence that $b_1, b_2, \ldots .$ are all $\equiv 0 \pmod{p}$ and finally that $b_{r-n} \equiv 0 \pmod{p}$. But b_{r-n} must be 1. Hence $f(x)$ cannot be zero.

Since the number of residues is finite, it must be possible to find two numbers r and s such that the residues of x^r and x^s are the same. Let s be the first number greater than r such that the residues of x^r and x^s are the same.

https://doi.org/10.1017/S0013091500024536 Published online by Cambridge University Press

Then $\qquad x^s - x^r \equiv 0 \ (\text{modd}\ p,\ P(x))$

$\qquad x^r (x^{s-r} - 1) \equiv 0 \quad ,,$

Then, since $\qquad x^r \not\equiv 0 \quad ,,$

$\qquad x^{s-r} - 1 \equiv 0 \quad ,,$

or, if $s - r = e$, $\qquad x^e \equiv 1 \quad ,,$

It follows that if t is any number x^t and x^{t+e} have the same residue, so that the residues are periodic with period e. This period e is a submultiple of $p^n - 1$ (*cf.* Dickson, *Linear Groups*, § 11). For as r takes the values 0, 1, 2, ..., the residues of x^r are 1, x, x^2 ..... There are $p^n - 1$ non-zero residues altogether. We can form a rectangular array of all these non-zero residues as follows:—

$$\begin{array}{lllll} 1 & x & x^2 & \ldots\ldots\ldots\ldots & x^{e-1} \\ u_1 & u_1 x & u_1 x^2 & \ldots\ldots\ldots\ldots & u_1 x^{e-1} \\ u_2 & u_2 x & u_2 x^2 & \ldots\ldots\ldots\ldots & u_2 x^{e-1} \\ \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \end{array}$$

where, if the power to which x is raised in the first row is greater than $(n - 1)$, it is understood that the residue (modd p, $P(x)$) is taken, and where u_1 is any non-zero residue not included in the first row, u_2 is any non-zero residue not included in the first two rows, and so on. Then all the residues in any line are different from each other and from those in preceding rows. Hence, as all the $p^n - 1$ non-zero residues must be included in the array, and there are e in each row, $p^n - 1$ is a multiple of e.

Also if $x^e \equiv 1$ (modd p, $P(x)$), then $x^{ke} \equiv 1$ (modd p, $P(x)$). Hence $x^{p^n-1} - 1 \equiv 0$ {modd p, $P(x)$} for all irreducible $P(x)$ of degree n, of the form given. This is the same as saying that $P(x)$ is a factor (mod p) of $x^{p^n-1} - 1$.

(7) Now let $P(x)$, no longer irreducible, be of the form $(x + a)^n$ (mod p) where $a = 1, 2 \ldots . (p - 1)$. Then we have

$$\begin{aligned} x &\equiv -a + (x + a) \\ &\equiv (p - a) + (x + a) \ (\text{mod}\ p) \\ x^p &\equiv (p - a)^p + (x + a)^p \ (\text{mod}\ p), \end{aligned}$$

since p is prime and therefore all the other terms are divisible by p.

Hence $\qquad x^p \equiv (p - a) + (x + a)^p$ (mod p) by Fermat's Theorem.

Similarly, $\quad (x^p)^p \equiv (p - a)^p + (x + a)^{p^2} \quad ,,$

or $\qquad x^{p^2} \equiv (p - a) + (x + a)^{p^2} \quad ,,$

Similarly $\qquad x^{p^3} \equiv (p - a) + (x + a)^{p^3} \quad ,,$, and so on.

https://doi.org/10.1017/S0013091500024536 Published online by Cambridge University Press

Hence if p^r is the lowest power of p which is greater than or equal to n

$$x^{p^r} \equiv (p - a) \; \{\text{modd } p, \; (x + a)^n\},$$

so that by Fermat's Theorem

$$x^{p^r(p-1)} \equiv 1 \qquad \{\text{modd } p, \; (x + a)^n\},$$

that is $(x + a)^n$ is a factor, *modulo* p, of $x^{p^r(p-1)} - 1$.

(8) Now let $P(x)$, of even degree n, be of the form $(x^2 + \lambda x + \mu)^{n/2}$ (mod p) where $x^2 + \lambda x + \mu$ is irreducible (mod p). Then, by paragraph (6) above, $x^2 + \lambda x + \mu$ is a factor (mod p) of $x^{p^2-1} - 1$. So we can write

$$x^{p^2-1} \equiv 1 + (x^2 + \lambda x + \mu) \, . \, Q(x) \quad (\text{mod } p),$$

where $Q(x)$ is an integral function of x of degree $p^2 - 3$. Therefore

$$(x^{p^2-1})^p \equiv 1 + (x^2 + \lambda x + \mu)^p \, . \, \{Q(x)\}^p \quad (\text{mod } p),$$
$$(x^{p^2-1})^{p^2} \equiv 1 + (x^2 + \lambda x + \mu)^{p^2} \, . \, \{Q(x)\}^{p^2} \quad (\text{mod } p),$$

and so on. Hence, if p^s is the lowest power of p which is equal to or greater than $\frac{1}{2}n$,

$$(x^{p^2-1})^{p^s} \equiv 1 \; (\text{modd } p, \; P(x)).$$

That is, $(x^2 + \lambda x + \mu)^{n/2}$ is a factor (mod p) of $x^{(p^2-1)p^s} - 1$. The s found here is evidently not greater than the r of the previous paragraph, and therefore $(x^2 + \lambda x + \mu)^{n/2}$ is a factor (mod p) of $x^{(p^2-1)p^r} - 1$.

Similarly, if $P(x)$ is of the form $(x^3 + \lambda_1 x^2 + \lambda_2 x + \mu)^{n/3}$, (mod p) where $x^3 + \lambda_1 x^2 + \lambda_2 x + \mu$ is irreducible (mod p), then $P(x)$ must be a factor (mod p) of $x^{(p^3-1)p^r} - 1$, and similar results can be obtained when $P(x)$ is a power of irreducible functions of higher degree.

(9) Combining these results we have:—

(*a*) if $n = 2$, $P(x)$ may take the forms (mod p) of (i) $(x + a)^2$, (ii) $(x + a_1)(x + a_2)$ $\{a_1 \neq a_2\}$, or (iii) $x^2 + \lambda x + \mu$ (irreducible mod p).

In case (i) $P(x)$ is a factor (mod p) of $x^{p(p-1)} - 1$ since $p^0 < n \leqq p$,
,, ,, (ii) ,, ,, ,, ,, $x^{p-1} - 1$,
,, ,, (iii) ,, ,, ,, ,, $x^{(p^2-1)} - 1$.

Therefore in all three cases $P(x)$ is a factor (mod p) of $(x^{p(p^2-1)} - 1)$.

(*b*) If $n = 3$, $P(x)$ may take the forms (mod p) of (i) $(x + a)^3$, (ii) $(x + a_1)^2 (x + a_2)$, (iii) $(x + a_1)(x + a_2)(x + a_3)$, (iv) $(x + a_1)(x^2 + \lambda x + \mu)$, (v) $x^3 + \lambda_1 x^2 + \lambda_2 x + \mu$ (irreducible).

In case (i) if $p = 2$ (so that $p < n < p^2$) $P(x)$ is a factor of $x^{p^2(p-1)} - 1$, while for all other values of p (giving $n \leqq p$), $P(x)$ is a factor of $x^{p(p-1)} - 1$. In case (ii), since $(x + a_1)^2$ is a factor of

$x^{p(p-1)}-1$, and $(x + a_2)$ is an independent factor of $x^{p-1} - 1$, $P(x)$ must be a factor of $x^{p(p-1)} - 1$. In case (iii), $P(x)$ is a factor of $x^{p-1} - 1$. In case (iv), since $(x + a)$ is a factor of $x^{p-1} - 1$ and $x^2 + \lambda x + \mu$, which does not contain $(x + a)$, is a factor of $x^{p^2-1} - 1$, $P(x)$ must be a factor of $x^{p^2-1} - 1$. In case (v), $P(x)$ is a factor of $x^{p^3-1} - 1$.

Hence, in all cases, $P(x)$ is a factor of $x^{p^2 q_3} - 1$ if $p = 2$, or of $x^{pq_3} - 1$ if p is any other prime, where q_3 is the L.C.M. of $p^2 - 1$ and $p^3 - 1$, that is, $q_3 = [(p^2 - 1)(p^3 - 1)]/(p - 1)$.

(*c*) Similar arguments show that, in general, when $P(x)$ is of the nth degree, it must be either irreducible, or made up of factors which have appeared among the functions of lower degree, or be a power of some irreducible function of lower degree, and in all three cases $P(x)$ must be a factor (mod p) of $x^{p^r q_n} - 1$, where p^r is the lowest power of $p \geqq n$, and where q_n is the L.C.M. of q_{n-1} and $p^n - 1$.

(10) Hence we have this theorem:—

If p is a prime number, and A is a matrix of order n with integral elements, such that $|A|$ is prime to p, then $A^q \equiv I$ (mod p), where $q = p^r q_n$, p^r being the lowest power of p which is greater than or equal to n, and q_n being determined by the recurrence relation $q_1 = p - 1$, $q_n = L\ C.M.$ of q_{n-1} and $(p^n - 1)$.

This relation gives

$$\begin{aligned}
q_2 &= \text{L.C.M. of } (p-1) \text{ and } (p^2-1) = p^2 - 1\\
q_3 &= \quad ,, \quad ,, \ (p^2-1) \ ,, \ (p^3-1) = \frac{(p^3-1)(p^2-1)}{p-1}\\
q_4 &= \quad ,, \quad ,, \ q_3 \ ,, \ (p^4-1) = \frac{(p^4-1)(p^3-1)}{p-1}\\
q_5 &= \quad ,, \quad ,, \ q_4 \ ,, \ (p^5-1) = \frac{(p^5-1)(p^4-1)(p^3-1)}{(p-1)^2}\\
q_6 &= \quad ,, \quad ,, \ q_5 \ ,, \ (p^6-1) = \frac{(p^6-1)(p^5-1)(p^4-1)}{(p-1)^2(p+1)}
\end{aligned}$$

and so on.

(11) The foregoing argument does not establish that this value of q is the lowest possible value satisfying the congruence $A^q \equiv I$ (mod p). But, by enumerating all possible cases for low values of n and p, it is found that the value of q given above is the lowest value which satisfies the congruence for these particular values. Thus for $p = 2$, $n = 2$, it is found that one matrix satisfies $A \equiv I$ (mod 2), some satisfy $A^2 \equiv I$ (mod 2) and the others satisfy $A^3 \equiv I$ (mod 2) so that the

lowest value of q which makes $A^q \equiv I \pmod{2}$ for all matrices is $q = 6$. This is also the value obtained from the above formula by putting $q = p(p^2 - 1)$. Similarly for $n = 2$, $p = 3, 5, 7$ the values of q are found to be 24, 120, 336 respectively; for $n = 3$, $p = 2, 3$, the values of q are found to be 84 and 312 respectively; and for $p = 2$, $n = 4, 5$ the values of q are found to be 420 and 26040 respectively. The same values of q are found from the formula.

MATHEMATICAL INSTITUTE,
16 CHAMBERS STREET, EDINBURGH, 1.

https://doi.org/10.1017/S0013091500024536 Published online by Cambridge University Press