MATH. SCAND. 2 (1954), 315–326

CHEBYSHEV POLYNOMIALS AND THE MODULARY GROUP OF LEVEL p

R. A. RANKIN

1. The inhomogeneous modulary group $\overline{G}(n)$ is the quotient group $\overline{\Gamma}(1)/\overline{\Gamma}(n)$, where $\overline{\Gamma}(1)$ is the full inhomogeneous modular group, and $\overline{\Gamma}(n)$ is the inhomogeneous principal congruence group of level n, where n is a positive integer. Each element of $\overline{G}(n)$ can be represented by an infinity of matrices

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad ad - bc \equiv 1 \pmod{n}, \tag{1}$$

where a, b, c and d are integers, and matrix multiplication is the group operation. If S and

$$S' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

represent two elements of the group $\overline{G}(n)$, these elements are not regarded as distinct if and only if

$$a - a' \equiv b - b' \equiv c - c' \equiv d - d' \equiv 0 \pmod{n},$$

or

$$a + a' \equiv b + b' \equiv c + c' \equiv d + d' \equiv 0 \pmod{n},$$

which we write symbolically as

$$S \equiv S' \pmod{n} \qquad \text{or} \qquad S \equiv -S' \pmod{n},$$

respectively. The unit element Θ of $\overline{G}(n)$ is represented by all matrices S for which

$$S \equiv \pm I \pmod{n},$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In this paper I only consider the groups $\overline{G}(p)$, where p is an odd prime, and write

$$q = \tfrac{1}{2}(p-1), \qquad r = \tfrac{1}{2}(p+1). \tag{2}$$

Received June 11, 1954.

It is known that $\overline{G}(p)$ is of order $\frac{1}{2}p(p^2-1)$ and that the order of an element of $\overline{G}(p)$ other than Θ is either p, or a divisor of q or r. Further, the elements whose orders divide p, q and r can be divided into $p+1$, $\frac{1}{2}p(p+1)$ and $\frac{1}{2}p(p-1)$ conjugate cyclic subgroups of orders p, q and r, respectively, no two of these subgroups having any common elements other than Θ. The $p+1$ subgroups of order p are conjugates of the subgroup generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and the $\frac{1}{2}p(p+1)$ subgroups of order q are conjugates of the subgroup generated by

$$\begin{pmatrix} g & 0 \\ 0 & g^{-1} \end{pmatrix},$$

where g is a primitive root modulo p. However the subgroups of order r are not represented so easily, and the only treatments known to me make use of representations in terms of matrices with elements belonging to the Galois field of order p^2 ([1], [2, pp. 419–491], [3], [4, pp. 363–383 (§§ 464–473)], [5], [6, §§ 101–120]).

It is the purpose of this paper to show how this can be avoided. At the same time the method reveals interesting congruence properties of the Chebyshev polynomials and of the numbers x for which x^2-1 is either a quadratic residue or non-residue modulo p.

2. For any positive integer n, and any θ real or complex, the functions $\cosh n\theta$ and $\sinh n\theta/\sinh\theta$ can be expanded as polynomials of degree n and $n-1$, respectively, in $x = \cosh\theta$; these polynomials we denote by $T_n(x)$ and $F_n(x)$, respectively. Further, we write $T_0(x) = 1$, $F_0(x) = 0$, and define $T_{-n}(x) = T_n(x)$, $F_{-n}(x) = -F_n(x)$. The functions T_n and F_n are recurring sequences in the sense of Lucas and Lehmer. It is easily verified that the following relations hold for all n and x. We omit the argument x when no confusion can arise.

(3) $$F_{n+1} = xF_n + T_n, \qquad F_{n-1} = xF_n - T_n\,,$$

(4) $$F_{n+1} - 2xF_n + F_{n-1} = T_{n+1} - 2xT_n + T_{n-1} = 0\,,$$

(5) $$F_{n+1}^{\,2} - 2xF_{n+1}F_n + F_n^{\,2} = 1\,,$$

(6) $$F_{mn}(x) = F_m\{T_n(x)\}\,F_n(x), \qquad T_{mn}(x) = T_m\{T_n(x)\}\,,$$

(7) $$T_{2n-1} - x = 2(x^2-1)F_{n-1}F_n, \qquad T_{2n-1} + x = 2T_{n-1}T_n\,,$$

(8) $$T_m^{\,2} - T_n^{\,2} = (x^2-1)F_{m-n}F_{m+n}\,,$$

(9) $$T_n^{\,2} = 1 + (x^2-1)F_n^{\,2}, \qquad T_n(-1) = (-1)^n, \qquad T_n(1) = 1\,.$$

Further, $T_n(x)$ and $F_{n+1}(x)$ are even functions or odd functions of x according as n is even or odd. For odd n the following expansions hold:

$$(10)\qquad T_n(x) = 2^{n-1}x^n + n\sum_{\nu=1}^{\frac{1}{2}(n-1)} (-1)^\nu \frac{(n-\nu-1)(n-\nu-2)\ldots(n-2\nu+1)}{\nu!}\, 2^{n-2\nu-1}\, x^{n-2\nu},$$

$$(11)\qquad F_n(x) = n\left\{1 + \sum_{\nu=1}^{\frac{1}{2}(n-1)} \frac{(n^2-1^2)(n^2-3^2)\ldots\{n^2-(2\nu-1)^2\}}{(2\nu+1)!}(x^2-1)^\nu\right\}.$$

In the second expansion the last term is $2^{n-1}(x^2-1)^{\frac{1}{2}(n-1)}$.

Suppose now that S is defined by (1) where a, b, c and d are integers such that $ad-bc \equiv 1 \pmod p$, and p is an odd prime. Then it is easily verified by induction, and with the help of (4), that for every positive integer n

$$(12)\qquad S^n \equiv \begin{pmatrix} aF_n - F_{n-1} & bF_n \\ cF_n & dF_n - F_{n-1} \end{pmatrix} \pmod p,$$

where

$$(13)\qquad \mathrm{tr} S = a+d = 2x,$$

and x is the argument of the polynomials F_n and F_{n-1}.

3. In the rest of the paper all congruences are modulo an odd prime p. We shall make use of rational numbers in congruences, as is legitimate when the denominators are prime to p.

In this section x denotes any integer or residue (not necessarily quadratic) modulo p. We use the letter t to stand for either q or r, and s to stand for either p, q or r. We deduce at once from (10) and (11) that

$$(14)\qquad T_p(x) \equiv 2^{p-1}x^p \equiv x, \qquad F_p(x) \equiv 2^{p-1}(x^2-1)^{\frac{1}{2}(p-1)} \equiv (x^2-1)^{\frac{1}{2}(p-1)},$$

so that we have, by (7) with $p = 2n-1$, for all x

$$(x^2-1)\, F_q(x)\, F_r(x) \equiv 0,$$

the left-hand member being a polynomial of degree p. It follows that the congruences

$$F_q(x) \equiv 0 \qquad \text{and} \qquad F_r(x) \equiv 0$$

have exactly $q-1$ and $r-1$ solutions, respectively, and have no common solutions. Also, from (3) and (14),

$$(15)\qquad F_{p-1}(x) \equiv x\,\{(x^2-1)^{\frac{1}{2}(p-1)} - 1\}, \qquad F_{p+1}(x) \equiv x\,\{(x^2-1)^{\frac{1}{2}(p+1)} + 1\}.$$

Now since, by (6), (7) and (14), $F_{p-1} = 2F_q T_q$, $F_{p+1} = 2F_r T_r$ and $T_q T_r \equiv 2x$ it follows that the solutions of $F_t(x) \equiv 0$ are, with the possible omission of $x \equiv 0$, the same as those of $F_{2t}(x) \equiv 0$. Further, since $F_2(0) = 0$ and $T_2(0) = -1$, we have, by (6),

$$F_{2m}(0) = F_m(-1)\, F_2(0) \equiv 0\,,$$

and therefore $x \equiv 0$ is a solution of $F_t(x) \equiv 0$ if and only if t is even. For $t = q$ this occurs if and only if $(-1)^q \equiv 1$ and, for $t = r$ if and only if $(-1)^q \equiv -1$ so that we have, by (14) and (15), the

THEOREM 1. *For each integer x one and only one of the three congruences hold:*

$$F_p(x) \equiv 0, \qquad F_q(x) \equiv 0, \qquad F_r(x) \equiv 0\,.$$

In fact the first congruence holds if and only if $x \equiv \pm 1$, the second if and only if x^2-1 is a quadratic residue modulo p, and the third if and only if x^2-1 is a quadratic non-residue modulo p. In particular, $F_q(x) \equiv 0$ for $q-1$ incongruent values of x and $F_r(x) \equiv 0$ for $r-1$ incongruent values of x.

Denote by $\mathscr{C}_p$, $\mathscr{C}_q$ and $\mathscr{C}_r$ the classes of residues x modulo p for which $F_p(x) \equiv 0$, $F_q(x) \equiv 0$ and $F_r(x) \equiv 0$, respectively. Note that $\mathscr{C}_t$ is empty if and only if $t = q = 1$, which occurs for $p = 3$. Also, if $x \in \mathscr{C}_s$ then $-x \in \mathscr{C}_s$.

We define the *Chebyshev order* n_x of a residue x modulo p to be the least positive integer n such that $F_n(x) \equiv 0$. We deduce that

$$(16) \qquad T_{n_x}(x) \equiv \pm 1; \qquad \text{and} \qquad T_{n_x}(x) \equiv -1 \quad \text{for even } n_x\,.$$

The first result follows at once from (9), while if for even $n_x = 2m$, $T_{2m}(x) \equiv 1$, we should have

$$2T_m{}^2 = 1 + T_{2m} \equiv 2\,,$$

and since $F_{2m} = 2F_m T_m$, this implies that $F_m(x) \equiv 0$, which is false.

Now, from (8) with $n = 1$, $T_m(\pm 1) = \pm 1$, and, by (6), we therefore have, when $F_n(x) \equiv 0$ that

$$\begin{aligned} F_{mn+l} = F_{mn}T_l + T_{mn}F_l &= F_m\{T_n(x)\}F_n(x)\,T_l(x) + T_m\{T_n(x)\}F_l(x) \\ &\equiv T_m(\pm 1)\,F_l(x) \equiv \pm F_l(x)\,. \end{aligned}$$

We deduce that, if $x \in \mathscr{C}_s$, then n_x divides s, and also that

$$(17) \qquad F_m(x) \equiv 0 \quad \text{if and only if} \quad n_x \mid m\,.$$

Note that $n_0 = 2$, and that $n_x > 1$ for all x, so that

$$n_x = p \qquad \text{for} \qquad x \in \mathscr{C}_p \, .$$

Let $\alpha(n)$ denote the number of incongruent values of x of Chebyshev order n modulo p. If for any $t > 1$ there exists a residue x modulo p such that the $t-1$ residues $x = T_1(x)$, $T_2(x)$, $\ldots$, $T_{t-1}(x)$ run through all the $t-1$ residues of $\mathscr{C}_t$, then we call x a *generator* of $\mathscr{C}_t$.

We prove the following theorem in which $\varphi(n)$ denotes Euler's function.

THEOREM 2. (i) *We have* $\alpha(1) = 0$, $\alpha(p) = 2$, *and if n is greater than unity and a divisor of q or r, then* $\alpha(n) = \varphi(n)$. *Otherwise* $\alpha(n) = 0$.

(ii) *Each class $\mathscr{C}_t$ $(t > 1)$ possesses generators x. The number of generators of $\mathscr{C}_t$ $(t > 1)$ is* $\frac{1}{2}\varphi(2t)$.

(iii) *A residue x modulo p is a generator of $\mathscr{C}_t$ $(t > 1)$ if and only if it is of Chebyshev order t and* $T_t(x) \equiv -1$.

(iv) *If x is a generator of $\mathscr{C}_t$ $(t > 1)$ then the Chebyshev order of $T_k(x)$ is $t/(k, t)$, and the full set of generators of C_t consists of those residues $T_k(x)$ for which $(k, t) = 1$ and k is odd.*

PROOF. To prove (i) it is enough to show that if $n > 1$ and if n divides q or r then $\alpha(n) = \varphi(n)$. In the first place, we note that $(q, r) = 1$, so that the residues x of Chebyshev order n belong either to $\mathscr{C}_q$ or $\mathscr{C}_r$, and not to both. Consider therefore the residues x of $\mathscr{C}_t$ $(t > 1)$ and let $n > 1$ be a divisor of t. In the first place, the polynomial congruence $F_n(x) \equiv 0$, which is of degree $n-1$, has exactly $n-1$ solutions modulo p. For let its number of solutions be k, where therefore $k \leqq n-1$. Then we have, by (6), putting $t = mn$, that

$$F_t(x) = F_m\{T_n(x)\}\, F_n(x) \, .$$

Now $F_m\{T_n(x)\}$ is a polynomial of degree $(m-1)n = t-n$ in x, and so has at most $t-n$ solutions modulo p, while $F_t(x) \equiv 0$ has exactly $t-1$ solutions. Thus $t-1 \leqq t-n+k$, showing that $k \geqq n-1$. Hence $k=n-1$.

Secondly, if x is of Chebyshev order d where d divides n, then $F_d(x)$ is a factor of $F_n(x)$, so that $F_n(x) \equiv 0$. These results show that for every divisor n of t we have

$$n-1 = \sum_{d|n} \alpha(d) \, .$$

From this, since $\alpha(1) = 0$, we deduce, for example by the Möbius conversion formula, that $\alpha(n) = \varphi(n)$ $(n > 1)$.

Since $\varphi(t) \geqq 1$, it follows that in each class $\mathscr{C}_t$ $(t > 1)$ there are residues x of order t, and that there are, in fact, $\varphi(t)$ of them. Further, if x is of order t, so clearly is $-x$. If t is even, then by (16), $T_t(x) \equiv -1$ for each of these $\varphi(t)$ residues. If, however, t is odd, then $0 \notin \mathscr{C}_t$ and, since $T_t(x)$ is an odd function of x it follows that, for half of the $\varphi(t)$ residues, $T_t(x) \equiv -1$, and for the other half $T_t(x) \equiv 1$. Since $\frac{1}{2}\varphi(2t)$ is $\varphi(t)$ or $\frac{1}{2}\varphi(t)$ according as t is even or odd, part (ii) will follow if we can prove (iii).

We show first that $n_x = t$ when x is a generator of $\mathscr{C}_t$. For if $n_x = n < t$ then, since n divides t, $2n-1 < t$, and we have, by (7), $T_{2n-1}(x) \equiv x$, which cannot occur for a generator x. Secondly, if x is a generator of $\mathscr{C}_t$ then $T_t(x) \equiv -1$. For

$$(18) \qquad T_{t-n} \pm T_n = T_n(T_t \pm 1) - (x^2-1)F_t F_n \equiv T_n(T_t \pm 1)\,,$$

so that, if, for odd $t > 1$, $T_t(x) \equiv 1$ then $T_{t-n}(x) \equiv T_n(x)$, and hence, for $1 \leqq n < t$, the residues $T_n(x)$ run through at most $\frac{1}{2}(t-1)$ members of $\mathscr{C}_t$; thus such a value of x cannot be a generator.

We now suppose that $n_x = t$, and that $T_t(x) \equiv -1$, and show that x is a generator of $\mathscr{C}_t$. For if $1 \leqq n < t$ we have, by (6),

$$F_t\{T_n(x)\}\, F_n(x) = F_{tn}(x) = F_n\{T_t(x)\}\, F_t(x) \equiv 0\,,$$

so that $F_t\{T_n(x)\} \equiv 0$, that is $T_n(x) \in \mathscr{C}_t$. Hence it remains to show that if $1 \leqq m \leqq n \leqq t$ and $T_m(x) \equiv T_n(x)$ then $m = n$. By (8), we have

$$(x^2-1)\, F_{m-n}(x)\, F_{m+n}(x) \equiv 0\,,$$

so that, by (17), either t divides $m-n$, that is $m = n$, or else t divides $m+n$, that is $m = t-n$. In the latter case we have, by (18),

$$0 \equiv T_{t-n} - T_n \equiv T_n(T_t - 1) \equiv -2T_n\,.$$

Hence $T_n(x) \equiv 0$, and therefore

$$F_{2n}(x) \equiv F_2\{T_n(x)\}\, F_n(x) \equiv F_2(0)\, F_n(x) \equiv 0\,,$$

which implies that $t = 2n$, that is $m = n$. This completes the proof of (iii).

To prove (iv) suppose that $1 \leqq k < t$ and that $h = (k, t)$, $t = hu$, $k = hv$. Then

$$0 \equiv F_{tv}(x) \equiv F_{uk}(x) \equiv F_u\{T_k(x)\}\, F_k(x)\,,$$

and therefore $F_u\{T_k(x)\} \equiv 0$. Thus $T_k(x)$ is of order n, say, where n divides u.

Conversely, since $F_{nk}(x) = F_n\{T_k(x)\}\, F_k(x)$, n is the smallest positive integer such that t divides nk, i.e. such that u divides nv, i.e. such that u divides n, since $(u, v) = 1$. Thus $n = u = t/(k, t)$. To complete the proof of (iv) we observe that the residues of order t are $T_k(x)$ for $(k,t) = 1$, and that $T_k(x)$ is a generator if and only if, in addition, k is odd. For

$$T_t\{T_k(x)\} = T_{tk}(x) = T_k\{T_t(x)\} = T_k(-1) = (-1)^k ,$$

by (9).

The following theorem shows, in particular, that if x is a generator of $\mathscr{C}_t$ $(t > 1)$, then $T_n(x)$ and $F_n(x)$ are periodic functions of n modulo p with period $2t$.

THEOREM 3. *If x is a generator of $\mathscr{C}_t$ $(t > 1)$, then*

$$T_{2t\pm n}(x) \equiv T_n(x), \qquad F_{2t\pm n}(x) \equiv \pm F_n(x) ,$$
$$T_{t\pm n}(x) \equiv -T_n(x) , \qquad F_{t\pm n}(x) \equiv \pm F_n(x) .$$

We omit the proof, which is straightforward.

We note also that, if t is odd and x is of Chebyshev order t, but not a generator of $\mathscr{C}_t$, then

$$\pm T_1(x),\ \pm T_2(x),\ \ldots\ ,\ \pm T_{\frac{1}{2}(t-1)}(x)$$

run through all the members of $\mathscr{C}_t$ and so provide an alternative method of generating the set.

As an example, consider $p = 29$ so that $q = 14$, $r = 15$. We find that 5 is a generator of $\mathscr{C}_{14}$ and -2 is a generator of $\mathscr{C}_{15}$. The members of the two classes are given in the following table:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$T_n(5)$	5	-9	-8	-13	-6	11	0	-11	6	13	8	9	-5	
$T_n(-2)$	-2	7	3	10	-14	-12	4	-4	12	14	-10	-3	-7	2

The class $\mathscr{C}_{14}$ has 6 generators, namely ± 5, ± 6, ± 8 (mod 29), while $\mathscr{C}_{15}$ has 4 generators, namely -2, 4, -10 and -7 (mod 29).

In conclusion, we prove

THEOREM 4. *If x is a generator of $\mathscr{C}_q$ and y is chosen so that $x^2-1 \equiv y^2$, then $x+y$ is a primitive root modulo p. Conversely, if g is a primitive root modulo p and $gg' \equiv 1$, then $x \equiv \frac{1}{2}(g+g')$ is a generator of $\mathscr{C}_q$.*

PROOF. If x is a generator of $\mathscr{C}_q$ and $x^2-1 \equiv g^2$, it is easily shown, by using (3), that

$$(x+y)^n \equiv T_n(x) + yF_n(x) . \tag{19}$$

Now $x+y \not\equiv 0$, so that it possesses an order, k say, modulo p. Since $(x+y)^q \equiv -1$, k cannot be odd, as otherwise it would divide q and we should obtain a contradiction. Hence $k = 2n$, say, and therefore, by (19),

$$0 \equiv (x+y)^n - (x+y)^{-n} \equiv (T_n+yF_n) - (T_n-yF_n) \equiv 2yF_n\,,$$

from which we deduce that $n = q$, that is, $x+y$ is a primitive root.

Conversely, if g is a primitive root modulo p and $x \equiv \frac{1}{2}(g+g')$ we can take $y \equiv \frac{1}{2}(g-g')$ as a solution of $x^2-1 \equiv y^2$. Then the preceding argument may be reversed to show that $n = q$ is the least positive integer for which $F_n(x) \equiv 0$ and that $T_n(x) \equiv -1$. Thus x is a generator of $\mathscr{C}_q$.

4. THEOREM 5. *If ξ is an element of the modulary group $\overline{G}(p)$ $(p > 2)$ other than the unit element Θ, and if S is any matrix representing ξ, then the order of ξ is the same as the Chebyshev order of x modulo p where x is any integer such that $2x \equiv \operatorname{tr} S$.*

PROOF. Let the representing matrix S be defined by (1), where $ad-bc \equiv 1$. Then the order $N(\xi)$ of ξ is the least positive integer N such that $S^N \equiv \pm I$, and is the same for every matrix representing ξ. Thus, by (12), N is the least positive integer for which

$$aF_N-F_{N-1} \equiv dF_N-F_{N-1} \equiv \pm 1, \qquad bF_N \equiv cF_N \equiv 0\,.$$

Thus either $N = n_x$, since then $F_{N-1} \equiv \pm 1$, by (5), or else $0 < N < n_x$ and $b \equiv c \equiv 0$. In the second case we deduce that $a \equiv d$ and $ad \equiv 1$, that is $a \equiv d \equiv \pm 1$, which is false since $\xi \neq \Theta$. This proves Theorem 5.

With the help of Theorem 5 and the results of § 3 we can show that the order of an element of $\overline{G}(p)$ other than Θ is either p or a divisior of q or r, and that the elements whose orders divide p, q or r can be divided into $p+1$, $\frac{1}{2}p(p+1)$ and $\frac{1}{2}p(p-1)$ conjugate cyclic subgroups of orders p, q and r respectively. Further the $p+1$ subgroups of order p are conjugates of the subgroup generated by

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{20}$$

while the $p(p-t)$ subgroups of order t ($t = q$ or r) are conjugates of the subgroup generated by

$$X = \begin{pmatrix} x & x+1 \\ x-1 & x \end{pmatrix}, \tag{21}$$

where x is a generator of $\mathscr{C}_t$. In proving these results we could at various points refer the reader to [1], [2, pp. 419–491] or [4, pp. 363–383 (§§ 464–473)], but prefer to give the argument in full. Also we shall adopt a wholly arithmetic approach and shall not derive the results by considering permutable matrices.

From Theorem 5 it follows that the elements of $\overline{G}(p)$ can be divided into four classes, (i) the unit element Θ, (ii) $\mathfrak{S}_p$, (iii) $\mathfrak{S}_q$ and (iv) $\mathfrak{S}_r$, where $\xi \in \mathfrak{S}_s$ if and only if $\xi \neq \Theta$, $N(\xi)\,|\,s$. We denote by N_s the number of elements in $\mathfrak{S}_s$.

The class $\mathfrak{S}_p$. For every element of $\mathfrak{S}_p$ we must have $x \in \mathcal{C}_p$, where $2x = \operatorname{tr} S$, that is $x \equiv \pm 1$. Then $2N_p$ is the number of solutions a,b,c,d of the congruences

$$a+d \equiv \pm 2, \qquad bc \equiv ad-1\ ,$$

the solutions $a \equiv d \equiv \pm 1$, $b \equiv c \equiv 0$ being excluded. Thus N_p+1 is the number of solutions of

$$a+d \equiv 2, \qquad bc \equiv ad-1\ .$$

By considering the cases $ad \not\equiv 1$, $ad \equiv 1$ separately we easily see that

$$N_p + 1 = (p-1)(p-1) + 2p - 1 = p^2\ ,$$

so that

(22) $$N_p = p^2 - 1\ .$$

Since two cyclic subgroups of order p are either identical or have only Θ in common, and since $p^2-1 = (p-1)(p+1)$, it follows that the elements of $\mathfrak{S}_p$ belong to $p+1$ different cyclic subgroups of $\overline{G}(p)$ of order p.

One of these subgroups is that generated by P (see (20)). Let S be any other matrix belonging to $\mathfrak{S}_p$ and suppose, as we may, that $a+d=2$. Also, write

(23) $$T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad \alpha\delta-\beta\gamma \equiv 1\ ,$$

so that

$$T^{-1}P^{\lambda}T = \begin{pmatrix} 1+\lambda\gamma\delta & \lambda\delta^2 \\ -\lambda\gamma^2 & 1-\lambda\gamma\delta \end{pmatrix}.$$

Suppose first that $c \not\equiv 0$. Then $T^{-1}P^{\lambda}T \equiv S$ if we take

$$\lambda \equiv -c, \quad \alpha \equiv 0, \quad \beta \equiv -1, \quad \gamma \equiv 1, \quad \delta \equiv -(a-d)/(2c)\ .$$

If $c \equiv 0$, then $ad \equiv 1$, that is, $a \equiv d \equiv 1$ and $S \equiv P^b$. Hence, in either case, S is the transform of a power of P and it follows that the $p+1$ subgroups of order p are conjugate.

The classes $\mathfrak{S}_q$, $\mathfrak{S}_r$. We can to a large extent treat these together. For every element of $\mathfrak{S}_t$ we must have $x \in \mathcal{C}_t$. Let $M_t(x)$ be the number of solutions of the congruence

$$a+d \equiv 2x, \qquad bc \equiv ad-1\ .$$

We can have $bc \equiv 0$ only when $ad \equiv 1$, i.e. when $x \equiv a+a^{-1}$. We then have
$$x^2 - 1 \equiv \{\tfrac{1}{2}(a-a^{-1})\}^2 ,$$
which, since $a \not\equiv \pm 1$, implies that $x \in \mathscr{C}_q$.

Thus, if $x \in \mathscr{C}_q$, of the p possible pairs a, d two give $ad \equiv 1$ and so
$$M_q(x) = (p-2)(p-1) + 2(2p-1) = p^2 + p = 2p(p-t) .$$
On the other hand, if $x \in \mathscr{C}_r$, we cannot have $ad \equiv 1$, and so
$$M_r(x) = p(p-1) = 2p(p-t) .$$
Hence

(24)
$$N_t = \tfrac{1}{2}(t-1)M_t(x) = p(p-t)(t-1) .$$
As a check we note that, by (22) and (24),
$$\begin{aligned}&1 + N_p + N_q + N_r \\ &\quad = 1 + (p^2-1) + \tfrac{1}{4}(p-3)p(p+1) + \tfrac{1}{4}(p-1)p(p-1) = \tfrac{1}{2}p(p^2-1) ,\end{aligned}$$
which is the order of $\overline{G}(p)$.

Now suppose that x is a generator of $\mathscr{C}_t$, and consider the $2p(p-t)$ members of $\mathfrak{S}_t$ whose representing matrices S have $a+d \equiv 2x$. Since $\operatorname{tr} S = \operatorname{tr} S^{-1}$, we may group these matrices into $p(p-t)$ pairs S, S^{-1}. Each pair generates a cyclic group of order t represented by
$$I, S, S^2, \ldots, S^{t-1} .$$
No two of these cyclic groups have a common element other than Θ. For if this were not so then we should have

(25)
$$S_1{}^m \equiv \pm S_2{}^n,$$
for some matrices S_1, S_2 each of trace $2x$, with
$$S_1 \not\equiv S_2, \qquad S_1 \not\equiv S_2{}^{-1},$$
and $1 \leqq m < t$, $1 \leqq n < t$. Taking the trace of each side we have
$$T_m(x) \equiv \pm T_n(x) ,$$
from which it follows, since x is a generator, and by (8) and (18), that either $m = n$ (for $+$ sign), or $m = t-n$ (for $-$ sign). By taking $S_2{}^{-1}$ in place of S_2, if necessary, we may therefore assume that $m = n$ and that $S_1{}^n \equiv S_2{}^n$. Hence we have, with an obvious notation,
$$\begin{gathered} a_1F_n - F_{n-1} \equiv a_2F_n - F_{n-1}, \qquad b_1F_n \equiv b_2F_n , \\ c_1F_n \equiv c_2F_n, \qquad d_1F_n - F_{n-1} \equiv d_2F_n - F_{n-1} . \end{gathered}$$

Since $F_n \not\equiv 0$ we deduce that $S_1 \equiv S_2$, which shows that (25) cannot hold.

Further, since it is easily seen that each member of $\mathfrak{S}_t$ with trace $2T_n(x)$ $(1 \leqq n < t)$ is the nth power of some element with trace $2x$, we conclude that the elements of $\mathfrak{S}_t$ can be divided into $N_t/(t-1) = p(p-t)$ cyclic subgroups of order t, no two of which possess common elements other than Θ.

Now suppose that S is any matrix (1) with $ad-bc \equiv 1$ and trace $2x$. We wish to choose a matrix T (see (23), (21)) to make

$$T^{-1}XT \equiv S\,. \tag{26}$$

This implies that

$$\gamma\delta(x+1) - \alpha\beta(x-1) \equiv a-x \equiv x-d\,, \tag{27}$$

$$\delta^2(x+1) - \beta^2(x-1) \equiv b\,, \tag{28}$$

$$-\gamma^2(x+1) + \alpha^2(x-1) \equiv c\,. \tag{29}$$

Suppose first that $c \not\equiv 0$. For different values of γ and α, each of $\alpha^2(x-1)$ and $\gamma^2(x+1)+c$ take $\frac{1}{2}(p+1)$ different values modulo p, and hence for at least one pair α, γ, the two expressions are congruent modulo p, so that (29) is satisfied. With these values of α, γ we can solve (27) together with $\alpha\delta-\beta\gamma \equiv 1$ for β and δ, since the determinant of the two congruences is $c \not\equiv 0$. These values must automatically satisfy (28) since $ad-bc \equiv 1$ and $c \not\equiv 0$.

If $c \equiv 0$ and $b \not\equiv 0$ we can similarly find a matrix T by solving first for δ and β and then choosing α and γ.

Finally, if $b \equiv c \equiv 0$, then $ad \equiv 1$, and so if we take $y \equiv \frac{1}{2}(a-d) \not\equiv 0$, we have $x^2-1 \equiv y^2$; that is, $x \in \mathscr{C}_q$. We now choose

$$\alpha \equiv y, \quad \beta \equiv \lambda y, \quad \gamma \equiv x-1, \quad \delta \equiv -\lambda(x-1), \quad 2\lambda y(x-1) \equiv -1$$

and the congruences (27), (28) and (29) are then all satisfied.

Thus in all cases we can find a T to satisfy (26) for each matrix S of $\mathfrak{S}_t$, and this shows that the $p(p-t)$ subgroups of order t are self-conjugate.

5. *Unsolved problem.* For large primes p, how small can $|x|$ be, where x is a generator of $\mathscr{C}_q$ or $\mathscr{C}_r$?

REFERENCES

1. J. Gierster, *Die Untergruppe der Galoisschen Gruppe der Modulargleichung für den Fall eines primzahligen Transformationsgrades*, Math. Ann. 18 (1881), 319–365.

2. F. Klein und R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen*, Band I, Leipzig, 1890.
3. J.-A. Serret, *Sur les fonctions rationelles linéaires prise suivant un module premier, et sur les substitutions auxquelles conduit la considération de ces fonctions*, C. R. Acad. Sci. Paris 48 (1859), 112–117, 178–182, 237–240.
4. J.-A. Serret, *Cours d'algèbre supérieure*, tome II, Paris, 1879.
5. G. Vivanti, *Elementi della teoria delle funzioni poliedriche e modulari*, Milano, 1906.
6. G. Vivanti, *Les fonctions polyédriques et modulaires* (traduit par A. Cahen), Paris, 1910.

THE UNIVERSITY, BIRMINGHAM, ENGLAND