On classification of finite groups with four generators three of which having prime orders $p, q, q (p<q)$ II

By K. R. YACOUB (Cairo)

In a previous paper [1] the author discussed the existence and the structure of finite groups with four generators a, b, c and d when the orders of b, c, d are respectively p, p, q with $p<q$.

The case $p>q$, or equivalently the case when the orders of b, c, d are respectively p, q, q with $p<q$ is discussed in the present paper. As in the previous paper, the order m of a is arbitrary but $m \notin \{p, q\}$. The symbol e is used also throughout this paper to denote the ideniity of the group unless otherwise stated.

Notation and preliminaries

We use frequently the three parameters λ, μ and ν where

$$\lambda \in \{2, \ldots, p-1\} \quad \text{i.e.} \quad \lambda \not\equiv 1 \pmod p,$$

$$\mu, \nu \in \{2, \ldots, q-1\} \quad \text{i.e.} \quad \mu, \nu \not\equiv 1 \pmod q.$$

The symbols k, k' and k^* are used to denote the respective orders of $\lambda \bmod p$, $\mu \bmod q$ and $\nu \bmod q$. Thus

$$\lambda^k \equiv 1 \pmod p, \quad \mu^{k'} \equiv 1 \pmod q, \quad \nu^{k^*} \equiv 1 \pmod q.$$

It may be noted that $k, k', k^* > 1$.

Two other parameters namely ω, ω' taken $\bmod q$ are also used but possibly $\omega, \omega' \equiv 1 \pmod q$; while $\mu, \nu \not\equiv 1 \pmod q$.

Finally, for positive integers x, y, z, the symbol $[x, y]$ is used for the *L.C.M* of x and y while the symbol $[x, y, z]$ is used for the *L.C.M* of x, y and z.

Two theorems, due to the author [2], are stated here without proof.

Theorem 1. *Let p and q be two distinct odd primes such that*

$$\text{(i) } p<q, \quad \text{(ii) } p \text{ does not divide } q-1.$$

Then there exist four types of groups with three generators a, b, c whose orders are respectively m (arbitrary), p and q. These groups, denoted by M_i: $i=1, 2, 3, 4$ are

$$M_1 = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r, ac = ca^s, bc = cb\},$$

with $$r^p \equiv 1 \equiv s^q \pmod m,$$

$$M_2 = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r, ac = c^\mu a,\ bc = cb\},\quad \mu \not\equiv 1 \pmod q,$$

with $$r^p \equiv 1 \pmod m,\quad k' \| [m, r-1],$$

$$M_3 = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = b^\lambda a,\ ac = ca^s,\ bc = cb\},\quad \lambda \not\equiv 1 \pmod p$$

with $$s^q \equiv 1 \pmod m,\quad k \| [m, s-1],$$

$$M_4 = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = b^\lambda a,\ ac = c^\mu a,\ bc = cb\},$$

with $$\lambda \not\equiv 1 \pmod p), \mu \not\equiv 1 \pmod q \quad \textit{and} \quad [k, k'] \| m.$$

Cor. 1. *Groups of the types M_2, M_3 and M_4 do not exist for $m=q$. For, in M_2, $\mu \not\equiv 1 \pmod q$ and its order* mod q, *namely k' is greater than* 1. *Thus if we take $m=q$, we have $k'|q$ and thus $k'=q$. Hence $\mu^q \equiv 1 \pmod q$ which combines with Fermat's Theorem to show that $\mu \equiv 1 \pmod q$. This contradiction shows that no group of the type M_2 exists for $m=q$. Similar arguments apply for M_3 and M_4.*

Cor. 2. *A group of the type M_1 exists for $m=q$ and is Abelian. For, if we take $m=q$ in M_1, we have $r^p \equiv 1 \pmod q$ which implies $r \equiv 1 \pmod q$ since p does not divide $q-1$. Also, we have $s^q \equiv 1 \pmod q$ which combines with Fermat's Theorem to show that $s \equiv 1 \pmod q$.*

The above two corollaries combine to show

Cor. 3. *The only group that exists with three generators b, c, d having the respective orders p, q, q is an Abelian group.*

Note. It may be noted that we changed a by d for later quotation.

Theorem 1*. *Let p and q be two distinct odd primes such that*

$$\text{(i)}\quad p < q, \qquad \text{(ii)}\quad p \quad \textit{divides} \quad q-1.$$

Then there exist four types of groups M_i^*: $i=1, 2, 3, 4$ with three generators a, b, c two of which having orders p and q. These groups are

$$M_1^* = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = ca^s,\ bc = c^\omega b\}$$

with $$r^p \equiv 1 \equiv s^{f(\omega)} \pmod m,\quad \omega^p \equiv 1 \pmod q,\quad f(\omega) = \begin{cases} q & \text{if} \quad \omega = 1 \\ 1 & \text{if} \quad \omega \neq 1 \end{cases}$$

$$M_2^* = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = c^\mu a,\ bc = c^\omega b\}$$

with $$r^p \equiv 1 \pmod m,\quad \omega^p \equiv 1 \pmod q,\quad k' \| [m, r-1]$$

$$M_3^* = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = b^\lambda a,\ ac = ca^s,\ bc = cb\}$$

with $$s^q \equiv 1 \pmod m,\quad k \| [m, s-1],$$

$$M_4^* = \{a, b, c;\ a^m = b^p = c^q = e,\ ab = b^\lambda a,\ ac = c^\mu a,\ bc = cb\}$$

with $$[k, k'] \| m.$$

Remark 1. From Theorem 1* (when p divides $q-1$) and Theorem 1 (when p does not divide $q-1$), we observe that

(i) $M_3 = M_3^*$, (ii) $M_4 = M_4^*$,

(iii) $M_1 = M_1^*$ with $\omega = 1$, (iv) $M_2 = M_2^*$ with $\omega = 1$.

Cor. 1* Groups of the types M_2^*, M_3^* and M_4^* do not exist for $m=q$. For if we take $m=q$ in M_2^*, we have $k'|[q, r-1]$ and thus $k'|q$, but $k'>1$ and therefore $k'=q$. Hence $\mu^q \equiv 1 \pmod q$ which by using Fermat's Theorem gives directly $\mu \equiv 1 \pmod q$. This contradiction shows that no group of the type M_2^* exists.
For the types M_3^* and M_4^* this follows directly if we remark that $M_3 = M_3^*$, $M_4 = M_4^*$ and use the argument of Cor. 1.

Cor. 2*. *A group of the type M_1^* exists when $m=q$. For, if we take $m=q$ in M_1^*, we have*

$$r^p \equiv 1 \pmod q, \quad s^{f(\omega)} \equiv 1 \pmod q.$$

The last congruence relation implies always $s \equiv 1 \pmod q$ whether $\omega \equiv 1$ or $\omega \not\equiv 1 \pmod q$. This is obvious from the definition of f when $\omega \not\equiv 1 \pmod q$. Again from the definition, for $\omega \equiv 1 \pmod q$, we have $f(1) = q$ and therefore $s^q \equiv 1 \pmod q$ which gives directly $s \equiv 1 \pmod q$ by using Fermat's Theorem. Then M_1^* will be

$$M_1^* = \{a, b, c;\ a^q = b^p = c^q = e,\ ab = ba^r,\ ac = ca,\ bc = c^\omega b\},$$

where

$$r^p \equiv 1 \equiv \omega^p \pmod q.$$

Changing* a by d and replacing r by ω^*, we have thus shown

Cor. 3*. *Let p and q be two distinct odd primes such that p divides $q-1$. Then there exist just one type of groups with three generators two of which being of order q and the third of order p. This group which we denote by $N(\omega, \omega')$ is*

$$N(\omega, \omega') = \{b, c, d;\ b^p = c^q = d^q = e,\ bc = c^\omega b,\ bd = d^{\omega'} b,\ cd = dc\}$$

where $$\omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

In fact, the original relation $ab = ba^r$ changes to $db = bd^{\omega^*}$ which is easily shown to be equivalent to $bd = d^{\omega'} b$ where $\omega' \omega^* \equiv 1 \pmod q$. It may be noted that if $\omega \equiv 1 \pmod q$, then $\omega' \equiv 1 \pmod q$ simultaneously. This is obvious for the symmetrical role played by c and d in the structure of the group. Thus the group $N(\omega, \omega')$ is either Abelian (when $\omega \equiv \omega' \equiv 1 \pmod q$) or non-Abelian (when $\omega, \omega' \not\equiv 1 \pmod q$).

Part I. The case p does not divide $q-1$.

Let G be a finite group with four generators a, b, c and d whose orders are m (arbitrary), p, q and q respectively, where p and q are distinct odd primes such that $p<q$ and p is not a divisor of $q-1$. Then

$$a^m = b^p = c^q = d^q = e.$$

* For later quotation, a is replaced by d.

By Cor. 3, the subgroup $\{b, c, d\}$ is Abelian. Evidently, the subgroups $\{a, b, c\}$ and $\{a, b, d\}$ may be one of the four types M_1, M_2, M_3 and M_4. Thus ten cases may arise and the corresponding types of groups, in ease they exist, may be listed in the following table.

Table 1. The case p does not divide $q-1$

Type of $\{a, b, c\}$	Type of $\{a, b, d\}$	Type of $G=\{a, b, c, d\}$
M_1	M_1	$T(1, 1)$
M_1	M_2	$T(1, 2)$
M_1	M_3	$T(1, 3)$
M_1	M_4	$T(1, 4)$
M_2	M_2	$T(2, 2)$
M_2	M_3	$T(2, 3)$
M_2	M_4	$T(2, 4)$
M_3	M_3	$T(3, 3)$
M_3	M_4	$T(3, 4)$
M_4	M_4	$T(4, 4)$

Remark 1. It should be remarked that other types may arise, for example the type $T(2, 1)$ but such a type is exactly the same type $T(1, 2)$ if we just interchange the two generators c and d which have the same order q.

Remark 2. Groups of the types $T(1, 3)$ and $T(1, 4)$ do not exist. In fact, for such two types of groups, the subgroup $\{a, b, c\}$ is of the type M_1 for which $ab=ba^r$ while the subgroup $\{a, b, d\}$, being of the type M_3 or M_4 for both of which, we have $ab=b^\lambda a$ with $\lambda \not\equiv 1 \pmod p$. This obvious contradiction shows that groups of the types $T(1, 3)$ and $T(1, 4)$ do not exist.
Using similar argument, we have

Remark 3. Groups of the types $T(2, 3)$ and $T(2, 4)$ do not exist. Thus it remains to discuss the existence of the six types

$$T(i, i)\colon\ i = 1, 2, 3, 4 \quad \text{and} \quad T(1, 2), \quad T(3, 4).$$

Theorem 2. *If there is a group G of the type $T(1, 1)$, then it has the defining relations*

$$(1) \quad G = \{a, b, c, d;\ \ a^m = b^p = c^q = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = da^t,$$
$$bc = cb,\ bd = db,\ cd = dc\}$$

where

$$(2) \qquad r^p \equiv s^q \equiv t^q \equiv 1 \pmod m.$$

Conversely, if r, s and t satisfy (2), then the group G generated by a, b, c and d with the defining relations (1) is of the desired type.

Proof. Assume the existence of a group G of the type $T(1, 1)$. Then for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_1

described in Theorem 1. Thus we have

$$\{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = ca^s,\ bc = cb\}$$

with

$$r^p \equiv 1 \equiv s^q \pmod{m};$$

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^t,\ bd = db\}$$

with

$$r^p \equiv 1 \equiv t^q \pmod{m}.$$

Moreover $cd=dc$ since the subgroup $\{b, c, d\}$ is Abelian. Thus we have shown that (1) and (2) are necessary.

For the converse, let K be the system of all formal quadruples $[x, y, z, w]$ where x is taken $\bmod m$, $y \bmod p$ and z, $w \bmod q$. In this system define multiplication by means of the formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where

$$x'' \equiv r^{y'} s^{z'} t^{w'} x + x' \pmod{m},$$

$$y'' \equiv y + y' \pmod{p},$$

$$z'' = z + z', \quad w'' \equiv w + w' \pmod{q}.$$

It is easily shown that, under this multiplication, the system K is a group of order pq^2m. Moreover, if

$$a' = [1, 0, 0, 0], \quad b' = [0, 1, 0, 0], \quad c' = [0, 0, 1, 0], \quad d' = [0, 0, 0, 1]$$

then, corresponding to the defining relations of G, it is easily shown

$$a'^m = b'^p = c'^q = d'^q = e', a'b' = b'a'^r, a'c' = c'a'^s, a'd' = d'a'^t,$$

$$b'c' = c'b',\ b'd' = d'b',\ c'd' = d'c'.$$

This shows that the group K is a homomorphic image of G. But as the order of K is pq^2m and the order of G is at most pq^2m, they have the same order and are isomorphic. This proves that a group of the required type exists.

Theorem 3. *If there is a group G of the type $T(2, 2)$, then it has the defining relations*

(3) $$G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = ba^r,\ ac = c^\mu a,\ ad = d^\nu a,$$
$$bc = cb,\ bd = db,\ cd = dc\},$$

where $\mu, \nu \not\equiv 1 \pmod{q}$ *and*

(4) $$r^p \equiv 1 \pmod{m}, \quad k' | [m, r-1], k^* | [m, r-1].$$

Conversely, if r and k', k^* (the respective orders of $\mu, \nu \bmod q$) satisfy (4), *then the group G generated by a, b, c, d with the defining relations* (3) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(2,2)$. Then for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_2 described in Theorem 1. Thus we have

$$\{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = c^\mu a,\ bc = cb\}, \quad \mu \not\equiv 1 \pmod q$$

with $$r^p \equiv 1 \pmod m, \quad k'\|[m, r-1],$$

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^\nu a,\ bd = db\}, \quad \nu \not\equiv 1 \pmod q$$

with $$r^p \equiv 1 \pmod m, \quad k^*\|[m, r-1].$$

Again $cd=dc$ since the subgroup $\{b, c, d\}$ is Abelian. Thus we have shown that (3) and (4) are necessary.

For the converse, we use the same system K of the previous theorem with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where
$$x'' \equiv r^{y'} x + x' \pmod m,$$
$$y'' \equiv y + y' \pmod p,$$
$$z'' \equiv z + \mu^x z',\ w'' \equiv w + \nu^x w' \pmod q.$$

Following the same procedure, it is easily shown that, under this multiplication, the system K is a group of order pq^2m which is isomorphic to a group of the required type.

Theorem 4. *If there is a group G of the type $T(3,3)$, then it has the defining relations*

(5) $$G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = b^\lambda a,\ ac = ca^s,\ ad = da^t,$$
$$bc = cb,\ bd = db,\ cd = dc\},$$

where $\lambda \not\equiv 1 \pmod p$ *and*

(6) $$s^q \equiv 1 \equiv t^q \pmod m, \quad k\|[m, s-1, t-1].$$

Conversely, if s, t and k (the order of λ $\bmod p$) satisfy (6), *then the group G generated by a, b, c, d with the defining relations* (5) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(3,3)$. Then, for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_3 described in Theorem 1. This with the fact that the subgroup $\{b, c, d\}$ is for such type is Abelian show that (5) and (6) are necessary.

For the converse, we use the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where
$$x'' \equiv s^{z'} t^{w'} x + x' \pmod m,$$
$$y'' \equiv y + \lambda^x y' \pmod p,$$
$$z'' \equiv z + z',\ w'' \equiv w + w' \pmod q,$$

in the system K of all formal quadruples $[x, y, z, w]$, used before.

Theorem 5. *If there is a group G of the type $T(4, 4)$, then it has the defining relations*

$$(7) \qquad G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = b^\lambda a,\ ac = c^\mu a,\ ad = d^\nu a,$$
$$bc = cb,\ bd = db,\ cd = dc\}$$

where $\lambda \not\equiv 1 \pmod p$ *and* $\mu, \nu \not\equiv 1 \pmod q$ *and*

$$(8) \qquad [k, k', k^*] | m.$$

Conversely, if k, k' and k^* (the respective orders of λ $\bmod p$, *μ* $\bmod q$ and *ν* $\bmod q$*), satisfy* (8) *then the group G generated by a, b, c, d with the defining relations* (7) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(4, 4)$. Then, for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_4 described in Theorem 1. This together with the fact that the subgroup $\{b, c, d\}$ is Abelian show that conditions (7) and (8) are necessary.

For the converse, we use again the same system K but with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where

$$x'' \equiv x + x' \pmod m,$$
$$y'' \equiv y + \lambda^x y' \pmod p,$$
$$z'' \equiv z + \mu^x z',\ w'' \equiv w + \nu^x w' \pmod q.$$

It is easily shown that the system K is a group of order pq^2m which is isomorphic to a group G of the required type.

Theorem 6. *If there is a group G of the type $T(1, 2)$, then it has the defining relations*

$$(9) \qquad G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = d^\nu a,$$
$$bc = cb,\ bd = db,\ cd = dc\},$$

where $\qquad \nu \not\equiv 1 \pmod q$ and

$$(10) \qquad r^p \equiv 1 = s^q \pmod m, \quad k^* | [m, r-1].$$

Conversely, if r, s, k^* (the order of ν $\bmod q$*) satisfy* (10) *then the group G generated by a, b, c, d with the defining relations* (9) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(1, 2)$. Then, for such a group, the subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are of the types M_1 and M_2 respectively. Thus by Theorem 1, we have

$$\{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = c^\mu a,\ bc = cb\}, \quad \mu \not\equiv 1 \pmod q,$$
$$r^p \equiv 1 \equiv s^q \pmod m,$$
$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^\nu a,\ bd = db\}, \quad \nu \not\equiv 1 \pmod q,$$
$$r^p \equiv 1 \pmod m, \quad k^* | [m, r-1].$$

Again $cd=dc$ as the subgroup $\{b, c, d\}$ is Abelian. Thus we have shown that (9) and (10) are necessary.

For the converse, we use again the system K of formal quadruples $[x, y, z, w]$ with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where

$$x'' \equiv r^{y'} s^{z'} x + x' \pmod m,$$

$$y'' \equiv y + y' \pmod p,$$

$$z'' \equiv z + z', \ w'' \equiv w + v^x w' \pmod q.$$

It is easily shown that, under this multiplication, the system K is a group of order pq^2m which is isomorphic to a group of the type required.

Theorem 7. *If there is a group G of the type $T(3, 4)$, then it has the defining relations*

(11) $$G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = b^\lambda a,\ ac = ca^s,\ ad = d^v a,$$
$$bc = cb,\ bd = db,\ cd = dc\}$$

where $\lambda \not\equiv 1 \pmod p$, $v \not\equiv 1 \pmod q$ *and*

(12) $$s^q \equiv 1 \pmod m, \quad k|[m, s-1], [k, k^*]|m.$$

Conversely, if s and k, k^* (the respective orders of λ $\mathrm{mod}\, p$, v $\mathrm{mod}\, q$) statisfy (2). *then the group G generated by a, b, c, d with the defining relations* (11) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(3, 4)$. Then, for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are of the types M_3 and M_4 respectively and conditions (11), (12) follow immediately.

For the converse, we use again the same system K as before, but with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where

$$x'' \equiv s^{z'} x + x' \pmod m,$$

$$y'' \equiv y + \lambda^x y' \pmod p,$$

$$z'' \equiv z + z', \ w'' \equiv w + v^x w' \pmod q,$$

and the proof follows directly the same procedure as before and may be omitted.

Part II. The case p divides $q-1$.

Let G be a finite group with four generators a, b, c, d whose orders are respectively m (arbitrary, p, q, q where p and q are distinct odd primes such that p divides $q-1$. Then

$$a^m = b^p = c^q = d^q = e.$$

Now, since p divides $q-1$, then by Cor. 3* the subgroup $\{b, c, d\}$ is of the type $N(\omega, \omega')$ which is Abelian for $\omega \equiv \omega' \equiv 1 \pmod q$ and non-Abelian when

$\omega, \omega' \not\equiv 1 \pmod q$. Moreover, the subgroup $\{a, b, c\}$ or the subgroup $\{a, b, d\}$ may be one of the four types M_i^*: $i=1, 2, 3, 4$ described in Theorem 1*. Thus, corresponding to the Abelian (or non-Abelian) type of the subgroup $\{b, c, d\}$, there are ten cases and the corresponding groups may be listed in the following table.

Table 1*. The case p divides $q-1$

Type of $\{a, b, c\}$	Type of $\{a, b, d\}$	Type of $\{b, c, d\}$	Type of $G=\{a, b, c, d\}$
M_1^*	M_1^*	Abelian [non-Abelian]	$T^*(1, 1)$ [$P^*(1, 1)$]
M_1^*	M_2^*	Abelian [non-Abelian]	$T^*(1, 2)$ [$P^*(1, 2)$]
M_1^*	M_3^*	Abelian [non-Abelian]	$T^*(1, 3)$ [$P^*(1, 3)$]
M_1^*	M_4^*	Abelian [non-Abelian]	$T^*(1, 4)$ [$P^*(1, 4)$]
M_2^*	M_2^*	Abelian [non-Abelian]	$T^*(2, 2)$ [$P^*(2, 2)$]
M_2^*	M_3^*	Abelian [non-Abelian]	$T^*(2, 3)$ [$P^*(2, 3)$]
M_2^*	M_4^*	Abelian [non-Abelian]	$T^*(2, 4)$ [$P^*(2, 4)$]
M_3^*	M_3^*	Abelian [non-Abelian]	$T^*(3, 3)$ [$P^*(3, 3)$]
M_3^*	M_4^*	Abelian [non-Abelian]	$T^*(3, 4)$ [$P^*(3, 4)$]
M_4^*	M_4^*	Abelian [non-Abelian]	$T^*(4, 4)$ [$P^*(4, 4)$]

*Remark 1**. As in Table 1 (when p does not divide $q-1$) other types may arise, but, in fact, they are not distinct from the above types.

*Remark 2**. Groups of the types $T^*(1, 3)$ and $T^*(1, 4)$ do not exist. Groups of the type $P^*(1, 4)$ do not exist.

*Remark 3**. Groups of the types $T^*(2, 3)$ and $P^*(2, 3)$ do not exist.

*Remark 4**. Groups of the types $T^*(3, 4)$ and $P^*(3, 4)$ do not exist. For groups of the types $T^*(\ldots, \ldots)$ mentioned in the above remarks, arguments similar to those when p is not a divisor of $q-1$ apply.

But for the types $P^*(\ldots, \ldots)$, in case they exist, a direct contradiction follows if we remark that $bd=db=d^{\omega'}b$ with $\omega' \not\equiv 1 \pmod q$.

Theorem 8. *Let p and q be two distinct odd primes such that p divides $q-1$. Then groups of the types*

$$T^*(i, i)\colon\ i = 1, 2, 3, 4 \quad \text{and} \quad T^*(1, 2), T^*(3, 4)$$

exist and have the same structure as the corresponding groups when p does not divide $q-1$.

In other words

$$T^*(i, i) = T(i, i) \quad \text{for} \quad i = 1, 2, 3, 4,$$

$$T^*(1, 2) = T(1, 2),\ T^*(3, 4) = T(3, 4).$$

This becomes obvious if we observe that for the types $T^*(\ldots, \ldots)$, the subgroup $\{b, c, d\}$ is Abelian which is just the case with the corresponding groups $T(\ldots, \ldots)$ when p divides $q-1$. This implies directly that $bd=db$ and consequently, in the defining relations of M_1^* and M_2^*, must have $\omega' \equiv 1 \pmod q$. In this case

$$M_1 = M_1^*,\ M_2 = M_2^*.$$

This combine together with the fact that we have always (Remark 1)

$$M_3 = M_3^*, \; M_4 = M_4^*$$

to make the theorem direct and immediate.

Now, it remains to discuss the existence of the groups $P^*(\dots, \dots)$ which arise when the subgroup $\{b, c, d\}$ is non-Abelian already described in Cor. 3* namely

$$\{b, c, d; \; b^p = c^q = d^q = e, \; bc = c^{\omega} b, bd = d^{\omega'} b, \; cd = dc\}$$

with $\qquad \omega, \omega' \not\equiv 1 \pmod q$ and

$$\omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

Remarks 2*, 3*, 4* show that groups of the types $P^*(1, 4)$, $P^*(2, 3)$ and $P^*(3, 4)$ do not exist. In addition we prove

Theorem 9. *Groups of the types* $P^*(1, 3)$ *and* $P^*(2, 4)$ *do not exist. For both types, in case they exist, the subgroup* $\{a, c, d\}$ *is either of the type* M_3^* *or* M_4^* *for both of which we have* $cd = dc$ *which contradicts the defining relations of the subgroup* $\{b, c, d\}$ *for which* $cd = d^{\omega'} c$ *with* $\omega' \not\equiv 1 \pmod q$.

Thus it remains to discuss the existence of the four types $P^*(i, i)$, $P^*(1, 2)$.

Theorem 10. *Groups of the types* $P^*(3, 3)$ *and* $P^*(4, 4)$ *do not exist.*

For both types of groups, the subgroup $\{b, c, d\}$ is non-Abelian for which $bc = c^{\omega} b$, with $\omega \not\equiv 1 \pmod q$. But for both types, the subgroup $\{a, b, c\}$, being of the type M_3^* or M_4^* has, among its defining relations, $bc = cb$. This obvious contradiction shows that groups of the types $P^*(3, 3)$ and $P^*(4, 4)$ do not exist.

Theorem 11. *If there is a group* G *of the type* $P^*(1, 1)$, *then it has the defining relations*

$$G = \{a, b, c, d; \; a^m = b^p = c^q = d^q = e, \; ab = ba^r, \; ac = ca, \; ad = da, \; bc = c^{\omega} b, \; bd = d^{\omega'} b, \; cd = dc\} \tag{13}$$

where $\qquad \omega, \omega' \not\equiv 1 \pmod q$ *and*

$$r^p \equiv 1 \pmod m, \quad \omega^p \equiv 1 = \omega'^p \pmod q. \tag{14}$$

Conversely, if r, s, ω *and* ω' *satisfy* (14), *then the group* G *generated by* a, b, c *and* d *with the defining relations* (13) *is of the desired type.*

Proof. Assume the existence of a group G of the type $P^*(1, 1)$. Then, for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_1^* described in Theorem 1*. Thus we have

$$\{a, b, c; \; a^m = b^p = c^q = e, \; ab = ba^r, \; ac = ca^s, \; bc = c^{\omega} b\}$$

with $\quad r^p \equiv 1 \equiv s^{f(\omega)} \pmod m, \quad \omega^p \equiv 1 \pmod q, \quad f(\omega) = \begin{cases} q & \text{if} \quad \omega = 1 \\ 1 & \text{if} \quad \omega \neq 1 \end{cases}$

$$\{a, b, d; \; a^m = b^p = d^q = e, \; ab = ba^r, \; ad = da^t, \; bd = d^{\omega'} b\}$$

with $\quad r^p \equiv 1 \equiv t^{f(\omega')} \pmod m, \quad \omega'^p \equiv 1 \pmod q, \quad f(\omega') = \begin{cases} q & \text{if} \quad \omega' = 1 \\ 1 & \text{if} \quad \omega' \neq 1 \end{cases}$

Moreover, by Cor. 3*, the subgroup $\{b, c, d\}$, being non-Abelian, has the defining relations

$$\{b, c, d;\ b^p = c^q = d^q = e,\ bc = c^{\omega} b,\ bd = d^{\omega'} b,\ cd = dc\}$$

with

$$\omega, \omega' \not\equiv 1 \pmod q \quad \text{and}$$

$$\omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

Now, since $\omega, \omega' \not\equiv 1 \pmod q$, then by the definition of f, we have $f(\omega)=1, f(\omega')=1$ and consequently $s \equiv 1 \equiv t \pmod m$. This shows that conditions (13) and (14) are necessary.

For the converse, we use again the system K of formal quadruples $[x, y, z, w]$ with the multiplication formulae

$$[x, y, z, w]\,[x', y', z', w'] = [x'', y'', z'', w'']$$

where

$$x'' \equiv r^{y'} x + x' \pmod m, \quad y'' \equiv y + y' \pmod p,$$

$$z'' \equiv z + \omega^y z',\ w'' \equiv w + \omega'^y w' \pmod q,$$

and the proof follows exactly the same procedure used before and may be omitted.

Theorem 12. *If there is a group G of the type $P^*(2, 2)$, then it has the defining relations*

$$(15)\quad G = \{a, b, c, d;\ a^m = b^p = c^q = d^q = e,\ ab = ba^r,\ ac = c^{\mu} a,\ ad = d^{\nu} a,$$
$$bc = c^{\omega} b,\ bd = d^{\omega'} b,\ cd = dc\}$$

where $\quad \mu, \nu \not\equiv 1 \pmod q$ *and* $\omega, \omega' \not\equiv 1 \pmod q$ *and*

$$(16)\quad r^p \equiv 1 \pmod m, \quad \omega^p \equiv 1 \equiv \omega'^p \pmod q, \quad k' | [m, r-1], k^* | [m, r-1].$$

Conversely, if $\mu, \nu, \omega, \omega' \not\equiv 1 \pmod q$ and if $r, \omega, \omega', k', k^*$ satisfy (16), *then the group G generated by a, b, c, d with the defining relations* (15) *is of the desired type.*

Proof. Assume the existence of a group G of the type $P^*(2, 2)$. Then, for such a group, the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are both of the same type M_2^* described in Theorem 1*. Thus we have

$$\{a, b, c;\ a^m = b^p = c^q = e,\ ab = ba^r,\ ac = c^{\mu} a,\ bc = c^{\omega} b\}, \mu \not\equiv 1 \pmod q,$$

with $\quad r^p \equiv 1 \pmod m, \quad \omega^p \equiv 1 \pmod q, \quad k' | [m, r-1],$

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^{\nu} a,\ bd = d^{\omega'} b\}, \nu \not\equiv 1 \pmod q$$

with $\quad r^p \equiv 1 \pmod m, \quad \omega'^p \equiv 1 \pmod q, k^* | [m, r-1].$

Also, the subgroup $\{b, c, d\}$ is non-Abelian and by Cor. 3*, we have

$$\{b, c, d;\ b^p = c^q = d^q = e,\ bc = c^{\omega} b,\ bd = d^{\omega'} b,\ cd = dc\}, \omega, \omega' \not\equiv 1 \pmod q$$

with $\quad \omega^p \equiv 1 \equiv \omega'^p \pmod q.$

Thus we have shown that (15) and (16) are necessary.

For the converse, we use again the system K of formal quadruples $[x, y, z, w]$ with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where
$$x'' \equiv r^{y'}x + x' \pmod{m}, \quad y'' = y + y' \pmod{p},$$
$$z'' \equiv z + \mu^x \omega^y z', \; w'' \equiv w + \mu^x \omega'^y w' \pmod{q}.$$

It is easily shown, that under this multiplication, the system K is a group of order pq^2m which is isomorphic to the group of the required type.

Theorem 13. *If there is a group G of the type $P^*(1, 2)$, then it has defining relations*

$$(17) \quad G = \{a, b, c, d;\; a^m = b^p = c^q = d^q = e,\; ab = ba^r,\; ac = ca,\; ad = d^v a,$$
$$bc = c^\omega b,\; bd = d^{\omega'} b,\; cd = dc\},$$

where
$$v, \omega, \omega' \not\equiv 1 \pmod{q} \quad \textit{and}$$

$$(18) \qquad r^p \equiv 1 \pmod{m}, \quad \omega^p \equiv 1 \equiv \omega'^p \pmod{q}, \quad k^* | [m, r-1].$$

Conversely, if $v, \omega, \omega' \not\equiv 1 \pmod{q}$ and if r, ω, ω' and k^* (the order of v mod q) satisfy (18), *then the group G generated by a, b, c, d with the defining relations* (17) *is of the required type.*

PROOF. Assume the existence of a group G of the type $P^*(1, 2)$. Then, for such a group, the subgroups $\{a, b, c\}$ and $\{a, b, d\}$ are respectively of the types M_1^* and M_2^* described in Theorem 1*. Thus we have

$$\{a, b, c;\; a^m = b^p = c^q = e,\; ab = ba^r,\; ac = ca^s, bc = c^\omega b\}$$

with
$$r^p \equiv 1 \equiv s^{f(\omega)} \pmod{m}, \quad \omega^p = 1 \pmod{q}, \quad f(\omega) = \begin{cases} q & \text{if } \omega = 1 \\ 1 & \text{if } \omega \neq 1 \end{cases}$$

$$\{a, b, d;\; a^m = b^p = d^q = e, ab = ba^r, ad = d^v a, bd = d^{\omega'} b\}$$

with
$$r^p \equiv 1 \pmod{m}, \quad \omega'^p \equiv 1 \pmod{q}, \quad k^* | [m, r-1].$$

Also for this type the subgroup $\{b, c, d\}$ is of the non-Abelian type described in Cor. 3* namely

$$\{b, c, d;\; b^p = c^q = d^q = e,\; bc = c^\omega b,\; bd = d^{\omega'} b,\; cd = dc\}$$

with
$$\omega, \omega' \not\equiv 1 \pmod{q}, \quad \omega^p \equiv 1 \equiv \omega'^p \pmod{q}.$$

Now, since $\omega \not\equiv 1 \pmod{q}$, then by the definition of f, we have $f(\omega) = 1$ and consequently $s \equiv 1 \pmod{m}$. Thus we have shown that (17) and (18) are necessary.

For the converse, we use the system K of formal quadruples $[x, y, z, w]$ with the multiplication formulae

$$[x, y, z, w][x', y', z', w'] = [x'', y'', z'', w'']$$

where
$$x'' \equiv r^{y'}x + x', \quad \pmod{m}, \quad y'' \equiv y + y' \pmod{p},$$
$$z'' \equiv z + \omega^y z', \; w'' \equiv w + v^x \omega'^y w' \pmod{q}.$$

As before, it is easily shown that under this multiplication, the system K is a group of order pq^2m which is isomorphic to the group G of the required type.

Conclusion. Finite groups exist with four generators three of which having orders p, q, q where p and q are distinct odd primes such that $p<q$. If p does not divide $q-1$, there exist six types of these groups which are described in Theorems 2—7. But if p divides $q-1$, then there exist nine types of such groups and are described in Theorems 8, 11, 12, 13.

References

[1] K. R. YACOUB, On classifictton of finite groups with four generators three of which having prime orders p, p, q $(p<q)$*I, Publ. Math. (Debrecen)* **33** (1986), 29—42.

[2] K. R. YACOUB, On finite groups with three independent generators two of which being of distinct odd primes, *Publ. Math. (Debrecen)* **13** (1966), 9—16.

MATHS. DEPT. FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
ABBASSIA, CAIRO-EGYPT.

(Received June 1, 1984)