we get finally from (8.1), noting also (7.2),

$$|e^{\frac{1}{4}(\varrho_1^2+2\xi\varrho_1)}|^{r_1} Z(r_1) > T^{\frac{1}{2}-\frac{7}{4}\sqrt{\eta}}.$$

Setting

$$\nu_1 = r_0+r_1, \qquad x_1 = e^{(r_0\xi_0+r_1\xi)/2}, \tag{8.2}$$

we deduce thus from (6.8)

$$\sum_p \varepsilon_k(p, l_2, l_1)\log p\cdot e^{-\frac{1}{\nu_1}\left(\log\frac{p}{x_1}\right)^2} > T^{\frac{1}{2}-2\sqrt{\eta}},$$

i.e. the first statement of Theorem 1. The second statement follows mutatis mutandis.

9. To complete the proof, it remains to show (1.7) and (1.8). By (8.2), (2.1), (2.3), (4.1), (4.4), (4.5)

$$x_1 \leqslant c_3 k^{5/2} e^{\eta^{-11/5}} T$$

and

$$x_1 \geqslant T^{1-\sqrt{\eta}},$$

so that (1.7) follows in view of (1.5) and (1.6). As to (1.8), (8.2), (4.4), (4.5) yield

$$\nu_1 \leqslant 1+2\eta\log T+\eta^{-6/5}$$

and

$$\nu_1 \geqslant 2\eta\log T,$$

which give the result.

References

[1] S. Knapowski and P. Turán, *Comparative prime-number theory III*, Acta Math. Hung. 13 (1962), pp. 343-364.

[2] — — *Further developments in the comparative prime-number theory II*, Acta Arith. 10 (1964), pp. 293-313.

[3] — — *Further developments in the comparative prime-number theory III*, Acta Arith. 11 (1965), pp. 115-127.

[4] — — *Further developments in the comparative prime-number theory IV*, Acta Arith. 11 (1965), pp. 147-161.

[5] C. L. Siegel, *On the zeros of the Dirichlet L-functions*, Annals of Math. (1945), pp. 405-422.

[6] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Akad. Kiadó, Budapest, 1953. A completely rewritten English edition is under preparation, and will appear in the Interscience Tracts series.

Reçu par la Rédaction le 28. 1. 1966

ACTA ARITHMETICA
XII (1966)

A refinement of a theorem of Schur on primes in arithmetic progressions II

by

J. Wójcik (Warszawa)

I. Schur [6] gave purely algebraic proofs of the existence of infinitely many primes in the following special arithmetic progressions:

$$2^\nu z+2^{\nu-1}\pm 1 \quad \text{where} \quad \nu\geqslant 1,$$

$$8nz+2n+1, \quad 8nz+4n+1, \quad 8nz+6n+1,$$

where n is an odd square-free integer >0 and

$$p^\nu nz+l_\nu,$$

where

$$l_\nu \equiv \begin{cases} 1 \bmod n, \\ -1 \bmod p^\nu \end{cases}$$

and p is an odd prime.

In the last case Schur assumed the existence of an integer c such that $\left(\frac{F_n(c)}{p}\right) = -1$, where F_n is the nth cyclotomic polynomial.

A. S. Bang [1] gave proofs similar to those of Schur for the existence of infinitely many primes in the following progressions:

$$4p^n z+2p^n+1, \qquad p\equiv 3 \bmod 4,$$

$$6p^{2n+1}z+2p^{2n+1}+1, \qquad p\equiv 2 \bmod 3,$$

$$6p^{2n}z+4p^{2n}+1, \qquad p\equiv 2 \bmod 3.$$

The main aim of the present paper is to prove on the same way a theorem which comprises all the above results as special cases and covers several new cases, e.g. the progressions:

$$48x+7, \quad 48x+25, \quad 48x+31, \quad 105x+64, \quad 105x+71, \quad 105x+76\ (^1).$$

(1) The last three progressions correspond to the case $p_\nu nz+l_\nu$ considered by Schur. However, it is impossible to find here an integer c satisfying $\left(\frac{F_n(c)}{p}\right) = -1$.

THEOREM 1. *Let $l^2 \equiv 1 \bmod m$, $m = p^\nu n$, where p is a prime, $\nu > 0$, $p \nmid n$, $l \equiv 1$ or $p \bmod n$. Then the arithmetical progression $mz+l$ $(z = 0, 1, \ldots)$ contains infinitely many primes.*

On putting $\nu = 0$, $l \equiv p \bmod n$ in the above statement one obtains the theorem of my previous paper [7]. The notation and results of that paper are used in the sequel. In particular Q is the rational field, ζ_r a primitive rth root of unity and

$$h_m(x) = \begin{cases} x + x^l & \text{if } \quad 2l \not\equiv m+2 \bmod 2m, \\ x^2 & \text{if } \quad 2l \equiv m+2 \bmod 2m. \end{cases}$$

We put $P_r = Q(\zeta_r)$, $K = Q(h_m(\zeta_m))$, $K_1 = Q(h_{p^\nu}(\zeta_{p^\nu}))$, $K_2 = Q(h_n(\zeta_n))$. As was shown in [7] (p. 434) K is the maximal subfield of P_m invariant with respect to the substitution $\zeta_m \to \zeta_m^l$.

For any given algebraic number field L, we denote by $|L|$ its degree ($|\ |$ denotes also the order of a group). If $L_1 \subset L_2$ $[L_2 : L_1]$ is the degree of L_2 over L_1 and N_{L_2/L_1} the norm from L_2 to L_1.

It is well known that for any integer $a \in P_m$, $(a, m) = 1$ implies $N_{P_m/Q}(a) \equiv 1 \bmod m$.

It follows that for any integer $a \in P_m$ such that $|Q(a)| = \frac{1}{2}\varphi(m)$, $(a, m) = 1$, we have

$$N_{Q(a)/Q}(a)^2 \equiv 1 \bmod m.$$

The behaviour of $N_{Q(a)/Q}(a) \bmod m$ is described by the following theorem which constitutes the main tool in proving Theorem 1 but seems also of independent interest.

THEOREM 2. *Let $m > 2$, $l^2 \equiv 1 \bmod m$. For the existence of an integer $a \in P_m$ satisfying*

$$(1) \qquad |Q(a)| = \tfrac{1}{2}\varphi(m), \qquad N_{Q(a)/Q}(a) \equiv l \bmod m$$

it is necessary and sufficient that m should have at most one prime factor p such that $l \not\equiv 1 \bmod p^\nu$, where $p^\nu \| m$. If this condition is satisfied, all the integers $a \in P_m$ satisfying (1) belong to K.

LEMMA 1. *If an integer $a \in P_m$ satisfies (1) then $a \in K$.*

Proof. By the first of the conditions (1), $Q(a)$ must be the maximal subfield of P_m invariant with respect to a substitution $\zeta_m \to \zeta_m^\lambda$, where $\lambda^2 \equiv 1 \bmod m$, $\lambda \not\equiv 1 \bmod m$. By the second condition of (1) $(a, m) = 1$. Let $\mathfrak{q}$ be any prime ideal factor of a in $Q(a)$; and let $N_{Q(a)/Q}\mathfrak{q} = q^f$ where q is a prime. Consider the authomorphism σ of P_m such that $\zeta_m^{(\sigma)} = \zeta_m^{q^f}$.

For any $\beta \in Q(a)$ we have

$$\beta = R(\zeta_m),$$

where R is a polynomial with rational integral coefficients, thus

$$\beta^{(\sigma)} = R(\zeta_m^{q^f}) \equiv R(\zeta_m)^{q^f} = \beta^{q^f} \bmod q.$$

By Fermat's theorem for the field $Q(a)$

$$\beta^{q^f} \equiv \beta \bmod \mathfrak{q},$$

thus

$$\beta^{(\sigma)} \equiv \beta \bmod \mathfrak{q}.$$

Since this holds for all $\beta \in Q(a)$, σ restricted to $Q(a)$ belongs to the inertia group of $\mathfrak{q}$. However, the latter is trivial because $(\mathfrak{q}, m) = 1$ and $\mathfrak{q}$ does not divide the discriminant of $Q(a)$. Thus $Q(a)$ is invariant with respect to σ and by the choice of λ, $q^f \equiv 1$ or $\lambda \bmod m$. By the multiplicative property of the norm, it follows that for $\mathfrak{a} = (a)$ we have

$$N_{Q(a)/Q}\mathfrak{a} \equiv 1 \quad \text{or} \quad \lambda \bmod m.$$

If $\lambda \equiv -1 \bmod m$, we get $N_{Q(a)/Q}a = \pm N_{Q(a)/Q}\mathfrak{a} \equiv \pm 1 \bmod m$ thus

$$(*) \qquad N_{Q(a)/Q}a \equiv 1 \quad \text{or} \quad \lambda \bmod m.$$

If $\lambda \not\equiv -1 \bmod m$, the field $Q(a)$ is not real, hence $N_{Q(a)/Q}a = N_{Q(a)/Q}\mathfrak{a}$. Thus (*) holds also in this case.

It follows from (1) and (*) that

$$l \equiv 1 \quad \text{or} \quad \lambda \bmod m.$$

If $l \equiv 1 \bmod m$, $K = P_m$ thus $a \in K$.
If $l \not\equiv 1 \bmod m$, $l \equiv \lambda \bmod m$ and

$$Q(a) = Q(h_m(\zeta_m)) = K.$$

LEMMA 2. *If $l^2 \equiv 1 \bmod m$, $l \not\equiv 1 \bmod p^\nu$ we have*

$$(2) \qquad K_1K_2 \subset K, \qquad K_1 \cap K_2 = Q$$

and

$$(3) \qquad [K : K_1K_2] = \begin{cases} 1 & \text{if} \quad l \equiv 1 \bmod n, \\ 2 & \text{if} \quad l \not\equiv 1 \bmod n. \end{cases}$$

Moreover, apart from the case $p = 2$, $l \not\equiv 1 \bmod n$, p has in K the factorization

$$(p) = \mathfrak{p}_1^e\mathfrak{p}_2^e \ldots \mathfrak{p}_g^e,$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$ are distinct prime ideals,

$$e = \begin{cases} |K_1| & \text{if} \quad l \equiv 1 \bmod n, \\ 2|K_1| & \text{if} \quad l \not\equiv 1 \bmod n \end{cases}$$

and $(\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_g)^{e/|K_1|}$ is a prime ideal of first degree in K_1.

Proof. As we have already mentioned, K is the maximal subfield of P_m invariant with respect to the substitution $\zeta_m \to \zeta_m^l$. Since applying this substitution we get

$$(4)\quad \begin{aligned} \zeta_{p^\nu} &= \zeta_m^n \to \zeta_m^{nl} = \zeta_{p^\nu}^l, \\ \zeta_n &= \zeta_m^{p^\nu} \to \zeta_m^{p^\nu l} = \zeta_n^l, \end{aligned}$$

whence $K_1 \to K_1$ and $K_2 \to K_2$, it follows that $K_1 \subset K$ and $K_2 \subset K$. Thus we obtain the first part of (2). On the other hand,

$$K_1 \subset P_{p^\nu}, \quad K_2 \subset P_n,$$

thus the discriminants of K_1 and K_2 are relatively prime. Hence

$$K_1 \cap K_2 = Q \quad \text{and} \quad |K_1K_2| = |K_1||K_2|.$$

Since $|K| = \frac{1}{2}\varphi(m)$, $|K_1| = \frac{1}{2}\varphi(p^\nu)$ and

$$|K_2| = \begin{cases} \varphi(n) & \text{if } l \equiv 1 \bmod n, \\ \frac{1}{2}\varphi(n) & \text{if } l \not\equiv 1 \bmod n, \end{cases}$$

we obtain (3). For further use we notice that if $l \not\equiv 1 \bmod n$ then

$$(5)\quad K = K_1K_2(\sqrt{\delta^2}), \quad \delta^2 \in K_1K_2,$$

where

$$(6)\quad \delta = (\zeta_{p^\nu} - \zeta_{p^\nu}^l)(\zeta_n - \zeta_n^l).$$

Indeed, by (4) δ is invariant with respect to the substitution $\zeta_m \to \zeta_m^l$, thus $\delta \in K$. On the other hand, δ is not invariant with respect to the substitution $\zeta_{p^\nu} \to \zeta_{p^\nu}$, $\zeta_n \to \zeta_n^l$ which leaves invariant K_1K_2, thus $\delta \notin K_1K_2$. Finally the last substitution and the substitution $\zeta_{p^\nu} \to \zeta_{p^\nu}^l$, $\zeta_n \to \zeta_n$ leave invariant δ^2, thus $\delta^2 \in K_1K_2$.

In order to determine the factorization of p in K put

$$\pi_k = (1-\zeta_{p^\nu}^k)(1-\zeta_{p^\nu}^{kl}).$$

Since π_k is invariant with respect to the substitution $\zeta_{p^\nu} \to \zeta_{p^\nu}^l$ we have $\pi_k \in K_1$ for all k. For $k \not\equiv 0 \bmod p$, the quotients

$$\frac{\pi_k}{\pi_1} = \frac{1-\zeta_{p^\nu}^k}{1-\zeta_{p^\nu}} \cdot \frac{1-\zeta_{p^\nu}^{kl}}{1-\zeta_{p^\nu}^l} \quad \text{and} \quad \frac{\pi_1}{\pi_k} = \frac{1-\zeta_{p^\nu}^{kk'}}{1-\zeta_{p^\nu}^k} \cdot \frac{1-\zeta_{p^\nu}^{kk'l}}{1-\zeta_{p^\nu}^{kl}}$$

where $kk' \equiv 1 \bmod p^\nu$ are algebraic integers, thus they are algebraic units. Substituting $x = 1$ in the identity

$$x^{p^{\nu-1}(p-1)} + x^{p^{\nu-1}(p-2)} + \ldots + 1 = \prod_{(k,p^\nu)=1} (x - \zeta_{p^\nu}^k)$$

we get

$$p = \prod_{(k,p^\nu)=1} (1-\zeta_{p^\nu}^k) = \prod{}' \pi_k,$$

where the product $\prod'$ is taken over such reduced residue classes $k \bmod p^\nu$ that the ratio of any two of them is not congruent to $l \bmod p^\nu$. The number of factors in Π' is clearly $\frac{1}{2}\varphi(p^\nu) = |K_1|$, thus

$$(7)\quad (p) = (\pi_1)^{|K_1|}$$

and the ideal (π_1) is prime of first degree in K_1.

On the other hand, since p does not divide the discriminant of K_2, p is in K_2 a product of distinct prime ideals, say

$$(8)\quad (p) = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_g.$$

Since the ideals $\mathfrak{q}_i$'s are coprime it follows from (7) and (8) that

$$(9)\quad \mathfrak{q}_i = \mathfrak{Q}_i^{|K_1|} \quad (i = 1, 2, \ldots, g),$$

$$(10)\quad (\pi_1) = \mathfrak{Q}_1\mathfrak{Q}_2 \ldots \mathfrak{Q}_g,$$

where $\mathfrak{Q}_i$'s are distinct ideals of K_1K_2. Moreover they are prime ideals of K_1K_2, since $\mathfrak{q}_i$ cannot have more than $|K_1|$ prime ideal factors in K_1K_2. If $l \equiv 1 \bmod n$, $K = K_1K_2$ by (3), and the lemma follows from (8), (9) and (10). It remains to consider the case $l \not\equiv 1 \bmod n$, $p > 2$. Then $l \not\equiv 1 \bmod p$ and the number

$$\frac{(\zeta_{p^\nu} - \zeta_{p^\nu}^l)^2}{\pi_1} = \zeta_{p^\nu}^2 \frac{1-\zeta_{p^\nu}^{l-1}}{1-\zeta_{p^\nu}} \cdot \frac{1-\zeta_{p^\nu}^{l-1}}{1-\zeta_{p^\nu}^l}$$

is an algebraic unit. Since $(\zeta_n - \zeta_n^l, p) = 1$, it follows from (6) and (10) that each $\mathfrak{Q}_i$ divides δ^2 in exactly first power. Thus by (5) and by a well known theorem ([5], p. 374-376)

$$(11)\quad \mathfrak{Q}_i = \mathfrak{P}_i^2 \quad (i = 1, 2, \ldots, g),$$

where $\mathfrak{P}_i$ is a prime ideal of K. The lemma follows now from (8), (9), (10) and (11).

LEMMA 3. *If $l^2 \equiv 1 \bmod p^\nu$ and $l \not\equiv 1 \bmod p^\nu$, then there exists an integer $\alpha \in K_1$ such that*

$$N_{K_1/Q}(\alpha) \equiv l \bmod p^\nu.$$

Proof. Suppose first that p^ν has a primitive root g. Since $p^\nu > 2$, $\varphi(p^\nu)$ is even and $g^{\varphi(p^\nu)/2} \equiv -1 \bmod p^\nu$. Since $\varphi(p^\nu)/2 = |K_1|$, we obtain the assertion of the lemma taking $\alpha = g$.

Suppose now that p^ν has no primitive root. Then $p = 2$, $\nu \geqslant 3$ and $l \equiv 2^{\nu-1} \pm 1 \bmod 2^\nu$ or $l \equiv -1 \bmod 2^\nu$.

If $l \equiv 2^{\nu-1}+1 \bmod 2^\nu$, we have $K_1 \supset Q(i)$, thus

$$N_{K_1/Q}(1+2i) = 5^{2^{\nu-3}} \equiv l \bmod 2^\nu.$$

If $l \equiv 2^{\nu-1}-1 \bmod 2^\nu$, $h_{2^\nu}(\zeta_{2^\nu})$ is a zero of the following polynomial generating K_1

$$(12)\quad f_\nu(x) = \prod_{\substack{|j|<2^{\nu-2}\\ j \text{ odd}}} \left(x-(\zeta_{2^\nu}^j-\zeta_{2^\nu}^{-j})\right) = i^{2^{\nu-2}} \prod_{\substack{0<k<2^{\nu-1}\\ k \text{ odd}}} \left(-ix-(\zeta_{2^\nu}^k+\zeta_{2^\nu}^{-k})\right)$$

$$= i^{2^{\nu-2}} \prod_{\substack{0<k<2^{\nu-1}\\ k \text{ odd}}} \left(-ix-2\cos\frac{\pi k}{2^{\nu-1}}\right) = i^{2^{\nu-2}} 2T_{2^{\nu-2}}\left(\frac{-ix}{2}\right),$$

where $T_r(x) = \cos(r \arccos x)$ and $k = 2^{\nu-2}-j$. We show that $f_\nu(1) \equiv 2^{\nu-1}-1 \bmod 2^\nu$. For $\nu = 3$ we have $f_3(x) = x^2+2$ and $f_3(1) = 3$. Assume that $\nu \geqslant 4$ and

$$(13)\quad f_{\nu-1}(1) \equiv 2^{\nu-2}-1 \bmod 2^{\nu-1}.$$

Since $T_{2r}(x) = 2T_r(x)^2-1$ we get from (12)

$$f_\nu(x) = f_{\nu-1}^2(x)-2.$$

Hence by (13) $f_\nu(1) \equiv 2^{\nu-1}-1 \bmod 2^\nu$ and the last congruence follows by induction for all $\nu \geqslant 3$. Taking $\alpha = 1-(\zeta_{2^\nu}-\zeta_{2^\nu}^{-1})$ we get the assertion of the lemma, since $N_{K_1/Q}(\alpha) = f_\nu(1)$.

If $l \equiv -1 \bmod 2^\nu$, $h_{2^\nu}(\zeta_{2^\nu})$ is a zero of the following polynomial generating K_1

$$f_\nu(x) = \prod_{\substack{0<k<2^{\nu-1}\\ k \text{ odd}}} \left(x-(\zeta_{2^\nu}^k+\zeta_{2^\nu}^{-k})\right) = \prod_{\substack{0<k<2^{\nu-1}\\ k \text{ odd}}} \left(x-2\cos\frac{\pi k}{2^{\nu-1}}\right) = 2T_{2^{\nu-2}}\left(\frac{x}{2}\right).$$

We have $f_\nu(1) = 2T_{2^{\nu-2}}(\frac{1}{2}) = 2\cos(2^{\nu-2}\arccos\frac{1}{2}) = 2\cos\frac{2}{3}\pi = -1$. Taking $\alpha = 1-(\zeta_{2^\nu}+\zeta_{2^\nu}^{-1})$ we get $N_{K_1/Q}(\alpha) = f_\nu(1) = -1$ and the proof of the lemma is complete.

Proof of Theorem 2. The last statement of the theorem follows at once from Lemma 1. We prove that the condition given in the theorem is necessary and sufficient for the existence of α satisfying (1).

Necessity. Suppose that m has two prime factors p_1 and p_2 such that $p_1^{\nu_1} \| m$, $p_2^{\nu_2} \| m$, $l \not\equiv 1 \bmod p_1^{\nu_1}$, $l \not\equiv 1 \bmod p_2^{\nu_2}$.

Without loss of generality we may assume that $p_1 = p$ is odd and put

$$(14)\quad m = p^\nu n, \quad \text{where} \quad l \not\equiv 1 \bmod n.$$

Since $p > 2$, $l^2 \equiv 1 \bmod p^\nu$ and $l \not\equiv 1 \bmod p^\nu$, it follows that

$$(15)\quad l \not\equiv 1 \bmod p.$$

Suppose that an integer $\alpha \in P_m$ satisfies the conditions (1). By Lemma 1 $Q(\alpha) = K$.

Let $\mathfrak{p}_i$ be any prime ideal factor of p in K. By Lemma 2 $\mathfrak{p}_i$ is of relative degree one over K_1K_2 thus there exists an integer $\gamma_i \in K_1K_2$ such that

$$\alpha \equiv \gamma_i \bmod \mathfrak{p}_i \quad (i = 1, 2, \ldots, g).$$

By the Chinese remainder theorem there exists an integer $\gamma_0 \in K_1K_2$ such that

$$\gamma_0 \equiv \gamma_i \bmod \mathfrak{p}_i \quad (i = 1, 2, \ldots, g)$$

and we get

$$\alpha \equiv \gamma_0 \bmod \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_g.$$

Since by Lemma 2 $(\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_g)^2$ is a prime ideal of K_1, it follows that

$$N_{K/K_1}\alpha \equiv N_{K/K_1}\gamma_0 = (N_{K_1K_2/K_1}\gamma_0)^2 \bmod (\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_g)^2.$$

Since $(\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_g)^{2|K_1|} = (p)$, it follows further that

$$N_{K/Q}\alpha = N_{K_1/Q}(N_{K/K_1}\alpha) \equiv N_{K_1/Q}(N_{K_1K_2/K_1}\gamma_0)^2 \bmod p.$$

Since $\beta_0 = N_{K_1K_2/K_1}\gamma_0 \in K_1$, we have

$$\beta_0^2 = N_{P_{p^\nu}/K_1}(\beta_0)$$

and

$$N_{K/Q}\alpha \equiv N_{K_1/Q}\beta_0^2 = N_{P_{p^\nu}/Q}\beta_0 \equiv 1 \bmod p.$$

This contradicts (1) and (15), because $K = Q(\alpha)$.

Sufficiency. If $l \equiv 1 \bmod m$, it is enough to take $\alpha = 1+m(\zeta_m+\zeta_m^{-1})$. Therefore, we can assume

$$m = p^\nu n, \quad p \nmid n, \quad l \not\equiv 1 \bmod p^\nu, \quad l \equiv 1 \bmod n.$$

By Lemma 3 there exists an integer $\beta \in K_1$ such that

$$(16)\quad N_{K_1/Q}(\beta) \equiv l \bmod p^\nu.$$

Let $\mathfrak{p}$ be a prime ideal factor of p in K, K_3 the decomposition field of $\mathfrak{p}$ relative to K_1 and let

$$K_4 = K_2 \cap K_3.$$

Let $\mathscr{G}$ be the Galois group of K and let $\mathscr{G}_i$ be the maximal subgroup of $\mathscr{G}$ leaving invariant K_i $(i = 1, \ldots, 4)$. Since K is an Abelian field, K_3 is independent of the choice of $\mathfrak{p}$. Since by Lemma 2 $\mathfrak{p}$ is itself an ideal of K_3, the relative decomposition group $\mathscr{G}_3$ is cyclic of degree f, where $f = |K|/eg$.

Since $N_{K_3/Q}\mathfrak{p} = p$, we have $\mathcal{G}_3 = \{1, \sigma, \ldots, \sigma^{f-1}\}$, where

$$\omega^{\sigma} \equiv \omega^{p} \bmod \mathfrak{p}_j \tag{17}$$

for any integer $\omega \in K$ and any prime ideal factor $\mathfrak{p}_j$ of p in K.

It follows from Lemma 2 that

$$\mathcal{G}_1 \cap \mathcal{G}_2 = 1, \quad \mathcal{G}_1\mathcal{G}_2 = \mathcal{G}, \quad \mathcal{G}_3 \subset \mathcal{G}_1, \quad \mathcal{G}_2\mathcal{G}_3 = \mathcal{G}_4 \tag{18}$$

and

$$|K_4| = \frac{|\mathcal{G}|}{|\mathcal{G}_4|} = \frac{|\mathcal{G}_1|}{|\mathcal{G}_3|} = [K_3 : K_1] = g.$$

Let $\omega_1, \omega_2, \ldots, \omega_g$ be an integral basis of K_4 and let

$$\mathcal{G}_1 = \mathcal{G}_3\sigma_1 + \mathcal{G}_3\sigma_2 + \ldots + \mathcal{G}_3\sigma_g \tag{19}$$

be the decomposition of $\mathcal{G}_1$ into cosets with respect to $\mathcal{G}_3$.

Since K_4 is normal, $\omega_i^{(\sigma_j)} \in K_3$ $(1 \leqslant i, j \leqslant g)$ and the coefficients of the system of congruences

$$\begin{aligned} x_1\omega_1^{(\sigma_1)} + \ldots + x_g\omega_g^{(\sigma_1)} &\equiv \beta \bmod \mathfrak{p}, \\ x_1\omega_1^{(\sigma_2)} + \ldots + x_g\omega_g^{(\sigma_2)} &\equiv 1 \bmod \mathfrak{p}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1\omega_1^{(\sigma_g)} + \ldots + x_g\omega_g^{(\sigma_g)} &\equiv 1 \bmod \mathfrak{p} \end{aligned} \tag{20}$$

all belong to K_3. On the other hand, by (18) and (19)

$$\mathcal{G} = \mathcal{G}_4\sigma_1 + \mathcal{G}_4\sigma_2 + \ldots + \mathcal{G}_4\sigma_g,$$

thus

$$|\omega_i^{(\sigma_j)}|^2 = \operatorname{disc} K_4 | \operatorname{disc} K_2 | n^n; \qquad (|\omega_i^{(\sigma_j)}|, p) = 1$$

and the system (20) has a solution in integers $x_1, \ldots, x_g \in K_3$. By the choice of K_3 $\mathfrak{p}$ is of first degree in K_3, thus there exists also a solution $x_1^0, \ldots, x_g^0$ in rational integers.

Setting $\gamma = x_1^0\omega_1 + \ldots + x_g^0\omega_g$ we get

$$\beta \equiv \prod_{j=1}^{g} \gamma^{(\sigma_j)} = N_{K_3/K_1}\gamma \bmod \mathfrak{p},$$

hence also

$$\beta \equiv N_{K_3/K_1}\gamma \bmod \mathfrak{P}, \tag{21}$$

where $\mathfrak{P} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_g$ is the prime ideal in K_1.

By Fermat's theorem for the field K_3 we have

$$\gamma^{p-1} \equiv 1 \bmod \mathfrak{p}_j \quad (j = 1, 2, \ldots, g). \tag{22}$$

On the other hand, $N_{K/Q}\mathfrak{p}_j = p^f$, thus (22) can be written in the form

$$\gamma^{\frac{1}{k}(N_{K/Q}\mathfrak{p}_j - 1)} \equiv 1 \bmod \mathfrak{p}_j \quad \text{where} \quad k = \frac{p^f - 1}{p - 1} \ (j = 1, 2, \ldots, g).$$

By Euler's criterion it follows that γ is a kth power residue mod $\mathfrak{p}_j$, hence there exist integers $\delta_j \in K$ such that

$$\gamma \equiv \delta_j^k \bmod \mathfrak{p}_j \quad (j = 1, \ldots, g). \tag{23}$$

By the Chinese remainder theorem there exists an integer $\delta_0 \in K$ such that

$$\delta_0 \equiv \delta_j \bmod \mathfrak{p}_j \quad (j = 1, 2, \ldots, g). \tag{24}$$

It follows from (23), (24) and (17) that

$$\gamma \equiv \delta_0^k \equiv \delta_0^{1+p+\ldots+p^{f-1}} \equiv \prod_{\tau \in \mathcal{G}_3} \delta_0^{(\tau)} = N_{K/K_3}(\delta_0) \bmod \mathfrak{p}_j \quad (j = 1, \ldots, g),$$

thus

$$\gamma \equiv N_{K/K_3}(\delta_0) \bmod \mathfrak{P}.$$

Since $\mathfrak{P}^{(\sigma_j)} = \mathfrak{P}$ $(1 \leqslant j \leqslant g)$, it follows that

$$N_{K_3/K_1}\gamma \equiv N_{K/K_1}\delta_0 \bmod \mathfrak{P}. \tag{25}$$

Let us put for $x \in K_1$ and rational integer s

$$f_s(x) = N_{K/K_1}(\delta_0 + x\zeta_n^s) - \beta. \tag{26}$$

For every s, $f_s(x)$ is a polynomial in x over K_1 and we have

$$f_s'(0) = \sum_{\tau \in \mathcal{G}_1} (\zeta_n^{(\tau)})^s \frac{N_{K/K_1}(\delta_0)}{\sigma_0^{(\tau)}}.$$

On the other hand,

$$|(\zeta_n^{(\tau)})^s|^2_{\substack{0 \leqslant s < \varphi(n) \\ \tau \in \mathcal{G}_1}} = \prod_{\substack{(t't'', n) = 1 \\ t' \neq t''}} |(\zeta_n^{t'} - \zeta_n^{t''})| n^n,$$

thus $\big(|(\zeta_n^{(\tau)})^s|, \mathfrak{P}\big) = 1$. If we had

$$f_s'(0) \equiv 0 \pmod{\mathfrak{P}} \quad (0 \leqslant s < \varphi(n)),$$

it would follow

$$\frac{N_{K/K_1}\delta_0}{\delta_0^{(\tau)}} \equiv 0 \pmod{\mathfrak{P}} \quad \text{for all } \tau \in \mathcal{G}_1,$$

which is impossible by (25), (21) and (16). Therefore, there exists an integer s_0 such that

$$f_{s_0}'(0) \not\equiv 0 \pmod{\mathfrak{P}}.$$

Since by (21), (25) and (26)

$$f_{s_0}(0) \equiv 0 \ (\mathrm{mod}\ \mathfrak{P}),$$

it follows by Hensel's Lemma (cf. [4], pp. 155-156) that the congruence

$$f_{s_0}(x) \equiv 0 \ (\mathrm{mod}\ \mathfrak{P}^h)$$

is soluble in integers $x \in K_1$ for every h. In particular taking $h = \nu|K_1|$ we have for some $x_0 \in K_1$

$$f_{s_0}(x_0) = N_{K/K_1}(\delta_0 + \zeta_n^{s_0}x_0) - \beta \equiv 0 \ (\mathrm{mod}\ p^\nu),$$

thus by (16)

(27) $$N_{K/Q}(\delta_0 + \zeta_n^{s_0}x_0) \equiv l \ (\mathrm{mod}\ p^\nu).$$

Let $\omega_1, \omega_2, \ldots, \omega_r$, where $r = |K| = \frac{1}{2}\varphi(m)$, be an integral basis of K and let $\mathfrak{q}$ be any prime ideal of degree one in K not dividing m and such that $N_{K/Q}\mathfrak{q} = q > r$. Finally let $\varrho(\tau)$ be a function defined on the group $\mathscr{G}$, with rational integral values incongruent mod q for distinct τ's.

Since

$$|\omega_i^{(\tau)}|^2_{\substack{1 \leq i \leq r \\ \tau \in \mathscr{G}}} = \mathrm{disc}\, K \,|\mathrm{disc}\, P_m|\, m^m; \qquad (|\omega_i^{(\tau)}|, q) = 1,$$

the system of congruences

$$a_1\omega_1^{(\tau)} + \ldots + a_r\omega_r^{(\tau)} \equiv \varrho(\tau) \ \mathrm{mod}\ \mathfrak{q} \qquad (\tau \in \mathscr{G})$$

has a solution in integers of K and since $\mathfrak{q}$ is of degree one, also a solution $a_1^0, \ldots, a_r^0$ in rational integers. Now, by the Chinese remainder theorem there exists an integer $a \in K$ satisfying the congruences

(28) $$a \equiv \delta_0 + \zeta_n^{s_0}x_0 \ \mathrm{mod}\ p^\nu,$$

(29) $$a \equiv 1 \ \mathrm{mod}\ n,$$

(30) $$a \equiv a_1^0\omega_1 + \ldots + a_r^0\omega_r \ \mathrm{mod}\ q.$$

If follows from (27), (28) and (29) that

$$N_{K/Q}(a) \equiv l \ \mathrm{mod}\ m.$$

On the other hand, by (30), $a^{(\tau)} \equiv \varrho(\tau) \ \mathrm{mod}\ \mathfrak{q} (\tau \in \mathscr{G})$, thus $a^{(\tau)}$ are distinct for distinct τ's and $|Q(a)| = |K| = \frac{1}{2}\varphi(m)$. This completes the proof.

LEMMA 4. *Let $l^2 \equiv 1 \ \mathrm{mod}\ m$, $m = p^\nu n$, $\nu > 0$, $p \nmid n$, $p \equiv l \ \mathrm{mod}\ n$. Then there exists an integer $a \in K$ generating K and such that $p \| N_{K/Q}a$.*

Proof. Let $\mathfrak{p}$ be a prime ideal factor of p in K and $\mathfrak{q}$ a prime ideal factor of $\mathfrak{p}$ in P_m. We have

$$(p) = (1 - \zeta_{p^\nu})^{\varphi(p^\nu)},$$

thus

$$\mathfrak{q} \,|\, 1 - \zeta_{p^\nu}$$

and since for all r and s

$$\zeta_{p^\nu}^r \equiv \zeta_{p^\nu}^s \ \mathrm{mod}\ (1 - \zeta_{p^\nu}),$$

we get

(31) $$\zeta_{p^\nu}^r \equiv \zeta_{p^\nu}^s \ \mathrm{mod}\ \mathfrak{q}.$$

Let x satisfy the congruence $(p^\nu + n)x \equiv 1 \ \mathrm{mod}\ m$. Since $1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ is an integral basis of P_m, we have for $\vartheta \in K$

$$\vartheta = R\big(h_m(\zeta_m)\big) = S(\zeta_m),$$

where R is a polynomial with rational coefficients, S a polynomial with rational integral coefficients.

By (31) and the choice of x we have

$$\zeta_m^p = \zeta_{p^\nu}^{px}\zeta_n^{px} \equiv \zeta_{p^\nu}^{lx}\zeta_n^{lx} \equiv \zeta_m^l \ \mathrm{mod}\ \mathfrak{q},$$

hence

$$\vartheta^p \equiv S(\zeta_m^p) \equiv S(\zeta_m^l) = R\big(h_m(\zeta_m^l)\big) = R\big(h_m(\zeta_m)\big) = \vartheta \ \mathrm{mod}\ \mathfrak{q},$$

because $h_m(\zeta_m^l) = h_m(\zeta_m)$. Since $\vartheta \in K$, it follows also that

$$\vartheta^p \equiv \vartheta \ \mathrm{mod}\ \mathfrak{p},$$

thus $\mathfrak{p}$ is of prime degree in K. Let $\mathfrak{p} = (p^2, a)$ for some integer $a \in K$. We have

$$p = (p^2, a_1)(p^2, a_2)\ldots(p^2, a_r)$$

thus

$$p = (p^2, Na), \qquad p \| Na.$$

The numbers a are distinct since in the opposite case we had $N_{K/Q}a = a^k$, a rational integer, $k > 1$ and $p^2 | Na$, which is impossible. This completes the proof.

Proof of Theorem 1. By the result of [7] it is sufficient to show the existence of at least one prime $\equiv l \ \mathrm{mod}\ m$. This we do separately for the case $l \equiv 1 \ \mathrm{mod}\ n$ and $l \equiv p \ \mathrm{mod}\ n$.

1. $l \equiv 1 \ \mathrm{mod}\ n$. If $l \not\equiv 1 \ \mathrm{mod}\ p^\nu$, there exists by Theorem 2 an integer $a \in Q\big(h_m(\zeta_m)\big) = K$ such that

(32) $$Q(a) = K \quad \text{and} \quad N_{K/Q}a \equiv l \ \mathrm{mod}\ m.$$

If $l \equiv 1 \ \mathrm{mod}\ p^\nu$, the above conditions are satisfied by $a = \zeta_m$. Let $a_1, a_2, \ldots, a_r$ be all the conjugates of a,

$$f(x, y) = \prod_{i=1}^{r}(x - a_i y)$$

and d be the discriminant of f. We put

$$d = d_1 d_2$$

where $(d_1, m) = 1$ and d_2 has only prime factors dividing m. By the Chinese remainder theorem there exist integers y_0 and x_0 such that

$$y_0 \equiv \begin{cases} 0 \bmod d_1, \\ -1 \bmod m, \end{cases} \qquad x_0 \equiv \begin{cases} 0 \bmod m, \\ 1 \bmod y_0, \end{cases}$$

and $f(x_0, y_0) > 1$.

We have

$$f(x_0, y_0) \equiv \begin{cases} N_{K/Q}\,\alpha \bmod m, \\ 1 \bmod y_0, \end{cases} \tag{33}$$

thus $\big(f(x_0, y_0), my_0 d\big) = 1$. By Lemma 1 of [7] all prime factors of $f(x_0, y_0)$ are congruent to 1 or $l \bmod m$. At least one of them must be congruent to $l \bmod m$, since otherwise we would have $l \not\equiv 1 \bmod m$ and $f(x_0, y_0) \equiv 1 \bmod m$ contrary to (32) and (33).

2. $l \equiv p \bmod n$. Since the case $l \equiv 1 \bmod n$ is already settled we may assume that $l \not\equiv 1 \bmod n$. Let α be an integer, whose existence is asserted in Lemma 4 and $\alpha_1, \ldots, \alpha_r$ be all its conjugates.

Put

$$G(x, y) = \prod_{i=1}^{r} (x - \alpha_i y)$$

and denote by d the discriminant of G. Finally, let $p^{\mu_1} \| d$, $M = \dfrac{nd}{p^{\mu_1}}$. By the Chinese remainder theorem there exist integers x_0 and y_0 such that

$$y_0 \equiv \begin{cases} 0 \bmod M, \\ -1 \bmod p^2, \end{cases} \qquad x_0 \equiv \begin{cases} 1 \bmod y_0, \\ 0 \bmod p^2 \end{cases}$$

and $G(x_0, y_0) > p$.

We have

$$G(x_0, y_0) \equiv \begin{cases} 1 \bmod y_0, \\ N_{K/Q}\,\alpha \bmod p^2, \end{cases} \tag{34}$$

hence by the choice of α

$$p \,\|\, G(x_0, y_0). \tag{35}$$

Let $C = \dfrac{G(x_0, y_0)}{p} > 1$. If q is a prime and $q|C$ then by (34) and (35) $q \nmid py_0$. Since $M|y_0$, $q \nmid mdy_0$ and by Lemma 1 of [7], $q \equiv 1$ or $l \bmod m$. If no prime factor of C were congruent to $l \bmod m$ we would have $C \equiv 1 \bmod m$. On the other hand, since $n \mid y_0$ it follows from (34) that $C \equiv 1/l \equiv l \bmod n$. The contradiction obtained completes the proof.

Remark. Using the notation of a congruence mod ∞ (cf. [3], p. 35) one can state a part of Theorem 1 in the following equivalent form:

Let $n = n_1 \infty$, where n_1 is a positive integer, $l \equiv 1 \bmod n$, $l^2 \equiv 1 \bmod p^\nu$, $m = p^\nu n$, $p \nmid n$. Then there exists infinitely many primes q satisfying the congruence $q \equiv l \bmod m$.

If instead of taking $n = n_1 \infty$, one takes $n = n_1$, $p = \infty$, $\nu = 1$, $l = 1 - n$ one obtains the existence of infinitely many primes in the arithmetic progression $nz - 1$, which has also been proved by purely algebraic means (cf. [2], p. 178-183).

References

[1] A. S. Bang, *Elementare Beviser for specielle Tilfalde of Dirichlets setning om Differensekker*, Doctoral dissertation, Copenhagen 1937.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin, Göttingen, Heidelberg 1950.

[3] — *Zahlentheorie*, Berlin 1963.

[4] K. Hensel, *Theorie der algebraischen Zahlen*, I Band, Leipzig und Berlin 1908.

[5] D. Hilbert, *Gessamelte Abhandlungen*, I Band, Berlin 1932.

[6] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, S-B Berlin Math. Ges. 11(1912), appendix to Archiv der Math. und Phys. (3) 20 (1912-1913).

[7] J. Wójcik, *A refinement of a theorem of Schur on primes in arithmetic progressions*, Acta Arith. 11 (1966), pp. 433-436.

Reçu par le Rédaction le 16. 2. 1965