If the numbers ξ_3 and η_3 or ξ_5 and η_5 were equivalent then since $\xi_3 = 1+i$ and $\eta_5 = 1+\zeta_{10}$, η_3 or ξ_5 would be a sum of two roots of unity. However if $\vartheta \neq 0$ is such a sum and $\bar{\vartheta}$ is its complex conjugate, then $\vartheta/\bar{\vartheta}$ is a root of unity. Since neither of the numbers $\eta_3/\bar{\eta}_3$ and $\xi_5/\bar{\xi}_5$ is an algebraic integer, the proof is complete.

Added in proof. 1. H. B. Mann has proved in Mathematika 12 (1965), pp. 107-117, that under the assumptions of Corollary 3, N divides the product of all primes $\leqslant k+1$. This leads to a much better estimation of N than that stated in the corollary. Mann's method could also be used to solve both Robinsons's problems considered in this paper.

2. In connection with Lemma 1 the question arises how much inequality (1) can be improved. Y. Wang has proved by Brun's method in a manuscript kindly placed at my disposal that for $N > N_0(h)$ one can replace $(\log N)^{20h}$ by $c(h)\times\times(\log N)^{4h+3}$. According to H. Halberstam (written communication), there is a possibility of reducing the exponent $4h+3$ to $2h+1$ by Selberg's method.

References

[1] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Norsk Videnskaps Selskabs Skrifter, Kristiania 1920.

[2] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, New York 1937.

[3] W. Hodge and D. Pedoe, *Methods of Algebraic Geometry II*, Cambridge 1952.

[4] R. M. Robinson, *Some conjectures about cyclotomic integers*, Math. Comp. 19 (1965), pp. 210-217.

[5] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64-89.

[6] A. Schinzel and Y. Wang, *A note on some properties of the functions* $\varphi(n)$, $\sigma(n)$ and $\theta(n)$, Ann. Polon. Math. 4 (1958), pp. 201-213.

Reçu par la Rédaction le 9. 7. 1965

ACTA ARITHMETICA
XI (1966)

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

by

J. Wójcik (Warszawa)

I. Schur ([1]) has given a purely algebraic proof of the following special case of Dirichlet's theorem on arithmetic progression.

Let $l^2 \equiv 1 \bmod m$. If the arithmetic progression $mz+l$ contains a prime $> \frac{1}{2}\varphi(m)$, then it contains infinitely many primes.

In this paper by a refinement of Schur's method we prove

THEOREM. *Let* $l^2 \equiv 1 \bmod m$. *If the arithmetic progression* $mz+l$ *contains a prime, then it contains infinitely many primes.*

Let Q be the rational field, ζ_m a primitive mth root of unity,

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

$K = Q\big(h(\zeta_m)\big)$.

Let r be the degree of K, N denote the norm from K to Q.

LEMMA 1. *Let* a *be any integral generating element of* K, $a_1, \ldots, a_r$ $(a_1 = a)$ *all its conjugates,*

$$G(x, y) = \prod_{i=1}^{r} (x - a_i y), \qquad d \textit{ the discriminant of } G.$$

If q *is a prime,* x, y *rational integers,* $q \mid G(x, y)$, $q \nmid mdy$, *then* q *is of the form* $mz+1$ *or* $mz+l$.

Proof. $a = \chi\big(h(\zeta_m)\big)$, where χ is a polynomial with rational coefficients and since a is a generating element of K

(1) $$\chi\big(h(\zeta_m^{s_1})\big) = \chi\big(h(\zeta_m^{s_2})\big),$$

where

(2) $$(s_1, m) = (s_2, m) = 1$$

implies

(3) $$h(\zeta_m^{s_1}) = h(\zeta_m^{s_2}).$$

Hence

$$h(\zeta_m^{-s_1}) = h(\zeta_m^{-s_2})$$

and since for $2l \not\equiv m+2 \bmod 2m$, as noticed by A. Schinzel,

$$\zeta_m^{(l+1)s_1+s_2(l-2)}\{h(\zeta_m^{-s_2})-h(\zeta_m^{-s_1})\}+\zeta_m^{-s_2}\{h(\zeta_m^{s_2})-h(\zeta_m^{s_1})\}$$
$$= (\zeta_m^{s_2(l-1)}+1)(\zeta_m^{s_1-s_2}-1)(\zeta_m^{ls_1-s_2}-1),$$

we infer that in this case $s_2 \equiv s_1 \bmod m$ or $s_2 \equiv ls_1 \bmod m$. $\zeta_m^{s_2(l-1)}+1 = 0$ is impossible, since it gives m even $s_2(l-1) \equiv \frac{1}{2}m \bmod m$ and in view of (2) $2l \equiv m+2 \bmod 2m$; a contradiction.

If $2l \equiv m+2 \bmod 2m$ we get from (3) $\zeta_m^{2s_1} = \zeta_m^{2s_2}$ hence $2s_1 \equiv 2s_2 \bmod m$ and either $s_1 \equiv s_2 \bmod m$ or $s_2 \equiv s_1+\frac{1}{2}m \equiv s_1 l \bmod m$. Thus in any case (1) and (2) imply

$$s_2 \equiv s_1 \bmod m \quad \text{or} \quad s_2 \equiv ls_1 \bmod m.$$

In virtue of a theorem of Schur (l.c., p. 41, Satz I) every prime q such that $q \mid G(z, 1)$ and $q \nmid md$ is of the form $mz+1$ or $mz+l$.

In our case $q \mid G(x, y)$ and $q \nmid y$. Finding z from the congruence $yz \equiv x \bmod q$ we get the desired conclusion.

LEMMA 2. *If p is a prime of the form $mz+l$ then there exists in K an integral generating element a such that $p \| Na$* (1).

Proof. Since $1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}$ form an integral basis in $Q(\zeta_m)$ we have for every integer $\vartheta \in K$, $\vartheta = \Theta\big(h(\zeta_m)\big) = \Omega(\zeta_m)$, where Θ is a polynomial with rational coefficients and Ω one with rational integral coefficients. Thus

$$\vartheta^p \equiv \Omega(\zeta_m^p) \equiv \Theta\big(h(\zeta_m^p)\big) \bmod p.$$

But since $p \equiv l \bmod m$, $h(\zeta_m^p) = h(\zeta_m)$. Thus

$$\vartheta^p \equiv \vartheta \bmod p$$

which shows that all prime ideal factors of p in K are of first degree. Let $\mathfrak{p}$ be any of them and a an integer of K such that $\mathfrak{p} = (p^2, a)$. We have

$$p = N\mathfrak{p} = (p^2, a_1)(p^2, a_2)\ldots(p^2, a_r)$$

where $a_1, a_2, \ldots, a_r$ are the conjugates of a. Hence $(p^2, Na) = p$, i.e. $p \| Na$. The numbers $a_1, \ldots, a_r$ must be all different, otherwise $Na = a^k$, where $k > 1$ and a is a rational integer, which gives $p^2 \mid Na$.

---

(1) $p^\nu \| a$ means that $p^\nu \mid a$ and $p^{\nu+1} \nmid a$.

LEMMA 3. *Let p, a have the same meaning as in Lemma 2 and $G_0(x, y) = \prod_{i=1}^{r}(x-a_i y)$. Let d_0 be the discriminant of G_0, $p^\nu \| d_0$, $M = md_0/p^\nu$. For every rational integer y divisible by M but not by p there exists a rational integer x such that $G_0(x, y)$ has a prime factor of the form $mz+l$ not dividing py.*

Proof. Let us choose x so that

$$x \equiv \begin{cases} 1 \bmod y, \\ 0 \bmod p^2 \end{cases} \tag{4}$$

and

$$G_0(x, y) > p. \tag{5}$$

We have from (4)

$$G_0(x, y) \equiv x^r \equiv 1 \bmod y \tag{6}$$

and

$$G_0(x, y) \equiv (-1)^r N(a) y^r \bmod p^2,$$

whence by the choice of a

$$p \| G_0(x, y). \tag{7}$$

Let $C = G_0(x, y)/p$. If q is a prime and $q \mid C$ then by (6) and (7) $q \nmid py$. Moreover since $M \mid y$, it follows that $q \nmid md_0 y$ and by Lemma 1, $q \equiv 1 \bmod m$, or $q \equiv l \bmod m$. If $l \equiv 1 \bmod m$, Lemma 3 follows since by (5) C must have at least one prime factor.

If $l \not\equiv 1 \bmod m$ and C had no prime factor $\equiv l \bmod m$ it would follow that

$$C = \prod q_i, \qquad q_i \equiv 1 \bmod m$$

thus $C \equiv 1 \bmod m$.

On the other hand, since $m \mid y$ it follows from (6) that

$$C \equiv 1/l \equiv l \bmod m.$$

The contradiction obtained completes the proof.

Proof of the theorem. Suppose that there exist only finitely many primes of the form $mz+l$, say $q_1, q_2, \ldots, q_k$ ($k \geqslant 1$ by the assumption).

Put in Lemma 3

$$p = q_1, \qquad y = M\prod_{i=2}^{k} q_i.$$

By the lemma there exists a rational integer x such that $G_0(x, y)$ has a prime factor $q \equiv l \bmod m$ not dividing py. The contradiction obtained completes the proof.

Reference

[1] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen,* Sitzungsber. Berl. Math. Ges. 11, pp. 40-50.

Reçu par la Rédaction le 24. 8. 1965

ACTA ARITHMETICA
XI (1966)

Polynome, welche für gegebene Zahlen Permutationspolynome sind

von

W. Nöbauer (Wien)

Herrn Professor Hlawka
zum 50. Geburtstag gewidmet

Man bezeichnet das ganzzahlige Polynom $g(x)$ als Permutationspolynom mod n (n natürliche Zahl), wenn die Abbildung $i \to g(i)$ mod n, $i = 1, 2, \ldots, n$, eine Permutation der Restklassen mod n ist. Es sei $\mathfrak{M}(g(x))$ die Menge aller natürlichen Zahlen $n > 1$, für welche $g(x)$ Permutationspolynom ist. In dieser Note werden einige Aussagen hergeleitet, die sich auf $\mathfrak{M}(g(x))$ beziehen.

Es gilt, wie etwa in [5] gezeigt wurde: Ist $n = ab$ und $(a, b) = 1$, so ist $g(x)$ dann und nur dann Permutationspolynom mod n, wenn es Permutationspolynom mod a und Permutationspolynom mod b ist. Für die vollständige Kenntnis von $\mathfrak{M}(g(x))$ genügt daher die Kenntnis aller in $\mathfrak{M}(g(x))$ enthaltenen Primzahlpotenzen. Ebenfalls wurde etwa in [5] gezeigt: Ist $n = p^e$ eine Primzahlpotenz mit $e > 1$, so ist $g(x)$ dann und nur dann Permutationspolynom mod n, wenn es Permutationspolynom mod p ist und wenn $g'(\xi) \not\equiv 0 \bmod p$ für jedes ganze ξ. Daraus folgt sogleich: Die Menge der in $\mathfrak{M}(g(x))$ enthaltenen Potenzen einer Primzahl p ist entweder leer, oder sie besteht aus p allein, oder sie besteht aus allen Potenzen von p. Bezeichnen wir also mit $\mathfrak{P}(g(x))$ die Menge aller in $\mathfrak{M}(g(x))$ enthaltenen Primzahlen und mit $\mathfrak{G}(g(x))$ die Menge aller jener Primzahlen, deren sämtliche Potenzen in $\mathfrak{M}(g(x))$ enthalten sind, so ist durch Angabe von $\mathfrak{P}(g(x))$ und von $\mathfrak{G}(g(x))$ das $\mathfrak{M}(g(x))$ vollständig bestimmt.

Wie sofort zu sehen, ist $f(g(x))$ dann und nur dann ein Permutationspolynom mod n, wenn $f(x)$ und $g(x)$ Permutationspolynome mod n sind. Es gelten daher die Beziehungen

$$(1) \qquad \mathfrak{A}\big(f(g(x))\big) = \mathfrak{A}(f(x)) \cap \mathfrak{A}(g(x)) \quad \text{für} \quad \mathfrak{A} = \mathfrak{M}, \mathfrak{P}, \mathfrak{G}$$

Selbstverständlich gilt $\mathfrak{G}(g(x)) \subseteq \mathfrak{P}(g(x))$.