A GROUP-THEORETICAL PROOF OF A THEOREM IN ELEMENTARY NUMBER THEORY

HUGO S. SUN
Fresno State College, Fresno, California

It is well known that if

$$N = 2^{\ell} p_1^{\ell_1} p_2^{\ell_2} \cdots p_s^{\ell_s}$$

then the number of solutions to the congruence $x^2 \equiv 1 \pmod{N}$ is 2^s if $\ell = 0$ or 1, 2^{s+1} if $\ell = 2$, 2^{s+2} if $\ell \geq 3$ [2, p. 191]. In this note, we give a group-theoretical proof of this fact. To fix the idea, let

$$N = 2^{\ell} p_1^{\ell_1} p_2^{\ell_2} \cdots p_s^{\ell_s} = 2^{\ell} N_0 = p_1^{\ell_1} N_1 = \cdots = p_s^{\ell_s} N_s .$$

Hence $N_i = N/p_i^{\ell_i}$, and the N_i are relatively prime, identifying 2 with p_0.

Lemma. Let $k_0, k_1, \cdots, k_s$ be integers such that $k_0N_0 + k_1N_1 + \cdots + k_sN_s = 1$, let $e_0 = \pm 1$, or ± 1 + some power of 2, $e_i = \pm 1$ for $1 \leq i \leq s$, and let

$$M = e_0k_0N_0 + e_1k_1N_1 + \cdots + e_sk_sN_s .$$

Then for any choice of e_i, $0 \leq i \leq s$, $(M,N) = 1$.

Proof. Since $p_i | N_j$ for $i \neq j$ and $p_i \nmid N_i$, p_i must not divide k_i, otherwise p_i would divide 1. Suppose $(M,N) \neq 1$, then some $p_i | M$, but this p_i must then divide $e_ik_iN_i$, which is impossible.

Theorem. The number of solutions to the congruence $x^2 \equiv 1 \pmod{N}$ is 2^s if $\ell = 0$ or 1, 2^{s+1} if $\ell = 2$, and 2^{s+2} if $\ell \geq 3$.

Proof. Let $<c>$ be a cyclic group of order N. First notice that a nontrivial automorphism λ of $<c>$ takes c to c^x, where $(x,N) = 1$; if λ is of order 2, then $x^2 \equiv 1 \pmod{N}$. Moreover, since every solution x_0 of $x^2 \equiv 1 \pmod{N}$ is prime to N, $\lambda(c) = c^{x_0}$ is an automorphism of order 2. Since the automorphism group of a cyclic group is abelian, the set of automorphisms of order 2 form a subgroup. The order of this subgroup is the number of solutions to the congruence $x^2 \equiv 1 \pmod{N}$.

Each Sylow p_i-subgroup is generated by c^{N_i} and is characteristic in $<c>$. An automorphism λ of order 2 must take c^{N_i} to c^{N_i} or c^{-N_i} for $1 \leq i \leq s$ since $x^2 \equiv 1 \pmod{p^n}$ has only two solutions ± 1 for an odd prime p. As for the 2-Sylow subgroup $<c^{N_0}>$, if its order is 2, it admits only the identity automorphism; if its order is 4, it admits 2 automorphisms, namely $c^{N_0} \to c^{N_0}$ and $c^{N_0} \to c^{-N_0}$; if its order is 2^{ℓ}, $\ell \geq 3$, it admits 4 automorphisms, with the other two being

$$c^{N_0} \longrightarrow c^{N_0(2^{\ell-1}+1)} \quad \text{and} \quad c^{N_0} \longrightarrow c^{N_0(2^{\ell-1}-1)} \; .$$

We have thus seen that an automorphism λ of order 2 either leaves a Sylow p_i-subgroup elementwise fixed or takes its elements to their inverses or, in case of the Sylow 2-subgroup of order $2^\ell \geq 8$, takes the elements to their $2^{\ell-1} \pm 1$ powers.

Conversely, mappings that act on one Sylow subgroup as above and leave all others elementwise fixed are automorphisms of order 2 and so are their compositions. In fact, let λ be such a mapping,

$$\lambda(c) = \lambda(c^{k_0N_0+\cdots+k_sN_s}) = \lambda(c^{k_0N_0})\lambda(c^{k_1N_1})\cdots\lambda(c^{k_sN_s}) = (c^{e_0k_0N_0})(c^{e_1k_1N_1}) \cdots (c^{e_sk_sN_s}) = c^M \, ,$$

clearly $(M,N) = 1$ by the lemma and λ is an automorphism of order 2.

Since the group of automorphisms of order 2 is a direct product of the groups of automorphisms of order 2 of its Sylow subgroups, the conclusion of the theorem is established.

REFERENCES

1. W. Burnside, Theory of Groups of Finite Order, Dover, 1955.
2. I. M. Vinogradov, Elements of Number Theory, Dover, 1954.

ERRATA

Please make the following corrections on errors occurring in "The Autobiography of Leonardo Pisano,*" appearing on page 99, Volume 11, No. 1, February 1973:

Page 100, line 13 — The fourth word in this line should be "quedam," not "quedem."

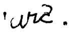
Page 101, line 11 — Please underline "per qualche giorno."

line 5 from bottom — Please underline the last word, "in."

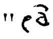
Page 102, line 6 — Please change the last underscored word from "posta" to "postea."

line 21 — Please underline the words "disputationis conflictum."

Page 103, line 1 — Please change the word "reconing" to read "reckoning."

line 20 — Please change the last word on this line to read "."

line 33 — Please change the next to last word to read " ."

line 5 from bottom — Please read the sixth from last word as "."

Page 104, line 1 — Please underline the word "algorismum."

[Continued on page 168.]