On a Theorem of Gauss

By Hansraj Gupta, Hoshiarpur (Punjab).

(*Received 3rd August*, 1934; *received in revised form 26th November*, 1934. *Read 2nd November*, 1934.)

§ 1. *Introduction.*

Professor Hemraj[1] has given a proof of a part of a theorem of Gauss without using the theory of quadratic residues. Proceeding on similar lines, I have obtained a complete proof which is rather simpler and certainly more concise.

In what follows $G(n, r)$ denotes[2] the sum of the products of the first n natural numbers taken r at a time; $\{n, m\}$ denotes as usual the greatest common factor of the two non-zero positive integers n and m; p stands for an odd prime unless stated otherwise; and $a, b, m, n, i, j, k, \mu, r$, etc., stand for positive integers or zero.

I write $a <. n$ when $\{a, n\} = 1$ and $a < n$; and denote by $\Pi (a <. n)$ the product of all a's less than n and prime to it.

If $n \equiv 0 \pmod{p^\mu}$, but $\not\equiv 0 \pmod{p^{\mu+1}}$, $p \geqq 2$, then I say that n is μ-potent in p, or that the p-potency of n is μ. We have $\mu = 0$ when $n \not\equiv 0 \pmod{p}$.

In my proof of Gauss' Theorem, viz.

$$\begin{aligned} \Pi (a <. m) &\equiv -1 \pmod{m} \text{ when } m = 2^2, p^\mu, 2p^\mu, \\ &\equiv 1 \pmod{m} \text{ otherwise,} \end{aligned}$$

I make use of the lemmas of § 2.

§ 2. Lemma 1. *If a be the p-potency of r, then the p-potency of $\binom{p^\mu}{r}$ is $\mu - a$, where $1 \leqq r \leqq p^\mu$ and $p \geqq 2$.*

We have $\binom{p^\mu}{r} = \dfrac{p^\mu !}{r!\,(p^\mu - r)!}$.

Therefore the p-potency of $\binom{p^\mu}{r}$

$$= \sum_{\kappa=1}^{\mu} \left\{ \left[\frac{p^\mu}{p^\kappa}\right] - \left[\frac{r}{p^\kappa}\right] - \left[\frac{p^\mu - r}{p^\kappa}\right] \right\} = \sum_{\kappa=1}^{\mu} \lambda_\kappa$$

where $\lambda_\kappa = 0$ or 1 according as $r \equiv 0$ or $\not\equiv 0 \pmod{p^\kappa}$. Since $r \equiv 0 \pmod{p^a}$ but $\not\equiv 0 \pmod{p^{a+1}}$, it follows that the p-potency of $\binom{p^\mu}{r}$ is $\mu - a$.

LEMMA 2. *The p-potency of $G(p^\mu - 1, r)$ is greater than or equal to $\mu - \beta$, where $1 \leqq r \leqq p^\mu - 1$, $p^\beta \leqq 2r < p^{\beta+1}$, p is an odd prime or 2, and $\beta \geqq 0$.*

We have[3]

$$G(p^\mu - 1, r) = \sum_{i=1}^{r} \left\{ f_i(r) \binom{p^\mu}{2r - i + 1} \right\}, \tag{1·3}$$

where the f's are positive integers. The result stated follows immediately from Lemma 1.

LEMMA 3. *If $\{m, n\} = 1$, then*

$$\Pi(a <. mn) \equiv \{\Pi(b <. n)\}^{\phi(m)} \pmod n,$$

where $\phi(m)$ denotes as usual the number of integers less than and prime to m.

If $b <. n$, then in the series of m terms

$$b,\ b + n,\ b + 2n,\ b + 3n,\ \ldots,\ b + (m - 1)n,$$

there are $\phi(m)$ integers less than and prime to mn. Each of these integers $\equiv b \pmod n$, so that their product $\equiv \{b\}^{\phi(m)} \pmod n$. Giving to b all values $<. n$, we get the result stated.

§ 3. *Proof of Gauss' Theorem.*

(i) We first consider the case when $m = 2^\mu$, $\mu \geqq 1$. We have

$$\Pi(a <. 2) \equiv \pm 1 \pmod 2,$$
$$\Pi(a <. 2^2) \equiv -1 \pmod{2^2},$$
$$\Pi(a <. 2^3) \equiv 1 . 3 . 5 . 7 \equiv 1 \pmod{2^3},$$
$$\Pi(a <. 2^4) \equiv 1 . 3 . 5 \ldots 15 \equiv 1 \pmod{2^4}.$$

Suppose that $\Pi(a <. 2^\mu) \equiv 1 \pmod{2^\mu}$ when $3 \leqq \mu \leqq i - 1$. Then

$$\Pi(a <. 2^i) \equiv 1 . 3 . 5 . 7 \ldots (2^{i-1} - 1) . (2^i - 1)(2^i - 3) \ldots \{2^i - (2^{i-1} - 1)\}.$$
$$\equiv \{\Pi(a <. 2^{i-1})\}^2 \pmod{2^i}$$
$$\equiv 1 \pmod{2^i}, \text{ since } 2i - 2 > i.$$

Hence by induction for $\mu \geqq 3$,

$$\Pi(a <. 2^\mu) \equiv 1 \pmod{2^\mu}.$$

(ii) Now consider the case when $m = p^\mu$, $\mu \geqq 1$. Let a be any number $<. p$, and let $\rho = p^{\mu-1} - 1$. Then

$$\prod_{\kappa=0}^{\rho} (a + \kappa p) = a^{\rho+1} + \sum_{r=1}^{\rho} \{G(p^{\mu-1} - 1, r)\, p^r a^{\rho-r+1}\}.$$

Since the p-potency of $G(p^{\mu-1}-1, r) \cdot p^r$ is greater than or equal to $\mu + r - \beta - 1$, where $p^\beta \leqq 2r < p^{\beta+1}$, that is, greater than or equal to μ, we have

$$\prod_{\kappa=0}^{\rho} (a + \kappa p) \equiv a^{\rho+1} \pmod{p^\mu}.$$

Hence $$\Pi (a < . p^\mu) \equiv \{\Pi (a < . p)\}^{\rho+1} \equiv \{(p-1)!\}^{\rho+1} \pmod{p^\mu}$$
$$\equiv \{jp - 1\}^{\rho+1} \pmod{p^\mu}$$

since[3] $(p-1)! \equiv -1 \pmod{p}$. So by Lemma 1

$$\Pi (a < . p^\mu) \equiv -1 \pmod{p^\mu}.$$

(iii) When $m = 2p^\mu$, we have from Lemma 3,

$$\Pi (a < . 2p^\mu) \equiv \{\Pi (a < . p^\mu)\}^{\phi(2)} \pmod{p^\mu}$$
$$\equiv -1 \pmod{p^\mu}.$$

Also $$\Pi (a < . 2p^\mu) \equiv \{\Pi (a < . 2)\}^{\phi(p^\mu)} \pmod{2}.$$
$$\equiv 1 \equiv -1 \pmod{2}.$$

Hence $$\Pi (a < . 2p^\mu) \equiv -1 \pmod{2p^\mu}.$$

(iv) When m is of any form other than those already considered, Gauss' Theorem follows immediately from Lemma 3.

Let $m = p^\mu n$, where $\mu \geqq 1$, $p \geqq 2$, $\{n, p\} = 1$, and $n > 2$. Then

$$\Pi (a < . m) \equiv \{\Pi (a < . p^\mu)\}^{\phi(n)} \pmod{p^\mu}$$
$$\equiv 1 \pmod{p^\mu},$$

since $\phi(n)$ is even. Considering in this manner all the different primes present in m, we obtain

$$\Pi (a < . m) \equiv 1 \pmod{m}, \quad m \neq 2^2, p^\mu, 2p^\mu, \text{ where } p \geqq 3.$$

This proves Gauss' Theorem completely.

REFERENCES.

1. Hemraj, *Journal Indian Math. Soc.*, 19 (1931), 34-39.
2. Hansraj Gupta, *Journal Indian Math. Soc.*, 19 (1931), 1-6.
3. Hansraj Gupta, *Proc. Edinburgh Math. Soc.*, 4 (1934-35), 61, equ. (1.3).

NOTE ADDED IN PROOF. For completion of the proof discussed in reference 1 above, see Hemraj, *Mathematics Student*, 2 (1934), 140-148.