THE GREATEST PRIME FACTOR OF x^2-1.

BY S. CHOWLA,

Department of Mathematics, Andhra University, Waltair.

Received October 11, 1934.

Theorem. If P_x *is the greatest prime factor of* $x^2 - 1$, *then*

(1) $P_x > c \log \log x$

where c *is an absolute positive constant.*

Remarks. (1) is a sharper form of the well-known result

$P_x \to \infty$ as $x \to \infty$,

which is a consequence of the Thue-Siegel theorem.[1]

It is noteworthy that it is not possible to derive (1) *from Siegel's method.*[2]

Proof. We need the following lemmas.

Lemma 1.[3] *Let* $x = t_1$, $y = u_1$, *be the smallest solution in positive integers of*

$$x^2 - Dy^2 = 1$$

where D *is not a perfect square. We define* $t_m = t_m$ (D), $u_m = u_m$ (D) *by*

$$t_m + u_m \sqrt{D} = (t_1 + u_1 \sqrt{D})^m$$

Then for every $m > 1$, u_m *contains at least one prime factor not contained in* D.

Lemma 2.[4]

$$t_1 (D) < \exp. (c_1 \sqrt{D} \log D),$$

$$u_1 (D) < \exp. (c_1 \sqrt{D} \log D),$$

where c_1 *is an absolute positive constant independent of* D.

Now let p_r denote the rth prime, $p_1 = 2$, $N_r = p_1 . p_2 . p_3 . \ldots . p_r$ the product of the first r primes. Let m be a positive integer (not a perfect square) composed of *powers not higher than the second* of primes chosen from $p_1, \ldots . p_r$. It is a consequence[5] of lemmas 1 and 2 that for every

$$x > e^{c_1 \sqrt{m} \log m}$$

---

[1] See Landau, *Vorlesungen über Zahlentheorie*, **3**.

[2] Landau, *ibid.*, 230.

[3] See Dickson's *History of the Theory of Numbers*, **2**, 391 and 396. The result is due to Störmer, 396.

[4] Schur, *Göttinger Nachrichten*, 1918.

[5] Remembering that if $x^2 - Dy^2 = 1$ there is a unique m such that $x = t_m(D)$, $y = u_m(D)$ $[y \neq 0]$.

the expression (x^2-1) has at least one prime factor not contained in m. It now follows that if

$$x > e^{2c_1 N_r \log N_r}$$

then (x^2-1) has at least one prime factor greater than p_r. Hence if

(2) $\exp. (2c_1 N_r \log N_r) < x \leqslant \exp. (2c_1 N_{r+1} \log N_{r+1})$ then $P_x > p_r$.

But

(3) $\log N_r \sim p_r$

From (2) and (3) it follows that for all x in (2),

(4) $P_x > p_r > c_2 \log \log x$,

where c_2 is an absolute positive constant. Since to every large x we can find a unique r to satisfy (2) our theorem is now proved.