THE GREATEST PRIME FACTOR OF x^2+1.

BY S. CHOWLA,

Department of Mathematics, Andhra University, Waltair.

Received October 12, 1934.

Theorem. If P_x *denotes 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) sharpens the well-known result

(2) $P_x \to \infty$ as $x \to \infty$,

which is a consequence of the Thue-Siegel[1] theorem. *It is noteworthy that Siegel's*[2] *method is not capable of yielding anything stronger than* (2).

Proof. All letters, Latin or Greek, denote integers; p denotes a prime; $m(p, x)$ is the highest power of p contained in x; D is a non-square integer; p_r is the rth prime; $N_r = p_1 . p_2 . p_3 \ldots\ldots p_r$, the product of the first r primes; given t_1, u_1 then t_r, u_r are defined by

(3) $(t_r + u_r \sqrt{D}) = (t_1 + u_1 \sqrt{D})^r$

so that

(4) $u_r = {}^rC_1\, u_1\, t_1^{r-1} + {}^rC_3\, u_1^3 t_1^{r-3}\, D + {}^rC_5\, u_1^5\, t_1^{r-5}\, D^2 + \ldots\ldots$

where

$${}^rC_s = \frac{r!}{s!\,(r-s)!}$$

We need the following lemmas.

Lemma 1. If p/D, s > 1, s $\equiv$ 1 (2) *then*

(5) $m(p, r\,u) < m\left(p, {}^rC_s\, u^s\, D^{\frac{s-1}{2}}\right)$ $\qquad [p \geqslant 5]$

(5) $m(p, r\,u) < m\left(p, {}^rC_s\, u^s\, D^{\frac{s-1}{2}}\right)$ $\qquad [p = 3, 3^2/D]$

Proof. Let $m(p, r) = \alpha$, $m(p, u) = \beta$ $\qquad [\alpha, \beta \geqslant 0]$.

Case (i) $p \geqslant 5$.

Denote by l.s. and r.s. the left and right sides of (5) respectively. Then we have

(6) $\text{l.s.} = \alpha + \beta.$

(7) $\text{r.s.} = m(p, {}^rC_s) + m\left(p, u^s\, D^{\frac{s-1}{2}}\right)$

(8) $\qquad \geqslant m(p, {}^rC_s) + \beta s + \frac{s-1}{2}$

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

[2] *Ibid.*

Further

$$m(p, {}^rC_s) = m\left(p, \frac{r(r-1)\cdots(r-s+1)}{s!}\right) \geqslant m\left(p, \frac{r}{s!}\right)$$

$$= a - m(p, s!) = a - \sum_{k=1}^{\infty}\left[\frac{s}{p^k}\right]$$

$$> a - s\left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right)$$

$$(9) \qquad = a - \frac{s}{p-1}$$

From (8) and (9),

$$(10) \quad \text{r.s.} > a + \beta + (s-1)\left(\tfrac{1}{2} + \beta\right) - \frac{s}{p-1}$$

$$(11) \quad > a + \beta \; [p \geqslant 5]$$

Our result follows from (6) and (11).

Case (ii) $p = 3$, $D \equiv 0 \; (3^2)$

In this case it follows from (7) and (8) that

$$\text{r.s.} \geqslant m(p, {}^rC_s) + \beta s + (s-1)$$

$$> a + \beta + (s-1)(1+\beta) - \frac{s}{p-1} \qquad \text{[from (9)]}$$

$$= a + \beta + (s-1)(1+\beta) - \frac{s}{2}$$

$$> a + \beta \; [\beta \geqslant 0],$$

while the l.s. is $a + \beta$.

Lemma 2. If $x = t_1$, $y = u_1$, *is the smallest solution in positive integers of* $x^2 - Dy^2 = -1$ *then the numbers* $u_r \begin{bmatrix} r \equiv 1 \; (2) \\ r \geqslant 3 \end{bmatrix}$ *defined in* (3), *contain at least one prime factor not contained in* D.

Proof. Observing that $u_r \equiv 1 \; (2)$ for $r \equiv 1 \; (2)$, lemma 2 follows immediately from (4) and lemma 1.

Since all the solutions of $x^2 - Dy^2 = -1$ are given by $x = t_r$, $y = u_r$ $[r \equiv 1(2)]$ it follows from lemma 2 that

Lemma 3.[3] *If*

$$(12) \quad x^2 - Dy^2 = -1$$

then y *contains at least one prime factor not contained in* D *for every solution* (x, y) *of* (12), *except, possibly, the smallest* $(y = u_1)$

Lemma 4.[4]

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

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

where c_1 *is an absolute positive constant.*

---

[3] This result has been proved by Störmer in *Videnskabs selskabets skrifter*, Christiania, 1897, No. 2, 48 pp. This paper was inaccessible to me.

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

Vijayaraghavan, *Proc. London Math. Soc.* (2), 1927, **26**, 403-414.

Proof of the theorem. Let m be a positive integer, not a perfect square, which is a product of powers not higher than the second of primes chosen from $p_1, p_2, p_3, \ldots, p_r$. It is a consequence of lemmas 3 and 4 that for every

$$x > \exp. (c_1 \sqrt{m} \log m)$$

the expression $x^2 + 1$ has at least one prime factor not contained in m. Giving to m all possible non-square values comprised in the expression $p_1^{\theta_1} . p_2^{\theta_2} \ldots p_r^{\theta_r}$ (where each θ is 0, 1 or 2) it follows that for every

$$x > \exp. (2 c_1 N_r \log N_r)$$

the expression $x^2 + 1$ has at least one prime factor greater than p_r. Hence when

$$(13) \quad \exp. (2c_1 N_r \log N_r) < x \leqslant \exp. (2c_1 N_{r+1} \log N_{r+1})$$

then

$$(14) \quad P_x > p_r.$$

But

$$(15) \quad \log N_r \sim p_r.$$

From (13), (14) and (15) it follows that for all x satisfying (13) we have

$$(16) \quad P_x > p_r > c_2 \log \log x \ (c_2 > 0)$$

Since to every large x we can find a unique r to satisfy (13), our theorem is now proved.