

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

$$(2) P_x \rightarrow \infty \text{ as } x \rightarrow \infty,$$

which is a consequence of the Thue-Siegel¹ theorem. It is noteworthy that Siegel's² 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 r th prime; $N_r = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r$, 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

$$(4) u_r = {}^r C_1 u_1 t_1^{r-1} + {}^r C_3 u_1^3 t_1^{r-3} D + {}^r C_5 u_1^5 t_1^{r-5} D^2 + \dots$$

where

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

We need the following lemmas.

Lemma 1. If $p|D$, $s > 1$, $s \equiv 1 \pmod{2}$ then

$$(5) m(p, ru) < m\left(p, {}^r C_s u^s D^{\frac{s-1}{2}}\right) \quad [p \geq 5]$$

$$(5) m(p, ru) < m\left(p, {}^r C_s u^s D^{\frac{s-1}{2}}\right) \quad [p = 3, 3^2|D]$$

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

Case (i) $p \geq 5$.

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

Then we have

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

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

$$(8) \geq m(p, {}^r C_s) + \beta s + \frac{s-1}{2}$$

¹ Landau, *Vorlesungen über Zahlentheorie*, 3.

² *Ibid.*

Further

$$\begin{aligned}
 m(p, {}^r C_s) &= m\left(p, \frac{r(r-1)\cdots(r-s+1)}{s!}\right) \geq m\left(p, \frac{r}{s!}\right) \\
 &= a - m(p, s!) = a - \sum_{k=1}^{\infty} \left[\frac{s}{p^k}\right] \\
 &> a - s\left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) \\
 (9) \quad &= a - \frac{s}{p-1}
 \end{aligned}$$

From (8) and (9),

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

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

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

Case (ii) $p = 3, D \equiv 0 \pmod{3^2}$

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

$$\begin{aligned}
 \text{r.s.} &\geq m(p, {}^r C_s) + \beta s + (s-1) \\
 &> a + \beta + (s-1)(1 + \beta) - \frac{s}{p-1} \quad \text{[from (9)]} \\
 &= a + \beta + (s-1)(1 + \beta) - \frac{s}{2} \\
 &> a + \beta \quad [\beta \geq 0],
 \end{aligned}$$

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 $\left[\begin{matrix} r \equiv 1 \pmod{2} \\ r \geq 3 \end{matrix} \right]$ defined in (3), contain at least one prime factor not contained in D .

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

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

*Lemma 3.*³ If
 (12) $x^2 - Dy^2 = -1$

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

$$\begin{aligned}
 t_1 &= t_1(D) < \exp. (c_1 \sqrt{D} \log D), \\
 u_1 &= u_1(D) < \exp. (c_1 \sqrt{D} \log D),
 \end{aligned}$$

where c_1 is an absolute positive constant.

³ This result has been proved by Stürmer 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 $p_1, p_2, p_3, \dots, p_r$. 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 $p_1^{\theta_1} p_2^{\theta_2} \dots p_r^{\theta_r}$ (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

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

then

$$(14) P_x > p_r.$$

But

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

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

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

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