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\textsuperscript{1} theorem. It is noteworthy that Siegel’s\textsuperscript{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 $r$th prime; $N_r = p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_r$, 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. $u_r = rC_1 u_1 t_1^{r-1} + rC_2 u_1^2 t_1^{r-2} D + rC_3 u_1^3 t_1^{r-3} D^2 + \cdots$

where

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

We need the following lemmas.

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

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

6. $m(p, r u) < m(p, rC_r u^s D^\frac{s-1}{2})$ \quad \[ p = 3, 3^2|D \]

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

Case (i) $p \geq 5$.

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

Then we have

7. l.s. = $a + \beta$.

8. r.s. = $m(p, rC_r) + m(p, u^s D^\frac{s-1}{2})$

9. $\geq m(p, rC_r) + \beta s + \frac{s-1}{2}$

\textsuperscript{1} Landau, \textit{Verlesungen über Zahlentheorie}, 3.
\textsuperscript{2} Ibid.
Further
\[ m \left( \hat{p}, \mathcal{C}_r \right) = m \left( \hat{p}, \frac{r(r-1) \cdots (r-s+1)}{s!} \right) \geq m \left( \hat{p}, \frac{r}{s!} \right) \]
\[ = a - m \left( \hat{p}, s! \right) = a - \sum_{k=1}^{\infty} \left[ \frac{s}{p^k} \right] \]
\[ > a - s \left( \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \]
\[ = a - \frac{s}{p-1} \]  
(9)

From (8) and (9),
\[ \text{r.s.} > a + \beta + (s - 1) \left( \frac{1}{2} + \beta \right) - \frac{s}{p-1} \]
\[ \text{(11)} \]

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

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

In this case it follows from (7) and (8) that
\[ \text{r.s.} \geq m \left( p, \mathcal{C}_r \right) + \beta s + (s - 1) \]
\[ > a + \beta + (s - 1) \left( 1 + \beta \right) - \frac{s}{p-1} \]
\[ = a + \beta + (s - 1) \left( 1 + \beta \right) - \frac{s}{2} \]
\[ > a + \beta \left[ \beta \geq 0 \right], \]
while the l.s. is \( a + \beta \).

Lemma 2. If \( x = t_1, y = u_1 \), is the smallest solution in positive integers
of \( x^2 - D y^2 = -1 \) then the numbers \( u_r \left[ \begin{array}{c} r \equiv 1 (2) \\ r \geq 3 \end{array} \right] \) 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 \( x^2 - D y^2 = -1 \) are given by \( x = t_r, y = u_r \)
\( [r \equiv 1(2)] \) it follows from lemma 2 that

Lemma 3.\(^3\) If
\[ x^2 - D y^2 = -1 \]
(12)
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.\(^4\)
\[ t_1 = t_{1_1} \leq \exp \left( c_1 \sqrt{\log D} \right), \]
\[ u_1 = u_{1_1} \leq \exp \left( c_1 \sqrt{\log D} \right), \]
where \( c_1 \) is an absolute positive constant.

\(^3\) This result has been proved by Skr.ner in Videnskabs selskabets skrifter, Christiani,
1897, No. 2, 43 pp. This paper was inaccessible to me.

\(^4\) Schur, Göttingen Nachrichten, 1918;
The Greatest Prime Factor of $x^2 + 1$

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 $p_1^{\theta_1}. p_2^{\theta_2} \cdots p_r^{\theta_r}$ (where each $\theta$ is 0, 1 or 2) it follows that for every

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

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

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

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

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

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