The greatest prime factor of $n^2 + 1$

Héctor Pastén

Pontificia Universidad Católica de Chile

Online Number Theory Seminar

The greatest prime factor

For $n \neq 0, \pm 1$ we define

$$\mathcal{P}(n) = \text{ the greatest prime factor of } n$$

and $\mathcal{P}(n) = 1$ for $n = 0, \pm 1$.

We are interested in $\mathcal{P}(n^2+1)$:

n	1	2	3	4	5	6	7	8	9	10
n^2+1	2	5	10	17	26	37	50	65	82	101
$\mathcal{P}(n^2+1)$	2	5	5	17	13	37	$\boxed{5}$	13	41	101

Note that $\mathcal{P}(n^2+1)$ can be smaller than n. Our goal is to show that it cannot be *too* small.

Does $\mathcal{P}(n^2+1)$ grow with n?

Proposition

We have $\mathcal{P}(n^2+1) \to \infty$ as n grows.

Proof. Suppose this fails. Then there are primes $p_1, ..., p_r$ such that the equation

$$x^2+1=\prod_{j=1}^{r} p_j^{z_j}$$

has infinitely many solutions in integers x and non-negative integers z_j. Considering the z_j modulo 3 we obtain finitely many non-zero integers $D_1, ..., D_k$ (supported on the p_j's) such that at least one of the equations

$$x^2+1=D_j y^3$$

has infinitely many integers solutions. Not possible by Siegel. □

Why $n^2 + 1$?

We want to give lower bounds for the growth of $\mathcal{P}(n^2 + 1)$. But...

Why $n^2 + 1$?

Some reasons:

- $x^2 + 1$ is one of the simplest polynomials for which the previous argument works, so that *a priori* one knows that the largest prime factor grows.
- $x^2 - 1$ also works, but $x^2 + 1$ is a bit more challenging (irreducible.)
- **Historical reasons:** work of Mahler and Chowla dating back to the 30's (independent) gave lower bounds for $\mathcal{P}(n^2 + 1)$.

The Chowla–Mahler theorem

We write $\log_k$ for the k-iterated logarithm. We always assume that the variables are large enough for the logarithms to be defined.

Theorem (Mahler 1933 - Chowla 1934)

There is a constant κ such that

$$\mathcal{P}(n^2+1) > \kappa \cdot \log_2(n).$$

This is done by analyzing the solutions of negative Pell equations

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

The basic idea is that, if $Dy^2 = n^2+1$ only has small prime factors (with D squarefree), then y would be too large.

Improvements

Until recently, the best improvement on the Mahler–Chowla theorem was the following bound proved around 2000 using linear forms in logarithms:

$$\mathcal{P}(n^2+1) > \kappa \cdot \frac{\log_3(n)}{\log_4(n)} \cdot \log_2(n).$$

This bound originates in the work of Stewart and Yu (2001) in the reducible case, and was later generalized by several authors. See for instance the references in the book "Unit Equations in Diophantine Number Theory" by Evertse–Győry.
The previous bound improved on

$$\mathcal{P}(n^2+1) > \kappa \cdot \log_2(n).$$

An observation

In the next discussion we will use the following observation many times. Let $\mathrm{rad}(n)$ be the largest square-free divisor of n. Then

$$\mathrm{rad}(n) \le \prod_{p \le \mathcal{P}(n)} p \le \exp(2\mathcal{P}(n))$$

by Chebyshev's bound. Thus

$$\boxed{\mathcal{P}(n) \ge \kappa \cdot \log \mathrm{rad}(n)}$$

and one can approach the problem by trying to give a lower bound for $\mathrm{rad}(n^2+1)$.

The *ABC* conjecture

Conjecture (Masser–Oesterle 1985)

For every triple of coprime integers a, b, c *with* $a + b = c$ *one has*

$$\max\{|a|, |b|, |c|\} \leq \mathrm{rad}(abc)^{M}$$

for some fixed M *(maybe any* $M > 1$ *up to finitely many exceptions?)*

A result assuming ABC

Assume the analogue of the ABC conjecture over $\mathbb{Z}[i]$. Then the equation

$$(n+i)-(n-i)=2i$$

gives

$$n \leq \max\{\cdots\} \leq \mathrm{rad}(2i(n^2+1))^M$$

hence

$$\mathcal{P}(n^2+1) \gg \log \mathrm{rad}(n^2+1) \gg \log(n).$$

Remarks:

- A more refined argument can conclude using just the usual ABC conjecture over $\mathbb{Z}$.
- There is a big gap between the bound

$$\mathcal{P}(n^2+1) > \kappa \cdot \frac{\log_3(n)}{\log_4(n)} \cdot \log_2(n)$$

and the expected $\mathcal{P}(n^2+1) \geq \kappa \cdot \log(n)$.

What we expect, what we know

- A more refined argument can conclude using just the usual ABC conjecture over $\mathbb{Z}$. So, one expects

$$\mathcal{P}(n^2+1) \geq \kappa \cdot \log(n)$$

- There is a big gap between the bound

$$\mathcal{P}(n^2+1) > \kappa \cdot \frac{\log_3(n)}{\log_4(n)} \cdot \log_2(n)$$

  and the expected $\mathcal{P}(n^2+1) \geq \kappa \cdot \log(n)$.

- Our contribution is to improve the unconditional lower bound.

  The best available result is a lower bound for $\mathcal{P}(n^2+1)$ roughly of size $\log_2(n)$. We obtain one roughly of size $(\log_2 n)^2$.

Main theorem for $\mathcal{P}(n^2+1)$

Theorem (P. 2023)

As n grows, we have:

- $\mathrm{rad}(n^2+1) \geq \exp\left(\kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}\right)$
- $\mathcal{P}(n^2+1) \geq \kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}$.

The second item is a consequence of the first one.

In case you want to see the details, the reference is

- H. Pasten, *The largest prime factor of n^2+1 and improvements on subexponential ABC*. Inventiones Mathematicae (2024)

Main theorem for *ABC*

The following result by Stewart–Yu (2001) was the strongest available unconditional sub-exponential bound towards the ABC conjecture:

Theorem (Stewart–Yu 2001)

For a, b, c coprime positive integers with $a + b = c$ let $R = \mathrm{rad}(abc)$ and $q = \min\{\mathcal{P}(a), \mathcal{P}(b), \mathcal{P}(c)\}$. Then

$$\log c \le q \cdot \exp\left(\kappa \cdot \frac{\log_3 R}{\log_2 R} \cdot \log R\right) \ll_\epsilon qR^\epsilon.$$

Our method gives:

Theorem (P. 2023)

Keep the same notation. Then

$$\log c \le q \cdot \exp\left(\kappa \cdot \sqrt{(\log R)\log_2 R}\right).$$

The basic idea

Instead of applying the ABC conjecture to the equation

$$(n+i)-(n-i)=2i$$

we apply the best available tools that have succeeded in giving unconditional results for ABC:

- Linear forms in logarithms
- Modular forms and elliptic curves.

The basic idea: the LFL part

Regarding LFL: We rearrange the equation

$$(n+i)-(n-i)=2i$$

as

$$1-\xi=\frac{2i}{n+i} \quad \text{where } \xi=\frac{n-i}{n+i}.$$

Two observations:

- $|1-\xi|$ is small as n grows
- ξ is an element of the multiplicative group $\Gamma \subseteq \mathbb{Q}(i)^\times$ generated by the primes that divide $(n+i)(n-i)=n^2+1$.

This allows us to apply a result by Evertse–Győry based on LFL.

The basic idea: the LFL part

However:

- A direct application of the Evertse–Győry theorem only recovers the bound
$$\mathcal{P}(n^2+1) > \kappa \cdot \frac{\log_3(n)}{\log_4(n)} \cdot \log_2(n).$$
- To get something better, one needs to show that only very few exponents in the prime factorization of
$$(n+i)(n-i) = n^2+1$$
can be big.

The basic idea: Elliptic curves and modular forms

Let $v_p(n)$ be the exponent of the prime p in the factorization of n.

In my paper "Shimura curves and the ABC conjecture" I proved

Theorem (P. 2017)

For a, b, c coprime positive integers with $a + b = c$ we have

$$\prod_{p|abc} v_p(abc) \ll_\epsilon \mathrm{rad}(abc)^{8/3+\epsilon}.$$

The proof is very difficult:
It requires arithmetic geometry, Arakelov theory, analytic number theory (zero-free regions for L-functions), cases of Colmez's conjecture, theory of classical and quaternionic modular forms, and more. This machinery works thanks to the modularity theorem of elliptic curves over $\mathbb{Q}$ (Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor.)

The basic idea: Elliptic curves and modular forms

This theorem allows one to control the exponents appearing in an ABC triple over $\mathbb{Z}$. But our problem is an ABC triple over $\mathbb{Z}[i]$!
Fortunately, in the same paper I prove a related result for elliptic curves over $\mathbb{Q}$:

Theorem (P. 2017)

Let S be a finite set of primes. For all elliptic curves $E/\mathbb{Q}$ which are semi-stable away from S, one has

$$\prod_{p|\Delta} v_p(\Delta) \ll_{S,\epsilon} N^{11/2+\epsilon}.$$

Here, Δ is the minimal discriminant and N is the conductor of E.
Since E is semi-stable away from S, the conductor N is equal to $\mathrm{rad}(\Delta)$ except for a bounded factor supported on S.

The basic idea: Elliptic curves and modular forms

The result on elliptic curves is useful for us thanks to the following elliptic curve:

$$E_n: \quad y^2 = x^3 + 3x + 2n.$$

It has

$$\Delta = 1728(n^2+1), \quad N = 6\mathrm{rad}(n^2+1).$$

and it is semi-stable away from $S = \{2, 3\}$. Then we get

$$\prod_{p \mid n^2+1} v_p(n^2+1) \ll_\epsilon \mathrm{rad}(n^2+1)^{11/2+\epsilon}.$$

This provides enough control on the exponents of the prime factorization of $(n+i)(n-i) = n^2+1$. Together with the Evertse–Gyory theorem we get the main result.

The subexponential ABC bound

Let us recall:

Theorem (P. 2023)

For a, b, c coprime positive integers with $a + b = c$ let $R = \mathrm{rad}(abc)$ and $q = \min\{\mathcal{P}(a), \mathcal{P}(b), \mathcal{P}(c)\}$. Then

$$\log c \le q \cdot \exp\left(\kappa \cdot \sqrt{(\log R)\log_2 R}\right).$$

This result is proved with the same strategy:

- Apply the Evertse–Győry theorem (now we need it for the archimedian and for p-adic absolute values)
- Control the necessary exponents using our product-of-valuations bound for ABC triples.

The product-of-valuations bound

Theorem (P. 2017)

Let S be a finite set of primes. For all elliptic curves $E/\mathbb{Q}$ which are semi-stable away from S, one has

$$\prod_{p|\Delta} v_p(\Delta) \ll_{S,\epsilon} N^{11/2+\epsilon}.$$

Let us give a sketch of the idea behind this theorem.

How to control the product of valuations

By Wiles et.al there is a modular parametrization

$$\phi : X_0(N) \to E, \quad \delta = \deg(\phi)$$

and by Jacquet–Langlands there is a Shimura curve parametrization ($N = DM$ admissible factorization):

$$\phi' : X_0^D(M) \to E, \quad \delta' = \deg(\phi')$$

Ribet–Takahashi proved an approximate formula (which I had to refine to include Eisenstein primes) that roughly says

$$\frac{\delta}{\delta'} \approx \prod_{p|D} v_p(\Delta_E)$$

How to control the product of valuations

$$\frac{\delta}{\delta'} \approx \prod_{p|D} v_p(\Delta_E)$$

The heuristic is: "all congruences / new congruences = level-lowering congruences" for the modular form $f \in S_2(\Gamma_0(N))$ attached to E.
An analytic computation gives

$$\prod_{p|D} v_p(\Delta_E) \approx \frac{\delta}{\delta'} \approx \frac{\|f\|_2}{\|g\|_2}$$

where g is certain quaternionic modular form obtained from f by the J–L transfer. (**Important point:** One has to bound the Manin constant).

It is easy to give an upper bound for $\|f\|_2$. The lower bound for $\|g\|_2$ is extremely complicated due to the lack of Fourier expansions in $X_0^D(M)$: here one uses Arakelov geometry, L-functions, proved cases of Colmez's conjecture, integral models of Shimura curves, etc.

Thanks for your attention.