Divisores de N próximo da raiz quadrada de N

Paulo Almeida

Primeiro Encontro Português de Teoria dos Números

2/11/2022

Overview

Prime divisors of N

Hardy and Ramanujan (1917)

Let $\omega(N)$ be the number of distinct prime divisors of N. Then

$$\omega(N) \simeq \log\log N,$$

for almost all N.

Erdős (1946)

Let $p_1 < p_2 < \cdots < p_r$ be the distinct prime factors of an integer N. Then

$$\log\log p_i \simeq i,$$

for almost all N.

Divisors of N - Random numbers

On average, an integer N has approximately $\log(N)$ divisors. So it is appropriate to rescale and consider the numbers $\log(d_i)$, rather than d_i.

Class	556543680	556544340	556538400
0–2	7	6	6
2–4	20	15	21
4–6	34	28	34
6–8	31	42	29
8–10	17	50	18
10–12	17	53	16
12–14	29	42	29
14–16	37	29	34
16–18	22	13	22
18–20	8	6	7

Factors of N near $\sqrt{N}$

Theorem (A. & Machiavelo)

Given $N \in \mathbb{N}$, $N > 3$, put $r := \lfloor \sqrt{N} \rfloor$ and write N in base r: $N = r^2 + br + c$ (where $0 \leq b, c < r$). If $r \nmid N$ and the polynomial $f(x) := x^2 + (b+1)x - (r-c)$ is irreducible (over $\mathbb{Z}$), then N has no factors in $\left[\frac{N}{\sqrt{N}+\sqrt[4]{N}}, \sqrt{N}\right]$. Otherwise, if $\delta \leq \epsilon$ and δ and $-\epsilon$ are the roots of $f(x)$, then $r - \delta$ and $r + \epsilon$ are non-trivial factors of N.

Proof

Proof.

Let $r = \lfloor \sqrt{N} \rfloor$ and $N = r^2 + br + c$, where $0 \leq b, c < r$. Suppose $N = mn$, with and $m \leq r$. Put $\delta = r - m \geq 0$ and $\epsilon = n - r \geq 0$. Then $N = (r - \delta)(r + \epsilon) = r^2 + (\epsilon - \delta)r - \epsilon\delta$. It follows that

$$\epsilon\delta \equiv r - c \pmod{r}.$$

Hence, if δ, ϵ are such that $\delta\epsilon < r$, then $\delta\epsilon = r - c$, and therefore $b + 1 = \epsilon - \delta$. Thus, $f(x) = (x - \delta)(x + \epsilon)$.

When does the inequality $\delta\epsilon < r$ hold?

Since $(n - m)^2 \geq 0$, $(n + m)^2 \geq 4mn = 4N \geq 4r^2$. So, $n - r \geq r - m$, that is $\epsilon \geq \delta$. So the inequality holds if $\epsilon < \sqrt{r}$, i.e., $n < r + \sqrt{r}$ and $m > N/(r + \sqrt{r})$. □

Example - Fermat numbers

Using this result one can check that $F_{20} = 2^{2^{20}} + 1$ has no factors in an interval that contains more than 10^{78900} numbers, instantaneously.

If $N = F_n = 2^{2^n} + 1$ is the n-th Fermat number, then $r = \lfloor \sqrt{N} \rfloor = 2^{2^{n-1}}$, and $N = r^2 + 1$. Therefore, $f(x) = x^2 + x - (r - 1)$, whose discriminant equals $4r - 3$, which is congruent to 5 modulo 8, for $n \geq 1$. Hence this discriminant is not a square, and thus $f(x)$ has no rational roots. This shows that F_n has no factors in the interval

$$\left[\frac{2^{2^n} + 1}{2^{2^{n-1}} + 2^{2^{n-2}}}, 2^{2^{n-1}} \right].$$

Theorem (A. & Machiavelo)

Given $N \in \mathbb{N}$, set $r = \lfloor \sqrt{N} \rfloor$. For any $\lambda \in \mathbb{N}$ exists a bound B_λ such that if, for all $t = 0, 1, \ldots, \lfloor B_\lambda \rfloor$, the number $\Delta_t = (t + 2r)^2 - 4N$ is not a square, then N has no factors in the interval $[r - \lambda\sqrt{r}, r]$.

Particular Case

Corollary

Given $N \in \mathbb{N}$, set $r = \lfloor \sqrt{N} \rfloor$, and let $\lambda \in \mathbb{N}$ be such that

$$(\lambda^2 + 3)\lambda < \sqrt{r}.$$

If, for all $t = 0, 1, \ldots, \lambda^2 + 2$, the number $\Delta_t = (t + 2r)^2 - 4N$ is not a square, then N has no factors in the interval $[r - \lambda\sqrt{r}, r]$.

Example

Let $N = 4n^2 + 1$. In this case $\Delta_t = t^2 + 8tn - 4$. Clearly, $\Delta_t \neq \square$ for $t \in \{0, 1, 3, 4, 5, 6\}$ and if $t = 2$, $\Delta_t = \square$ if and only if $n = \square$. Therefore, if n is not a square then the number $4n^2 + 1$ has no factors in the interval $[2n - 2\sqrt{2n}, 2n]$.

When can we get squares?

If $N = F_m = 2^{2^m} + 1$ ($m \in \mathbb{N}$) is a Fermat number, then $r = 2^{2^{m-1}}$, and

$$\Delta_{t,m} = 2^{2^{m-1}+2}\, t + t^2 - 4.$$

Suppose that t is odd. Then $t^2 \equiv 1 \pmod 8$, and $\Delta_{t,m} \equiv -3 \pmod 8$, which entails that $\Delta_{t,m}$ is not a square. Since

$$\Delta_{2t,m} = 4\left(2^{2^{m-1}+1}\, t + t^2 - 1\right),$$

one sees that $\Delta_{2t,m}$ is a square if and only if the number

$$\Delta'_{t,m} = 2^{2^{m-1}+1}\, t + t^2 - 1$$

is a square.

First factorizations

Now, $\Delta'_{4k,m} \equiv -1 \pmod 8$ and $\Delta'_{4k+2,m} \equiv 3 \pmod 8$ imply that $\Delta'_{t,m}$ cannot be a square when t is even, while $\Delta'_{pk,m} \equiv -1 \pmod p$ implies that $\Delta'_{t,m}$ is not a square if t is divisible by any prime $p \equiv 3 \pmod 4$. It follows, in particular, that $\Delta'_{t,m}$ can only be a square for numbers

$$t \equiv 1 \pmod 4.$$

Notice $\Delta'_{1,1} = 4$ and $\Delta'_{5,2} = 64$, which gives us the equations $x^2 + 2x - 3 = 0$ and $x^2 + 10x - 39 = 0$ and the factorizations $5 = 1 \times 5$ and $17 = 1 \times 17$.

If $m \geq 3$

Since $\Delta'_{4k+1,m} = 2^{2^{m-1}+1}(4k+1) + 8k(2k+1)$, one sees that in order for $\Delta'_{4k+1,m}$ to be a square, k must be even. Define

$$\Gamma_{k,m} = 2^{2^{m-1}-3}(8k+1) + k(4k+1) = \frac{1}{16}\Delta'_{8k+1,m} = \frac{1}{64}\Delta_{16k+2,m}.$$

If $m = 3$ and $k = 14$ we obtain the square $\Gamma_{14,3} = 1024$ which gives us the equation $x^2 + 226x - 3615 = 0$ and the factorization $257 = 1 \times 257$.

If $m \geq 4$

$\Gamma_{k,m} \equiv k(4k+1) \pmod 8$, and this can only be a square in the cases $k \equiv 0, 4, 5 \pmod 8$. But $k \equiv 5 \pmod 8$ implies that there is a prime $p \equiv \pm 3 \pmod 8$ that divides k, and for such a prime

$$\left(\frac{\Gamma_{k,m}}{p}\right) = \left(\frac{2}{p}\right) = -1,$$

which implies that $\Gamma_{k,m}$ is not a square. So $4 \mid k$.

$$\Omega_{k,m} = 2^{2^{m-1}-5}(32k+1) + k(16k+1) = \frac{1}{256}\Delta_{64k+2,m}.$$

When is $\Omega_{k,m}$ a square?

- $\nu_2(k) \equiv 0 \pmod 2$, if $\nu_2(k) < 2^{m-1} - 5$;
- $k \equiv 2 \pmod 3$;
- $k \equiv 1, 2 \pmod 5$ (for $k \equiv 0, 3, 4 \pmod 5$, $\Omega_{k,m} \equiv 3, 3, 2 \pmod 5$);
- $k \equiv 0, 1, 4 \pmod 8$ (for $k \equiv 2, 3, 5, 6, 7 \pmod 8$, $\Omega_{k,m} \equiv 2, 3, 5, 6, 7 \pmod 8$);
- If $p \mid 32k + 1$ then $p \equiv 1 \pmod 4$ (if $p \equiv 3 \pmod 4$ then $\left(\frac{k(16k+1)}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{32k}{p}\right)\left(\frac{32k+2}{p}\right) = \left(\frac{-1}{p}\right) = -1$);
- no prime congruent to -1 modulo 8 can divide $16k + 1$ (if p is such a prime, then $32k + 1 \equiv -1 \pmod p$, $\left(\frac{2}{p}\right) = 1$, and $\left(\frac{-1}{p}\right) = -1$, so $\left(\frac{-2}{p}\right) = -1$);
- no prime congruent to ± 3 modulo 8 can divide k.

Up to 1000, the only numbers k that simultaneously satisfy all these conditions are:

$$41, 137, 161, 272, 356, 476, 497, 932, 956, 977.$$

Prime divisors of Fermat numbers give a help

Theorem

Let p be a prime divisor of a Fermat number F_a, for some $a \geq 3$, and assume that k is such that

$$\left(\frac{8k^2 + k - \frac{p-1}{64}}{p}\right) = -1.$$

Then $\Omega_{k,m} \neq \square$, for $m \geq a + 2$. Moreover, if $p = 17$ and k is such that

$$\left(\frac{k^2 - 2k - 8}{17}\right) = -1,$$

then $\Omega_{k,m} \neq \square$, for $m \geq 3$.

Using $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, and the two prime divisors of F_5, 641 and 6700417, one eliminates all the above values except for $k = 137$.

A larger desert in the distribution of divisors of F_m

It follows from all this that, in particular,

$$\Delta_{t,m} \neq \square \text{ for } t = 0, 1, \ldots, 64 \times 136 + 2 > 93^2 + 2.$$

Since $(93^2 + 3) \times 93 < 2^{2^{m-2}}$ for $m \geq 7$, one concludes that:

For $m \geq 7$, the Fermat number F_m has no factor in the interval

$$\left[2^{2^{m-1}} - 93 \times 2^{2^{m-2}}, 2^{2^{m-1}}\right].$$

For $m = 4$ the only $\Omega_{k,4}$ that is a square is $\Omega_{1016,4} = 4096^2$, from where we get $65537 = 1 \times 65537$ and F_4 is a prime number. From $\Omega_{102656,5} = 418736^2$ we obtain the decomposition $F_5 = 641 \times 6700417$, similarly from $\Omega_{1051122369536,6} = 4205026314784^2$ we obtain $F_6 = 274177 \times 67280421310721$.

But we can go further

Elimination of the value $k = 137$. One has

$$\Omega_{137,m} \equiv 2^{2^{m-1}-5} \times 7 + 9 \equiv -2^{2^{m-1}-3} - 2 \pmod{11}$$

and

$$\Omega_{137,m} \equiv -2^{2^{m-1}-4} + 34 \pmod{41}$$

Since 2^{2^n} is eventually periodic modulo p, one can easily check that there is no value of m such that $\Omega_{137,m}$ is a quadratic residue modulo 11 and, at the same time, a quadratic residue modulo 41.

Using this idea, we eliminate almost all $k \leq 10^6$, except for $128996, 411392, 559217, 662537, 706832, 804857$ and 870401, using just a prime and considering all the possibilities that 2^{m-1} modulus $p-1$ can have, for $p \leq 20000$.

Even versus odd

Using primes for which $\Omega_{p,m}$ is a square only when m is odd and other primes for which $\Omega_{p,m}$ is a square only when m is even, we can eliminate all the 7 exceptions above.

128996 is eliminated using 13 (m always odd) and 193 (m always even);
411392 is eliminated using 11 (m always odd) and 7 (m always even);
559217 is eliminated using 193 (m always odd) and 19 (m always even);
662537 is eliminated using 31 (m always odd) and 13 (m always even);
706832 is eliminated using 97 (m always odd) and 31 (m always even);
804857 is eliminated using 7 (m always odd) and 193 (m always even);
870401 is eliminated using 11 (m always odd) and 13 (m always even).

How large can the desert be?

Therefore

$$\Delta_{t,m} \neq \square \text{ for } t = 0, 1, \ldots, 64 \times 10^6 + 2 \geq 8000^2 + 2.$$

Since $(8000^2 + 3) \times 8000 < 2^{2^{m-2}}$ for $m \geq 8$, we obtain the following result

Theorem (A. & Machiavelo)

For $m \geq 8$, $F_m = 2^{2^m} + 1$ has no factors in the interval

$$\left[2^{2^{m-1}} - 8000 \times 2^{2^{m-2}}, 2^{2^{m-1}}\right].$$

This work was supported in part by The Center for Research and Development in Mathematics and Applications (CIDMA), through the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), reference UIDB/04106/2020

FCT Fundação para a Ciência e a Tecnologia

CIDMA

REPÚBLICA PORTUGUESA

Thank you for your attention!