On the factorization of $x^2 + x$ and the non-factorization of $x^2 + 7$

by Michael Filaseta

University of South Carolina

Joint Work with M. Bennett & O. Trifonov

Part I: On the factorization of $x^2 + x$

Part I: On the factorization of $x(x+1)$

Part I: On the factorization of $n(n + 1)$

Part I: On the factorization of $n(n+1)$

Well-Known: The largest prime factor of $n(n+1)$ tends to infinity with n.

Part I: On the factorization of $n(n+1)$

Well-Known: The largest prime factor of $n(n+1)$ tends to infinity with n.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Lehmer: Gave some explicit estimates:

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Lehmer: Gave some explicit estimates:

$n(n+1)$ divisible only by primes $\leq 11 \implies n \leq$

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Lehmer: Gave some explicit estimates:

$n(n+1)$ divisible only by primes $\leq 11 \implies n \leq$

... only by primes $\leq 41 \implies n \leq$

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Lehmer: Gave some explicit estimates:

$n(n+1)$ divisible only by primes $\leq 11 \implies n \leq 9800$

... only by primes $\leq 41 \implies n \leq$

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Lehmer: Gave some explicit estimates:

$n(n+1)$ divisible only by primes $\leq 11 \implies n \leq 9800$

... only by primes $\leq 41 \implies n \leq 63927525375$

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > 1$.

Let $p_1, p_2, \ldots, p_r$ be primes. There is an N such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^\theta$.

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

$$abc\text{-conjecture} \implies \theta =$$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

$$abc\text{-conjecture} \implies \theta = 1 - \varepsilon$$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

abc-conjecture $\implies$ $\theta = 1 - \varepsilon$

unconditionally one can obtain $\theta =$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^\theta$.

abc-conjecture $\implies$ $\theta = 1 - \varepsilon$

unconditionally one can obtain $\theta = 1 - \varepsilon$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

$$abc\text{-conjecture} \implies \theta = 1 - \varepsilon$$

unconditionally one can obtain $\theta = 1 - \varepsilon$

(ineffective)

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Effective Approach:

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Effective Approach: (Linear Forms of Logarithms)

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Effective Approach: (Linear Forms of Logarithms)

$$\theta = \frac{c}{\log \log n}$$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Effective Approach: (Linear Forms of Logarithms)

$$\theta = \frac{c}{\log \log n}$$

Problem: Can we narrow the gap between these ineffective and effective results?

Some Motivation:

Some Motivation:

Theorem (R. Gow, 1989): If $n > 2$ is even and

$$L_n^{(n)}(x) = \sum_{j=0}^{n} \binom{2n}{n-j} \frac{(-x)^j}{j!}$$

is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Some Motivation:

Theorem (R. Gow, 1989): If $n > 2$ is even and

$$L_n^{(n)}(x) = \sum_{j=0}^{n} \binom{2n}{n-j} \frac{(-x)^j}{j!}$$

is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Theorem (joint work with R. Williams): For almost all positive integers n the polynomial $L_n^{(n)}(x)$ is irreducible (and, hence, has Galois group A_n for almost all even n).

Some Motivation:

Theorem (R. Gow, 1989): If $n > 2$ is even and

$$L_n^{(n)}(x) = \sum_{j=0}^{n} \binom{2n}{n-j} \frac{(-x)^j}{j!}$$

is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Theorem (joint work with R. Williams): For almost all positive integers n the polynomial $L_n^{(n)}(x)$ is irreducible (and, hence, has Galois group A_n for almost all even n).

Work in Progress with Trifonov: We're attempting to show the irreducibility of $L_n^{(n)}(x)$ for all $n > 2$.

Some Motivation:

Theorem (R. Gow, 1989): If $n > 2$ is even and

$$L_n^{(n)}(x) = \sum_{j=0}^{n} \binom{2n}{n-j} \frac{(-x)^j}{j!}$$

is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Theorem (joint work with R. Williams): For almost all positive integers n the polynomial $L_n^{(n)}(x)$ is irreducible (and, hence, has Galois group A_n for almost all even n).

Work in Progress with Trifonov: $L_n^{(n)}(x)$ is irreducible for n large and $n \equiv 2 \pmod{4}$.

Some Motivation:

Theorem (R. Gow, 1989): If $n > 2$ is even and

$$L_n^{(n)}(x) = \sum_{j=0}^{n} \binom{2n}{n-j} \frac{(-x)^j}{j!}$$

is irreducible, then the Galois group of $L_n^{(n)}(x)$ is A_n.

Theorem (joint work with R. Williams): For almost all positive integers n the polynomial $L_n^{(n)}(x)$ is irreducible (and, hence, has Galois group A_n for almost all even n).

Work in Progress with Trifonov: $L_n^{(n)}(x)$ is irreducible for n large and $n \equiv 2 \pmod{4}$. This is effective.

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Theorem: If $n \geq 9$ and

$$n(n+1) = 2^k 3^\ell m,$$

then

$$m \geq$$

Want: Let $p_1, p_2, \ldots, p_r$ be primes. There is an $N = N(\theta, p_1, \ldots, p_r)$ such that if $n \geq N$ and

$$n(n+1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m$$

for some integer m, then $m > n^{\theta}$.

Theorem: If $n \geq 9$ and

$$n(n+1) = 2^k 3^{\ell} m,$$

then

$$m \geq n^{1/4}.$$

Conjecture: For $n > 512$,

$$n(n+1) = 2^u 3^v m \implies m > \sqrt{n}.$$

Conjecture: For $n > 512$,

$$n(n+1) = 2^u 3^v m \implies m > \sqrt{n}.$$

Comment: The conclusion holds for

$$512 < n \leq$$

Conjecture: For $n > 512$,

$$n(n+1) = 2^u 3^v m \implies m > \sqrt{n}.$$

Comment: The conclusion holds for

$$512 < n \leq 10^{1000}.$$

Part II: On the non-factorization of $x^2 + 7$

Part II: On the non-factorization of $x^2 + 7$

Classical Ramanujan-Nagell Theorem: If x and n are positive integers satisfying

$$x^2 + 7 = 2^n,$$

then

$$x \in \{1, 3, 5, 11, 181\}.$$

Part II: On the non-factorization of $x^2 + 7$

Classical Ramanujan-Nagell Theorem: If x and n are positive integers satisfying

$$x^2 + 7 = 2^n,$$

then

$$x \in \{1, 3, 5, 11, 181\}.$$

Problem: If $x^2 + 7 = 2^n m$ and x is not in the set above, then can we say that m must be large?

Problem: If $x^2 + 7 = 2^n m$ and x is not in the set above, then can we say that m must be large?

Connection with Part I:

Problem: If $x^2 + 7 = 2^n m$ and x is not in the set above, then can we say that m must be large?

Connection with Part I:

$$x^2 + 7 = 2^n m$$

Problem: If $x^2+7=2^n m$ and x is not in the set above, then can we say that m must be large?

Connection with Part I:

$$x^2+7=2^n m$$

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)=\left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2} m$$

Problem: If $x^2 + 7 = 2^n m$ and x is not in the set above, then can we say that m must be large?

Connection with Part I:

$$x^2 + 7 = 2^n m$$

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n-2} m$$

↑ ↑ ↑ ↑

difference is constant — prime — prime

Theorem: If x, n and m are positive integers satisfying

$$x^2 + 7 = 2^n m \quad \text{and} \quad x \notin \{1, 3, 5, 11, 181\},$$

then

$$m \geq \text{???}$$

Theorem: If x, n and m are positive integers satisfying

$$x^2 + 7 = 2^n m \quad \text{and} \quad x \notin \{1, 3, 5, 11, 181\},$$

then

$$m \geq x^{1/2}.$$

Part III: The Method

Part III: Beukers’ Method

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E.$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E.$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1 \quad \leftarrow \ \times Q$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E. \quad \leftarrow \ \times m_2$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E.$$

Then

$$3^k (Q m_1 - P m_2) = \pm Q - E m_2.$$

Part III: Beukers' Method

$$n(n+1) = 3^k 2^\ell m$$

$$3^k m_1 - 2^\ell m_2 = \pm 1$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E.$$

Then

$$3^k \left(Q m_1 - P m_2 \right) = \pm Q - E m_2.$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E$$

and

$$Q m_1 - P m_2 \neq 0.$$

Then

$$3^k \left(Q m_1 - P m_2\right) = \pm Q - E m_2.$$

Main Idea: Find "small" integers P, Q, and E such that

$$3^k P - 2^\ell Q = E$$

and

$$Q m_1 - P m_2 \neq 0.$$

Then

$$3^k (Q m_1 - P m_2) = \pm Q - E m_2.$$

Obtain an upper bound on 3^k.

Main Idea: Find “small” integers P, Q, and E such that

$$3^k P - 2^\ell Q = E$$

and

$$Qm_1 - Pm_2 \neq 0.$$

Then

$$3^k\,(Qm_1 - Pm_2) = \pm Q - Em_2.$$

Obtain an upper bound on 3^k. Since $3^k m_1 \geq n$, it follows that m_1 and, hence, $m = m_1 m_2$ are not small.

The "small" integers P, Q, and E are obtained through the use of Padé approximations for $(1 - x)^k$.

The “small” integers P, Q, and E are obtained through the use of Padé approximations for $(1-x)^k$.

More precisely, there exist P, Q, and E in $\mathbb{Z}[x]$ with $\deg P = \deg Q = r$ and $\deg E = k - r - 1$ such that

$$P_r(x) - (1-x)^k Q_r(x) = x^{2r+1} E_r(x).$$

What’s Needed for the Method to Work:

What's Needed for the Method to Work:

One largely needs to be dealing with two primes (like 2 and 3) with a difference of powers of these primes being small (like $\mathbf{3^2 - 2^3 = 1}$).

What's Needed for the Method to Work:

One largely needs to be dealing with two primes (like 2 and 3) with a difference of powers of these primes being small (like $3^2 - 2^3 = 1$).

In the case of $x^2 + 7 = 2^n m$, the difference of the primes $(1 + \sqrt{-7})/2$ and $(1 - \sqrt{-7})/2$ each raised to the 13^{th} power has absolute value ≈ 2.65 and the prime powers themselves have absolute value ≈ 90.51.