Curious patterns in the divisors of $x^n - 1$

Lola Thompson

Oberlin College Talk

January 11, 2011

The "building blocks" of polynomials

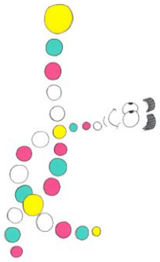


Figure: "D.N.A., the building blocks of life." - Jurassic Park

Primes are the "building blocks" of integers: every positive integer (except 1) can be written uniquely as a product of primes.

What are the "building blocks" of polynomials?

The “building blocks” of polynomials

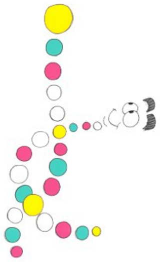


Figure: “D.N.A., the building blocks of life.” - Jurassic Park

Primes are the “building blocks” of integers: every positive integer (except 1) can be written uniquely as a product of primes.

What are the “building blocks” of polynomials?

Polynomials that cannot be factored any further. These are called *irreducible polynomials*.

The “building blocks” of polynomials

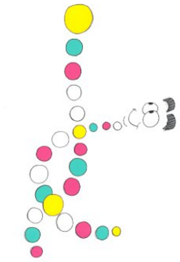


Figure: “D.N.A., the building blocks of life.” - Jurassic Park

Primes are the “building blocks” of integers: every positive integer (except 1) can be written uniquely as a product of primes.

What are the “building blocks” of polynomials?

Polynomials that cannot be factored any further. These are called *irreducible polynomials*.

Example $x^3 - 1 = (x-1)(x^2+x+1)$.

Polynomial divisors of $x^n - 1$

Let's examine what the "building blocks" of polynomials of the form $x^n - 1$ look like...

Fact: For every n, there is a unique irreducible polynomial that divides $x^n - 1$ but does not divide $x^k - 1$ for any $k < n$.

We denote this polynomial $\Phi_n(x)$ and call it the n^{th} *cyclotomic polynomial*.

Polynomial divisors of $x^n - 1$

Let's examine what the "building blocks" of polynomials of the form $x^n - 1$ look like...

Fact: For every n, there is a unique irreducible polynomial that divides $x^n - 1$ but does not divide $x^k - 1$ for any $k < n$.

We denote this polynomial $\Phi_n(x)$ and call it the n^{th} *cyclotomic polynomial*.

Example $x^2 + 1$ divides $x^4 - 1$.

Polynomial divisors of $x^n - 1$

Let's examine what the "building blocks" of polynomials of the form $x^n - 1$ look like...

Fact: For every n, there is a unique irreducible polynomial that divides $x^n - 1$ but does not divide $x^k - 1$ for any $k < n$.

We denote this polynomial $\Phi_n(x)$ and call it the n^{th} *cyclotomic polynomial*.

Example $x^2 + 1$ divides $x^4 - 1$.
It does not divide $x^3 - 1$, $x^2 - 1$ or $x - 1$.

Polynomial divisors of $x^n - 1$

Let's examine what the "building blocks" of polynomials of the form $x^n - 1$ look like...

Fact: For every n, there is a unique irreducible polynomial that divides $x^n - 1$ but does not divide $x^k - 1$ for any $k < n$.

We denote this polynomial $\Phi_n(x)$ and call it the n^{th} *cyclotomic polynomial*.

Example $x^2 + 1$ divides $x^4 - 1$.
It does not divide $x^3 - 1$, $x^2 - 1$ or $x - 1$.
So, $\Phi_4(x) = x^2 + 1$.

More Examples of Cyclotomic Polynomials

$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$

It turns out that $x^n - 1$ is a product of cyclotomic polynomials. More precisely, $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

More Examples of Cyclotomic Polynomials

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$

It turns out that $x^n - 1$ is a product of cyclotomic polynomials. More precisely, $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Example $x^4 - 1 = (x-1)(x+1)(x^2+1) = \Phi_1(x)\Phi_2(x)\Phi_4(x)$.

Outline

Heights of Polynomials

Definition

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value.

Q: What are the heights of the first 8 cyclotomic polynomials?

$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$

Heights of Polynomials

Definition

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value.

Q: What are the heights of the first 8 cyclotomic polynomials?

$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$

A: 1 (for all of them!)

Heights of $\Phi_n(x)$, $1 \leq n \leq 50$

n	Height	n	Height	n	Height	n	Height	n	Height
1	1	11	1	21	1	31	1	41	1
2	1	12	1	22	1	32	1	42	1
3	1	13	1	23	1	33	1	43	1
4	1	14	1	24	1	34	1	44	1
5	1	15	1	25	1	35	1	45	1
6	1	16	1	26	1	36	1	46	1
7	1	17	1	27	1	37	1	47	1
8	1	18	1	28	1	38	1	48	1
9	1	19	1	29	1	39	1	49	1
10	1	20	1	30	1	40	1	50	1

Heights of $\Phi_n(x)$, $51 \leq n \leq 100$

n	Height	n	Height	n	Height	n	Height	n	Height
51	1	61	1	71	1	81	1	91	1
52	1	62	1	72	1	82	1	92	1
53	1	63	1	73	1	83	1	93	1
54	1	64	1	74	1	84	1	94	1
55	1	65	1	75	1	85	1	95	1
56	1	66	1	76	1	86	1	96	1
57	1	67	1	77	1	87	1	97	1
58	1	68	1	78	1	88	1	98	1
59	1	69	1	79	1	89	1	99	1
60	1	70	1	80	1	90	1	100	1

Motivation for Study

- We observed in the previous slide that $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Any conjectures?

Motivation for Study

- We observed in the previous slide that $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Any conjectures?
- It's tempting to guess that the height of a cyclotomic polynomial is always 1. However, the pattern breaks down at $\Phi_{105}(x)$:

Motivation for Study

- We observed in the previous slide that $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Any conjectures?

- It's tempting to guess that the height of a cyclotomic polynomial is always 1. However, the pattern breaks down at $\Phi_{105}(x)$:

- $\Phi_{105}(x) = 1 + x + x^2 - x^5 - x^6 - \mathbf{2}x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} - x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} - x^{39} - x^{40} - \mathbf{2}x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}$

Motivation for Study

- We observed in the previous slide that $\Phi_1(x), \Phi_2(x), ..., \Phi_{100}(x)$ all have height 1, i.e. all of the coefficients are in the set $\{0, \pm 1\}$. Any conjectures?

- It's tempting to guess that the height of a cyclotomic polynomial is always 1. However, the pattern breaks down at $\Phi_{105}(x)$:

- $\Phi_{105}(x) = 1 + x + x^2 - x^5 - x^6 - \mathbf{2}x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} - x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} - x^{39} - x^{40} - \mathbf{2}x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}$

- So $\Phi_{105}(x)$ has height 2!

Motivation for Study

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

Motivation for Study

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

- The answer to (1) is known. The height can get arbitrarily large.

Motivation for Study

The fact that $\Phi_n(x)$ has height 1 when $n \leq 104$ and $\Phi_{105}(x)$ has height 2 leads to some natural questions:

(1) Can the height of $\Phi_n(x)$ get larger than 2? How large can it get?

(2) How quickly does the height of $\Phi_n(x)$ grow? Can we find an upper bound for it?

- The answer to (1) is known. The height can get arbitrarily large.
- In this talk, we'll answer (2) and give a generalization of this result to a larger family of polynomials.

Erratic Functions

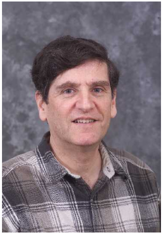
Figure: Record Snowfall

Everyone likes records (record snowfall, record number of home runs,...).

When faced with an erratic function $f(n)$, we want to know: "what is its record behavior?" How large can it get? How small?

On the other hand, we would also like to know: "how does $f(n)$ behave typically?"

"Champion" Upper Bound


Theorem (Bateman, Pomerance, Vaughan)

Let $A(n)$ denote the height of $\Phi_n(x)$. Let k be the number of distinct prime factors of n. Then $A(n) \leq n^{2^{k-1}/k-1}$.

"Typical" Upper Bound

Theorem (Maier)

Let $\psi(n)$ be **any** *function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Let $A(n)$ denote the height of $\Phi_n(x)$. Then $A(n) \leq n^{\psi(n)}$ for almost all n.*

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$?

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$? 3

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$? 3

Example: $6 = 2 \cdot 3 = 1 \cdot 6$. What is $d(6)$?

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$? 3

Example: $6 = 2 \cdot 3 = 1 \cdot 6$. What is $d(6)$? 4

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$? 3

Example: $6 = 2 \cdot 3 = 1 \cdot 6$. What is $d(6)$? 4

Example: Let p be *any* prime. What is $d(p)$?

A few new functions

Let $d(n)$ denote the number of positive divisors of n.

Example: $4 = 2 \cdot 2 = 1 \cdot 4$. What is $d(4)$? 3

Example: $6 = 2 \cdot 3 = 1 \cdot 6$. What is $d(6)$? 4

Example: Let p be *any* prime. What is $d(p)$? 2

A few new functions

Recall: $A(n)$ is the height of $\Phi_n(x)$.

Let $B(n)$ denote the maximal height over **all** polynomial divisors of $x^n - 1$.

A few new functions

Recall: $A(n)$ is the height of $\Phi_n(x)$.

Let $B(n)$ denote the maximal height over **all** polynomial divisors of $x^n - 1$.

Example $B(6) = 2$. Why?

A few new functions

Recall: $A(n)$ is the height of $\Phi_n(x)$.

Let $B(n)$ denote the maximal height over **all** polynomial divisors of $x^n - 1$.

Example $B(6) = 2$. Why?

- Factor $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.

A few new functions

Recall: $A(n)$ is the height of $\Phi_n(x)$.

Let $B(n)$ denote the maximal height over **all** polynomial divisors of $x^n - 1$.

Example $B(6) = 2$. Why?

- Factor $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
- Observe that $(x+1)(x^2+x+1) = x^3 + 2x^2 + 2x + 1$.

A few new functions

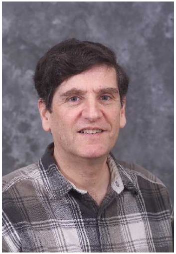
Recall: $A(n)$ is the height of $\Phi_n(x)$.

Let $B(n)$ denote the maximal height over **all** polynomial divisors of $x^n - 1$.

Example $B(6) = 2$. Why?

- Factor $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
- Observe that $(x+1)(x^2+x+1) = x^3 + 2x^2 + 2x + 1$.
- Check that the other divisors of $x^6 - 1$ only have coefficients ≤ 2 (in absolute value).

"Champion" Upper Bound

Theorem (Pomerance, Ryan)

Let $B(n)$ denote the maximal height over all divisors of $x^n - 1$. For all sufficiently large n, we have $B(n) \leq e^{n^{(\log 3+\varepsilon)/\log\log n}}$.

“Typical” Upper Bound

Theorem (T.)

Let $\psi(n)$ be any function defined for all positive integers such that $\psi(n) \to \infty$ for $n \to \infty$. Then $B(n) \leq n^{d(n)\psi(n)}$ for almost all n.

Summary

- "Typically," the coefficients of divisors of $x^n - 1$ grow relatively slowly (at least, compared with "champion" n's).

Summary

- "Typically," the coefficients of divisors of $x^n - 1$ grow relatively slowly (at least, compared with "champion" n's).
- However, the coefficients of divisors of $x^n - 1$ **can** get very large on rare occasions.

Summary

- "Typically," the coefficients of divisors of $x^n - 1$ grow relatively slowly (at least, compared with "champion" n's).

- However, the coefficients of divisors of $x^n - 1$ **can** get very large on rare occasions.

- Thus, if we want a bound that holds for all n, it needs to be MUCH larger than the bound for "typical" n.

Switching Gears...

Degrees of divisors of $x^n - 1$

Instead of looking at the **coefficients** of divisors of $x^n - 1$, we could ask questions about the **degrees**.

How often does $x^n - 1$ have a divisor of every degree between 1 and n?

Degrees of divisors of $x^n - 1$

Instead of looking at the **coefficients** of divisors of $x^n - 1$, we could ask questions about the **degrees**.

How often does $x^n - 1$ have a divisor of every degree between 1 and n?

Example $n = 6$
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

Degrees of divisors of $x^n - 1$

Instead of looking at the **coefficients** of divisors of $x^n - 1$, we could ask questions about the **degrees**.

How often does $x^n - 1$ have a divisor of every degree between 1 and n?

Example $n = 6$
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$
So, $x^6 - 1$ has a divisor of every degree

When does $x^n - 1$ have a divisor of every degree?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Table: $n \leq 100$ with this property

A related problem

Definition

A positive integer n is **practical** if every m with $1 \leq m \leq n$ can be written as a sum of distinct divisors of n.

Example. $n = 6$

$$\left.\begin{array}{r}
\text{Divisors: } 1, 2, 3, 6 \\
\text{Sums:} \qquad\qquad \\
1 \\
2 \\
3 \\
3+1 \\
3+2 \\
6
\end{array}\right\} \quad \therefore \text{ 6 is practical}$$

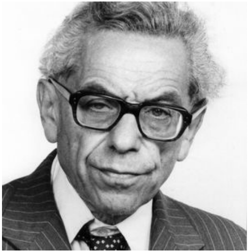
Practical numbers

Srinivasan coined the term ‘practical number’ in 1948. He attempted to classify them, remarking that

> *the revelation of the structure of these numbers is bound to open some good research in the theory of numbers... Our table shows that about 25 per cent of the first 200 natural numbers are ‘practical.’ It is a matter for investigation what percentage of the natural numbers will be ‘practical’ in the long run.*

Practical numbers

It was not long before Srinivasan's questions were answered.



In a 1950 paper, P. Erdős asserted (without proof) that the practical numbers have asymptotic density 0.

Practical numbers

More recent work has focused on counting the practical numbers:

Theorem (Saias, 1997)

Let $PR(X) = \#$ *of practical numbers in* $[1, X]$. *Then, for* $X \geq 2$*, there exist two positive constants* C_1 *and* C_2 *such that*

$$C_1 \frac{X}{\log X} \leq PR(X) \leq C_2 \frac{X}{\log X}.$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\gcd(1, 6) = 1$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\gcd(1, 6) = 1$$
$$\gcd(2, 6) = 2$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\gcd(1,6) = 1$$
$$\gcd(2,6) = 2$$
$$\gcd(3,6) = 3$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\begin{aligned} \gcd(1, 6) &= 1 \\ \gcd(2, 6) &= 2 \\ \gcd(3, 6) &= 3 \\ \gcd(4, 6) &= 2 \end{aligned}$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\begin{aligned} \gcd(1,6) &= 1 \\ \gcd(2,6) &= 2 \\ \gcd(3,6) &= 3 \\ \gcd(4,6) &= 2 \\ \gcd(5,6) &= 1 \end{aligned}$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\begin{aligned}
\gcd(1,6) &= 1\\
\gcd(2,6) &= 2\\
\gcd(3,6) &= 3\\
\gcd(4,6) &= 2\\
\gcd(5,6) &= 1\\
\gcd(6,6) &= 6
\end{aligned}$$

The φ function

Let $\varphi(n)$ denote the number of integers between 1 and n that are relatively prime to n.

Example $\varphi(6) = 2$, since:

$$\begin{aligned} \gcd(1,6) &= 1 \\ \gcd(2,6) &= 2 \\ \gcd(3,6) &= 3 \\ \gcd(4,6) &= 2 \\ \gcd(5,6) &= 1 \\ \gcd(6,6) &= 6 \end{aligned}$$

Example $\varphi(p) = p - 1$.

Practical vs. φ-Practical

Definition

A positive integer n is *φ-practical* if every m with $1 \leq m \leq n$ can be written as $\sum_{d \in \mathcal{D}} \varphi(d)$, where $\mathcal{D}$ is a subset of divisors of n.

Note: This is equivalent to the condition that $x^n - 1$ has a divisor of every degree between 1 and n.

φ-practical example

Example. $n = 6$

$$\left.\begin{aligned} \text{Divisors: } 1, 2, 3, 6 \\ \varphi \text{ values: } 1, 1, 2, 2 \\ \text{Sums of } \varphi \text{ values:} \\ 1 \\ 2 \\ 1+2 \\ 2+2 \\ 1+2+2 \\ 1+1+2+2 \end{aligned}\right\} \qquad \therefore 6 \text{ is } \varphi\text{-practical}$$

φ-practical numbers are rare

We can use an argument that is similar to Erdős' proof to show that the φ-practical numbers are very rare:

Theorem (T., 2010)

The set of φ-practical numbers has asymptotic density 0.

Counting the number of φ-practicals

In fact, we can obtain good upper and lower bounds for the size of the set of φ-practical numbers:

Theorem (T., 2011)

Let $F(X) = \#$ of φ-practical numbers in $[1, X]$. Then there exist positive constants C_1 and C_2 such that

$$C_1 \frac{X}{\log X} \leq F(X) \leq C_2 \frac{X}{\log X}.$$

Comparison with the prime numbers

What's the big deal about $X/\log X$?

Theorem (Chebyshev, 1852)

Let $\pi(X) = \#$ of primes in $[1, X]$. There exist positive constants C_1 and C_2 such that

$$C_1 \frac{X}{\log X} \leq \pi(X) \leq C_2 \frac{X}{\log X}.$$

Comparison with the prime numbers

The celebrated **Prime Number Theorem** says:


Theorem (Hadamard & de la Valée Poussin, 1896)

Let $\pi(X) = \#$ *of primes in* $[1, X]$*. Then, we have*

$$\lim_{X \to \infty} \frac{\pi(X)}{X/\log X} = 1.$$

An asymptotic estimate for the φ-practicals?

We can use Sage to compute $F(X)/\frac{X}{\log X}$:

X	$F(X)/(X/\log X)$
100	1.28944765207667
1000	1.20194941854289
10000	1.10339877656275
100000	1.07081719749688
1000000	1.02871673165658
10000000	1.02435010928622
100000000	1.01792184432701
1000000000	1.00271691477998

Table: Ratios for φ-practicals

Estimating the constants C_1 and C_2

The data seem to suggest:

$$\lim_{X\to\infty} \frac{F(X)}{X/\log X} = 1.$$

The Bad News:

The Good News:

Estimating the constants C_1 and C_2

The data seem to suggest:

$$\lim_{X\to\infty} \frac{F(X)}{X/\log X} = 1.$$

The Bad News: No one has been able to show that

$$\lim_{X\to\infty} \frac{PR(X)}{X/\log X}$$

even exists!

The Good News:

Estimating the constants C_1 and C_2

The data seem to suggest:

$$\lim_{X\to\infty} \frac{F(X)}{X/\log X} = 1.$$

The Bad News: No one has been able to show that

$$\lim_{X\to\infty} \frac{PR(X)}{X/\log X}$$

even exists!

The Good News: We still have $43\frac{1}{2}$ years to catch up with Hadamard and de la Valée Poussin!

Summary

- Most of the time, $x^n - 1$ **does not** have a divisor of every degree between 1 and n.

Summary

- Most of the time, $x^n - 1$ **does not** have a divisor of every degree between 1 and n.

- We can get an estimate for the number of integers in $[1, X]$ that **do** have this property.

Summary

- Most of the time, $x^n - 1$ **does not** have a divisor of every degree between 1 and n.
- We can get an estimate for the number of integers in $[1, X]$ that **do** have this property.
- The count is similar to the number of primes in $[1, X]$.

Summary

- Most of the time, $x^n - 1$ **does not** have a divisor of every degree between 1 and n.
- We can get an estimate for the number of integers in $[1, X]$ that **do** have this property.
- The count is similar to the number of primes in $[1, X]$.
- There is still plenty of work to be done.

Where do we go from here?

- So far, we have only discussed what happens when we factor $x^n - 1$ into polynomials with integer coefficients.

Where do we go from here?

- So far, we have only discussed what happens when we factor $x^n - 1$ into polynomials with integer coefficients.

- We have been able to answer the same questions when we factor $x^n - 1$ in other systems (for example, "mod p").

Where do we go from here?

- So far, we have only discussed what happens when we factor $x^n - 1$ into polynomials with integer coefficients.
- We have been able to answer the same questions when we factor $x^n - 1$ in other systems (for example, "mod p").
- We have even been able to prove results of this nature for much more general rings...

Where do we go from here?

- So far, we have only discussed what happens when we factor $x^n - 1$ into polynomials with integer coefficients.
- We have been able to answer the same questions when we factor $x^n - 1$ in other systems (for example, "mod p").
- We have even been able to prove results of this nature for much more general rings...
- But that's a talk for another day!

Analogues of other famous problems

Conjecture (“Goldbach's Conjecture”)

Every even integer greater than 2 *can be expressed as a sum of two primes.*

Conjecture ("Twin Prime Conjecture")

There are infinitely many integers n *for which* n *and* $n + 2$ *are both prime.*

Analogues of other famous problems

Conjecture ("Goldbach's Conjecture")

Every even integer greater than 2 can be expressed as a sum of two primes.

Conjecture ("Twin Prime Conjecture")

There are infinitely many integers n for which n and $n + 2$ are both prime.

These conjectures are actually theorems (!) when the word "prime" is replaced with "practical number."

Analogues of other famous problems

Conjecture ("Goldbach's Conjecture")

Every even integer greater than 2 can be expressed as a sum of two primes.

Conjecture ("Twin Prime Conjecture")

There are infinitely many integers n for which n and $n + 2$ are both prime.

These conjectures are actually theorems (!) when the word "prime" is replaced with "practical number."

Open Question: Do the same theorems hold for the φ-practical numbers?

Analogues of other famous problems

Conjecture ("Goldbach's Conjecture")

Every even integer greater than 2 *can be expressed as a sum of two primes.*

Conjecture ("Twin Prime Conjecture")

There are infinitely many integers n for which n and $n+2$ are both prime.

These conjectures are actually theorems (!) when the word "prime" is replaced with "practical number."

Open Question: Do the same theorems hold for the φ-practical numbers? (This would make a fantastic student project...)

Thank You!