The degrees of the polynomial divisors of $x^n - 1$

Paul Pollack & Lola Thompson

University of Georgia

October 21, 2012

Introduction

Recall that over $\mathbb{Z}$,

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x),$$

where $\Phi_d(x) \in \mathbb{Z}[x]$ is the dth cyclotomic polynomial.

Introduction

Recall that over $\mathbb{Z}$,

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where $\Phi_d(x) \in \mathbb{Z}[x]$ is the dth cyclotomic polynomial.

The polynomials $\Phi_d(x)$ are irreducible. Since $\deg \Phi_d(x) = \varphi(d)$, the set of degrees of polynomial divisors of $\Phi_d(x)$ is the set of subset sums of the multiset $\{\varphi(d) : d \mid n\}$.

Question

As n ranges over the natural numbers, how does the set of degrees of divisors of $x^n - 1$ behave?

Three possible questions

Let's be more precise. Here are three questions we could ask, each of a statistical nature:

Three possible questions

Let's be more precise. Here are three questions we could ask, each of a statistical nature:

Question: How often does $x^n - 1$ ...

- have **at least one** divisor of each degree $0 \le m \le n$?

Three possible questions

Let's be more precise. Here are three questions we could ask, each of a statistical nature:

Question: How often does $x^n - 1$ ...

- have **at least one** divisor of each degree $0 \leq m \leq n$?
- have **at most one** divisor of each degree $0 \leq m \leq n$?

Three possible questions

Let's be more precise. Here are three questions we could ask, each of a statistical nature:

Question: How often does $x^n - 1 \ldots$

- have **at least one** divisor of each degree $0 \le m \le n$?
- have **at most one** divisor of each degree $0 \le m \le n$?
- have **exactly one** divisor of each degree $0 \le m \le n$?

How often does $x^n - 1$ ...

...have **at least one** divisor of each degree?

How often does $x^n - 1$ ...

... have **at least one** divisor of each degree?

Example

$n = 6$.
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
So, $x^6 - 1$ has ≥ 1 divisor of each degree.

... have **at least one** divisor of each degree?

Example

$n = 6$.
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
So, $x^6 - 1$ has ≥ 1 divisor of each degree.

How often does $x^n - 1$ ...

... have **at least one** divisor of each degree?

Example

$n = 6$.
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
So, $x^6 - 1$ has ≥ 1 divisor of each degree.

Equivalent question: How often is every integer between 0 and n a subsum of degrees of irreducible divisors of $x^n - 1$?

How often does $x^n - 1$ ...

... have **at least one** divisor of each degree?

Example

$n = 6$.
$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$.
So, $x^6 - 1$ has ≥ 1 divisor of each degree.

Equivalent question: How often is every integer between 0 and n a subsum of degrees of irreducible divisors of $x^n - 1$?

Definition

An integer n with the above property is called $\mathbb{Q}$-**practical**.

When does $x^n - 1$ have at least one divisor of each 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 : $\mathbb{Q}$-practical values of $n \leq 100$

Counting the number of $\mathbb{Q}$-practicals

From Lola Thompson's Ph.D. thesis:

Definition

Let $F(X)$ denote the number of $\mathbb{Q}$-practical integers belonging to the interval $[1, X]$.

Theorem (Thompson, 2012)

There exist two positive constants C_1 and C_2 so that for $X \geq 2$, we have

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

An asymptotic estimate?

Table : Comparison of $\mathbb{Q}$-practical counts with $X/\log X$

X	$F(X)/(X/\log X)$
10^4	1.10339877656275
10^5	1.07081719749688
10^6	1.02871673165658
10^7	1.02435010928622
10^8	1.01792184432701
10^9	1.00271691477998

An asymptotic estimate?

Table : Comparison of $\mathbb{Q}$-practical counts with $X/\log X$

X	$F(X)/(X/\log X)$
10^4	1.10339877656275
10^5	1.07081719749688
10^6	1.02871673165658
10^7	1.02435010928622
10^8	1.01792184432701
10^9	1.00271691477998

Question

Is there a "$\mathbb{Q}$-practical number theorem" stating that $F(X) \sim X/\log X$?

... have **at most one** divisor of each degree?

A natural dual to the notion of $\mathbb{Q}$-practical:

Definition

A positive integer n is **$\mathbb{Q}$-efficient** if $x^n - 1$ has **at most one** monic divisor in $\mathbb{Q}[x]$ of each degree $m \in [0, n]$.

How often does $x^n - 1$...

... have **at most one** divisor of each degree?

A natural dual to the notion of $\mathbb{Q}$-practical:

Definition

A positive integer n is **$\mathbb{Q}$-efficient** if $x^n - 1$ has **at most one** monic divisor in $\mathbb{Q}[x]$ of each degree $m \in [0, n]$.

Example

77 is $\mathbb{Q}$-efficient since the multiset of totients of its divisors consists of $1, 6, 10, 60$, whose subset sums are the sixteen *distinct* integers 0, 1, 6, 7, 10, 11, 16, 17, 60, 61, 66, 67, 70, 71, 76, 77.

When does $x^n - 1$ have ≤ 1 divisor of each 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 : $\mathbb{Q}$-efficient values of $n \leq 100$

$\mathbb{Q}$-efficient

Theorem (P., Thompson)

The set of $\mathbb{Q}$-efficient numbers has positive asymptotic density.

A sketch of the argument

Let's call a number **inefficient** if it is not $\mathbb{Q}$-efficient.

Observation

If n is inefficient, then every multiple of n is also inefficient.

A sketch of the argument

Let's call a number **inefficient** if it is not $\mathbb{Q}$-efficient.

Observation

If n is inefficient, then every multiple of n is also inefficient.

Definition

Call n **primitive inefficient** if n is inefficient but every proper divisor of n is efficient.

Then the set of inefficients is exactly the set of numbers with at least one primitive inefficient divisor; in other words, it is the **set of multiples** of the primitive inefficient numbers.

More sketchiness

Definition

A set A of natural numbers is called **thin** if as $T \to \infty$, the set of integers n with a divisor in $A \cap [T, \infty)$ has upper density tending to zero.

More sketchiness

Definition

A set A of natural numbers is called **thin** if as $T \to \infty$, the set of integers n with a divisor in $A \cap [T, \infty)$ has upper density tending to zero.

Theorem (Erdős)

If A is a thin set of natural numbers, then the set of multiples of A possesses an asymptotic density. If $1 \notin A$, then this density is strictly less than 1.

More sketchiness

Definition

A set A of natural numbers is called **thin** if as $T \to \infty$, the set of integers n with a divisor in $A \cap [T, \infty)$ has upper density tending to zero.

Theorem (Erdős)

If A is a thin set of natural numbers, then the set of multiples of A possesses an asymptotic density. If $1 \notin A$, then this density is strictly less than 1.

Proposition (P & T, using an idea of Erdős)

The set of primitive inefficient numbers is a thin set not containing 1.

...have **exactly one** divisor of each 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 : $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient $n \leq 100$

Exactly 1 divisor of each degree

Theorem (P., Thompson)

There are precisely six integers that are both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient, namely $2^{2^i} - 1$ for $i = 0, \dots, 5$.

Example

Taking $i = 3$ gives the number 255, and the multiset of $\varphi(d)$ for $d \mid 255$ is exactly $\{1, 2, 4, 8, 16, 32, 64, 128\}$.

In fact, for all of these examples, the multiset of $\varphi(d)$ for $d \mid 2^{2^i} - 1$ is exactly the set of consecutive powers of 2 up to $2^{2^i - 1}$.

Exactly 1 divisor of each degree

Theorem (P., Thompson)

There are precisely six integers that are both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient, namely $2^{2^i} - 1$ for $i = 0, \ldots, 5$.

Sketch of proof (necessity): If n is both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient, then we have an identity of generating functions (in the variable T):

$$\prod_{d|n}(1 + T^{\varphi(d)}) = \sum_{m=0}^{n} T^m = \frac{T^{n+1} - 1}{T - 1}.$$

Exactly 1 divisor of each degree

Theorem (P., Thompson)

There are precisely six integers that are both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient, namely $2^{2^i} - 1$ for $i = 0, \ldots, 5$.

Sketch of proof (necessity): If n is both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient, then we have an identity of generating functions (in the variable T):

$$\prod_{d|n}(1 + T^{\varphi(d)}) = \sum_{m=0}^{n} T^m = \frac{T^{n+1} - 1}{T - 1}.$$

Plug in $T = 1$. With $D = \tau(n)$, we get

$$2^D = n + 1, \quad \text{so} \quad n = 2^D - 1.$$

Since $n = 2^D - 1$, we have

$$\frac{T^{n+1} - 1}{T - 1} = \frac{T^{2^D} - 1}{T - 1}$$
$$= (T+1)(T^2+1)(T^4+1)\cdots(T^{2^{D-1}}+1).$$

This product is supposed to be the same as the D-term product

$$\prod_{d \mid n} (1 + T^{\varphi(d)}).$$

This forces the multiset of values $\varphi(d)$ to be exactly

$$1, 2, 4, 8, \ldots, 2^{D-1}.$$

In particular, $\varphi(p) = p - 1$ is a power of 2 for each $p \mid n$, and so each prime divisor of n is a Fermat number

$$F_j := 2^{2^j} + 1.$$

Additional elementary considerations show the prime factorization of n has to look like $F_0 F_1 \cdots F_i$ for some i. But F_5 is not prime! So the only examples with $n > 1$ are

$$F_0 F_1 F_2 \dots F_i,$$

for $0 \le i \le 4$. Since

$$F_0 F_1 \cdots F_i = 2^{2^{i+1}} - 1,$$

we obtain the list given in our theorem.

How do these results change...

...if we factor $x^n - 1$ in $\mathbb{F}_p[x]$?

Efficient numbers become much less common: For example, if n is odd, then $\Phi_n(x)$ already has two distinct divisors in $\mathbb{F}_2[x]$ of the same degree unless 2 is a primitive root mod n. So our second and third questions take on a very different feel. But we can still ask the first question essentially verbatim.

Definition

We say that an integer n is $\mathbb{F}_p$-**practical** if $x^n - 1$ has a divisor of every degree between 0 and n in $\mathbb{F}_p[x]$.

Counting the $\mathbb{F}_p$-practicals up to X

Notation:
For each rational prime p, let

$$F_p(X) = \#\{n \le X : n \text{ is } \mathbb{F}_p\text{-practical}\}.$$

Computations in Sage yield the following table of ratios:

X	$F_2(X)/(X/\log X)$
10^2	1.56575786323595
10^3	1.67858453279266
10^4	1.64865092658374
10^5	1.69274543111457
10^6	1.66167434786971
10^7	1.66061354691737

Table : Ratios for $\mathbb{F}_2$-practicals

A conjecture

Our computational results seem to suggest the following conjecture:

Conjecture

Let p be a rational prime. Then, for X sufficiently large, we have

$$F_p(X) \ll \frac{X}{\log X}.$$

What we can actually show

From Thompson's Ph.D. thesis:

Theorem (Thompson)

Assuming GRH, for each prime p, we have

$$F_p(X) \ll X\sqrt{\frac{\log\log X}{\log X}}.$$

Thank you!