On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

University of Georgia

February 6, 2013

Introduction

Definition

Let $\Phi_n(x)$ denote the n^{th} *cyclotomic polynomial*, which we define in the following manner:

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has the following properties:

- $\Phi_n(x) \in \mathbb{Z}[x]$

Introduction

Definition

Let $\Phi_n(x)$ denote the n^{th} *cyclotomic polynomial*, which we define in the following manner:

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has the following properties:

- $\Phi_n(x) \in \mathbb{Z}[x]$
- monic

Introduction

Definition

Let $\Phi_n(x)$ denote the n^{th} *cyclotomic polynomial*, which we define in the following manner:

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has the following properties:

- $\Phi_n(x) \in \mathbb{Z}[x]$
- monic
- irreducible

Introduction

Definition

Let $\Phi_n(x)$ denote the n^{th} *cyclotomic polynomial*, which we define in the following manner:

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n^{th} \text{ root of } 1}} (x - \zeta).$$

$\Phi_n(x)$ has the following properties:

- $\Phi_n(x) \in \mathbb{Z}[x]$
- monic
- irreducible
- $\deg \Phi_n(x) = \varphi(n)$

Introduction

Moreover, we have the following identity:

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

Introduction

Moreover, we have the following identity:

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

In this talk, we will examine the degrees that occur for the (not necessarily irreducible) polynomial divisors of $x^n - 1$.

Introduction

Some natural questions:

Introduction

Some natural questions:

- How often does $x^n - 1$ have **at least one** divisor of each degree $1 \leq m \leq n$?

Introduction

Some natural questions:

- How often does $x^n - 1$ have **at least one** divisor of each degree $1 \leq m \leq n$?
- How often does $x^n - 1$ have **at most one** divisor of each degree $1 \leq m \leq n$?

Introduction

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Some natural questions:

- How often does $x^n - 1$ have **at least one** divisor of each degree $1 \leq m \leq n$?
- How often does $x^n - 1$ have **at most one** divisor of each degree $1 \leq m \leq n$?
- How often does $x^n - 1$ have **exactly one** divisor of each degree $1 \leq m \leq n$?

Introduction

Some natural questions:

- How often does $x^n - 1$ have **at least one** divisor of each degree $1 \leq m \leq n$?
- How often does $x^n - 1$ have **at most one** divisor of each degree $1 \leq m \leq n$?
- How often does $x^n - 1$ have **exactly one** divisor of each degree $1 \leq m \leq n$?
- For a given m, how often does $x^n - 1$ have a divisor of degree m?

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

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

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

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

Example $n = 6$

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

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

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

Example $n = 6$

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

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

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

Example $n = 6$

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

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

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

Example $n = 6$

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

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

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

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

Example $n = 6$

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

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

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

Example $n = 6$

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

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

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

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

Example $n = 6$

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

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.

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 : Values of $n \leq 100$ 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. $n = 6$

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

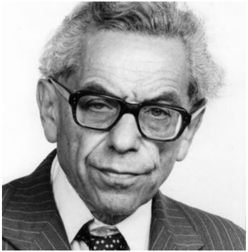
Practical numbers

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

Theorem (Saias, 1997)

There exist two constants C_1 and C_2 such that

$$C_1 \frac{X}{\log X} \le PR(X) \le C_2 \frac{X}{\log X},$$

where $PR(X) = \#\{n \le X : n \text{ is practical}\}$.

Practical vs. $\mathbb{Q}$-Practical

Definition

A positive integer n is $\mathbb{Q}$-*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.

$\mathbb{Q}$-practical example

Example. $n = 6$

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

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

We can prove the following analogue of Saias' result for the $\mathbb{Q}$-practical numbers:

Theorem (T.)

There exist two positive constants c_1 and c_2 such that

$$c_1 \frac{X}{\log X} \leq F(X) \leq c_2 \frac{X}{\log X},$$

where $F(X) = \#\{n \leq X : n \text{ is } \mathbb{Q}\text{-practical}\}$.

Proof of the upper bound

The proofs of Saias et al. relied heavily on the following:

Theorem (Stewart)

Let $n = p_1^{e_1} \cdots p_j^{e_j}$, $n > 1$, with $p_1 < p_2 < \cdots < p_j$ prime and $e_i \geq 1$ for $i = 1, ..., j$. Then n is practical iff for all $i = 1, ..., j$, $p_i \leq \sigma(p_1^{e_1} \cdots p_{i-1}^{e_{i-1}}) + 1$.

Unfortunately, there's no simple method for building up $\mathbb{Q}$-practical numbers from smaller ones.

Example $3^2 \times 5 \times 17 \times 257 \times 65537 \times (2^{31} - 1)$ is $\mathbb{Q}$-practical, but none of the numbers 3^2, $3^2 \times 5$, $3^2 \times 5 \times 17$, $3^2 \times 5 \times 17 \times 257$, $3^2 \times 5 \times 17 \times 257 \times 65537$ are $\mathbb{Q}$-practical.

Proof of the upper bound

Instead, we devise the following workaround:

Definition

Let $n = p_1^{e_1} \cdots p_k^{e_k}$. Let $m_i = p_1^{e_1} \cdots p_i^{e_i}$. We define an integer n to be *weakly $\mathbb{Q}$-practical* if the inequality $p_{i+1} \leq m_i + 2$ holds for all i.

Lemma

Every $\mathbb{Q}$-practical number is weakly $\mathbb{Q}$-practical.

Note: The converse does **not** hold. For example, 45 is not $\mathbb{Q}$-practical but it is weakly $\mathbb{Q}$-practical.

Proof of the upper bound

To prove our theorem, we consider two cases:

- If n is **even** & $\mathbb{Q}$-practical then $p_{i+1} \leq m_i + 2 \leq \sigma(m_i) + 1$ for all $i \geq 1$. Hence, each m_i satisfies the inequality in Stewart's Condition, so n is practical.

Proof of the upper bound

To prove our theorem, we consider two cases:

- If n is **even** & $\mathbb{Q}$-practical then $p_{i+1} \leq m_i + 2 \leq \sigma(m_i) + 1$ for all $i \geq 1$. Hence, each m_i satisfies the inequality in Stewart's Condition, so n is practical.
- On the other hand, observe that for every $n \in (0, X]$, there is a unique k such that $2^k n \in (X, 2X]$. Then, if n is **odd** & $\mathbb{Q}$-practical, $2^k n$ will be practical.

Proof of the upper bound

To prove our theorem, we consider two cases:

- If n is **even** & $\mathbb{Q}$-practical then $p_{i+1} \leq m_i + 2 \leq \sigma(m_i) + 1$ for all $i \geq 1$. Hence, each m_i satisfies the inequality in Stewart's Condition, so n is practical.
- On the other hand, observe that for every $n \in (0, X]$, there is a unique k such that $2^k n \in (X, 2X]$. Then, if n is **odd** & $\mathbb{Q}$-practical, $2^k n$ will be practical.
- Thus, $F(X) \leq PR(2X) \ll \frac{X}{\log X}$, by Saias' Theorem.

Lower Bound Proof Sketch

Saias obtains his lower bound by comparing the set of practical numbers with the set of integers with 2-dense divisors:

Definition

An integer n is 2-*dense* if $\max_{1 \le i \le \tau(n)-1} \frac{d_{i+1}(n)}{d_i(n)} \le 2$.

Note: All integers with 2-dense divisors are practical, but the same cannot be said about the $\mathbb{Q}$-practical numbers. For example, $n = 66$ is 2-dense but it is not $\mathbb{Q}$-practical.

Lower Bound Proof Sketch

We obtain our lower bound by comparing the set of $\mathbb{Q}$-practical numbers with the set of integers with strictly 2-dense divisors:

Definition

An integer n is *strictly 2-dense* if $\max_{1<i<\tau(n)-1} \frac{d_{i+1}(n)}{d_i(n)} < 2$ and $\frac{d_2(n)}{d_1(n)} = 2 = \frac{d_{\tau(n)}(n)}{d_{\tau(n)-1}(n)}$.

It turns out that all strictly 2-dense integers are $\mathbb{Q}$-practical.

Lower Bound Proof Sketch

- The main idea behind the proof is to show that a positive proportion of 2-dense integers are strictly 2-dense, except for some possible obstructions at small primes.

Lower Bound Proof Sketch

- The main idea behind the proof is to show that a positive proportion of 2-dense integers are strictly 2-dense, except for some possible obstructions at small primes.
- To do this, first we find an upper bound for the number of integers up to X that are 2-dense but not strictly 2-dense:

$$\sum_{k>C} \sum_{\substack{m \in (2^{k-1}, 2^k) \\ m \text{ 2-dense}}} \sum_{\substack{p \in (2^{k-1}, 2^{k+1}) \\ p \text{ prime}}} \sum_{\substack{j \le X/mp \\ mpj \text{ 2-dense} \\ P^-(j) > p}} 1. \quad (1)$$

Lower Bound Proof Sketch

- The main idea behind the proof is to show that a positive proportion of 2-dense integers are strictly 2-dense, except for some possible obstructions at small primes.
- To do this, first we find an upper bound for the number of integers up to X that are 2-dense but not strictly 2-dense:

$$\sum_{k>C} \sum_{\substack{m\in(2^{k-1},2^k) \\ m \text{ 2-dense}}} \sum_{\substack{p\in(2^{k-1},2^{k+1}) \\ p \text{ prime}}} \sum_{\substack{j\le X/mp \\ mpj \text{ 2-dense} \\ P^-(j)>p}} 1. \tag{1}$$

- Using sieve methods developed by Saias and Tenenbaum, along with Brun's sieve and other classical techniques from multiplicative number theory, we can show that the number counted in (1) is $\le \varepsilon \frac{X}{\log X}$.

Lower Bound Proof Sketch

- The final step is to show that a subset of the strictly 2-dense integers is in one-to-one correspondence with a positive proportion of the 2-dense integers with obstructions at $k < C$.

Corollary (T.)

For X sufficiently large, we have

$$\#\{n \le X : n \text{ is practical but not } \mathbb{Q}\text{-practical}\} \gg \frac{X}{\log X}.$$

Moreover, we also have

$$\#\{n \le X : n \text{ is } \mathbb{Q}\text{-practical but not practical}\} \gg \frac{X}{\log X}.$$

Comparison with the prime numbers

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

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 $\mathbb{Q}$-practicals?

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

X	$F(X)/(X/\log X)$
10^2	1.28944765207667
10^3	1.20194941854289
10^4	1.10339877656275
10^5	1.07081719749688
10^6	1.02871673165658
10^7	1.02435010928622
10^8	1.01792184432701
10^9	1.00271691477998

Table : Ratios for $\mathbb{Q}$-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!

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

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

...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 $m \in [1, n]$.

Example: 255 is $\mathbb{Q}$-efficient since the totients of its divisors are: $1, 2, 4, 8, 16, 32, 64, 128$.

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

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Theorem (Pollack, T.)

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

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

...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

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Theorem (Pollack, T.)

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

Proof Sketch

Exactly 1 divisor of each degree

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Theorem (Pollack, T.)

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

Proof Sketch

Let $F_m := 2^{2^m} + 1$ represent the m^{th} Fermat number.

Exactly 1 divisor of each degree

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Theorem (Pollack, T.)

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

Proof Sketch

Let $F_m := 2^{2^m} + 1$ represent the m^{th} Fermat number. One can show that $x^n - 1$ has exactly one divisor of each degree iff each $\varphi(d)$ represents a distinct power of 2.

Exactly 1 divisor of each degree

Theorem (Pollack, T.)

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

Proof Sketch

Let $F_m := 2^{2^m} + 1$ represent the m^{th} Fermat number. One can show that $x^n - 1$ has exactly one divisor of each degree iff each $\varphi(d)$ represents a distinct power of 2. It is well-known that if p is an odd prime for which $p - 1$ is a power of 2, then $p = F_m$ for some m.

Exactly 1 divisor of each degree

Theorem (Pollack, T.)

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

Proof Sketch

Let $F_m := 2^{2^m} + 1$ represent the m^{th} Fermat number. One can show that $x^n - 1$ has exactly one divisor of each degree iff each $\varphi(d)$ represents a distinct power of 2. It is well-known that if p is an odd prime for which $p - 1$ is a power of 2, then $p = F_m$ for some m. Thus, the integers n that are both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient are precisely those which are expressible as products of consecutive Fermat primes.

Exactly 1 divisor of each degree

Theorem (Pollack, T.)

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

Proof Sketch

Let $F_m := 2^{2^m} + 1$ represent the m^{th} Fermat number. One can show that $x^n - 1$ has exactly one divisor of each degree iff each $\varphi(d)$ represents a distinct power of 2. It is well-known that if p is an odd prime for which $p - 1$ is a power of 2, then $p = F_m$ for some m. Thus, the integers n that are both $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient are precisely those which are expressible as products of consecutive Fermat primes. But F_5 is not prime!

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

...have a divisor of degree m?

Theorem (Pollack, T.)

Let $\delta := 1 - \frac{1+\log\log 2}{\log 2} \approx 0.0860713$. *Fix a value* δ' *with* $0 < \delta' < \delta$. *If* $3 \le m \le X$, *we have*

$$\#\{n \le X : x^n - 1 \text{ has a divisor of degree } m\} \ll \frac{X}{(\log m)^{\delta'}}.$$

A theorem of Ford

Theorem (Ford)

Let $H(X, Y, Z)$ represent the count of $n \leq X$ possessing a divisor from the interval $(Y, Z]$. Write $Z = Y^{1+u}$. For X, Y sufficiently large with $2Y \leq Z \leq Y^2 \leq X$, we have

$$H(X, Y, Z) \asymp X u^{\delta} (\log \frac{2}{u})^{-3/2}.$$

Proof sketch

If $x^n - 1$ has a divisor of degree m, then we can write $m = \sum_{d \in \mathcal{D}} \varphi(d)$ where $\mathcal{D}$ is some subset of divisors of n.

Proof sketch

If $x^n - 1$ has a divisor of degree m, then we can write $m = \sum_{d \in \mathcal{D}} \varphi(d)$ where $\mathcal{D}$ is some subset of divisors of n. Moreover, there must be some d for which $\varphi(d)$ is larger than average, and so $\varphi(d) \geq \frac{m}{\#\{d \,:\, d|n,\ d \leq m\}}$.

Proof sketch

If $x^n - 1$ has a divisor of degree m, then we can write $m = \sum_{d \in \mathcal{D}} \varphi(d)$ where $\mathcal{D}$ is some subset of divisors of n. Moreover, there must be some d for which $\varphi(d)$ is larger than average, and so $\varphi(d) \geq \frac{m}{\#\{d\,:\,d|n,\ d \leq m\}}$. The count in the denominator is typically around $\log m$.

Proof sketch

If $x^n - 1$ has a divisor of degree m, then we can write $m = \sum_{d \in \mathcal{D}} \varphi(d)$ where $\mathcal{D}$ is some subset of divisors of n. Moreover, there must be some d for which $\varphi(d)$ is larger than average, and so $\varphi(d) \geq \frac{m}{\#\{d\,:\,d|n,\ d \leq m\}}$. The count in the denominator is typically around $\log m$. But $\varphi(d) \leq m$ and $\varphi(d)$ is not too different from d.

Proof sketch

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

If $x^n - 1$ has a divisor of degree m, then we can write $m = \sum_{d \in \mathcal{D}} \varphi(d)$ where $\mathcal{D}$ is some subset of divisors of n. Moreover, there must be some d for which $\varphi(d)$ is larger than average, and so $\varphi(d) \geq \frac{m}{\#\{d\,:\,d|n,\ d \leq m\}}$. The count in the denominator is typically around $\log m$. But $\varphi(d) \leq m$ and $\varphi(d)$ is not too different from d. So, solving this problem roughly amounts to knowing how often an integer n has a divisor $d \in (\frac{m}{\log m}, m)$, which is where Ford's theorem is useful.

Switching gears...

How do these results change...

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

Definition

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

Notation:

For each rational prime p, let

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

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

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

Overarching Goal

Our computational results seem to suggest the following conjecture:

Conjecture

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

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

Density 0 argument

We'll sketch a proof of the following (weaker) theorem:

Theorem (T.)

Let p be a prime number. Assuming that the Generalized Riemann Hypothesis holds, we have $F_p(X) = o(X)$ as $X \to \infty$.

Proof sketch

Let $\ell_p(d)$ denote the multiplicative order of $p \pmod{d}$.

- We show that, when n has the "normal" number of prime factors, there exists an index j for which

$$1 + \sum_{i \le j} \ell_p(d_i) \frac{\varphi(d_i)}{\ell_p(d_i)} < \ell_p(d_{j+k})$$

holds for all $k \ge 1$. Thus, such an n cannot be $\mathbb{F}_p$-practical.

Proof sketch

On the degrees of divisors of $x^n - 1$

Paul Pollack & Lola Thompson

At least one divisor of each degree

At most one divisor of each degree

Exactly one divisor of each degree

A divisor of degree m

Variants over $\mathbb{F}_p$

Let $\ell_p(d)$ denote the multiplicative order of $p \pmod{d}$.

- We show that, when n has the "normal" number of prime factors, there exists an index j for which

$$1 + \sum_{i \le j} \ell_p(d_i) \frac{\varphi(d_i)}{\ell_p(d_i)} < \ell_p(d_{j+k})$$

  holds for all $k \ge 1$. Thus, such an n cannot be $\mathbb{F}_p$-practical.

- Since the set of n having many more (or many fewer) than the normal number of prime factors has asymptotic density 0, then the $\mathbb{F}_p$-practicals must lie within a set with asymptotic density 0.

Key Lemmas

Recall that $\Omega(n)$ has normal order $\log\log n$.

Lemma

Let n be a positive integer. Fix $\varepsilon = 1/1000$. If n is in the set with asymptotic density 1 for which

$$(1-\varepsilon)\log\log n \leq \Omega(n) \leq (1+\varepsilon)\log\log n,$$

then there exists an integer j such that

$$\frac{d_{j+1}}{d_j} > e^{(\log n)^{0.3}}.$$

Key Lemmas

Lemma (Friedlander, Pomerance, Shparlinski)

Let n and d be positive integers with $d \mid n$. Then $\frac{d}{\ell_p(d)} \leq \frac{n}{\ell_p(n)}$.

Lemma (Li, Pomerance)

Under the GRH, for any fixed integer $a > 1$, the number of positive integers $n \leq X$ coprime to a with $\ell_a(n) \leq \frac{X}{(\log X)^{2\log_3 X}}$ is $o(X)$.

Main argument

- Let n be a positive integer with divisors $d_1 < d_2 < \cdots < d_{\tau(n)}$.

Main argument

- Let n be a positive integer with divisors $d_1 < d_2 < \cdots < d_{\tau(n)}$.
- Suppose that n has the normal number of prime factors.

Main argument

- Let n be a positive integer with divisors $d_1 < d_2 < \cdots < d_{\tau(n)}$.
- Suppose that n has the normal number of prime factors.
- Furthermore, let p be a rational prime with $p \nmid n$.

Main argument

- Let n be a positive integer with divisors $d_1 < d_2 < \cdots < d_{\tau(n)}$.
- Suppose that n has the normal number of prime factors.
- Furthermore, let p be a rational prime with $p \nmid n$.
- On one hand, we have

$$1 + \sum_{i \leq j} \ell_p(d_i) \frac{\varphi(d_i)}{\ell_p(d_i)} = 1 + \sum_{i \leq j} \varphi(d_i) \leq j d_j \leq d_j \log n.$$

Main argument

- On the other hand, by Li and Pomerance's lemma, we may assume that $\ell_p(n) > \frac{n}{(\log n)^{2\log_3 n}}$.

Main argument

- On the other hand, by Li and Pomerance's lemma, we may assume that $\ell_p(n) > \frac{n}{(\log n)^{2\log_3 n}}$.

- As a result, for all $k \geq 1$, we have

$$\ell_p(d_{j+k}) > \frac{d_{j+k}}{(\log n)^{2\log_3 n}} \geq d_j \frac{e^{(\log n)^{0.3}}}{(\log n)^{2\log_3 n}} \geq d_j \log n,$$

where the first two inequalities follow from the remaining lemmas.

Main argument

- On the other hand, by Li and Pomerance's lemma, we may assume that $\ell_p(n) > \frac{n}{(\log n)^{2\log_3 n}}$.
- As a result, for all $k \geq 1$, we have

$$\ell_p(d_{j+k}) > \frac{d_{j+k}}{(\log n)^{2\log_3 n}} \geq d_j \frac{e^{(\log n)^{0.3}}}{(\log n)^{2\log_3 n}} \geq d_j \log n,$$

where the first two inequalities follow from the remaining lemmas.
- Therefore, we have $1 + \sum_{i \leq j} \ell_p(d_i) \frac{\varphi(d_i)}{\ell_p(d_i)} < \ell_p(d_{j+k})$ holds for all $k \geq 1$.

What we **can** show...

Theorem (T.)

Assuming GRH, for each prime p, we have

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

A divisor of degree m?

Theorem (Pollack, T.)

Assuming GRH, if $3 \le m \le X$, then the number of $n \le X$ for which $x^n - 1$ has a divisor of degree m in $\mathbb{F}_p[x]$ is

$$\ll_p \frac{X}{(\log m)^{2/35}}.$$

Thank you!