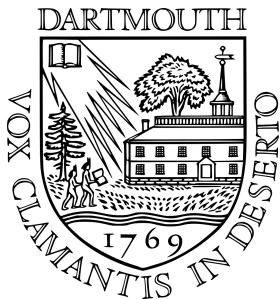


# On the divisors of $x^n - 1$ in $\mathbb{F}_p[x]$



Lola Thompson

Dartmouth College

October 2, 2011

# Motivation

---

Which polynomials  $f$  with integer coefficients have a divisor of every degree up to  $\deg f$ ?

- Certainly, any polynomial that splits completely into linear factors, like  $f(x) = x^n$ , has this property.

# Motivation

---

Which polynomials  $f$  with integer coefficients have a divisor of every degree up to  $\deg f$ ?

- Certainly, any polynomial that splits completely into linear factors, like  $f(x) = x^n$ , has this property.
- There are other, less obvious choices for  $f$ . In this talk, we will consider polynomials of the form  $x^n - 1$  and determine when members of this family have a divisor of every degree in a given polynomial ring.

# Outline

---

Introduction

Connection with the practical numbers

Factoring  $x^n - 1$  over  $\mathbb{Z}$

Factoring  $x^n - 1$  over  $\mathbb{F}_p$

# Introduction

---

We can use the identity

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

to show that the following statements are equivalent:

# Introduction

---

We can use the identity

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

to show that the following statements are equivalent:

- $x^n - 1$  has a divisor of every degree between 1 and  $n$ .

# Introduction

---

We can use the identity

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

to show that the following statements are equivalent:

- $x^n - 1$  has a divisor of every degree between 1 and  $n$ .
- Every integer  $m$  with  $1 \leq m \leq n$  can be written in the form

$$m = \sum_{d \in \mathcal{D}} \varphi(d),$$

where  $\mathcal{D}$  is a subset of divisors of  $n$ .

## Introduction

---

**Example.**  $n = 6$

Divisors: 1, 2, 3, 6

Totients: 1, 1, 2, 2

Totient-sums:

1

2

1 + 2

2 + 2

1 + 2 + 2

1 + 1 + 2 + 2

$\therefore 6$  is  $\varphi$ -practical

## Connection with the practical numbers

---

The term “ $\varphi$ -practical” stems from the striking similarity between the condition given in the second statement and the definition of a practical number:

### 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  $n$ .

## Connection with the 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.*

## Connection with the practical numbers

---



Counting the size of the set of practical numbers up to  $X$  has been of interest for some time. The tightest bounds were given by E. Saias:

**Theorem (Saias, 1997)**

*There exist two constants  $C_1$  and  $C_2$  such that*

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

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

## Factoring $x^n - 1$ in $\mathbb{Z}[x]$

---

At last year's Québec-Maine Conference, we discussed an analogue of Saias' result for the  $\varphi$ -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  $F(X) = \#\{n \leq X : n \text{ is } \varphi\text{-practical}\}$ .*

## 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  $\max_{1 \leq j \leq \tau(n)-1} \frac{d_{j+1}(n)}{d_j(n)} \leq 2$ .

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

## Lower Bound Proof Sketch

---

We obtain our lower bound by comparing the set of  $\varphi$ -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  $\varphi$ -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:

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

## 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:

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

- 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  $\leq \varepsilon \frac{X}{\log X}$ .

## 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

$$\#\{n \leq X : n \text{ is practical but not } \varphi\text{-practical}\} \gg \frac{X}{\log X}.$$

Moreover, we also have

$$\#\{n \leq X : n \text{ is } \varphi\text{-practical but not practical}\} \gg \frac{X}{\log X}.$$

## Factoring $x^n - 1$ in $\mathbb{F}_p[x]$

---

### Definition

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

In order to better understand the relationship between  $\varphi$ -practical and  $p$ -practical numbers, we define an intermediate set of numbers which we call the  $\lambda$ -practical numbers:

### Definition

An integer  $n$  is  *$\lambda$ -practical* if and only if it is  $p$ -practical for every rational prime  $p$ .

## Comparing The Three Sets

---

1	2	3	4		6		8	
	12		14	15	16		18	20
21			24				28	30
	32				36			40
	42			45			48	
			54		56			60
		63	64					70
	72							80
			84					90
					96			100

Table:  $\varphi$ -practicals,  $\lambda$ -practicals\*, 2-practicals\*

## Density Considerations

---

### Theorem (T.)

*For  $X$  sufficiently large, the order of magnitude of  $\lambda$ -practicals in  $[1, X]$  that are not  $\varphi$ -practical is  $\frac{X}{\log X}$ . Moreover, for each prime  $p$ , the order of magnitude of  $p$ -practicals in  $[1, X]$  that are not  $\lambda$ -practical is at least  $\frac{X}{\log X}$ .*

### Proof.

(Sketch) The proof of the first statement boils down to constructing a family of  $\lambda$ -practical numbers that are not  $\varphi$ -practical and showing that the members of this family are in one-to-one correspondence with a positive proportion of the  $\varphi$ -practical numbers. The second statement has a similar argument.

## Future Work

---

For each rational prime  $p$ , let

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

Computations in Sage yield the following table of ratios:

$X$	$F_2(X)/(X/\log X)$
100	1.56575786323595
1000	1.67858453279266
10000	1.64865092658374
100000	1.69274543111457
1000000	1.66167434786971
10000000	1.66061354691737

Table: Ratios for 2-practicals

## Future Work

---

Our computational results seem to suggest the following conjecture:

### Conjecture

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

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

We hope to have this proven soon!