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

Paul Pollack & Lola Thompson

University of Georgia

October 21, 2012
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 $d$th cyclotomic polynomial.
Recall that over $\mathbb{Z}$,

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

where $\Phi_d(x) \in \mathbb{Z}[x]$ is the $d$th 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

- have at least 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 $x^n - 1$ . . .

- 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 $x^n - 1$ . . .

- have at least one divisor of each degree $0 \leq m \leq n$?
- have at most one divisor of each degree $0 \leq m \leq n$?
- have exactly one divisor of each degree $0 \leq m \leq n$?
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 $\geq 1$ 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 $\geq 1$ 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 \( \geq 1 \) 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 \( \geq 1 \) 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?

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

Table: $\mathbb{Q}$-practical values of $n \leq 100$
The degrees of the polynomial divisors of $x^n - 1$

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 $X/\log X$

<table>
<thead>
<tr>
<th>$X$</th>
<th>$F(X)/(X/\log X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^4$</td>
<td>1.10339877656275</td>
</tr>
<tr>
<td>$10^5$</td>
<td>1.07081719749688</td>
</tr>
<tr>
<td>$10^6$</td>
<td>1.02871673165658</td>
</tr>
<tr>
<td>$10^7$</td>
<td>1.02435010928622</td>
</tr>
<tr>
<td>$10^8$</td>
<td>1.01792184432701</td>
</tr>
<tr>
<td>$10^9$</td>
<td>1.00271691477998</td>
</tr>
</tbody>
</table>
An asymptotic estimate?

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

<table>
<thead>
<tr>
<th>( X )</th>
<th>( F(X)/(X/\log X) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^4 )</td>
<td>1.10339877656275</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>1.07081719749688</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>1.02871673165658</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>1.02435010928622</td>
</tr>
<tr>
<td>( 10^8 )</td>
<td>1.01792184432701</td>
</tr>
<tr>
<td>( 10^9 )</td>
<td>1.00271691477998</td>
</tr>
</tbody>
</table>

Question

Is there a “\( \mathbb{Q} \)-practical number theorem” stating that \( F(X) \sim X/\log X \)?
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 $m \in [0, n]$. 
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 $\leq 1$ divisor of each degree?

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

Table: $\mathbb{Q}$-efficient values of $n \leq 100$
The degrees of the polynomial 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

Variants over \( \mathbb{F}_p \)

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

Paul Pollack & Lola Thompson

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

...have exactly one divisor of each degree?

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

Table: $\mathbb{Q}$-practical and $\mathbb{Q}$-efficient $n \leq 100$
The degrees of the polynomial divisors of $x^n - 1$

Paul Pollack & Lola Thompson

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 $i = 0, \ldots, 5$.

Example

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

In fact, for all of these examples, the multiset of $\varphi(d)$ for $d | 2^{2^i} - 1$ 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 \( T \)):

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

\[
\prod_{d|n} (1 + T^{\varphi(d)}).
\]

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 \( F_0F_1 \cdots F_i \) for some \( i \). But \( F_5 \) is not prime! So the only examples with \( n > 1 \) are

\[
F_0F_1F_2 \cdots F_i,
\]

for \( 0 \leq i \leq 4 \). Since

\[
F_0F_1 \cdots F_i = 2^{2^{i+1}} - 1,
\]

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

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

Computations in Sage yield the following table of ratios:

<table>
<thead>
<tr>
<th>$X$</th>
<th>$F_2(X)/(X/\log X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^2$</td>
<td>1.56575786323595</td>
</tr>
<tr>
<td>$10^3$</td>
<td>1.67858453279266</td>
</tr>
<tr>
<td>$10^4$</td>
<td>1.64865092658374</td>
</tr>
<tr>
<td>$10^5$</td>
<td>1.69274543111457</td>
</tr>
<tr>
<td>$10^6$</td>
<td>1.66167434786971</td>
</tr>
<tr>
<td>$10^7$</td>
<td>1.66061354691737</td>
</tr>
</tbody>
</table>

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

$$F_p(X) \ll X \sqrt{\frac{\log \log X}{\log X}}.$$
The degrees of the polynomial 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

Variants over $\mathbb{F}_p$

Thank you!