Primitive Prime Divisors
In Orbits of Quadratic Polynomials

Anna Haensch + Kevin Doerksen
wesleyan University Simon Fraser University
Object of Interest:

\[ y(z) = z^2 - k \quad \text{for } R > 2 \]

The orbit of \( y \) at \( 0 \) is the set

\[ \{ y(0), y^2(0), y^3(0), \ldots \} \]

* For this choice of \( y \),

0 is a wandering point.
Def: A primitive prime divisor of a sequence \( \{a_1, a_2, \ldots \} \) is a prime \( p \) such that \( p \mid a_m \) for any \( m < n \).

Problem: For what values of \( n \) does the sequence \( \{\varphi(0), \varphi^2(0), \varphi^3(0), \ldots \} \) have primitive prime divisors?
Motivation

Zsigmondy's Theorem:

Let $a > b > 1$ be integers and define $A_n = a^n - b^n$. Then $A_n$ has a primitive prime divisor for all $n > 7$. 
Main Theorem

Let \( \varphi: \mathbb{Z} \to \mathbb{Z} \) be \( \varphi(z) = z^2 - k, \, k > 2 \)

There exist explicit constants \( C_1, C_2 \) such that \( \varphi^n(0) \) has a primitive prime divisor for all

\[ n > C_1 \log \log (k) + C_2 \]
Example \quad \gamma(z) = z^2 - 5

\gamma(0) = 5 \cdot -1
\gamma^2(0) = 5 \cdot 2^3
\gamma^3(0) = 5 \cdot 79
\gamma^4(0) = 5 \cdot 2^3 \cdot 29 \cdot 369
\gamma^5(0) = 5 \cdot 11 \cdot 509 \cdot 869521
\gamma^6(0) = 5 \cdot 2^3 \cdot 79 \cdot 54724038799 \cdot 6853081
$\{ \varphi(0), \varphi^2(0), \ldots \}$ is a rigid divisibility sequence, this means

$$\text{ord}_p (\varphi^n(0)) = e > 0$$

$$\Rightarrow \text{ord}_p (\varphi^{nm}(0)) = e \quad \forall \, m \in \mathbb{Z}$$
IDEA BEHIND PROOF

TWO KEY IDEAS

1. Every $\phi^n(0)$ can decompose into two parts: $\phi^n(0) = a_n \cdot b_n$, where
   - $a_n =$ product of primes which appear in previous iterates
     = "old stuff"
   - $b_n =$ product of primitive primes of $\phi^n(0)$
     = "new stuff"
2. **Rigid Divisibility of \( \{ \phi^n(0) \} \)**

\[ a_n = \int \frac{dT}{d\ln b_d} \]

\[ \phi_n(0) \]
Sketch of Proof:

1) Find explicit upper and lower bounds for $H(\phi^n(0))$:

Silverman \Rightarrow \left| \frac{1}{d^n} h(\phi^n(0)) - h(0) \right| \leq \frac{C_1}{d-1}

In our case (after simplification):

\[ \frac{1}{k+1} \left( \frac{k}{2} \right)^{2^{n-2}} \leq H(\phi^n(0)) \leq (k+1)(k^{2^n}) \]
(2) **Bound the contribution to $\phi^n(0)$ from the primes which appear in previous iterates.**

"**Bound the old stuff**"

$$a_n = \prod_{d|n} b_n$$

$$\leq \prod_{d|n} (k+1)^{k^d}$$

$$\leq (k+1)^{d(n)} \cdot k \cdot e^{2^{k^d}+1}$$
(3) Find a lower bound on the contribution to $\phi^n(0)$ from primitive primes.

"Lower bound on the new stuff"

$\phi^n(0) = a_n \cdot b_n$

$\therefore b_n = \frac{\phi^n(0)}{a_n}$

\begin{align*}
\geq & \quad \text{Lower bound for } \phi^n(0) \\
& \quad \text{Upper bound for } a_n \\
= & \quad \frac{\left(\frac{1}{k+1}\right) \left(\frac{k}{2}\right)^{2^{n-2}}}{(k+1)^{d(n)} \cdot k \cdot e^{2^{\log(2)+1}}} 
\end{align*}
4) Simplify and use number algebra to solve for $n$ in terms of $k$:

\[ b_n > \frac{\exp(2^{n/2})}{\exp((2n+1) \log(k+1))} \]

\[ b_n \text{ will be greater than 1 whenever } 2^{n/2} > (2n+1) \log(k+1) \]

\[ n > c_1 \log \log k + c_2 \]

Where

\[ c_1 = \frac{2}{\log(3) - \log(2)} \quad c_2 = \frac{2(\log(2) + \log(10))}{\log(3) - \log(2)} \]
<table>
<thead>
<tr>
<th>k</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>100</td>
<td>23</td>
</tr>
<tr>
<td>1000</td>
<td>25</td>
</tr>
<tr>
<td>$10^4$</td>
<td>26</td>
</tr>
<tr>
<td>$10^{10}$</td>
<td>31</td>
</tr>
<tr>
<td>$10^{20}$</td>
<td>34</td>
</tr>
<tr>
<td>$10^{100}$</td>
<td>42</td>
</tr>
<tr>
<td>$10^{1000}$</td>
<td>53</td>
</tr>
</tbody>
</table>

*Poor use of space*