**The Minnesota Journal of Undergraduate Mathematics**

# Good Reduction of Preperiodic Points

Sarah Blackwell

Saint Louis University

The Minnesota Journal of Undergraduate Mathematics

Volume 4 (2018-19 Academic Year)

*Sponsored by*
School of Mathematics
University of Minnesota
Minneapolis, MN 55455

The Minnesota Journal of Undergraduate Mathematics

Volume 4 (2018-19 Academic Year)

# Good Reduction of Preperiodic Points

Sarah Blackwell*

Saint Louis University

Abstract. This paper considers dynamical systems of rational functions modulo primes in order to compare the original orbits of a function to the reduced orbit. It is already known what happens to the period, or the repeating iterate values, of a certain preperiodic point when we reduce modulo a certain prime. We show that when a tail, or the values of iterates that occur before the iterates become periodic, is reduced modulo a prime, there is no apparent restriction on what possible tail lengths can be achieved.

## 1. Introduction and Main Result

A dynamical system is a function together with the set of points it acts on, such that we can take iterations of the function on a specific point and determine how the iterates of the point change over time. One of the main objects of study in the arithmetic of dynamical systems is points with a finite forward orbit. By *forward orbit* we mean the collection of values of iterates as the function is applied. Orbits will be finite when the values eventually repeat. Points with finite forward orbits are called *preperiodic points*. In Section 2 we will provide a formal definition of *preperiodic*.

In this paper we consider dynamical systems of rational functions modulo primes in order to compare the original orbits of a function to the reduced orbit. It is already known what happens to the period, or the repeating iterate values, of a certain preperiodic point when we reduce modulo a certain prime [3, 10]. What remains to be shown is what happens to the tail, or the values of iterates that occur before the iterates become periodic. That is, when we reduce a tail modulo a certain prime, what kind of reduction of the tail can we get?

We will first state our theorem, and then provide background and relevant formal definitions. In our theorem statement and throughout the paper we use the notation $\bar{Q}$ to denote the reduced point $Q$ modulo the given prime. Here is our main result.

**Theorem 1.1.** *Let $f$ be a rational function of degree at least 2 and let $p$ be a prime of good reduction. Let $Q$ be a $(m,n)$ minimal preperiodic point for $f$, where $m > 0$ is the length of the*

[*] *Corresponding author*

*tail and $n$ is the minimal period. Then $\bar{Q}$ is a $(m',n')$ minimal preperiodic point, where $n'$ is given in Theorem 2.14 below and $0 \leq m' \leq m$.*

By Theorem 2.14 it is known that for a given point a bound on the possible minimal periods exists, depending only on primes of good reduction of the map. The ideal next step would be to find an upper bound on possible tails without dependence on the map. Morton and Silverman conjectured in 1994 that this bound exists [6]. Then, in 2009 Faber et. al. showed that an upper bound on the possible tails does exist [1]. Since then, some explicit values for bounds under specific conditions have been provided. In 2011 Faber et. al. found an explicit bound of 6 for the number of pre-images of 0 under quadratic maps with rational coefficients [2]. In another 2011 paper Hutz et. al. found bounds on the number of rational pre-images of any algebraic number under quadratic maps with rational coefficients [4]. We initially hoped that our research would provide some insight into this problem. However since our theorem does not place a restriction on what tail lengths modulo the prime can be achieved, this does not help find a bound independent of the map. So while our theorem successfully describes the reduction of tails modulo primes, it does not lead to similar further applications.

In this paper, the software Sage was used for all calculations [11].

## 2. Background

We begin with some basic definitions concerning dynamical systems. Dynamical systems are built from iterations of functions. In this paper we will particularly consider rational functions.

**Definition 2.1.** The *degree* of a rational function $f = \frac{p(x)}{q(x)}$, where $p(x)$ and $q(x)$ are polynomials, is the maximum of the degrees of $p(x)$ and $q(x)$.

**Definition 2.2.** The *$n$-th iterate of $f$*, denoted $f^n$, is the composition of $f$ with itself $n$ times:

$$f^n(x) = f(f^{n-1}(x)) = f(f(...f(x)...)) \text{ (n times)}.$$

**Example 2.3.** Let $f(x) = x^3 + 1$. Then the 2nd iterate of $f$ is

$$f^2 = (x^3+1)^3 + 1 = x^9 + 3x^6 + 3x^3 + 2.$$

**Example 2.4.** Let $f(x) = 2x$. Then the 4th iterate of $f$ is

$$f^4 = f(f(f(f(x)))) = 2(2(2(2x))) = 16x.$$

When we consider the iterates of a rational function $f$ at a particular point $Q$, we will often speak of the (forward) *orbit* of $Q$, or the list of iterates of $f$ evaluated at $Q$, beginning with $f^0(Q) = Q$, and continuing with $f^1(Q), f^2(Q), \ldots$. Orbits can either contain finitely or infinitely many different values. Here we are more interested in orbits with finitely many different values, which occur when $Q$ is preperiodic.

**Definition 2.5.** A point $Q$ is *preperiodic* if there exist $n$ and $m$ such that $m \geq 0$, $n \geq 1$ and

$$f^{m+n}(Q) = f^m(Q).$$

Then, for the smallest $m$ and $n$ that satisfy the above equation, we call $m$ the *tail* and $n$ the *minimal period*. We will call a point $Q$ with tail $m$ and minimal period $n$ an $(m,n)$ *preperiodic point*.

That is, preperiodic points have finite orbits, since at some point the orbit will become periodic. By *periodic* we mean a point with no tail and non-zero period. All periodic points are preperiodic. For a preperiodic point, the tail is the non-periodic part of the point's orbit, that is, the iterations of the point before the values begin to repeat.

**Example 2.6.** Let $f(x) = 2x$. Then $x = 0$ is preperiodic with $m = 0$, $n = 1$.

**Example 2.7.** Let $f(x) = x^2 - 2$. Then $x = 0$ is preperiodic with $m = 2$, $n = 1$. To see this, calculate $f^2(0) = f(f(0)) = f(-2) = 2$ and $f^3(0) = f(f(f(0))) = f(f(-2)) = f(2) = 2$.

$$\begin{tikzcd} 0 \arrow[r] & -2 \arrow[r] & 2 \arrow[loop right] \end{tikzcd}$$

**Example 2.8.** Let $f(x) = -x^3 + 11x^2 - 39x + 47$. Then $x = 4$ is preperiodic, since

$$f^4(4) = f(f(f(f(4)))) = f(f(f(3))) = f(f(2)) = f(5) = 2.$$

So $m = 2$, $n = 2$.

$$\begin{tikzcd} 4 \arrow[r] & 3 \arrow[r] & 2 \arrow[r, bend left] & 5 \arrow[l, bend left] \end{tikzcd}$$

In order to reduce these rational functions modulo a prime and be able to compare the dynamics of the reduced map to the original map, we must define a notion of good and bad reduction. Bad reduction occurs when the dynamics of the original map are unrelated to the dynamics of the reduced map. Good reduction means that reduction modulo a prime commutes with iteration. Now we will formally define good and bad reduction.

**Definition 2.9.** Let $f(x) = \frac{r(x)}{q(x)}$ and $\bar{f}(x) = \frac{r(x)}{q(x)}(\text{mod } p) = \frac{\bar{r}(x)}{\bar{q}(x)}$, for polynomials $r, q \in \mathbb{Z}[x]$. Then a prime $p$ is a *prime of good reduction* if at least one of the following is true:

(1) degree$(f)$ = degree$(\bar{f})$,

(2) $\bar{r}(x)$ and $\bar{q}(x)$ have no common zeroes.

Otherwise, $p$ is a *prime of bad reduction*.

**Example 2.10.** Let $f(x) = 2x^2 + 3$. Then $p = 3$ is a prime of good reduction, since $\bar{f}(x) = 2x^2$ has the same degree as $f$. However, $p = 2$ is a prime of bad reduction, since $\bar{f}(x) = 1$ does not have the same degree as $f$. This means that for $p = 2$ the dynamics of $\bar{f}$ are unrelated to the dynamics of $f$. For instance, $\bar{f}$ is a constant function and $f$ is not.

**Example 2.11.** Let $f(x) = \frac{2x^2+6}{4x+9}$. Then $p = 5$ is a prime of good reduction. Let $r(x) = 2x^2 + 6$ and $q(x) = 4x + 9$. Reduce mod 5 to get $\bar{r}(x) = 2x^2 + 1$ and $\bar{q}(x) = 4x + 4$. Note that $\bar{r}$ and $\bar{q}$ do not share any zeros. However, $p = 3$ is a prime of bad reduction, since $\bar{r}(x) = 2x^2$ and $\bar{q}(x) = x$ share a zero at $x = 0$.

**Example 2.12.** One might hope to use polynomial interpolation to construct an orbit with any possible behavior under reduction, but in most cases there will not be good reduction at the required prime. For instance, by polynomial interpolation we can construct a polynomial $f$ over $\mathbb{Q}$ such that $f(0) = 3$, $f(3) = 5$, $f(5) = 8$, $f(8) = 10$, and $f(10) = 5$. With this setup, we see that 0 is a $(2,3)$ preperiodic point. If we were to reduce mod 5, we would expect $\bar{0}$ to be a $(0,2)$ preperiodic point. But in order for us to consider these dynamics, we must determine whether 5 is truly a prime of good reduction. We first calculate $f$ explicitly:

$$\begin{aligned} f(x) &= 3\left(\left(\tfrac{x-3}{-3}\right)\left(\tfrac{x-5}{-5}\right)\left(\tfrac{x-8}{-8}\right)\left(\tfrac{x-10}{-10}\right)\right) \\ &+ 5\left(\left(\tfrac{x}{3}\right)\left(\tfrac{x-5}{-2}\right)\left(\tfrac{x-8}{-5}\right)\left(\tfrac{x-10}{-7}\right)\right) \\ &+ 8\left(\left(\tfrac{x}{5}\right)\left(\tfrac{x-3}{2}\right)\left(\tfrac{x-8}{-3}\right)\left(\tfrac{x-10}{-5}\right)\right) \\ &+ 10\left(\left(\tfrac{x}{8}\right)\left(\tfrac{x-3}{5}\right)\left(\tfrac{x-5}{3}\right)\left(\tfrac{x-10}{-2}\right)\right) \\ &+ 5\left(\left(\tfrac{x}{10}\right)\left(\tfrac{x-3}{7}\right)\left(\tfrac{x-5}{5}\right)\left(\tfrac{x-8}{2}\right)\right). \end{aligned}$$

We can simplify this polynomial to the nicer form

$$f(x) = \frac{-1}{400}x^4 - \frac{1}{600}x^3 + \frac{121}{400}x^2 - \frac{19}{120}x + 3.$$

If we find a common denominator in order to rewrite $f$ as $f(x) = \frac{r(x)}{q(x)}$, where $r, q \in \mathbb{Z}[x]$, we see that $q = 1200$ (if we take the least common denominator):

$$f(x) = \frac{r(x)}{q(x)} = \frac{-300x^4 - 2x^3 + 363x^2 - 190x + 3600}{1200}.$$

Then $\bar{q} \equiv 0 \pmod 5$. But this means that all zeroes of $\bar{r}$ are zeroes of $\bar{q}$, so 5 is not a prime of good reduction, and reduction mod 5 does not commute with iteration. That is, the dynamics of $f$ are unrelated to the dynamics of $\bar{f}$ when we reduce mod 5.

We must provide one more definition, and then we can state a theorem.

**Definition 2.13.** Let $Q$ be a periodic point of a function $f(x)$, and let $Q$ have minimal period $n$. Then the *multiplier of* $Q$, denoted $\lambda_Q$, is given by $\lambda_Q = (f^n)'(Q)$.

We are now ready to state a result on the effects of the reduction of a map modulo a prime on the period of a point. We refer to this result in our theorem statement. The version of the theorem that we state is for one dimension and is given by Silverman [10, Theorem 2.21] (see also [5, 7, 6, 8, 9, 12]). A higher dimensional version is given by Hutz [3].

**Theorem 2.14** ([10]). *Let $f(x) : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism over a number field $K$. Let $p \in K$ be a prime of good reduction, and let $k$ be the residue field. Let $Q$ be a periodic point for $f$. Define*

$$\begin{array}{ll} n & \textit{the minimal period of } Q, \\ n' & \textit{the minimal period of } \bar{Q}, \\ r & \textit{the multiplicative order of } \overline{\lambda_Q}. \end{array}$$

*Then*

$$n = n' \text{ or } n = n' r p^e$$

*for some bounded integer $e \geq 0$.*

## 3. Proof of Main Result

We are now ready to prove our main result.

*Proof.* We proceed with two cases.

**Case 1:** Let $f^s(Q) \not\equiv f^t(Q) \pmod{p}$ for all $s,t \in \mathbb{Z}$ such that $t \neq s$ and $0 \leq s,t \leq m$. Then no points in the tail collapse, so the tail remains length $m$. Apply Theorem 2.14 to $f^m(Q)$ to find the reduced period $n'$. So $\bar{Q}$ is a $(m,n')$ preperiodic point.

**Case 2:** Otherwise, there exist $s,t \in \mathbb{Z}$ such that $f^s(Q) \equiv f^t(Q) \pmod{p}$, where $0 \leq s < m$ and $s < t \leq m+n$. Assume $s$ is the smallest such integer that fulfills these conditions. Let $R = f^s(Q)$. Then $R$ is an $(m-s,n)$ preperiodic point. Also, $R \equiv f^{t-s}(R) \pmod{p}$, since $f^{t-s}(R) = f^{t-s}(f^s(Q)) = f^t(Q) \equiv f^s(Q) \equiv R \pmod{p}$. We claim that $\bar{R}$ is a $(0,n')$ preperiodic point, where $n'$ is given by Theorem 2.14, and thus $\bar{Q}$ is a $(s,n')$ preperiodic point.

Consider $k = t-s \in \mathbb{Z}$, so $1 \leq k \leq m+n$ and $R \equiv f^k(R) \pmod{p}$. Then

$$f(R) \equiv f^{k+1}(R) \pmod{p}$$

$$f^2(R) \equiv f^{k+2}(R) \pmod{p}$$

$$\vdots$$

$$f^k(R) \equiv f^{2k}(R) \equiv R \pmod{p}.$$

We see that the tail completely collapses and a periodic cycle is left with a period of $k$ or smaller. The minimal period $n'$ is given by Theorem 2.14. Thus $\bar{R}$ is a $(0,n')$ preperiodic point, so $\bar{Q}$ is a $(s,n')$ preperiodic point as desired. Furthermore, we observe that $n' \mid k$ since $k$ is a period of $R$ and $n'$ is the minimal period of the reduced map.

□

Note that in Case 2 of the proof, nothing is preventing $m' = s$ from taking on any value from 0 to $m$. It may be possible to achieve all values from 0 to $m$ by finding an appropriate function and starting point. By our reasoning above we have that $n' \mid t-s$, that is, $jn' = t-s$ for some $j \in \mathbb{Z}$, $j > 0$. In order to have $f^s(Q) \equiv f^{jn'+s}(Q) \pmod{p}$, we need a prime $p$ that divides $T = f^s(Q) - f^{jn'+s}(Q)$ for some $j$. Since $f^s(Q)$ is strictly preperiodic, that is, preperiodic and not periodic, this equation is not identically 0 for any $j$. If we put a parameter into $f$, it seems reasonable to expect that for some choice of parameter $T$ will not be a unit, and so for this parameter choice we will have a prime dividing $T$. That is, we can alter $f$ by allowing one or more of the coefficients of $f$ to be a variable and search for a specific value of that variable that has the needed properties. For example, we could consider $f(x) = x^2 + c$ and choose $c$ such that $T$ is not a unit, and hence divisible by some prime. Determining which function (or family of functions) to start with in this process remains ambiguous, but with further study we could hope to make this process more concrete.

## 4. Examples of Main Result

First we present three examples that align with different cases in the proof.

**Example 4.1.** (Case 1) Let

$$f(x) = -x^3 + 11x^2 - 39x + 47$$

over $\mathbb{Q}$. Then $x = 4$ is a $(2,2)$ preperiodic point.

$$\begin{tikzcd}
4 \arrow[r] & 3 \arrow[r] & 2 \arrow[r, bend left] & 5 \arrow[l, bend left]
\end{tikzcd}$$

Now reduce mod 5 to get

$$\bar{f}(x) \equiv 4x^3 + x^2 + x + 2 \pmod{5}.$$

Then $\bar{x} \equiv 4$ is a $(2,2)$ preperiodic point.

$$\begin{tikzcd}
4 \arrow[r] & 3 \arrow[r] & 2 \arrow[r, bend left] & 0 \arrow[l, bend left]
\end{tikzcd}$$

**Example 4.2.** (Case 2) Let

$$f(x) = x^2 - 1$$

over $\mathbb{Q}$. Then $x = 1$ is a $(1,2)$ preperiodic point.

$$\begin{tikzcd}
1 \arrow[r] & 0 \arrow[r, bend left] & -1 \arrow[l, bend left]
\end{tikzcd}$$

Now reduce mod 2 to get

$$\bar{f}(x) \equiv x^2 + 1 \pmod{2}.$$

Then $\bar{x} \equiv 1$ is a $(0,2)$ preperiodic point.

$$\begin{tikzcd}
1 \arrow[r, bend left] & 0 \arrow[l, bend left]
\end{tikzcd}$$

**Example 4.3.** (Case 2) Let

$$f(x) = x^2 + 1$$

over $\mathbb{Q}(w)$, where $w = \sqrt{\frac{-3}{2} + \frac{i\sqrt{3}}{2}}$. Then $w$ is a $(2,1)$ preperiodic point, as $f(w) = w^2 + 1$, $f(w^2 + 1) = -w^2 - 1$ and $f(-w^2 - 1) = -w^2 - 1$.

$$\begin{tikzcd}
w \arrow[r] & w^2 + 1 \arrow[r] & -w^2 - 1 \arrow[loop right]
\end{tikzcd}$$

Now reduce the map mod $p$ where $p = w^2 + w + 1$. Then $\bar{w}$ is a $(1,1)$ preperiodic point, as $\bar{f}(w) \equiv -w$ and $\bar{f}(-w) \equiv -w$.

$$\begin{tikzcd}
w \arrow[r] & -w \arrow[loop right]
\end{tikzcd}$$

Now we give three examples that take $(3,1)$ preperiodic points to $(0,1)$, $(1,1)$, and $(2,1)$ preperiodic points after reduction. Note that reducing a rational function by a prime larger than all coordinates will result in no change in the length of the tail (as in Case 1). In this way we could take a $(3,1)$ preperiodic point to a $(3,1)$ preperiodic point after reduction.

**Example 4.4.** Let

$$f(x) = x^2 - 2$$

over $\mathbb{Q}(w)$, where $w = \sqrt{2}$. Then $w$ is a $(3,1)$ preperiodic point.

$$\begin{tikzcd} w \arrow[r] & 0 \arrow[r] & -2 \arrow[r] & 2 \arrow[loop right] \end{tikzcd}$$

Now reduce mod $w$ to get

$$\bar{f}(x) \equiv x^2 \pmod{w}.$$

Then $\bar{w}$ is a $(0,1)$ preperiodic point.

$$\begin{tikzcd} w \arrow[loop right] \end{tikzcd}$$

**Example 4.5.** Let

$$f(x) = x^3 - \frac{4}{3}x^2 - \frac{5}{3}x + 1$$

over $\mathbb{Q}$. Then $x = 0$ is a $(3,1)$ preperiodic point.

$$\begin{tikzcd} 0 \arrow[r] & 1 \arrow[r] & -1 \arrow[r] & \frac{1}{3} \arrow[loop right] \end{tikzcd}$$

Now reduce mod 2 to get

$$\bar{f}(x) \equiv x^3 + x + 1 \pmod{2}.$$

Then $\bar{x} \equiv 0$ is a $(1,1)$ preperiodic point.

$$\begin{tikzcd} 0 \arrow[r] & 1 \arrow[loop right] \end{tikzcd}$$

**Example 4.6.** Let

$$f(x) = x^3 - \frac{1}{2}x^2 - \frac{5}{2}x + 1$$

over $\mathbb{Q}$. Then $x = 0$ is a $(3,1)$ preperiodic point.

$$\begin{tikzcd} 0 \arrow[r] & 1 \arrow[r] & -1 \arrow[r] & 2 \arrow[loop right] \end{tikzcd}$$

Now reduce mod 3 to get

$$\bar{f}(x) \equiv x^3 + x^2 + 2z + 1 \pmod{3}.$$

Then $\bar{x} \equiv 0$ is a $(2,1)$ preperiodic point.

$$\begin{tikzcd} 0 \arrow[r] & 1 \arrow[r] & 2 \arrow[loop right] \end{tikzcd}$$

In the last few examples we saw that it is possible to obtain every value from 0 to $m$ for $m'$, when $m = 3$. For an arbitrary value of $m$ we expect to see all possible collapsing upon passing to field extensions. Certainly, our theorem does not rule out any possibilities for values of $m'$ (where $0 \leq m' \leq m$). Further research on this topic would include providing a proof for this expectation. Whether it is possible to obtain all values for $m'$ from 0 to $m$ over the rationals, without passing to field extensions, is also an open question.

## References

[1] Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve. Uniform bounds on pre-images on quadratic dynamical systems. *Mathematical Research Letters*, 16(1):87–101, 2009.

[2] Xander Faber, Benjamin Hutz, and Michael Stoll. Pre-images of the origin: On the number of rational iterated pre-images of the origin under quadratic dynamical systems. *International Journal of Number Theory*, 7(7):1781–1806, 2011.

[3] Benjamin Hutz. Good reduction of periodic points on projective varieties. *Illinois Journal of Mathematics*, 53(4):1109–1126, 2009.

[4] Benjamin Hutz, Trevor Hyde, and Benjamin Krause. Pre-images of quadratic dynamical systems. *Involve*, 4(4):343–363, 2011.

[5] Hua-Chieh Li. Counting periodic points of $p$-adic power series. *Compositio Mathematica*, 100(3):351–364, 1996.

[6] Patrick Morton and Joseph H. Silverman. Rational periodic points of rational functions. *International Mathematics Research Notices*, (2):97–110, 1994.

[7] Patrick Morton and Joseph H. Silverman. Periodic points, multiplicities, and dynamical units. *J Reine Angew. Math.*, 461:81–122, 1995.

[8] Wladyslaw Narkiewicz. Polynomial cycles in algebraic number fields. *Colloquium Mathematicum*, 58:151–155, 1989.

[9] Tadeusz Pezda. Polynomial cycles in certain local domains. *Acta Arithmetica*, 63:11–22, 1994.

[10] Joseph H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2007.

[11] William Stein and David Joyner. SAGE: System for algebra and geometry experimentation. *Communications in Computer Algebra (SIGSAM Bulletin)*, July 2005. `http://www.sagemath.org`.

[12] Michael Zieve. *Cycles of Polynomial Mappings*. PhD thesis, University of California at Berkeley, 1996.

## 5. Acknowledgments

This research project was completed at Saint Louis University. The author would like to thank her advisor on this project, Dr. Benjamin Hutz, for guiding her throughout the research process.

## Student biography

**Sarah Blackwell:** (*Corresponding author:* seblackwell@uga.edu) Sarah Blackwell graduated from Saint Louis University in 2016 with a B.A. in mathematics. She is currently pursuing her Ph.D. in mathematics at the University of Georgia. In addition to dynamical systems, her mathematical interests include topology and number theory.