On the Number of Rational Iterated Pre-Images of -1 under Quadratic Dynamical Systems

Trevor Hyde
Department of Mathematics
Amherst College
Amherst, Massachusetts 01002 USA

Received: October 21, 2009 *Accepted: March 10, 2010*

ABSTRACT

For the class of functions $f_c(x) = x^2 + c$, we prove a conditional bound on the number of rational solutions to $f_c^N(x) = -1$ and make computational conjectures for a bound on the number of rational solutions to $f_c^N(x) = a$ for a in a specific subset of the rationals.

I. INTRODUCTION

a. Definitions

Fix a rational number $c \in \mathbb{Q}$ and define a function f by $f_c(x) = x^2 + c$. Let f_c^N denote the N^{th} iterate of f_c defined as $f_c^N(x) = f_c\left(f_c^{N-1}(x)\right)$. Important concepts in the theory of arithmetic dynamics include periodic points, preperiodic points and pre-images:

Definition: A point x_0 is *periodic* if $f_c^N(x_0) = x_0$ for some $N \geq 1$.
Definition: A point x_0 is *preperiodic* if $f_c^N(x_0) = f_c^M(x_0)$ for some $N, M > 0$ such that $N \neq M$.
Definition: Fix $a \in \mathbb{Q}$. A point x_0 is an N^{th} *pre-image of* a if $f_c^N(x) = a$, we say $x_0 \in f_c^{-N}(a)$.

In this paper we investigate pre-images.[1] More precisely, we consider the problem of determining how many pre-images of a fixed rational number are rational. Before discussing what is known, we introduce some terminology.

Definition: The set of *rational pre-images of* a is

$$\bigcup_{N\geq 1} f_c^{-N}(a)(\mathbb{Q}) = \{x_0 \in \mathbb{Q} : f_c^N(x_0) = a \text{ for some } N \geq 1\}$$

Definition: The set of points in the (x,c)-plane satisfying the equation $f_c^N(x) = a$ is called the N^{th} *pre-image curve of* a, denoted $Y^{pre}(N, a)$.

Here is an example of the type of problem we will consider.

Example: $a = -\frac{3}{4}$ and $c = -\frac{229}{144}$
Let us find the set of rational pre-images:

$$f_c^{-1}(a)(\mathbb{Q}) = \left\{\pm\frac{11}{12}\right\},$$

$$f_c^{-2}(a)(\mathbb{Q}) = \left\{\pm\frac{19}{12}\right\},$$

$$f_c^{-3}(a)(\mathbb{Q}) = \left\{\pm\frac{1}{12}\right\},$$

and

$$f_c^{-4}(a)(\mathbb{Q}) = \emptyset.$$

Since $c \in \mathbb{Q}$, we have $f_c\left(\frac{p}{q}\right) \in \mathbb{Q}$ for all rational numbers $\frac{p}{q}$. Therefore, if $f_c^{-N}(a)(\mathbb{Q}) = \emptyset$ then $f_c^{-M}(a)(\mathbb{Q}) = \emptyset$ for all $M > N > 0$. Hence, there are 6 rational pre-images of $a = -\frac{3}{4}$ for $c = -\frac{229}{144}$.

In [3], the authors prove that for all $a \in \mathbb{Q}$, there are finitely many rational pre-

[1] For more on periodic and preperiodic points, see [4], [5].

images of a and that there exists a bound $\kappa(a)$ *independent* of c, on the size of the set of rational pre-images of a.

Theorem 1.1. ([3], Thm. 1.2 for B=D=1) *Fix* $a \in \mathbb{Q}$. *If we define the quantity*

$$\kappa(a) = \sup_{c \in \mathbb{Q}} \# \left\{ \bigcup_{N \geq 1} f_c^{-N}(a)(\mathbb{Q}) \right\},$$

Then $\kappa(a)$ *is finite.*

This result has a strong analog in the theory of elliptic curves.[2] Let $E/\mathbb{Q}$ be an elliptic curve with a group of rational points $E(\mathbb{Q})$. *Mazur's Theorem* says that the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of fifteen possible groups. In the language of arithmetic dynamics, if $\mathcal{O}$ is the identity for $E(\mathbb{Q})$ and $[m]: E(\mathbb{Q}) \longrightarrow E(\mathbb{Q})$ is the multiplication by m map (if $\mathcal{P} \in E(\mathbb{Q})$ then $[m](\mathcal{P})$ "adds" $\mathcal{P}$ to itself m times) then *Mazur's Theorem* says that the number of pre-images of $\mathcal{O}$ under $[m]$ is finite and bounded above independent of the choice of elliptic curve $E/\mathbb{Q}$.

Theorem 1.2. ([2], Thm. 2.1—Mazur) *Let* $E/\mathbb{Q}$ *be an elliptic curve. If we define the quantity*

$$\kappa' = \sup_{E(\mathbb{Q})} \# \left\{ \bigcup_{N \geq 1} [m]^{-N}(\mathcal{O})(\mathbb{Q}) \right\}$$

then κ' is finite.

b. Computing $\kappa(a)$.

Although Theorem 1.1 ensures that $\kappa(a)$ exists, it does not provide a method for computing $\kappa(a)$. In [2], the authors conditionally prove $\kappa(0) \leq 8$ and conjecture $\kappa(0) = 6$. Let $X^{pre}(N, a)$ be the projective closure of the affine curve $Y^{pre}(N, a)$. The key to their proof is the fact that $X^{pre}(3, 0)$ is birationally equivalent to a rank 1 elliptic curve, and then use a height argument to reduce the problem to a finite amount of computation. They conclude 0 has at most 2 rational 3rd pre-images for all $c \in \mathbb{Q}$ excluding finitely many c corresponding to periodic points ([2], Prop. 5.3). A nearly identical argument will be used in this paper to prove:

Theorem 1.3. *Suppose for* $c \in \mathbb{Q}$ *such that* $c \neq -2, f_c^N(x) = -1$ *has no rational solution for* $N \geq 4$, *then* $\kappa(-1) = 6$.

Remark: Note that -1 is a periodic point of f_{-2}. For this morphism, -1 has at least one rational *N*th pre-image for arbitrary *N*.

Falting's Theorem tells us that curves with genus[3] greater than 1 contain finitely many rational points. From [3] (Thm. 3.2), we know that the genus of $X^{pre}(4, -1)$ is 5 and thus contains finitely many rational points. In other words, the are finitely many rational c-values for which $f_c^{-4}(-1)(\mathbb{Q}) \neq \emptyset$.

In a search performed by Benjamin Hutz across a-values up to height[4] 50, only $a \in \left\{ -\frac{5}{4}, -1, -\frac{3}{4}, -\frac{1}{2}, 0, \frac{1}{4} \right\}$ have *3rd* pre-image curves birational to an elliptic curve with rank 1 (vital to the proof for the value of $\kappa(a)$ for $a = -1, 0$).

In the last section, we present computational evidence for no rational *4th* pre-images of -1 as well as for the conjectural $\kappa(a)$ of the other rank 1 a-values.

II. BACKGROUND

a. Elliptic Curves

Consider a rational cubic polynomial in two variables

$$a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3 + a_4x^2 + a_5xy + a_6y^2 + a_7x + a_8y + a_9 = 0$$

with each $a_i \in \mathbb{Q}$ (we say a polynomial is *rational* if all of its coefficients are in $\mathbb{Q}$). The solutions of such an equation form an affine planar curve, which we shall call E. Suppose we want to find all the rational points of E (a *rational* point is a point with both coordinates in $\mathbb{Q}$). There is no known algorithm for finding a rational point on an

[2] See section II for background on elliptic curves.

[3] Genus is an invariant of algebraic varieties. Defining it here would take us too far afield. It suffices to know that an elliptic curve is technically defined as a non-singular curve with genus 1 and a rational point.

[4] See section II b.

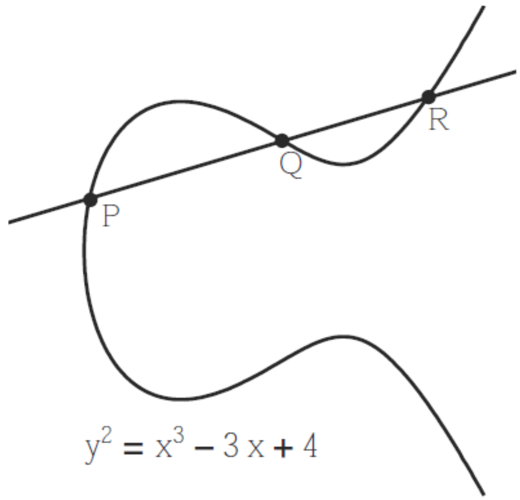

Figure 1. Finding a third rational point given two on an elliptic curve.

arbitrary cubic curve, but suppose we were able to find two rational points $\mathcal{P}$ and $\mathcal{Q}$ on E. The line $\overline{\mathcal{PQ}}$ would be rational and in general, $\overline{\mathcal{PQ}}$ would intersect E at one other point, $\mathcal{R}$.[5]

The intersection of $\overline{\mathcal{PQ}}$ and E results in a rational cubic: since two of its roots are rational so is the third. Thus, given any two[6] rational points on E we have a binary operation that gives a third rational point on E. After working through some technical details, one can see that the set of rational points on E forms a group $E(\mathbb{Q})$ with respect to the "addition" of points. A non-singular cubic curve with at least one rational point is called an *elliptic curve*.

A fundamental result in the theory of elliptic curves is due to Mordell (see [7]).

Theorem 2.1. ([7], Mordell's Theorem) *If a non-singular plane cubic curve E contains a rational point, the group of rational points* $E(\mathbb{Q})$ is finitely generated.

Since the operation on $E(\mathbb{Q})$ is commutative, the group of rational points (called the *Mordell-Weil group*) is isomorphic to the direct product of a finite number of copies of $\mathbb{Z}$ (the number of copies is known as the *rank* of $E(\mathbb{Q})$ and a finite number of cyclic groups (called *torsion subgroups* of $E(\mathbb{Q})$).

For a more complete treatment of elliptic curves, see [6] and [7].

b. Height Functions

Height functions measure the arithmetic complexity of a number. We define the height of a rational number $\frac{m}{n}$ as follows:

Definition: The height of $\frac{m}{n} \in \mathbb{Q}$ with $(m,n) = 1$ is

$$H\left(\frac{m}{n}\right) = max(|m|,|n|).$$

If E is an elliptic curve and $\mathcal{P} \in E(\mathbb{Q})$, then we say the height of $\mathcal{P}$ is the height of the x-coordinate of $\mathcal{P}$:

$$H(\mathcal{P}) = H(x(\mathcal{P})).$$

Height functions have quasi-multiplicative properties but often it is useful to convert these to additive properties by way of the *logarithmic height*.

[5] There are exceptions in the non-projective plane, but if we embed E in the projective plane $\mathbb{P}^2$ and count multiplicities, then the statement holds in general.

[6] A single rational point can be "added" to itself by finding the tangent to the curve at that point which will intersect the curve a one other point.

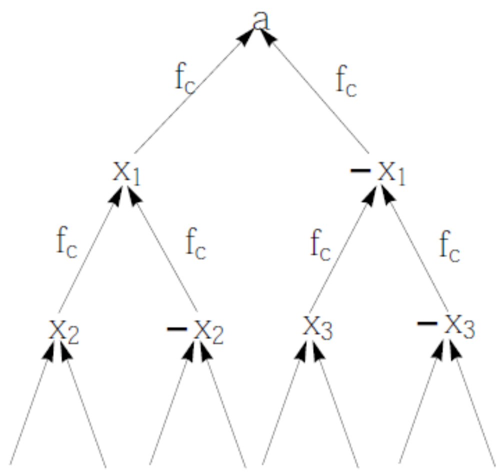

Figure 2. Pre-images of a.

Definition: The *logarithmic height*, denoted h, is defined on $\mathbb{P}^1$ as $h\left(\frac{m}{n}\right) = \log H\left(\frac{m}{n}\right)$.

The following theorem describes the relationship between the height of a point and its double.

Theorem 2.2. [7] *There is a constant C, independent of $\mathcal{P}$, such that*

$$h(2\mathcal{P}) \geq 4h(\mathcal{P}) - C$$

for all $\mathcal{P} \in E(\mathbb{Q})$.

The difficulty in working with this formula is the constant C. However, we can work around C with the *canonical height*.

Definition: The *canonical height*, denoted $\hat{h}$, is defined as

$$\hat{h}(\mathcal{P}) = \frac{1}{\deg f} \lim_{N\to\infty} \frac{h\big(f([2^N]\mathcal{P})\big)}{4^N},$$

where $f: E(\mathbb{Q}) \longrightarrow \mathbb{R}$ is any even function.

Now we can restate Theorem 2.2 using the canonical height.

Theorem 2.3. ([6], Thm. 9.3b) *For all $\mathcal{P} \in E(\mathbb{Q})$,*

$$\hat{h}(2\mathcal{P}) \geq 4\hat{h}(\mathcal{P}).$$

The following theorem describes the relationship between the canonical and logarithmic height.

Theorem 2.4. ([6], Thm. 9.3b) *Let f be an even function. Then for all $\mathcal{P} \in E(\mathbb{Q})$,*

$$(\deg f)\hat{h}(\mathcal{P}) = h_f(\mathcal{P}) + C,$$

where C is a constant independent of $\mathcal{P}$.

For a more complete treatment of height functions, see [6] and [7].

III. COMPUTING $\kappa(-1)$

In this section we will prove our main result, Theorem 1.3, by proving that there are at most 2 rational 1*st*, 2*nd*, and 3*rd* pre-images. We begin with a trivial maximum upper bound on the size of the set $f_c^{-N}(a)$. Since f_c is quadratic, the *N*th pre-image curve has $deg\big(X^{pre}(N,a)\big) = 2^N$; thus, there are at most 2^N elements in $f_c^{-N}(a)(\mathbb{Q})$ (see Figure 2). Non-zero rational pre-images will always come in pairs because if $x_0 \in f_c^{-N}(a)(\mathbb{Q})$ then $-x_0 \in f_c^{-N}(a)(\mathbb{Q})$.

a. Second Pre-Images

We are ready to prove:

Proposition 3.1. *The set $f_c^{-2}(-1)(\mathbb{Q})$ has at most 2 elements for all $c \in \mathbb{Q}$.*

Proof. Fix $a \in \mathbb{Q}$ and suppose there exists $c \in \mathbb{Q}$ such that for rational numbers q, r, s,

$$f_c(\pm q) = s, \quad f_c(\pm r) = -s, \quad \text{and} \quad f_c(\pm s) = a.$$

That is, suppose there exists $c \in \mathbb{Q}$ such that a has four rational 2*nd* pre-images. From the above system we derive,

$$s = \tfrac{1}{2}(q^2 - r^2), \quad c = \tfrac{1}{2}(q^2 + r^2),$$

and

$$c = -(s^2 - a).$$

Substitution yields

$$\frac{1}{2}(q^2 + r^2) = \frac{1}{4}(q^2 - r^2) - a,$$

and after homogenizing and rearranging,

$$Q^4 - 2Q^2R^2 + R^4 - 2Q^2W^2 - 2R^2W^2 - 4aW^4 = 0,$$

with $Q, R, W \in \mathbb{Z}$.

Let this equation define an algebraic set $S^{pre}(a)$ in the projective (Q,R,W)-space. For arbitrary a, the set $S^{pre}(a)$ is a genus 1 curve containing the rational point $(Q,R,W)=(1,1,0)$. Thus $S^{pre}(a)$ is an elliptic curve. Hereafter, we will refer to $S^{pre}(a)$ as the *full 2nd pre-image curve*.

For $a=-1$, Bosma et al. [1] tell us that $S^{pre}(a)$ has rank 0 and torsion subgroup of order 8. So $\#S^{pre}(a)$ is finite and all rational points can be obtained using the arithmetic of the elliptic curve. This produces six points in $S^{pre}(a)$:

$$\mathcal{P}_1 = (1:1:0), \quad \mathcal{P}_2 = (1:-1:0),$$
$$\mathcal{P}_3 = (-1:1:1), \quad \mathcal{P}_4 = (1:1:1),$$
$$\mathcal{P}_5 = (1:-1:1), \quad \mathcal{P}_6 = (1:1:-1).$$

$\mathcal{P}_1$ and $\mathcal{P}_2$ are points at infinity and hence not on the same affine part of the curve. The four other points correspond to $c=-1$, which has two distinct 2^{nd} pre-images because $s=0$. Therefore, there does not exist $c\in\mathbb{Q}$ such that $f_c^{-2}(a)(\mathbb{Q})$ has four elements. This concludes the proof.

b. Third Pre-Images

Next we prove:

Proposition 3.2. *The set $f_c^{-3}(-1)(\mathbb{Q})$ has at most 2 elements for all $c\in\mathbb{Q}$.*

Proof. The proof is nearly identical to that of [2] (Prop. 5.3). Consequently, we omit some details for the sake of brevity. From [3] (Thm. 3.2) we find that $X^{pre}(3,-1)$ has genus 1 and contains the rational point $(x,c)=(0,-1)$ so it is birational to an elliptic curve with an affine Weierstrass model [1] of the form $v^2=u^3+2u^2-5u+3$, hereafter referred to as E. The birational map for the c-coordinate from E to $X^{pre}(3,-1)$ is given by

$$c=\frac{-u^4-2u^2+4u-2}{(u^2-1)^2}.$$

According to Bosma et al. [1], E has rank 1 and no torsion. For $\mathcal{P}\in E(\mathbb{Q})$, let $u(\mathcal{P})$ denote the u-coordinate of $\mathcal{P}$. Define the even rational function g as

$$g(\mathcal{P})=\frac{-u(\mathcal{P})^4-2u(\mathcal{P})^2+4u(\mathcal{P})-2}{(u(\mathcal{P})^2-1)^2}.$$

Then we may define a new height function $h_g(\mathcal{P})=h(g(\mathcal{P}))$.

If (x_1,c_0) and (x_2,c_0) are rational points on $X^{pre}(3,-1)$ corresponding to points $\mathcal{P}_1$ and $\mathcal{P}_2$ on E, then $h_g(\mathcal{P}_1)=h_g(\mathcal{P}_2)$ because h_g depends only on c. Our strategy relies on the fact that E has rank 1, because we will be able to show that if a point $\mathcal{P}$ has sufficiently large height, then $-\mathcal{P}$ is the only other point of the same height. This reduces our problem to checking a finite number of points.

Following [2] (Prop. 5.3) and [6], we can bound the difference between the canonical height $\hat{h}$ on E and the modified height h_g. Since $\deg(g)=8$, the difference is bounded by the inequality

$$\left|8\hat{h}(\mathcal{P})-h_g(\mathcal{P})\right|\le\frac{1}{3}logC$$

where $\mathcal{P}\in E(\mathbb{Q})$, for an explicit constant $C\approx 1.41\times 10^{129}$ computed with *PARI/gp* [8].

$E(\mathbb{Q})$ has rank 1, so we can choose a generator $\mathcal{P}_0=(-1,-3)$, and for any $n\ge 1$ the above inequality and properties of the canonical height reveal

$$h_g([n+1]\mathcal{P}_0)-h_g([n]\mathcal{P}_0)>8\hat{h}([n+1]\mathcal{P}_0)-8\hat{h}([n]\mathcal{P}_0)-\frac{2}{3}logC$$
$$=8(n+1)^2\hat{h}(\mathcal{P}_0)-8n^2\hat{h}(\mathcal{P}_0)-\frac{2}{3}logC$$
$$=8(2n+1)\hat{h}(\mathcal{P}_0)-\frac{2}{3}logC$$

It follows that the difference above is positive as soon as

$$n\ge\frac{1}{2}\left(\frac{logC}{12\hat{h}(\mathcal{P}_0)}-1\right)\approx 417.25$$

With $\hat{h}(\mathcal{P}_0) \approx 0.059$ [8]. This tells us that if $n > 417$, $g([n+1]\mathcal{P}_0) \neq g([n]\mathcal{P}_0)$ and for $c = g([n]\mathcal{P}_0)$, we have $\#f_c^{-3}(-1)(\mathbb{Q}) = 2$. Therefore, our problem is reduced to verifying that for $1 \leq n \leq 417$, $\#f_c^{-3}(-1)(\mathbb{Q}) = 2$. This computation was done with PARI/gp [8] and the result was affirmative. ☐

c. Proof of Theorem 1.3

We are now ready to prove Theorem 1.3.

Proof. For any rational $c \neq 2$, Proposition 3.1 and Proposition 3.2 imply that

$$\kappa(-1) \leq \#f_c^{-1}(-1)(\mathbb{Q}) + \#f_c^{-2}(-1)(\mathbb{Q}) + \#f_c^{-3}(-1)(\mathbb{Q}) \leq 2 + 2 + 2 = 6$$

For

$$c = -\frac{113}{64},$$

$$\#\left\{\bigcup_{N\geq 1} f_c^{-N}(-1)(\mathbb{Q})\right\} = 6$$

So this bound is optimal. Hence, $\kappa(-1) = 6$. ☐

IV. COMPUTATIONAL EVIDENCE

a. Fourth Pre-images

We proved $\kappa(-1) = 6$ under the condition that $f_c^{-4}(-1)(\mathbb{Q}) = \emptyset$. A search for points on the elliptic curve birational to $X^{pre}(3,-1)$ up to logarithmic height 10^5 found no c-values with 4th pre-images.

b. Conjectural $\kappa(a)$

Recall that a search of rationals up to height 50 found only 6 a-values for which $X^{pre}(3,a)$ is birational to a rank 1 elliptic curve.

$$a \in \left\{-\frac{5}{4}, -1, -\frac{3}{4}, -\frac{1}{2}, 0, \frac{1}{4}\right\}.$$

Of these, $\kappa(a)$ has been conditionally proven for $a = 0$ [2] and $a = -1$. Here we conjecture $\kappa(a)$ for $a \in \left\{-\frac{5}{4}, -\frac{3}{4}, -\frac{1}{2}, \frac{1}{4}\right\}$.

With Bosma et al [1] it was determined for each $a \in \left\{-\frac{5}{4}, -\frac{3}{4}, -\frac{1}{2}, \frac{1}{4}\right\}$ that $S^{pre}(a)$ is birational to an elliptic curve with rank 0 and torsion subgroup of order 4, implying $\#S^{pre}(a)$ is finite. Mapping back from the elliptic curve to $S^{pre}(a)$, we find only two rational points $(Q,R,W) = (1,\pm 1,0)$ which are points at infinity. Thus $\#f_c^{-2}(a)(\mathbb{Q}) \leq 2$ for each a.

Since $X^{pre}(3,a)$ has rank 1, we were able to utilize the arithmetic of the curve to search for c-values corresponding to rational 3rd pre-images. Searching points with *PARI/gp* [8] up to logarithmic height 2.5×10^4, each a value had two rational 3rd pre-images and 0 rational 4th pre-images. There were finitely many exceptions corresponding to f_c for which a was a periodic point. We conclude with a conjecture.

Conjecture 4.1. *If* rank $X^{pre}(3,a) = 1$, then $\kappa(a) = 6$.

REFERENCES

1. Wieb Bosma, John Cannon, and Catherine Playoust. "The magma algebra system I" *The User language* **24**(3-4) (1997) 235-265.
2. Xander Faber and Benjmin Hutz. "On the number of rational iterated pre-images of the origin under quadratic dynamical systems" *arXiv*:0810.1715 (2008).
3. Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve. "Uniform bounds on pre-images under quadratic dynamical systems" *Mathematical Research Letters* 16(1) (2009) 87-101.
4. Patrick Morton and Joseph H. Silverman. "Rational periodic points of rational functions" *International Mathematics Research Notices* **2** (1994) 97-110.
5. Bjorn Poonen. "The complete classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$:

a refined conjecture" *Mathematische Zeitscrift* **228**(1) (1998) 11-29.
6. Joseph Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics* (Springer-Verlag, New York, 1992).
7. Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics (Springer-Verlag, New York, 1992).
8. The PARI Group, Bordeaux. *PARI/gp, version 2.3.2*, (2007). Available from http://pari.math.u-bordeaux.fr/


Why Sigma Xi?
THE HONOR SOCIETY FOR SCIENTISTS AND ENGINEERS
Recent chapter events have included:
Student research symposia
Outreach and mentoring
Workshop series
Social events
Resource activities for K-12 students and teachers
Awards for outstanding teaching and research
Lectureship series
Gain professional credentials
Being active in Sigma Xi demonstrates to employers and graduate schools that you have achieved a high standard of excellence. As a member of this prestigious society, you join the company of over 180 Nobel Prize winners and other distinguished scientists and engineers.
Receive research funding
Twice annually, the Sigma Xi Grants-in-Aid of Research program awards research grants to nearly 1,000 graduate and undergraduate students. As a Sigma Xi member you will be eligible to apply for grants from all available funds.
Build your professional network
Gain valuable leadership experience and make career contacts. Through local chapters, Sigma Xi provides a unique platform for interacting within a multi-disciplinary community of researchers, educators, administrators and others, both within and outside your institution.
Become a lifelong learner
Stay current in all fields with American Scientist, Sigma Xi's award winning magazine. As a member benefit, your American Scientist subscription is a valuable resource that offers articles in a variety of disciplines, resources and a comprehensive book review section.
Contribute to the scientific community
Sigma Xi members form a powerful international network at over 500 institutions. Through individual members and chapters, Sigma Xi addresses ethics, education, advocacy for research funding, public understanding of science, diversity and international networking.
Have fun
Build community and a sense of belonging with other scientists at your institution. Get involved in a special event with the help of others at your local chapter.
www.sigmaxi.org
Sigma Xi, The Scientific Research Society • 99 Alexander Drive • P.O. Box 13975 • Research Triangle Park, NC 27709 • 919-549-4691 • 800-243-6534