Dynamical Systems Techniques Applied to Number Theory

Yunus Emre Kara

May 25, 2007

Outline

Introduction
- Definitions
- Dynamical Systems Tools
- The function g_a
- Some observations on g_a

Results
- Main Results
- Other Results

Conclusion

Elementary Dynamical Systems Definitions

- The ***orbit*** of x is the set of points $x, f(x), f^2(x), \ldots$.
- The point x is a ***fixed point for*** f if $f(x) = x$.
- The point x is a ***periodic point of period*** n ***for*** f if $f^n(x) = x$.
- The orbit of a periodic point of period n is called an ***n-cycle***.
- The least positive n for which $f^n(x) = x$ is called ***the minimal period of*** x.
- The orbit of a periodic point of minimal period n is called a ***minimal n-cycle***.
- We let $\mathcal{N}_m(f)$ denote the number of points of minimal period m for the function f.

Dynamical Systems Tools

Lemma

- *If x_0 is a point of period n that has minimal period m, then $m|n$.*
- *Two minimal m-cycles are either disjoint or identical.*
- *For all $m \geq 1$, $m|\mathcal{N}_m$ whenever $\mathcal{N}_m$ is finite. Moreover, $\frac{\mathcal{N}_m}{m}$ is equal to the number of distinct minimal m-cycles.*

Definition

Let $\psi(m)$ be an integer-valued function defined on the set of all positive integers. If $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where the p_i's are distinct prime numbers, r and k_i's are positive integers, we let $\Phi_1(1, \psi) = \psi(1)$ and let

$$\begin{aligned}\Phi_1(m, \psi) &= \psi(m) - \sum_{i=1}^{r} \psi\left(\frac{m}{p_i}\right) + \sum_{i_1<i_2} \psi\left(\frac{m}{p_{i_1} p_{i_2}}\right) \\ &\quad - \sum_{i_1<i_2<i_3} \psi\left(\frac{m}{p_{i_1} p_{i_2} p_{i_3}}\right) + \dots + (-1)^r \psi\left(\frac{m}{p_{i_1} p_{i_2} \dots p_{i_r}}\right),\end{aligned}$$

where the summation $\sum_{i_1<i_2<\dots<i_j}$ is taken over all integers $i_1, i_2, \dots, i_j$ with $1 \le i_1 < i_2 < \dots < i_j \le r$.

Theorem

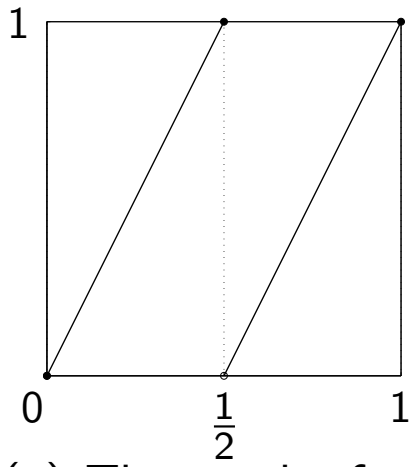
Let S be a nonempty set and let f be a map from S into itself such that, for every positive integer m, the equation $f^m(x) = x$ has only finitely many distinct solutions. Let $\psi(m)$ denote the number of these solutions. Then, for every positive integer m the number of periodic points of f with least period m is $\Phi_1(m, \psi)$ (i.e. $\mathscr{N}_m(f) = \Phi_1(m, \psi)$). Consequently, $\Phi_1(m, \psi) \equiv 0 \pmod{m}$.

The function g_a

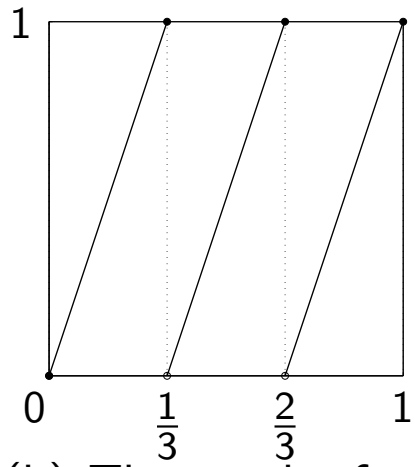
For each $a \geq 2$, let us define a function $g_a : [0,1] \longrightarrow [0,1]$ as

$$g_a(x) = \begin{cases} 0 & \text{for } x = 0 \\ a \cdot x - j & \text{for } \dfrac{j}{a} < x \leq \dfrac{j+1}{a} \end{cases}$$

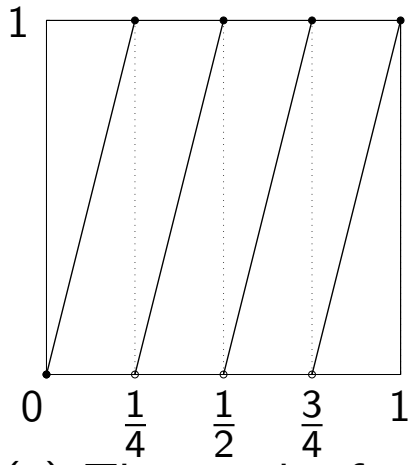
for $0 \leq j \leq a-1$.



(a) The graph of g_2



(b) The graph of g_3



(c) The graph of g_4

Some observations on g_a

Let a and b be positive integers.

- $g_{ab} = g_a \circ g_b = g_b \circ g_a$.

Some observations on g_a

Let a and b be positive integers.

- $g_{ab} = g_a \circ g_b = g_b \circ g_a$.
- ${g_a}^n = g_{a^n}$.

Some observations on g_a

Let a and b be positive integers.

- $g_{ab} = g_a \circ g_b = g_b \circ g_a$.
- ${g_a}^n = g_{a^n}$.
- The function g_a has a many fixed points, which are $j/(a-1)$ for $j = 0, \ldots, a-1$.

Some observations on g_a

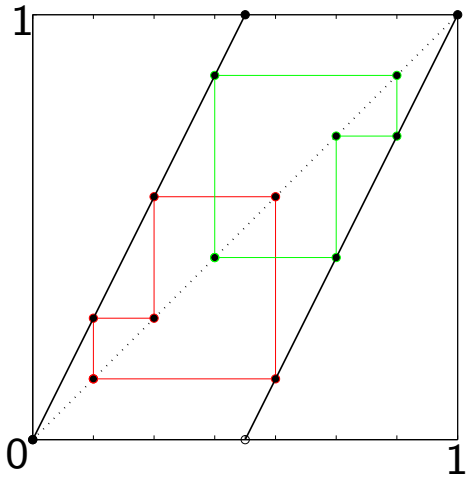
Let a and b be positive integers.

- $g_{ab} = g_a \circ g_b = g_b \circ g_a$.
- ${g_a}^n = g_{a^n}$.
- The function g_a has a many fixed points, which are $j/(a-1)$ for $j = 0, \ldots, a-1$.
- The function g_a has a^n many periodic points of period n, which are $j/(a^n-1)$ for $j = 0, \ldots, a^n - 1$.

Some observations on g_a

Let a and b be positive integers.

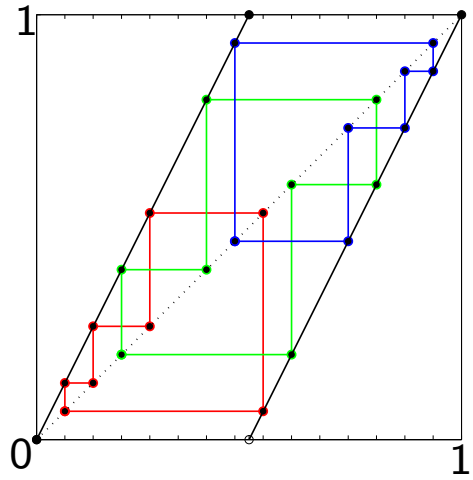
- $g_{ab} = g_a \circ g_b = g_b \circ g_a$.
- ${g_a}^n = g_{a^n}$.
- The function g_a has a many fixed points, which are $j/(a-1)$ for $j = 0, \ldots, a-1$.
- The function g_a has a^n many periodic points of period n, which are $j/(a^n-1)$ for $j = 0, \ldots, a^n - 1$.
- g_a satisfies the conditions of the previous theorem.



Red: $\left\{\frac{1}{7}, \frac{2}{7}, \frac{4}{7}\right\}$

Green: $\left\{\frac{3}{7}, \frac{6}{7}, \frac{5}{7}\right\}$

(3-cycles of g_2)



Red: $\left\{\frac{1}{15}, \frac{2}{15}, \frac{4}{15}, \frac{8}{15}\right\}$

Green: $\left\{\frac{3}{15}, \frac{6}{15}, \frac{12}{15}, \frac{9}{15}\right\}$

Blue: $\left\{\frac{7}{15}, \frac{14}{15}, \frac{13}{15}, \frac{11}{15}\right\}$

(4-cycles of g_2)

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For all integers $a \geq 2$ and all primes p, $a^p \equiv a \pmod{p}$.

Main Results Cont'd

Theorem

- *Let p and q be distinct primes and $a \geq 2$. Then $pq|(a^{pq} - a^p - a^q + a)$.*

Main Results Cont'd

Theorem

- *Let p and q be distinct primes and $a \geq 2$. Then $pq|(a^{pq} - a^p - a^q + a)$.*
- *Let p be a prime and $a \geq 2$ be an integer. Then $p^k|a^{p^k} - a^{p^{k-1}}$ for all $k \geq 1$.*

Other Results

- **Proposition:** If $\gcd(j, a^n - 1) = 1$, then $j/(a^n - 1)$ is a minimal n-periodic point of g_a.
- **Corollary:** Let m, n, a be integers such that $m, n \geq 1$ and $a \geq 2$. Then $m|n$ if and only if $a^m - 1|a^n - 1$.
- **Proposition:** If $j_1/(a^n - 1)$ and $j_2/(a^n - 1)$ belong to the same n-cycle, then $\gcd(j_1, a^n - 1) = \gcd(j_2, a^n - 1)$.
- **Corollary:** For any integer $a \geq 2$ and $n \geq 1$, $n|\phi(a^n - 1)$.

CONCLUSION

QUESTIONS?