Periods of sequences given by linear recurrence relations mod p

Alan Koch
Chrissy Franzel, Chuya Guo, Rose Psalmond,
Shan Shan, Hilary Tobiasz, Meina Zhou

Agnes Scott College

September 17, 2013

Outline

. . .

An example

Consider the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots .$$

Usually defined recursively

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n, n \geq 0. \end{aligned}$$

...

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . .

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . .

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . .

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . .

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . .

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . .

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . .

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . .

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . .

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,. . .

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,. . .

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, . . .

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . .

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . .

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . .

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . .

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,. . .

19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,. . .

Let p be a prime, and consider the Fibonacci sequence mod p.

- 2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,...
- 3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, ...
- 5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ...
- 7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, ...
- 11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ...
- 13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,...
- 17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,...
- 19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,...

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, 1, 0, 1, 1,...

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, ...

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ...

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, ...

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ...

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,...

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,...

19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,...

Each is periodic. Let $k(p)$ denote the period length.

...

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, ... $k(2) = 3$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, ... $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, ... $k(3) = 8$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

- 2 : 0, 1, 1, 0, 1, ... $k(2) = 3$
- 3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, ... $k(3) = 8$
- 5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ... $k(5) = 20$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

- 2 : 0, 1, 1, 0, 1, . . . $k(2) = 3$
- 3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, . . . $k(3) = 8$
- 5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . . $k(5) = 20$
- 7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . . $k(7) = 8$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, ... $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, ... $k(3) = 8$

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ... $k(5) = 20$

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, ... $k(7) = 8$

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ... $k(11) = 10$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, . . . $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, . . . $k(3) = 8$

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . . $k(5) = 20$

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . . $k(7) = 8$

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . . $k(11) = 10$

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . . . $k(13) = 28$

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Let p be a prime, and consider the Fibonacci sequence mod p.

- 2 : 0, 1, 1, 0, 1, . . . $k(2) = 3$
- 3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, . . . $k(3) = 8$
- 5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . . $k(5) = 20$
- 7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . . $k(7) = 8$
- 11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . . $k(11) = 10$
- 13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . . . $k(13) = 28$
- 17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,. . . $k(17) = 36$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, ... $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, ... $k(3) = 8$

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ... $k(5) = 20$

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, ... $k(7) = 8$

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ... $k(11) = 10$

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,.... $k(13) = 28$

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,... $k(17) = 36$

19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,... $k(19) = 18$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, ... $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, ... $k(3) = 8$

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, ... $k(5) = 20$

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, ... $k(7) = 8$

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, ... $k(11) = 10$

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . . . $k(13) = 28$

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,... $k(17) = 36$

19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,... $k(19) = 18$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Let p be a prime, and consider the Fibonacci sequence mod p.

2 : 0, 1, 1, 0, 1, . . . $k(2) = 3$

3 : 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, . . . $k(3) = 8$

5 : 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, . . . $k(5) = 20$

7 : 0, 1, 1, 2, 3, 5, 1, 6, 0, 1, . . . $k(7) = 8$

11 : 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, . . . $k(11) = 10$

13 : 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 10, 2, 12, 1, 0, 1,. . . . $k(13) = 28$

17 : 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0, 1,. . . $k(17) = 36$

19 : 0, 1, 1, 2, 3, 5, 8, 13, 2, 15, 17, 13, 11, 5, 16, 2, 18, 1, 0, 1,. . . $k(19) = 18$

Question. Is there a formula to compute $k(p)$? . . .

The answer...

Probably not.

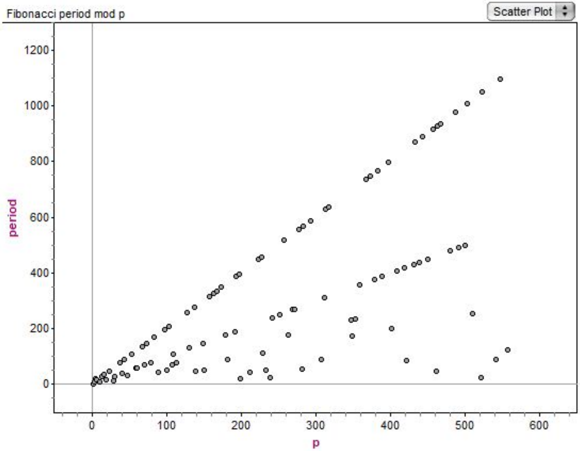

Figure: Fibonacci period as a function of p

But...

The figure suggests some results.

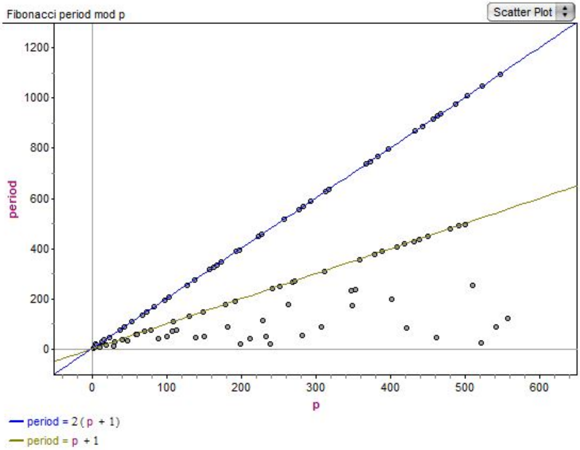

Figure: The lines are $k(p) = 2(p + 1)$ and $k(p) = p + 1$

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.
- $k(p) = p^2 - 1$ if and only if $p = 5$.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p + 1), k(p) \nmid (p + 1)$.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p+1), k(p) \nmid (p+1)$.

Facts about $k(p), p > 2$

[D.D. Wall, 1960]

- $k(p)$ is even.
- $k(p) \mid p^2 - 1$.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p+1), k(p) \nmid (p+1)$.

. . .

Generalization 1

What if we change the initial conditions?

Generalization 1

What if we change the initial conditions?
Often not interesting.

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.
- If $p \equiv \pm 1 \mod 5$ or $p = 5$ then

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.
- If $p \equiv \pm 1 \mod 5$ or $p = 5$ then
  - There are exactly $p(p-1)$ choices of initial conditions such that the period is $k(p)$.

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.
- If $p \equiv \pm 1 \mod 5$ or $p = 5$ then
  - There are exactly $p(p-1)$ choices of initial conditions such that the period is $k(p)$.
  - There are exactly $p-1$ choices of initial conditions such that the period is $k(p)/2$.
    Example 1. $p = 5 : 1, 3, 4, 2, 1, 3 \ldots$ (recall $k(5) = 20$)
    Example 2. $p = 11 : 1, 4, 5, 9, 3, 1, 4 \ldots$ (recall $k(11) = 10$)

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.
- If $p \equiv \pm 1 \mod 5$ or $p = 5$ then
  - There are exactly $p(p-1)$ choices of initial conditions such that the period is $k(p)$.
  - There are exactly $p-1$ choices of initial conditions such that the period is $k(p)/2$.
    Example 1. $p = 5 : 1, 3, 4, 2, 1, 3 \ldots$ (recall $k(5) = 20$)
    Example 2. $p = 11 : 1, 4, 5, 9, 3, 1, 4 \ldots$ (recall $k(11) = 10$)

Generalization 1

What if we change the initial conditions?
Often not interesting.

- If $p \equiv \pm 2 \mod 5$ then any change of initial conditions produces the same period.
- If $p \equiv \pm 1 \mod 5$ or $p = 5$ then
  - There are exactly $p(p-1)$ choices of initial conditions such that the period is $k(p)$.
  - There are exactly $p - 1$ choices of initial conditions such that the period is $k(p)/2$.
    Example 1. $p = 5 : 1, 3, 4, 2, 1, 3 \dots$ (recall $k(5) = 20$)
    Example 2. $p = 11 : 1, 4, 5, 9, 3, 1, 4 \dots$ (recall $k(11) = 10$)

The exception is the initial conditions $F_0 = F_1 = 0$ which produces a period length 1.

. . .

Generalization 2

What if we change the recurrence relation?

Generalization 2

What if we change the recurrence relation? Fix a prime $p > 2$. Consider a sequence $\{s_n\}$ which satisfies the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Generalization 2

What if we change the recurrence relation? Fix a prime $p > 2$. Consider a sequence $\{s_n\}$ which satisfies the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Must $\{s_n\}$ be periodic? If so:

1. What is the period?

Generalization 2

What if we change the recurrence relation? Fix a prime $p > 2$. Consider a sequence $\{s_n\}$ which satisfies the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Must $\{s_n\}$ be periodic? If so:

1. What is the period?
2. How much does the period length depend on the initial conditions s_0, s_1?

Generalization 2

What if we change the recurrence relation? Fix a prime $p > 2$. Consider a sequence $\{s_n\}$ which satisfies the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Must $\{s_n\}$ be periodic? If so:

1. What is the period?
2. How much does the period length depend on the initial conditions s_0, s_1?

Generalization 2

What if we change the recurrence relation? Fix a prime $p > 2$. Consider a sequence $\{s_n\}$ which satisfies the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Must $\{s_n\}$ be periodic? If so:

1. What is the period?
2. How much does the period length depend on the initial conditions s_0, s_1?

Clearly, period length depends only on the congruence classes of the parameters.

...

Some facts

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).
2. If k is the smallest positive integer such that $s_k = s_0$ and $s_{k+1} = s_1$ then the period is k.

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).
2. If k is the smallest positive integer such that $s_k = s_0$ and $s_{k+1} = s_1$ then the period is k.
3. If $t_0 = s_n$ and $t_1 = s_{n+1}$ and both sequences have the same recurrence relation, the two sequences have the same period.

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).
2. If k is the smallest positive integer such that $s_k = s_0$ and $s_{k+1} = s_1$ then the period is k.
3. If $t_0 = s_n$ and $t_1 = s_{n+1}$ and both sequences have the same recurrence relation, the two sequences have the same period.
4. The period is bounded by $p^2 - 1$.

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).
2. If k is the smallest positive integer such that $s_k = s_0$ and $s_{k+1} = s_1$ then the period is k.
3. If $t_0 = s_n$ and $t_1 = s_{n+1}$ and both sequences have the same recurrence relation, the two sequences have the same period.
4. The period is bounded by $p^2 - 1$.

Some facts

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{Z}, p \nmid c_2.$$

1. If $s_i = s_{i+k}$ and $s_{i+1} = s_{i+1+k}$ then $\{s_n\}$ is periodic (and period is a divisor of k).
2. If k is the smallest positive integer such that $s_k = s_0$ and $s_{k+1} = s_1$ then the period is k.
3. If $t_0 = s_n$ and $t_1 = s_{n+1}$ and both sequences have the same recurrence relation, the two sequences have the same period.
4. The period is bounded by $p^2 - 1$.

1, **2**, and **3** are straightforward; **4** follows from **3** since there are only $p^2 - 1$ nontrivial choices for consecutive pairs of elements mod p. . . .

Generalization 3

What if the recurrence is third order?

Generalization 3

What if the recurrence is third order? Fourth order?

What if the recurrence is third order? Fourth order? w^{th} order?

$$s_{n+w} = \sum_{i=1}^{w} c_i s_{n+w-i}, c_i \in \mathbb{Z}, p \nmid c_w.$$

Generalization 3

What if the recurrence is third order? Fourth order? w^{th} order?

$$s_{n+w} = \sum_{i=1}^{w} c_i s_{n+w-i}, c_i \in \mathbb{Z}, p \nmid c_w.$$

Must $\{s_n\}$ be periodic?

Generalization 3

What if the recurrence is third order? Fourth order? w^{th} order?

$$s_{n+w} = \sum_{i=1}^{w} c_i s_{n+w-i}, c_i \in \mathbb{Z}, p \nmid c_w.$$

Must $\{s_n\}$ be periodic? Yes, and bounded by $p^w - 1$.

Generalization 3

What if the recurrence is third order? Fourth order? w^{th} order?

$$s_{n+w} = \sum_{i=1}^{w} c_i s_{n+w-i}, c_i \in \mathbb{Z}, p \nmid c_w.$$

Must $\{s_n\}$ be periodic? Yes, and bounded by $p^w - 1$.

1. What is the period?

. . .

Generalization 3

What if the recurrence is third order? Fourth order? w^{th} order?

$$s_{n+w} = \sum_{i=1}^{w} c_i s_{n+w-i}, c_i \in \mathbb{Z}, p \nmid c_w.$$

Must $\{s_n\}$ be periodic? Yes, and bounded by $p^w - 1$.

1. What is the period?
2. How much does the period length depend on the initial conditions $s_0, s_1, \ldots, s_{w-1}$?

...

Outline

. . .

Some notation

Let:

- p be prime

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p-1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p - 1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p - 1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.
- $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with coefficients in the field F.

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p - 1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.
- $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with coefficients in the field F.
- $\mathrm{ord}(A), A \in \mathrm{GL}_n(F)$, be the order of A, i.e. the smallest positive integer k for which $A^k = I$ (if it exists).

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p-1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.
- $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with coefficients in the field F.
- $\mathrm{ord}(A), A \in \mathrm{GL}_n(F)$, be the order of A, i.e. the smallest positive integer k for which $A^k = I$ (if it exists).
- $|a|, a \neq 0 \in \mathbb{F}_{p^n}$ be the multiplicative order of a, i.e. the smallest positive integer k for which $a^k = 1$.

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p-1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.
- $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with coefficients in the field F.
- $\mathrm{ord}(A), A \in \mathrm{GL}_n(F)$, be the order of A, i.e. the smallest positive integer k for which $A^k = I$ (if it exists).
- $|a|, a \neq 0 \in \mathbb{F}_{p^n}$ be the multiplicative order of a, i.e. the smallest positive integer k for which $a^k = 1$.

Some notation

Let:

- p be prime
- $\mathbb{F}_p$ denote the set $\{0, 1, 2, \ldots, p-1\}$ with addition and multiplication defined modulo p.
  ($\mathbb{F}_p$ is the unique field of order p.)
- $\mathbb{F}_{p^w}$ be the unique field of order p^w.
- $\mathrm{GL}_n(F)$ be the group of invertible $n \times n$ matrices with coefficients in the field F.
- $\mathrm{ord}(A), A \in \mathrm{GL}_n(F)$, be the order of A, i.e. the smallest positive integer k for which $A^k = I$ (if it exists).
- $|a|, a \neq 0 \in \mathbb{F}_{p^n}$ be the multiplicative order of a, i.e. the smallest positive integer k for which $a^k = 1$.

. . .

An observation

Since period length depends only on the congruence classes for the parameters, we can consider sequences $\{s_n\} \subset \mathbb{F}_p$ which satisfy the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{F}_p, c_2 \neq 0.$$

An observation

Since period length depends only on the congruence classes for the parameters, we can consider sequences $\{s_n\} \subset \mathbb{F}_p$ which satisfy the recurrence relation

$$s_{n+2} = c_1 s_{n+1} + c_2 s_n, c_1, c_2 \in \mathbb{F}_p, c_2 \neq 0.$$

This allows us to use the theory of matrices over a field.

...

$s_{n+2} = c_1 s_{n+1} + c_2 s_n$, $c_1, c_2 \in \mathbb{F}_p$, $c_2 \neq 0$

A second-order linear recurrence relation gives rise to a 2×2 matrix.

A second-order linear recurrence relation gives rise to a 2×2 matrix. Let

$$A = A(c_1, c_2) = \begin{bmatrix} 0 & 1 \\ c_2 & c_1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p), \mathbf{x}_n = \begin{bmatrix} s_n \\ s_{n+1} \end{bmatrix}, n \geq 0.$$

A second-order linear recurrence relation gives rise to a 2×2 matrix. Let

$$A = A(c_1, c_2) = \begin{bmatrix} 0 & 1 \\ c_2 & c_1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p), \mathbf{x}_n = \begin{bmatrix} s_n \\ s_{n+1} \end{bmatrix}, n \geq 0.$$

Then

$$\begin{aligned} A\mathbf{x}_n &= \begin{bmatrix} 0 & 1 \\ c_2 & c_1 \end{bmatrix} \begin{bmatrix} s_n \\ s_{n+1} \end{bmatrix} \\ &= \begin{bmatrix} s_{n+1} \\ c_2 s_n + c_1 s_{n+1} \end{bmatrix} = \begin{bmatrix} s_{n+1} \\ s_{n+2} \end{bmatrix} \\ &= \mathbf{x}_{n+1} \end{aligned}$$

So $A^n \mathbf{x}_0 = \mathbf{x}_n$.

. . .

Suppose $\{s_n\}$ has period k.

Suppose $\{s_n\}$ has period k.
Then k is the smallest positive integer such that $\mathbf{x}_k = \mathbf{x}_0$.

Suppose $\{s_n\}$ has period k.
Then k is the smallest positive integer such that $\mathbf{x}_k = \mathbf{x}_0$.
Then k is the smallest positive integer such that $A^k \mathbf{x}_0 = \mathbf{x}_0$.

Suppose $\{s_n\}$ has period k.
Then k is the smallest positive integer such that $\mathbf{x}_k = \mathbf{x}_0$.
Then k is the smallest positive integer such that $A^k \mathbf{x}_0 = \mathbf{x}_0$.
So either $A^k = I$ or 1 is an eigenvalue for A^k and $\mathbf{x}_0$ is in its eigenspace.

Suppose $\{s_n\}$ has period k.
Then k is the smallest positive integer such that $\mathbf{x}_k = \mathbf{x}_0$.
Then k is the smallest positive integer such that $A^k \mathbf{x}_0 = \mathbf{x}_0$.
So either $A^k = I$ or 1 is an eigenvalue for A^k and $\mathbf{x}_0$ is in its eigenspace.
So either $A^k = I$ or there is an eigenvalue $\lambda \in \mathbb{F}_p$ for A such that $\lambda^k = 1$ and $\mathbf{x}_0$ is in its eigenspace (not obvious detail omitted).

$A = A(c_1, c_2) = \begin{bmatrix} 0 & 1 \\ c_2 & c_1 \end{bmatrix}, \mathbf{x}_n = \begin{bmatrix} s_n \\ s_{n+1} \end{bmatrix} = A^n \mathbf{x}_0$

Suppose $\{s_n\}$ has period k.
Then k is the smallest positive integer such that $\mathbf{x}_k = \mathbf{x}_0$.
Then k is the smallest positive integer such that $A^k \mathbf{x}_0 = \mathbf{x}_0$.
So either $A^k = I$ or 1 is an eigenvalue for A^k and $\mathbf{x}_0$ is in its eigenspace.
So either $A^k = I$ or there is an eigenvalue $\lambda \in \mathbb{F}_p$ for A such that $\lambda^k = 1$ and $\mathbf{x}_0$ is in its eigenspace (not obvious detail omitted). . . .

Outline

. . .

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

(Recall $p \equiv 2 \mod 5 \to k(p) \mid 2(p+1) \to k(7) \mid 16$.)

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
(Recall $p \equiv 2 \mod 5 \rightarrow k(p) \mid 2(p+1) \rightarrow k(7) \mid 16$.)
It can be shown that $\mathrm{ord}(A) = 8$.

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
(Recall $p \equiv 2 \mod 5 \to k(p) \mid 2(p+1) \to k(7) \mid 16$.)
It can be shown that $\mathrm{ord}(A) = 8$.
The characteristic equation for A is

$$\Delta(A) = \lambda^2 - \lambda - 1 = 0,$$

which has no solutions in $\mathbb{F}_7$.

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
(Recall $p \equiv 2 \mod 5 \to k(p) \mid 2(p+1) \to k(7) \mid 16$.)
It can be shown that $\text{ord}(A) = 8$.
The characteristic equation for A is

$$\Delta(A) = \lambda^2 - \lambda - 1 = 0,$$

which has no solutions in $\mathbb{F}_7$.
Since A has no eigenvalue in $\mathbb{F}_7$, the period is $k = 8$.

Fibonacci recurrence relation, $p = 7$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
(Recall $p \equiv 2 \mod 5 \rightarrow k(p) \mid 2(p+1) \rightarrow k(7) \mid 16$.)
It can be shown that $\text{ord}(A) = 8$.
The characteristic equation for A is

$$\Delta(A) = \lambda^2 - \lambda - 1 = 0,$$

which has no solutions in $\mathbb{F}_7$.
Since A has no eigenvalue in $\mathbb{F}_7$, the period is $k = 8$.
Notice that the period of the sequence is $k = 8$ regardless of initial conditions. . . .

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

The eigenspace for λ_1 has basis $\left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right\}$.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

The eigenspace for λ_1 has basis $\left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right\}$.

Thus the period of the sequence is

- $k = 5$ if $s_1 = 4s_0 \Leftarrow p - 1$ choices for this pair.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

The eigenspace for λ_1 has basis $\left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right\}$.

Thus the period of the sequence is

- $k = 5$ if $s_1 = 4s_0 \Leftarrow p - 1$ choices for this pair.
- $k = 10$ otherwise $\Leftarrow (p^2 - 1) - (p - 1) = p(p - 1)$ choices.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

The eigenspace for λ_1 has basis $\left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right\}$.

Thus the period of the sequence is

- $k = 5$ if $s_1 = 4s_0 \Leftarrow p - 1$ choices for this pair.
- $k = 10$ otherwise $\Leftarrow (p^2 - 1) - (p - 1) = p(p - 1)$ choices.

Fibonacci recurrence relation, $p = 11$

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

The characteristic equation is still $\Delta(A) = \lambda^2 - \lambda - 1 = 0$, which gives eigenvalues $\lambda_1 = 4, \lambda_2 = 8 \in \mathbb{F}_{11}$.

Easy to show $|4| = 5, |8| = 10$, and $\text{ord}(A) = \text{lcm}(|4|, |8|) = 10$.

The eigenspace for λ_1 has basis $\left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right\}$.

Thus the period of the sequence is

- $k = 5$ if $s_1 = 4s_0 \Leftarrow p - 1$ choices for this pair.
- $k = 10$ otherwise $\Leftarrow (p^2 - 1) - (p - 1) = p(p - 1)$ choices.

. . .

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

- if $p = 5$ then $d = 0$ and there is exactly one eigenvalue, namely $\lambda = 3$.

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

- if $p = 5$ then $d = 0$ and there is exactly one eigenvalue, namely $\lambda = 3$.
- if $p \equiv \pm 1 \mod 5$ then 5 is a quadratic residue, so we get two eigenvalues.

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

- if $p = 5$ then $d = 0$ and there is exactly one eigenvalue, namely $\lambda = 3$.
- if $p \equiv \pm 1 \mod 5$ then 5 is a quadratic residue, so we get two eigenvalues.
- if $p \equiv \pm 2 \mod 5$ then 5 is not a quadratic residue and we get no eigenvalues (in $\mathbb{F}_p$).

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

- if $p = 5$ then $d = 0$ and there is exactly one eigenvalue, namely $\lambda = 3$.
- if $p \equiv \pm 1 \mod 5$ then 5 is a quadratic residue, so we get two eigenvalues.
- if $p \equiv \pm 2 \mod 5$ then 5 is not a quadratic residue and we get no eigenvalues (in $\mathbb{F}_p$).

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, general $p > 2$

Over $\mathbb{R}$ the equation $\lambda^2 - \lambda - 1 = 0$ has solutions

$$\lambda = \frac{1 \pm \sqrt{5}}{2}.$$

Over $\mathbb{F}_p$, the multiplicative inverse to 2 is $(p+1)/2$.
The ability to solve this equation in $\mathbb{F}_p$ comes down to finding a "square root of 5 mod p", i.e., a $d \in \mathbb{F}_p$ with $d^2 = 5$.
If $p \neq 5$ this equation can be solved if and only if 5 is a quadratic residue mod p.

- if $p = 5$ then $d = 0$ and there is exactly one eigenvalue, namely $\lambda = 3$.
- if $p \equiv \pm 1 \mod 5$ then 5 is a quadratic residue, so we get two eigenvalues.
- if $p \equiv \pm 2 \mod 5$ then 5 is not a quadratic residue and we get no eigenvalues (in $\mathbb{F}_p$).

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\text{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are
  $(1,3), (2,1), (3,4), (4,2)$.
  All other initial conditions give $k = 20$.

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\mathrm{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are
  $(1, 3), (2, 1), (3, 4), (4, 2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \leq |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\text{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are $(1,3), (2,1), (3,4), (4,2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \leq |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:
  - $|\lambda_1|$ is even. Then $|\lambda_1| = |\lambda_2|$ and for all (s_0, s_1), $k = \text{ord}(A) = |\lambda_1|$.

$s_{n+2} = s_{n+1} + s_n$

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\text{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are $(1,3), (2,1), (3,4), (4,2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \leq |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:
  - $|\lambda_1|$ is even. Then $|\lambda_1| = |\lambda_2|$ and for all (s_0, s_1), $k = \text{ord}(A) = |\lambda_1|$.
  - $|\lambda_1|$ is odd. Then $|\lambda_2| = 2|\lambda_1|$ and $k = |\lambda_1|$ provided $s_1 = \lambda_1 s_0$; otherwise $k = \text{ord}(A) = |\lambda_2|$.

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\text{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are $(1, 3), (2, 1), (3, 4), (4, 2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \leq |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:
  - $|\lambda_1|$ is even. Then $|\lambda_1| = |\lambda_2|$ and for all (s_0, s_1), $k = \text{ord}(A) = |\lambda_1|$.
  - $|\lambda_1|$ is odd. Then $|\lambda_2| = 2|\lambda_1|$ and $k = |\lambda_1|$ provided $s_1 = \lambda_1 s_0$; otherwise $k = \text{ord}(A) = |\lambda_2|$.
- if $p \equiv \pm 2 \mod 5$ then $k = \text{ord}(A)$ for all initial conditions.

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\mathrm{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are $(1,3), (2,1), (3,4), (4,2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \leq |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:
  - $|\lambda_1|$ is even. Then $|\lambda_1| = |\lambda_2|$ and for all (s_0, s_1), $k = \mathrm{ord}(A) = |\lambda_1|$.
  - $|\lambda_1|$ is odd. Then $|\lambda_2| = 2|\lambda_1|$ and $k = |\lambda_1|$ provided $s_1 = \lambda_1 s_0$; otherwise $k = \mathrm{ord}(A) = |\lambda_2|$.
- if $p \equiv \pm 2 \mod 5$ then $k = \mathrm{ord}(A)$ for all initial conditions.

if $p = 5$ then $\lambda = 3$.
if $p \equiv \pm 1 \mod 5$ then two eigenvalues.
if $p \equiv \pm 2 \mod 5$ then no eigenvalues.

- if $p = 5$ then $\text{ord}(A) = 20$ and $|3| = 4$.
  The initial conditions (s_0, s_1) which give $k = 5$ are $(1,3), (2,1), (3,4), (4,2)$.
  All other initial conditions give $k = 20$.
- if $p \equiv \pm 1 \mod 5$ we have eigenvalues λ_1, λ_2, say $|\lambda_1| \le |\lambda_2|$.
  Note $\lambda_1 \lambda_2 = -1$, $\lambda_1 + \lambda_2 = 1$.
  Two cases:
  - $|\lambda_1|$ is even. Then $|\lambda_1| = |\lambda_2|$ and for all (s_0, s_1), $k = \text{ord}(A) = |\lambda_1|$.
  - $|\lambda_1|$ is odd. Then $|\lambda_2| = 2|\lambda_1|$ and $k = |\lambda_1|$ provided $s_1 = \lambda_1 s_0$; otherwise $k = \text{ord}(A) = |\lambda_2|$.
- if $p \equiv \pm 2 \mod 5$ then $k = \text{ord}(A)$ for all initial conditions.

...

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \mathrm{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \mathrm{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

- $k(p) \mid p^2 - 1$.
  $|\lambda_1|, |\lambda_2|$ divide $|\mathbb{F}_{p^2}^\times| = p^2 - 1$.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \mathrm{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

- $k(p) \mid p^2 - 1$.
  $|\lambda_1|, |\lambda_2|$ divide $|\mathbb{F}_{p^2}^\times| = p^2 - 1$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
  $\lambda_1, \lambda_2 \in \mathbb{F}_p$ so their orders divide $p - 1$.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \mathrm{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

- $k(p) \mid p^2 - 1$.
  $|\lambda_1|, |\lambda_2|$ divide $|\mathbb{F}_{p^2}^\times| = p^2 - 1$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
  $\lambda_1, \lambda_2 \in \mathbb{F}_p$ so their orders divide $p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p+1), k(p) \nmid (p+1)$.
  In this case $\lambda_2 = \lambda_1^p$. The result follows from this relationship.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}, p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $GL_2(\mathbb{F}_{p^2})$ and has order $\text{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \text{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

- $k(p) \mid p^2 - 1$.
  $|\lambda_1|, |\lambda_2|$ divide $|\mathbb{F}_{p^2}^{\times}| = p^2 - 1$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
  $\lambda_1, \lambda_2 \in \mathbb{F}_p$ so their orders divide $p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p+1), k(p) \nmid (p+1)$.
  In this case $\lambda_2 = \lambda_1^p$. The result follows from this relationship.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
  Note $A(1,1)$ is not diagonalizable when $p = 5$.

Back to the Fibonacci sequence

In $\mathbb{F}_{p^2}$, $p \neq 5$, $\lambda^2 - \lambda - 1 = 0$ has two distinct solutions λ_1, λ_2.
Then A is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ and has order $\mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Note $k(p) = \mathrm{ord}(A)$ since $\mathbf{x}_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector.

- $k(p) \mid p^2 - 1$.
  $|\lambda_1|, |\lambda_2|$ divide $|\mathbb{F}_{p^2}^{\times}| = p^2 - 1$.
- If $p \equiv \pm 1 \mod 5$ then $k(p) \mid p - 1$.
  $\lambda_1, \lambda_2 \in \mathbb{F}_p$ so their orders divide $p - 1$.
- If $p \equiv \pm 2 \mod 5$ then $k(p) \mid 2(p+1), k(p) \nmid (p+1)$.
  In this case $\lambda_2 = \lambda_1^p$. The result follows from this relationship.
- $k(p) = p^2 - 1$ if and only if $p = 5$.
  Note $A(1, 1)$ is not diagonalizable when $p = 5$.
- $k(p)$ is even.
  Follows mostly from the previous results.

Fix a prime p.

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p, c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.
Note the Fibonacci period is $k_{(1,1)}(0, 1)$, and that p is suppressed in this notation.

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.
Note the Fibonacci period is $k_{(1,1)}(0, 1)$, and that p is suppressed in this notation.

Questions.

1. What are the possible values of $k_{(c_1,c_2)}(s_0, s_1)$?

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.
Note the Fibonacci period is $k_{(1,1)}(0, 1)$, and that p is suppressed in this notation.

Questions.

1. What are the possible values of $k_{(c_1,c_2)}(s_0, s_1)$?
2. Which positive integers k are realizable as a period length, i.e. for which k is there a choice of $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, such that $k_{(c_1,c_2)}(s_0, s_1) = n$?

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.
Note the Fibonacci period is $k_{(1,1)}(0, 1)$, and that p is suppressed in this notation.

Questions.

1. What are the possible values of $k_{(c_1,c_2)}(s_0, s_1)$?
2. Which positive integers k are realizable as a period length, i.e. for which k is there a choice of $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, such that $k_{(c_1,c_2)}(s_0, s_1) = n$?

Fix a prime p.
For $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, let $k_{(c_1,c_2)}(s_0, s_1)$ be the period of $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ with initial conditions s_0, s_1.
Note the Fibonacci period is $k_{(1,1)}(0, 1)$, and that p is suppressed in this notation.

Questions.

1. What are the possible values of $k_{(c_1,c_2)}(s_0, s_1)$?
2. Which positive integers k are realizable as a period length, i.e. for which k is there a choice of $c_1, c_2, s_0, s_1 \in \mathbb{F}_p$, $c_2 \neq 0$, such that $k_{(c_1,c_2)}(s_0, s_1) = n$?

For brevity, write k for $k_{(c_1,c_2)}(s_0, s_1)$.

...

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)
  - Then $k = |\lambda_1|$.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)
  - Then $k = |\lambda_1|$.
  - Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$ we have $k \mid (p-1)$.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)
  - Then $k = |\lambda_1|$.
  - Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$ we have $k \mid (p-1)$.
- **Subcase 2.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ is not in an eigenspace.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)
    - Then $k = |\lambda_1|$.
    - Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$ we have $k \mid (p-1)$.
- **Subcase 2.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ is not in an eigenspace.
    - Then $k = \mathrm{ord}(A) = \mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.

Possible values

The matrix $A = A(c_1, c_2)$ has characteristic equation

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 1. $c_1^2 + 4c_2$ is a quadratic residue $\mod p$.

- Let $\lambda_1, \lambda_2 \in \mathbb{F}_p$ be the (distinct, nonzero) eigenvalues.
- A is similar to $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.
- **Subcase 1.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ be in one of the two eigenspaces, say the subspace corresponding to eigenvalue λ_1. (So $s_1 = \lambda_1 s_0$.)
  - Then $k = |\lambda_1|$.
  - Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$ we have $k \mid (p-1)$.
- **Subcase 2.** $(s_0, s_1) \in (\mathbb{F}_p)^2$ is not in an eigenspace.
  - Then $k = \mathrm{ord}(A) = \mathrm{lcm}(|\lambda_1|, |\lambda_2|)$.
  - Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$ we have

$$k \mid (p-1).$$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 2. $c_1^2 + 4c_2$ is not a quadratic nonresidue $\mod p$.

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 2. $c_1^2 + 4c_2$ is not a quadratic nonresidue $\mod p$.

- Let $\lambda, \lambda^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ be the eigenvalues.

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 2. $c_1^2 + 4c_2$ is not a quadratic nonresidue $\mod p$.

- Let $\lambda, \lambda^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ be the eigenvalues.
- A is diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^p \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 2. $c_1^2 + 4c_2$ is not a quadratic nonresidue $\mod p$.

- Let $\lambda, \lambda^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ be the eigenvalues.
- A is diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^p \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

- Then $k = \mathrm{ord}(A) = \mathrm{lcm}(|\lambda|, |\lambda^p|) = |\lambda|$.

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 2. $c_1^2 + 4c_2$ is not a quadratic nonresidue $\mod p$.

- Let $\lambda, \lambda^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ be the eigenvalues.
- A is diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^p \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

- Then $k = \mathrm{ord}(A) = \mathrm{lcm}(|\lambda|, |\lambda^p|) = |\lambda|$.
- Since $|a| \mid (p^2 - 1), |a| \nmid (p - 1)$ for all $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, we have

$$k \mid (p^2 - 1), k \nmid (p - 1).$$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 3. $c_1^2 + 4c_2 = 0.$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 3. $c_1^2 + 4c_2 = 0$.

- Then there is an eigenvalue $\lambda \in \mathbb{F}_p$ with algebraic multiplicity 2.

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 3. $c_1^2 + 4c_2 = 0$.

- Then there is an eigenvalue $\lambda \in \mathbb{F}_p$ with algebraic multiplicity 2.
- A is *not* diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 3. $c_1^2 + 4c_2 = 0.$

- Then there is an eigenvalue $\lambda \in \mathbb{F}_p$ with algebraic multiplicity 2.
- A is *not* diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

- Then $k = \mathrm{ord}(A) = p|\lambda|.$

Possible values

$$\Delta(A) = \lambda^2 - c_1\lambda - c_2 = 0.$$

Case 3. $c_1^2 + 4c_2 = 0$.

- Then there is an eigenvalue $\lambda \in \mathbb{F}_p$ with algebraic multiplicity 2.
- A is *not* diagonalizable; it is similar to

$$\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2})$$

- Then $k = \mathrm{ord}(A) = p|\lambda|$.
- Since $|a| \mid (p-1)$ for all nonzero $a \in \mathbb{F}_p$, we have

$$k = pm, \text{ for some } m \mid (p-1).$$

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]
Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]
Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?
Answer. Either

- k divides $p^2 - 1$, or

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]
Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?
Answer. Either

- k divides $p^2 - 1$, or
- $p \mid k$ and $k \mid (p(p-1))$,

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]

Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?

Answer. Either

- k divides $p^2 - 1$, or
- $p \mid k$ and $k \mid (p(p-1))$,

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]
Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?
Answer. Either

- k divides $p^2 - 1$, or
- $p \mid k$ and $k \mid (p(p-1))$,

the latter case holding if and only if $c_1^2 - 4c_2 = 0$.

Summary

[C. Franzel, R. Psalmond, H, Tobiasz, 2011]
Question. What are the possible values of $k := k_{(c_1,c_2)}(s_0, s_1)$?
Answer. Either

- k divides $p^2 - 1$, or
- $p \mid k$ and $k \mid (p(p-1))$,

the latter case holding if and only if $c_1^2 - 4c_2 = 0$.
Example. For $p = 17$ the only possible periods are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 18, 24, 32,$$
$$34, 36, 48, 68, 72, 96, 136, 144, 272, 288.$$

...

Realizability

Example. For $p = 17$ the only possible periods are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 18, 24, 32,$$
$$34, 36, 48, 68, 72, 96, 136, 144, 272, 288.$$

Example. For $p = 17$ the only possible periods are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 18, 24, 32,$$
$$34, 36, 48, 68, 72, 96, 136, 144, 272, 288.$$

Question. Do all of the above numbers actually arise as periods?

Realizability

Example. For $p = 17$ the only possible periods are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 18, 24, 32,$$
$$34, 36, 48, 68, 72, 96, 136, 144, 272, 288.$$

Question. Do all of the above numbers actually arise as periods? We say a positive integer k is *realizable* mod p if there exists c_1, c_2, s_0, s_1 such that $k = k_{(c_1,c_2)}(s_0, s_1)$.

Realizability

Example. For $p = 17$ the only possible periods are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 18, 24, 32,$$
$$34, 36, 48, 68, 72, 96, 136, 144, 272, 288.$$

Question. Do all of the above numbers actually arise as periods?
We say a positive integer k is *realizable* mod p if there exists c_1, c_2, s_0, s_1 such that $k = k_{(c_1,c_2)}(s_0, s_1)$.
Note that 1 is realizable for all p. ($s_0 = s_1 = 0$).

. . .

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k$.

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k$.

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k$.

The three cases will correspond to the three possibilities for the eigenvalues λ_1, λ_2 of the constructed matrix $A(c_0, c_1)$:

1. $\lambda_1, \lambda_2 \in \mathbb{F}_p$

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k.$

The three cases will correspond to the three possibilities for the eigenvalues λ_1, λ_2 of the constructed matrix $A(c_0, c_1)$:

1. $\lambda_1, \lambda_2 \in \mathbb{F}_p$
2. $\lambda_1, \lambda_2 = \lambda_1^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k.$

The three cases will correspond to the three possibilities for the eigenvalues λ_1, λ_2 of the constructed matrix $A(c_0, c_1)$:

1. $\lambda_1, \lambda_2 \in \mathbb{F}_p$
2. $\lambda_1, \lambda_2 = \lambda_1^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$
3. $\lambda_1 = \lambda_2 \in \mathbb{F}_p.$

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k$.

The three cases will correspond to the three possibilities for the eigenvalues λ_1, λ_2 of the constructed matrix $A(c_0, c_1)$:

1. $\lambda_1, \lambda_2 \in \mathbb{F}_p$
2. $\lambda_1, \lambda_2 = \lambda_1^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$
3. $\lambda_1 = \lambda_2 \in \mathbb{F}_p$.

If k is realizable, then $k \mid p^2 - 1$ or $k \mid p(p-1)$

Theorem. [C. Franzel, R. Psalmond, H. Tobiasz, 2011] Any k satisfying the divisibility criteria above is realizable.
We will investigate three cases.

1. $k \mid p - 1$
2. $k \mid p^2 - 1, k \nmid p - 1$
3. $k \mid p(p-1), p \mid k.$

The three cases will correspond to the three possibilities for the eigenvalues λ_1, λ_2 of the constructed matrix $A(c_0, c_1)$:

1. $\lambda_1, \lambda_2 \in \mathbb{F}_p$
2. $\lambda_1, \lambda_2 = \lambda_1^p \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$
3. $\lambda_1 = \lambda_2 \in \mathbb{F}_p.$

. . .

Case 1: $k \mid p-1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)

Case 1: $k \mid p - 1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \notin \{0, \lambda_1\}$.

Case 1: $k \mid p - 1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \notin \{0, \lambda_1\}$.
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix}$$

Case 1: $k \mid p - 1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \notin \{0, \lambda_1\}$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix}$$

Case 1: $k \mid p - 1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \notin \{0, \lambda_1\}$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix}$$

Then λ_1 is an eigenvalue for A, and $\begin{bmatrix} 1 \\ \lambda_1 \end{bmatrix}$ is a corresponding eigenvector.

Case 1: $k \mid p-1$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$.
  (Technical detail: yes, you can do this.)
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \notin \{0, \lambda_1\}$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix}$$

Then λ_1 is an eigenvalue for A, and $\begin{bmatrix} 1 \\ \lambda_1 \end{bmatrix}$ is a corresponding eigenvector. The sequence

$$\begin{aligned} s_0 &= 1 \\ s_1 &= \lambda_1 \\ s_{n+2} &= (\lambda_1 + \lambda_2)s_{n+1} - \lambda_1\lambda_2 s_n \end{aligned}$$

has period k.

Example: $p = 17, k = 8$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$. One choice: $\lambda_1 = 2$.

Example: $p = 17, k = 8$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$. One choice: $\lambda_1 = 2$.
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \neq 0, \lambda_1$. One choice: $\lambda_2 = 1$.

Example: $p = 17, k = 8$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$. One choice: $\lambda_1 = 2$.
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \neq 0, \lambda_1$. One choice: $\lambda_2 = 1$.
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 15 & 3 \end{bmatrix}$$

Example: $p = 17, k = 8$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$. One choice: $\lambda_1 = 2$.
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \neq 0, \lambda_1$. One choice: $\lambda_2 = 1$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 15 & 3 \end{bmatrix}$$

Example: $p = 17, k = 8$

- Pick $\lambda_1 \in \mathbb{F}_p, |\lambda_1| = k$. One choice: $\lambda_1 = 2$.
- Let $\lambda_2 \in \mathbb{F}_p, \lambda_2 \neq 0, \lambda_1$. One choice: $\lambda_2 = 1$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 15 & 3 \end{bmatrix}$$

The sequence

$$\begin{aligned} s_0 &= 1 \\ s_1 &= 2 \\ s_{n+2} &= 3s_{n+1} + 15s_n \end{aligned}$$

has period $k = 8$:

$$1, 2, 4, 8, 16, 15, 13, 9, 1, 2, \ldots.$$

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well.

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix}$$

  (Technical detail 2: $-\lambda^{p+1}, \lambda + \lambda^p \in \mathbb{F}_p$.)

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well.
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix}$$
  (Technical detail 2: $-\lambda^{p+1}, \lambda + \lambda^p \in \mathbb{F}_p$.)

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well.
- Let
  $$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix}$$
  (Technical detail 2: $-\lambda^{p+1}, \lambda + \lambda^p \in \mathbb{F}_p$.)

Then $\text{ord}(A) = k$.

Case 2: $k \mid p^2 - 1, k \nmid p - 1$

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$.
  (Technical detail 1: yes, you can do this.)
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix}$$

  (Technical detail 2: $-\lambda^{p+1}, \lambda + \lambda^p \in \mathbb{F}_p$.)

Then $\text{ord}(A) = k$. The sequence

$$\begin{aligned} s_0 &= 0 \\ s_1 &= 1 \\ s_{n+2} &= \lambda + \lambda^p s_{n+1} - \lambda^{p+1} s_n \end{aligned}$$

has period k.

. . .

Example: $p = 17, k = 18$

We write $\mathbb{F}_{p^2} = \{a + b\alpha : a, b \in \mathbb{F}_p, \alpha^2 = 3\}$.

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$. One choice: $\lambda_1 = 2 + \alpha$.

Example: $p = 17, k = 18$

We write $\mathbb{F}_{p^2} = \{a + b\alpha : a, b \in \mathbb{F}_p, \alpha^2 = 3\}$.

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$. One choice: $\lambda_1 = 2 + \alpha$.
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well. $\lambda^p = 2 + 16\alpha = 2 - \alpha$.

Example: $p = 17, k = 18$

We write $\mathbb{F}_{p^2} = \{a + b\alpha : a, b \in \mathbb{F}_p, \alpha^2 = 3\}$.

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$. One choice: $\lambda_1 = 2 + \alpha$.
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well. $\lambda^p = 2 + 16\alpha = 2 - \alpha$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 4 \end{bmatrix}$$

Example: $p = 17, k = 18$

We write $\mathbb{F}_{p^2} = \{a + b\alpha : a, b \in \mathbb{F}_p, \alpha^2 = 3\}$.

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$. One choice: $\lambda_1 = 2 + \alpha$.
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well. $\lambda^p = 2 + 16\alpha = 2 - \alpha$.
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 4 \end{bmatrix}$$

Example: $p = 17, k = 18$

We write $\mathbb{F}_{p^2} = \{a + b\alpha : a, b \in \mathbb{F}_p, \alpha^2 = 3\}$.

- Pick $\lambda := \lambda_1 \in \mathbb{F}_{p^2}, |\lambda| = k$. One choice: $\lambda_1 = 2 + \alpha$.
- Let $\lambda_2 = \lambda^p$. Note $|\lambda^p| = k$ as well. $\lambda^p = 2 + 16\alpha = 2 - \alpha$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^{p+1} & \lambda + \lambda^p \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 4 \end{bmatrix}$$

The sequence

$$\begin{aligned} s_0 &= 0 \\ s_1 &= 1 \\ s_{n+2} &= 4s_{n+1} - s_n \end{aligned}$$

has period $k = 18$:

$$0, 1, 4, 15, 5, 5, 15, 4, 1, 0, 16, 13, 2, 12, 12, 2, 13, 16, 0, 1, \ldots$$

Case 3: $k \mid p(p-1), p \mid k$

Let $m = k/p \in \mathbb{Z}$.

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$.
  (Technical detail: yes, you can still do this since $m \mid p-1$.)

Case 3: $k \mid p(p-1), p \mid k$

Let $m = k/p \in \mathbb{Z}$.

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$.
  (Technical detail: yes, you can still do this since $m \mid p - 1$.)
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}$$

Case 3: $k \mid p(p-1), p \mid k$

Let $m = k/p \in \mathbb{Z}$.

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$.
  (Technical detail: yes, you can still do this since $m \mid p - 1$.)
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}$$

Case 3: $k \mid p(p-1), p \mid k$

Let $m = k/p \in \mathbb{Z}$.

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$.
  (Technical detail: yes, you can still do this since $m \mid p - 1$.)
- Let
$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}$$

Then A has exactly one eigenvalue λ and is clearly not diagonalizable, so A is similar to $\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix}$ which has order pm.

Case 3: $k \mid p(p-1), p \mid k$

Let $m = k/p \in \mathbb{Z}$.

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$.
  (Technical detail: yes, you can still do this since $m \mid p - 1$.)
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}$$

Then A has exactly one eigenvalue λ and is clearly not diagonalizable, so A is similar to $\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix}$ which has order pm. The sequence

$$\begin{aligned} s_0 &= 0 \\ s_1 &= 1 \\ s_{n+2} &= 2\lambda s_{n+1} - \lambda^2 s_n \end{aligned}$$

has period k.

Example: $p = 17, k = 68, m = 68/17 = 4$

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$. One choice: $\lambda = 4$.

Example: $p = 17, k = 68, m = 68/17 = 4$

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$. One choice: $\lambda = 4$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 8 \end{bmatrix}$$

Example: $p = 17, k = 68, m = 68/17 = 4$

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$. One choice: $\lambda = 4$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 8 \end{bmatrix}$$

Example: $p = 17, k = 68, m = 68/17 = 4$

- Pick $\lambda \in \mathbb{F}_p, |\lambda| = m$. One choice: $\lambda = 4$.
- Let

$$A = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 8 \end{bmatrix}$$

The sequence

$$s_0 = 0, s_1 = 1, s_{n+2} = 8s_{n+1} + s_n$$

has period $k = 68$:

$$0, 1, 8, 14, 1, 5, 7, 10, 2, 9, 6, 6, 3, 13, 5, 2, 4,$$
$$0, 4, 15, 5, 4, 3, 11, 6, 8, 2, 7, 7, 12, 1, 3, 8, 16,$$
$$0, 16, 9, 3, 16, 12, 10, 7, 15, 8, 11, 11, 14, 4, 12, 15, 13,$$
$$0, 13, 2, 12, 13, 14, 6, 11, 9, 15, 10, 10, 5, 16, 14, 9, 1,$$
$$0, 1, \ldots$$

A New Question

For a fixed p, we know that $p^2 - 1$ is the maximum period.

A New Question

For a fixed p, we know that $p^2 - 1$ is the maximum period.
Question How likely will a choice of c_1, c_2 give $k_{(c_1,c_2)}(0,1) = p^2 - 1$?

A New Question

For a fixed p, we know that $p^2 - 1$ is the maximum period.
Question How likely will a choice of c_1, c_2 give $k_{(c_1,c_2)}(0,1) = p^2 - 1$?
Recall: $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cannot be an eigenvector for $A(c_1, c_2)$ and hence will give the longest period for the recurrence relation.

...

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$.
  $(\phi(n) =^{\#} \{1 \leq a \leq n : \gcd(a, n) = 1\})$

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$.
  $(\phi(n) =^{\#} \{1 \leq a \leq n : \gcd(a, n) = 1\})$
- For a given choice of λ we get

$$c_1 = \lambda + \lambda^p, c_2 = -\lambda^{p+1}$$

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$. $(\phi(n) =^\# \{1 \leq a \leq n : \gcd(a, n) = 1\})$
- For a given choice of λ we get

$$c_1 = \lambda + \lambda^p, c_2 = -\lambda^{p+1}$$

- Two different choices of eigenvalue, say λ and γ, will give the same values for c_1, c_2 if and only if $\gamma = \lambda^p$ or (equivalently) $\lambda = \gamma^p$.

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$. $(\phi(n) =^{\#} \{1 \leq a \leq n : \gcd(a, n) = 1\})$
- For a given choice of λ we get

$$c_1 = \lambda + \lambda^p, c_2 = -\lambda^{p+1}$$

- Two different choices of eigenvalue, say λ and γ, will give the same values for c_1, c_2 if and only if $\gamma = \lambda^p$ or (equivalently) $\lambda = \gamma^p$.

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$. $(\phi(n) =^{\#} \{1 \leq a \leq n : \gcd(a,n) = 1\})$
- For a given choice of λ we get

$$c_1 = \lambda + \lambda^p, c_2 = -\lambda^{p+1}$$

- Two different choices of eigenvalue, say λ and γ, will give the same values for c_1, c_2 if and only if $\gamma = \lambda^p$ or (equivalently) $\lambda = \gamma^p$.

Theorem. [K., M. Zhou, 2013)] The number of linear recurrence relations for which $k_{(c_1,c_2)}(0,1) = p^2 - 1$ is

$$\frac{\phi(p^2 - 1)}{2}.$$

Sketch of results

Suppose $k_{(c_1,c_2)}(0,1) = p^2 - 1$. Then

- $A(c_1, c_2)$ has two eigenvectors $\lambda, \lambda^p \notin \mathbb{F}_p$.
- $|\lambda| = p^2 - 1$.
- There are $\phi(p^2 - 1)$ elements in $\mathbb{F}_{p^2}$ of order $p^2 - 1$.
  $(\phi(n) =^{\#} \{1 \leq a \leq n : \gcd(a, n) = 1\})$
- For a given choice of λ we get

$$c_1 = \lambda + \lambda^p, c_2 = -\lambda^{p+1}$$

- Two different choices of eigenvalue, say λ and γ, will give the same values for c_1, c_2 if and only if $\gamma = \lambda^p$ or (equivalently) $\lambda = \gamma^p$.

Theorem. [K., M. Zhou, 2013)] The number of linear recurrence relations for which $k_{(c_1,c_2)}(0,1) = p^2 - 1$ is

$$\frac{\phi(p^2 - 1)}{2}.$$

So the probability that a random (c_1, c_2) gives maximal period is $\phi(p^2 - 1)/(2(p^2 - 1))$.

$\phi(p^k) = p^{k-1}(p-1), p$ prime; $\phi(mn) = \phi(m)\phi(n), \gcd(m,n) = 1.$

$\phi(p^k) = p^{k-1}(p-1), p$ prime; $\phi(mn) = \phi(m)\phi(n), \gcd(m,n) = 1.$

Example ($p = 17, p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$

$\phi(p^k) = p^{k-1}(p-1), p$ prime; $\phi(mn) = \phi(m)\phi(n), \gcd(m,n) = 1.$

Example ($p = 17, p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$

$\phi(p^k) = p^{k-1}(p-1), p$ prime; $\phi(mn) = \phi(m)\phi(n), \gcd(m,n) = 1.$

Example ($p = 17, p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$
So there are 48 choices of (c_1, c_2) which give the maximum period (probability: $48/288 = 1/6$).

$\phi(p^k) = p^{k-1}(p-1)$, p prime; $\phi(mn) = \phi(m)\phi(n)$, $\gcd(m,n) = 1$.

Example ($p = 17$, $p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$
So there are 48 choices of (c_1, c_2) which give the maximum period (probability: $48/288 = 1/6$).

Example ($p = 2017$, $p^2 - 1 = 4068288 = 2^6 \cdot 3^2 \cdot 7 \cdot 1009$)

We have

$$\begin{aligned}\phi(4068288) &= \phi(2^6)\phi(3^2)\phi(7)\phi(1009) \\ &= 32 \cdot 6 \cdot 6 \cdot 1008 = 1161216\end{aligned}$$

$\phi(p^k) = p^{k-1}(p-1)$, p prime; $\phi(mn) = \phi(m)\phi(n)$, $\gcd(m,n) = 1$.

Example ($p = 17$, $p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$

So there are 48 choices of (c_1, c_2) which give the maximum period (probability: $48/288 = 1/6$).

Example ($p = 2017$, $p^2 - 1 = 4068288 = 2^6 \cdot 3^2 \cdot 7 \cdot 1009$)

We have

$$\begin{aligned} \phi(4068288) &= \phi(2^6)\phi(3^2)\phi(7)\phi(1009) \\ &= 32 \cdot 6 \cdot 6 \cdot 1008 = 1161216 \end{aligned}$$

$\phi(p^k) = p^{k-1}(p-1)$, p prime; $\phi(mn) = \phi(m)\phi(n)$, $\gcd(m,n) = 1$.

Example ($p = 17, p^2 - 1 = 288 = 2^5 \cdot 3^2$)

$\phi(288) = \phi(2^5)\phi(3^2) = (2^4(2-1))(3^1(3-1)) = 16 \cdot 6 = 96$
So there are 48 choices of (c_1, c_2) which give the maximum period (probability: $48/288 = 1/6$).

Example ($p = 2017, p^2 - 1 = 4068288 = 2^6 \cdot 3^2 \cdot 7 \cdot 1009$)

We have

$$\begin{aligned}\phi(4068288) &= \phi(2^6)\phi(3^2)\phi(7)\phi(1009) \\ &= 32 \cdot 6 \cdot 6 \cdot 1008 = 1161216\end{aligned}$$

So there are 580608 choices of (c_1, c_2) which give maximum period (probability: $1161216/4068288 = 288/1009 \approx .285$).

...

Question

Is it possible to actually list the (c_1, c_2) as opposed to counting them?

Question

Is it possible to actually list the (c_1, c_2) as opposed to counting them?

Yes.

. . .

Outline

. . .

The Question

Now consider a sequence $\{s_n\}$ which follows the recurrence relation

$$s_{n+3} = c_1 s_{n+2} + c_2 s_{n+1} + c_3 s_n.$$

The Question

Now consider a sequence $\{s_n\}$ which follows the recurrence relation

$$s_{n+3} = c_1 s_{n+2} + c_2 s_{n+1} + c_3 s_n.$$

What can we say about the period?

The Question

Now consider a sequence $\{s_n\}$ which follows the recurrence relation

$$s_{n+3} = c_1 s_{n+2} + c_2 s_{n+1} + c_3 s_n.$$

What can we say about the period?
Do the results of Franzel-Psalmond-Tobiasz generalize? . . .

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.
2. If A has at most two distinct eigenvalues, then $v_1 = v_2 = v_3 = 1, k \mid p(p-1)$ and $p \mid k$.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.
2. If A has at most two distinct eigenvalues, then $v_1 = v_2 = v_3 = 1, k \mid p(p-1)$ and $p \mid k$.
3. If $v_1 = v_2 = 2$ then $v_3 = 1$ and $k \mid p^2 - 1$.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.
2. If A has at most two distinct eigenvalues, then $v_1 = v_2 = v_3 = 1, k \mid p(p-1)$ and $p \mid k$.
3. If $v_1 = v_2 = 2$ then $v_3 = 1$ and $k \mid p^2 - 1$.
4. If $v_1 = 3$ then $v_2 = v_3 = 3$ and $k \mid p^3 - 1$.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \le i \le 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.
2. If A has at most two distinct eigenvalues, then $v_1 = v_2 = v_3 = 1, k \mid p(p-1)$ and $p \mid k$.
3. If $v_1 = v_2 = 2$ then $v_3 = 1$ and $k \mid p^2 - 1$.
4. If $v_1 = 3$ then $v_2 = v_3 = 3$ and $k \mid p^3 - 1$.

Yes.

Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{bmatrix}$$

and let $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{p^3}$ be its eigenvalues.
For $1 \leq i \leq 3$, let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$, and k the period.
Then [S. Shan, 2012]:

1. If the eigenvalues are distinct, and $v_1 = v_2 = v_3 = 1$, then $k \mid p - 1$.
2. If A has at most two distinct eigenvalues, then $v_1 = v_2 = v_3 = 1, k \mid p(p-1)$ and $p \mid k$.
3. If $v_1 = v_2 = 2$ then $v_3 = 1$ and $k \mid p^2 - 1$.
4. If $v_1 = 3$ then $v_2 = v_3 = 3$ and $k \mid p^3 - 1$.

. . .

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

- $k \mid p^3 - 1$,

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

- $k \mid p^3 - 1$,
- $k \mid p^2 - 1$, *or*

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

- $k \mid p^3 - 1$,
- $k \mid p^2 - 1$, *or*
- $k \mid p(p-1)$.

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

- $k \mid p^3 - 1$,
- $k \mid p^2 - 1$, *or*
- $k \mid p(p-1)$.

Theorem

For a sequence given by a third order linear recurrence relation, the period k satisfies

- $k \mid p^3 - 1$,
- $k \mid p^2 - 1$, *or*
- $k \mid p(p-1)$.

Furthermore, any k satisfying one of the above divisibility criteria is realizable.

...

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.
- Let $q = \text{lcm}(p^{v_1} - 1, p^{v_2} - 1, \ldots, p^{v_t} - 1)$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.
- Let $q = \operatorname{lcm}(p^{v_1} - 1, p^{v_2} - 1, \ldots, p^{v_t} - 1)$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.
- Let $q = \operatorname{lcm}(p^{v_1} - 1, p^{v_2} - 1, \ldots, p^{v_t} - 1)$.

Theorem (S. Shan, 2012)

With the notation above, $k \mid p^M q$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \leq i \leq t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.
- Let $q = \text{lcm}(p^{v_1} - 1, p^{v_2} - 1, \ldots, p^{v_t} - 1)$.

Theorem (S. Shan, 2012)

With the notation above, $k \mid p^M q$.

Does it generalize further?

Yes, but it's awkward to state.
Let $\{s_n\}$ be a sequence satisfying an w^{th} order linear recurrence relation. Let k be its period.

- Let $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{p^w}$ be the distinct eigenvalues.
- For $1 \le i \le t$ let m_i be the algebraic multiplicity of λ_i.
- Let $M = \max\{m_i\}$.
- Let $v_i = \min\{r : \lambda_i \in \mathbb{F}_{p^r}\}$.
- Let $q = \operatorname{lcm}(p^{v_1} - 1, p^{v_2} - 1, \ldots, p^{v_t} - 1)$.

Theorem (S. Shan, 2012)

With the notation above, $k \mid p^M q$.

There is a converse which, to date, defies a nice description.

...

Thank you.