Fibonacci Subgroup Generators

Don Reble

2022 March 20

1 Introduction

As detailed in [1], a Fibonacci Primitive Root (FPR) is a primitive root G of a prime P such that $G^2 \equiv G + 1 \bmod P$.

The sequence of values $G^0, G^1, G^2, \ldots$ can then be computed using addition instead of multiplication, since $G^{k+2} \equiv G^{k+1} + G^k$.

Whether primitive root or not, a root of $G^2 \equiv G + 1$ additively generates a subgroup modulo P: it is a Fibonacci Subgroup Generator (FSG).

To find the FSGs for a given P, note that

$$(2G - 1)^2 = 4G^2 - 4G + 1 \equiv 5 \bmod P$$

Then 5 is a quadratic residue, and $P \in \{1, 9\} \bmod 10$.

> Or: $P = 5$, $\sqrt{5} \equiv 0$, and $G = 3; G^2 \equiv 4$.
> I exclude $P = 5$ from the following.

And so $G \equiv (1 \pm \sqrt{5})/2 \bmod P$, as noted in [1]. There are two FSGs: G_1 and G_2, since $G_1 - G_2 = \pm\sqrt{5} \neq 0$.

Any linear combination $F_k = a \cdot G_1^k - b \cdot G_2^k$ also gives an additive sequence. Set $a = b = 1/(G_1 - G_2)$: then $F_0 = 0$ and $F_1 = 1$. This yields the Fibonacci sequence modulo P:

$$F_k \equiv \frac{G_1^k - G_2^k}{G_1 - G_2}$$

If $x^2 - x - 1$ has roots G_1, G_2, then
$x^2 - x - 1 = (x - G_1)(x - G_2) = x^2 - (G_1 + G_2)x + G_1G_2$.
So $G_1G_2 \equiv -1 \bmod P$; $G_1 + G_2 = +1 \bmod P$.

1.1 $P \equiv 1 \bmod 4$ $\quad(\{1, 9\} \bmod 20)$

When $P \equiv 1 \bmod 4$, -1 is a quadratic residue. $G_1G_2 \equiv -1$, so G_1, G_2 are both quadratic residues, or neither is. A quadratic residue is not a primitive root.

If G_1, G_2 are quadratic non-residues, then:

Let $H = (P - 1)/2$: H is even, and $2H$ is the size of P's multiplicative group. If x is a quadratic non-residue, then $x^H \equiv -1$, and $G_2 \equiv -1/G_1 \equiv (G_1^H)/G_1 \equiv G_1^{H-1}$. Symmetrically, $G_1 \equiv G_2^{H-1}$.

So G_1 and G_2 generate the same subgroup. They are both primitive roots, or neither is; and P has two FPRs or none.

1.2 $P \equiv 3 \bmod 4$ $(\{11, 19\} \bmod 20)$

When $P \equiv 3 \bmod 4$, -1 is a quadratic non-residue. $G_1 G_2 \equiv -1$, so exactly one of G_1, G_2 is a quadratic residue, and P has one FPR or none.

Call the quadratic non-residue G_1: then $G_2 \equiv -1/G_1 \equiv G_1^{H-1}$ (as above, but now $H = (P-1)/2$ is odd). G_2 generates a proper subgroup of G_1's subgroup.

1.3 FSG examples

$P = 11$, $\sqrt{5} \equiv 4$, $G_1, G_2 = 4, 8$								
G_1^k	1	4	5	9	3			
	1	4	5	9	3	1	4	...
G_2^k	1	8	9	6	4			
	10	3	2	5	7	1	8	...
$G_1^k - G_2^k$	0	7	7	3	10			
	2	1	3	4	7	0	7	...
F_k	0	1	1	2	3			
	5	8	2	10	1	0	1	...

$P = 19$, $\sqrt{5} \equiv 9$, $G_1, G_2 = 5, 15$											
G_1^k	1	5	6	11	17	9	7	16	4		
	1	5	6	11	17	9	7	16	4	1	5 ...
G_2^k	1	15	16	12	9	2	11	13	5		
	18	4	3	7	10	17	8	6	14	1	15 ...
$G_1^k - G_2^k$	0	9	9	18	8	7	15	3	18		
	2	1	3	4	7	11	18	10	9	0	9 ...
F_k	0	1	1	2	3	5	8	13	2		
	15	17	13	11	5	16	2	18	1	0	1 ...

$P = 29$, $\sqrt{5} \equiv 11$, $G_1, G_2 = 6, 24$										
G_1^k	1	6	7	13	20	4	24			
	28	23	22	16	9	25	5	1	6	...
G_2^k	1	24	25	20	16	7	23			
	1	24	25	20	16	7	23	1	24	...
$G_1^k - G_2^k$	0	11	11	22	4	26	1			
	27	28	26	25	22	18	11	0	11	...
F_k	0	1	1	2	3	5	8			
	13	21	5	26	2	28	1	0	1	...

$P = 31$, $\sqrt{5} \equiv 6$, $G_1, G_2 = 13, 19$																	
G_1^k	1	13	14	27	10	6	16	22	7	29	5	3	8	11	19		
	30	18	17	4	21	25	15	9	24	2	26	28	23	20	12	1	13 ...
G_2^k	1	19	20	8	28	5	2	7	9	16	25	10	4	14	18		
	1	19	20	8	28	5	2	7	9	16	25	10	4	14	18	...	
$G_1^k - G_2^k$	0	25	25	19	13	1	14	15	29	13	11	24	4	28	1		
	29	30	28	27	24	20	13	2	15	17	1	18	19	6	25	0	25 ...
F_k	0	1	1	2	3	5	8	13	21	3	24	27	20	16	5		
	21	26	16	11	27	7	3	10	13	23	5	28	2	30	1	0	1 ...

$P = 41$, $\sqrt{5} \equiv 13$, $G_1, G_2 = 7, 35$												
G_1^k	1	7	8	15	23	38	20	17	37	13		
	9	22	31	12	2	14	16	30	5	35		
	40	34	33	26	18	3	21	24	4	28		
	32	19	10	29	39	27	25	11	36	6	1	7 ...
G_2^k	1	35	36	30	25	14	39	12	10	22		
	32	13	4	17	21	38	18	15	33	7		
	40	6	5	11	16	27	2	29	31	19		
	9	28	37	24	20	3	23	26	8	34	1	35 ...
$G_1^k - G_2^k$	0	13	13	26	39	24	22	5	27	32		
	18	9	27	36	22	17	39	15	13	28		
	0	28	28	15	2	17	19	36	14	9		
	23	32	14	5	19	24	2	26	28	13	0	13 ...
F_k	0	1	1	2	3	5	8	13	21	34		
	14	7	21	28	8	36	3	39	1	40		
	0	40	40	39	38	36	33	28	20	7		
	27	34	20	13	33	5	38	2	40	1	0	1 ...

Here, FPRs are in boldface.

P	$\sqrt{5}$	FSGs	P	$\sqrt{5}$	FSGs	P	$\sqrt{5}$	FSGs
11	4	4 **8**	271	33	17 **255**	619	134	243 377
19	9	5 **15**	281	75	38 244	631	219	**110** 522
29	11	6 24	311	117	**59** 253	641	84	**279 363**
31	6	**13** 19	331	98	117 215	659	258	**201** 459
41	13	**7 35**	349	62	144 206	661	115	58 604
59	8	26 **34**	359	148	**106** 254	691	248	222 470
61	26	**18 44**	379	39	20 **360**	701	53	**27 675**
71	17	9 **63**	389	86	**152 238**	709	341	171 539
79	20	**30** 50	401	178	112 290	719	60	**330** 390
89	19	10 80	409	150	**130 280**	739	237	**119** 621
101	45	23 79	419	41	21 **399**	751	330	211 **541**
109	21	**11 99**	421	200	111 311	761	183	92 670
131	23	12 **120**	431	181	91 **341**	769	92	339 431
139	12	64 76	439	139	70 **370**	809	124	343 467
149	68	**41 109**	449	118	**166 284**	811	57	29 783
151	55	28 124	461	43	22 440	821	396	**213 609**
179	30	75 **105**	479	22	**229** 251	829	191	96 734
181	27	14 168	491	147	**74** 418	839	156	342 **498**
191	14	**89** 103	499	50	225 **275**	859	306	277 583
199	76	62 138	509	243	122 388	881	228	327 555
211	65	33 179	521	199	100 422	911	135	68 844
229	66	82 148	541	196	173 369	919	286	317 603
239	31	16 **224**	569	104	**233 337**	929	61	**31 899**
241	103	**52 190**	571	24	274 **298**	941	455	228 714
251	16	118 **134**	599	49	25 **575**	971	347	174 **798**
269	126	**72 198**	601	273	**137 465**	991	63	32 960

2 Pisano- and zero-periods

The Fibonacci numbers modulo M are of course periodic; there are only so many pairs of values; a repetition is inevitable. The previous section explains

why $P-1$ is a period for prime $P \in 1,9 \bmod 10$, and the examples show that that period can be fundamental ($P = 11, 19, 31, 41$) or not ($P = 29$).

The fundamental period is called the *Pisano period*. (OEIS A001175)

Recall that $F_{m+2k} = aF_{m+k} - bF_m$, where $a = F_{2k}/F_k$ and $b = (-1)^k$. Let $F_m \bmod P$ and $F_{m+k} \bmod P$ be two closest zeroes in the Fibonacci sequence modulo P. $F_{m+2k} \bmod P$ is a linear combination of those two zeroes, and so is zero; and so inductively for each F_{m+jk}. This works for negative k also:
the zeroes of the sequence occur periodically.

This *zero-period* is a factor of the Pisano period (OEIS A001177). As the $P = 41$ example shows, it might be a proper factor. That particular zero-period is $(P-1)/2 = H$.

Two FPRs

If P has two FPRs, then $G_1^H \equiv -1 \equiv G_2^H$, and $F_H \equiv (-1--1)/(G_1 - G_2) \equiv 0$. The zero-period is at most H, not $P-1$.

One FPR

If P has one FPR (G_1), then $P \equiv 3 \bmod 4$, $H = (P-1)/2$ is odd, and as above, $G_2 = G_1^{H-1}$.

$$\begin{aligned} G_1^k - G_2^k &\equiv G_1^k - G_1^{k(H-1)} \\ &\equiv (G_1^k) \cdot (1 - G_1^{k(H-2)}) \end{aligned}$$

That is zero only when the right-side factor is zero: $G_1^{k(H-2)} \equiv 1$. Then $k(H-2)$ is a multiple of $P-1 = 2H$.
Odd $H-2$ has no common factor with $2H$, so $2H$ divides k. And so the zero-period of $(G_1^k - G_2^k)/(G_1 - G_2) = F_k$ is $2H = P-1$.

No FPR

If P has no FPR, there are subcases:

- $P \equiv 1 \bmod 4$, G_1 and G_2 are quadratic residues:
  $G_1^H \equiv 1 \equiv G_2^H$, and $F_H \equiv 0$. The zero-period divides H.
- $P \equiv 1 \bmod 4$, G_1 and G_2 are quadratic non-residues:
  G_1 and G_2 generate the same subgroup, and for some proper factor of A of $P-1$, $G_1^A \equiv 1 \equiv G_2^A$. The zero-period divides A.
- $P \equiv 3 \bmod 4$, G_2 generates a subgroup of G_1's subgroup, and for some proper factor of A of $P-1$, $G_1^A \equiv 1 \equiv G_2^A$. The zero-period divides A.

In each case, the zero-period of F_k is less than $P-1$.

In summary

For primes $P \equiv \{1, 9\} \bmod 10$, the zero-period of the Fibonacci sequence modulo P is $P-1$ if-and-only-if there is exactly one FPR, which implies that $P \equiv 3 \bmod 4$.

2.1 Primes $\equiv \{3, 7\} \bmod 10$

Modulo primes $Q \equiv \{3, 7\} \bmod 10$, 5 has no square root: but in the polynomial field $(\mathbf{Z}/Q\mathbf{Z})[x]/(x^2 - x - 1)$ it does. Thereby one can show that the zero-period is a factor of $Q + 1$. (See [4].)

Also, $F_0 = 0$ and $F_2 = 1$, so 2 is not a zero-period of $F_k \bmod Q$; and F_{Q-1} and F_{Q+1} are not both congruent to zero.
$Q - 1$ is not a zero-period.

3 Eldar's conjecture

In a posting to seqfan[5], Ami Eldar mentions some OEIS[6] sequences,

```
%N A002145 Primes of the form 4n+3.
%N A003147 Primes with a Fibonacci primitive root.
%N A106535 Numbers k such that the smallest x > 1 for which
           Fibonacci(x) = 0 mod k is x = k - 1.
```

and conjectures that A106535 is the intersection of sequences A003147 and A002145. The previous section shows that the *primes* within A106535 are indeed 3-mod-4 primes with a FPR. It remains to show that all A106535 values are prime.

Jianing Song has claimed that. The following proof is derived from Song's work.

3.1 Song's proof

Some facts from Renault[3]:

Let $\pi(n)$ be the period of the Fibonacci sequence modulo n;
let $\alpha(n)$ be its zero-period.

- R1 $\alpha(\mathrm{lcm}(m, n)) = \mathrm{lcm}(\alpha(m), \alpha(n)) \le \alpha(m) \cdot \alpha(n)$
- R2 for prime power p^e, $\alpha(p^e) = p^{e-t}\alpha(p)$ for some $t \le e$
- R3 for prime p, $\pi(p)$ divides $p - (\frac{p}{5})$ (Legendre symbol); therefore $\alpha(p) | \pi(p) \le p + 1$.
- R4 $\alpha(n) \le \pi(n) \le 6n$

Let n be an element of A106535: $\alpha(n) = n - 1$. Then

If n is divisible by the square of a prime p, let p^e be that prime component of n; let $p^e \cdot r = n$. $\alpha(n) = \mathrm{lcm}(\alpha(p^e), \alpha(r))$.

- If $p | \alpha(p^e)$ then $p | \mathrm{lcm}(\alpha(p^e), \alpha(r)) = \alpha(n) = n - 1$. [R1]
  But p divides n, not $n - 1$.
- If $p \nmid \alpha(p^e)$ then $\alpha(p^e) = \alpha(p)$ [R2]
  $\alpha(n) \le \alpha(p^e) \cdot \alpha(r) = \alpha(p) \cdot \alpha(r)$ [R1]
  $\alpha(n) = n - 1 = rp^e - 1 \le (p + 1) \cdot 6r$ [R3,R4]
  $p^e \le 6(p + 1) + 1/r$
  $p < 7$ [$e > 1$]

So a squared prime factor p is 2, 3, or 5. But $2 | \alpha(2^2) = 6$, $3 | \alpha(3^2) = 12$ and $5 | \alpha(5^2) = 25$, so those primes are out: n is squarefree.

Note that neither 5 nor 6 divides n, because

- if $5 | n$, then $5 = \alpha(5) | \alpha(n) = n - 1$, and so $5 \nmid n$.

- if $6|n$, then $2|n$ and $3 = \alpha(2)|\alpha(n) = n - 1$, and so $3 \not| n$ and $6 \not| n$.

A few possibilities remain:

- n is odd and composite,
- $n = 2m$ for odd composite m,
- $n = 2p$ for odd prime p,
- n is prime.

n is odd and composite

In this case, partition the prime factors of n into two sets: those p for which $\alpha(p) = p \pm 1$, and those q for which $\alpha(q)$ is a proper factor of $q \pm 1$, therefore $\alpha(q) \le \frac{q+1}{2}$.
Let $n = n_p \cdot n_q$; $n_p = \prod_{i=1}^{s} p_i$; $n_q = \prod_{j=1}^{t} q_j$.
s and t are the quantities of the prime factors.

Then $\alpha(n) = \text{lcm}(\alpha(n_p), \alpha(n_q)) \le \alpha(n_p) \cdot \alpha(n_q)$, and

$$\begin{aligned}
\alpha(n_p) &= LCM_{i=1}^{s}(\alpha(p_i)) \le 2\prod_{i=1}^{s}\frac{p_i+1}{2} && (1)\\
\alpha(n_q) &= LCM_{j=1}^{t}(\alpha(q_j)) \le \prod_{j=1}^{t}\frac{q_j+1}{2} && (2)\\
\alpha(n) &\le 2\cdot\left(\prod_{i=1}^{s}\frac{p_i+1}{2}\right)\cdot\left(\prod_{j=1}^{t}\frac{q_j+1}{2}\right)\\
\alpha(n) &\le 2\prod_{k=1}^{s+t}\frac{r_k+1}{2} && (3)\\
\frac{\alpha(n)}{n} = 1 - \frac{1}{n} &\le 2\prod_{k=1}^{s+t}\frac{r_k+1}{2r_k} = \frac{x}{y}\\
n &\le \frac{y}{y-x}
\end{aligned}$$

(1) all $\alpha(p_i)$ values are even;
and if there are no p_i values, then $\alpha(n_p) = 1 \le 2$
(2) if there are no q_j values, then $\alpha(n_q) = 1 \le 1$
(3) renaming the prime factors

The possible factors of $\frac{x}{y}$ decrease with r_k: $\frac{3+1}{6}$, $\frac{7+1}{14}$, $\frac{11+1}{22}$, ...
n is composite, so there are least two r_k values. $\frac{x}{y}$ is at most $2 \cdot \frac{4}{6} \cdot \frac{8}{14} = \frac{16}{21}$, and $n \le \frac{21}{5}$. But A106535 has no values below 5.

$n = 2m$ for odd composite m

In this case, let $n = 2\prod_{i=1}^{t} r_i$, where r_i are the prime factors of m, and $t \ge 2$.
$\alpha(n) = n - 1$ is odd, so all $\alpha(r_i)$ values are odd, and $\alpha(r_i) \le \frac{r_i+1}{2}$.

$$\begin{aligned}
\alpha(n) &= \text{lcm}(\alpha(2), \alpha(m)) \le 3 \cdot LCM_{i=1}^{t}\alpha(r_i)\\
\alpha(n) &\le 3\cdot\prod_{i=1}^{t}\frac{r_i+1}{2} && (4)
\end{aligned}$$

$$\begin{aligned} \frac{\alpha(n)}{n} = 1 - \frac{1}{n} &\leq 3 \prod_{k=1}^{s+t} \frac{r_k + 1}{2r_k} = \frac{x}{y} \\ n &\leq \frac{y}{y - x} \end{aligned}$$

$3 \not| n$, so the possible factors of $\frac{x}{y}$ are $\frac{7+1}{14}$, $\frac{11+1}{22}$, ...
m is composite, so there are least two r_k values. $\frac{x}{y}$ is at most $3 \cdot \frac{8}{14} \cdot \frac{12}{22} = \frac{72}{77}$, and $n \leq \frac{77}{5}$. But A106535 has no even values below 16.

$n = 2p$ for odd prime p

As in the $n = 2m$ case, $\alpha(p) \leq \frac{p+1}{2}$, so $\alpha(n) = 2p - 1 \leq 3 \cdot \frac{p+1}{2}$ and $p \leq 5$.
But A106535 hasn't 6 nor 10.

n is prime

This is the only possible case. All A106535 values are prime, and Eldar's conjecture is true.

References

[1] Daniel Shanks, *Fibonacci Primitive Roots*, Fibonacci Quarterly, Vol 10 No 2 (1972) pp 163-168, 181.
`https://www.fq.math.ca/Scanned/10-2/shanks-a.pdf`

[2] Daniel Shanks and Larry Taylor, *An Observation on Fibonacci Primitive Roots*, Fibonacci Quarterly, Vol 11 No 2 (1973) pp 159-160.
`https://www.fq.math.ca/Scanned/11-2/shanks.pdf`

[3] M. Renault,
The Fibonacci sequence under various moduli,
Masters Thesis, Wake Forest University, 1996.
`http://webspace.ship.edu/msrenault/fibonacci/fib.htm`

[4] Wikipedia, *Pisano period*,
`https://en.wikipedia.org/wiki/Pisano_period`

[5] *(OEIS) Sequence Fanatics Discussion List*,
`http://list.seqfan.eu/pipermail/seqfan`

[6] Neil Sloane, *The Online Encyclopedia of Integer Sequences,*
`http://oeis.org`