Number Theory Section Summary: 13.1
Fibonacci Numbers

1. Summary

Leonardo de Pisa (1180-1250?), better known as Fibonacci, wrote the *Liber Abaci*, in which he included a problem about rabbits:

A man put one pair of rabbits in a certain place entirely surrounded by a wall. How many pairs of rabbits can be produced from that pair in a year, if the nature of these rabbits is such that every month each pair bears a new pair which from the second month on becomes productive?

Ignoring the terrible incestuous implications, the resulting sequence of numbers of pairs of rabbits is known as the **Fibonacci numbers**:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots.$$

This works out to the recursive sequence

$$\overline{u_n = u_{n-1} + u_{n-2}}$$

for $n \geq 3$, where $u_1 = u_2 = 1$, the first known recursive definition in mathematics.

2. Theorems

Theorem 13.1: For the Fibonacci sequence, $\gcd(u_n, u_{n+1}) = 1$ for every $n \geq 1$.

Proof: direct, and using lemma, p. 27.

Theorem 13.2: For $m \geq 1$ and $n \geq 1$, $u_m | u_{mn}$.

Proof: by induction on n (straightforward, using (1)).

Lemma: If $m = qn + r$, then $\gcd(u_m, u_n) = \gcd(u_r, u_n)$

Theorem 13.3: The greatest common divisor of two Fibonacci numbers is again a Fibonacci number; specifically $\gcd(u_m, u_n) = u_d$ where $d = \gcd(m, n)$.

Corollary: In the Fibonacci sequence, $u_m | u_n$ if and only if $m|n$ for $n \geq m \geq 3$.

3. Properties/Tricks/Hints/Etc.

- For every prime p, there are infinitely many Fibonacci numbers that are divisible by p, equally spaced along the Fibonacci sequence.
- It is not known if there are infinitely many prime Fibonacci numbers.
- $$\boxed{u_{m+n} = u_{m-1}u_n + u_m u_{n+1}} \tag{1}$$

  Proof: by induction on n.

Theorem 13.1 : $\gcd(u_n, u_{n+1}) = 1 \quad \forall n \geq 1$

Proof:

Let $d = \gcd(u_n, u_{n+1})$. Since

$$u_{n+1} = u_n + u_{n-1},$$

$$u_{n-1} = u_{n+1} - u_n$$

So if $d | u_{n+1}$ & $d | u_n$, then $d | u_{n-1}$.

$$d \leq \gcd(u_{n-1}, u_n)$$

Do this $n+1$ more times, &

$$d \leq \gcd(u_1, u_2) = 1$$

So d is $\underline{1}$. Q.E.D.

Alternatively, show this using the Euclidean Algorithm (or lemma, p27):

Want $\gcd(u_n, u_{n+1})$:

$$
\begin{aligned}
u_{n+1} &= 1 u_n + u_{n-1} \qquad & \gcd(u_n, u_{n+1}) &= \\
u_n &= 1 \cdot u_{n-1} + u_{n-2} & \gcd(u_{n-1}, u_n) &= \\
&\ \vdots & &\ \vdots \\
u_4 &= 1 \cdot u_3 + \boxed{u_2} & \gcd(u_3, u_4) &= \\
\underset{2}{\underset{\shortparallel}{u_3}} &= 2 \cdot \underset{1}{\underset{\shortparallel}{u_2}} + 0 & \gcd(u_2, u_3) &= 1
\end{aligned}
$$

QED

Theorem 13.2: For $m, n \geq 1$ u_{mn} is divisible by u_m.

By induction on n.

<u>Anchor</u>: $n = 1$

$u_{m \cdot 1}$ is divisible by u_m. ✓

Inductive Step: Assume true for all $n = 1, \dots, k$; & show it for $n = k+1$.

$$
\begin{aligned}
u_{m(k+1)} &= u_{mk+m} \\
&= u_{mk-1} u_m + u_{mk} u_{m+1}
\end{aligned}
$$

But $u_n \mid u_n$, & $u_n \mid u_{nk}$ by the inductive hypothesis, so $u_n \mid u_{n(k+1)}$.

Q.E.D.

Lemma: If $m = qn + r$, then

$$\gcd(u_m, u_n) = \gcd(u_r, u_n).$$

Let $\delta = \gcd(u_m, u_n)$. Note that

$$u_m = u_{qn+r} = \underbrace{u_{qn-1} u_r}_{a} + \underbrace{u_{qn} u_{r+1}}_{c}.$$

$b = u_n$

Claim: $\underline{\gcd(a+c, b) = \gcd(a, b)}$ when $b \mid c$.

Let $d = \gcd(a, b)$. Thus $d \mid b$, & $d \mid c$.
Hence $d \mid a + c$. Therefore $d \leq D = \gcd(a+c, b)$.
$\exists (\alpha, \beta) /$ $D = \alpha(a+c) + \beta b$
$= \alpha a + b(\alpha c' + \beta)$ where $c = c'b$

Clearly $d \mid D$. So we could write $D = dd'$.
Can we show that $D \mid a$ & $D \mid b$? If so, $D \mid d$, and $D \leq d \Rightarrow d = D$.

$D \mid b$ as $\gcd(a+c, b)$. So $b = Db'$

$D \mid a + c$, so $a + c = D\varphi$ &

$$a = D\varphi - c = D\varphi - c'b$$
$$= D\varphi - c'Db'$$
$$= D(\varphi - b'c'), \text{ so } D \mid a.$$

Q.E.D.

Therefore, by the claim,

$$\delta = \gcd(u_m, u_n)$$
$$= \gcd(u_{qn-1} u_r + u_{qn} u_{r+1}, u_n)$$
$$\boxed{\delta = \gcd(u_{qn-1} u_r, u_n)}$$

Claim: $\gcd(u_{qn-1}, u_n) = 1$

Know: $u_n \mid u_{qn}$, and $\gcd(u_{qn-1}, u_{qn}) = 1$.

Conclude that

$$\gcd(u_{qn-1}, u_n) = 1$$

Otherwise, if it were $d \neq 1$, then

$d \mid u_n$ and $d \mid u_{qn-1}$; since $u_n \mid u_{qn}$,

$d \mid u_{qn}$, contradicting

$$\gcd(u_{qn-1}, u_{qn}) = 1.$$

Claim: $\gcd(a, c) = 1 \Rightarrow$

$$\gcd(a, bc) = \gcd(a, b)$$

Given $\gcd(a,c) = 1$, and let $d = \gcd(a,b)$.

$$d \leq \gcd(a, bc) = s$$

Suppose $d < s$ (but remember that $d \mid s$).

Certainly $s \mid a$, $s \nmid b$, So there's some prime factor of s, p, that divides c.

Since $s \mid a$, so does p: $p \mid a$.

$p \leq \gcd(a, c)$, a contradiction.

$$\delta = \gcd(u_{qn-1}u_r, u_n)$$

$$\gcd(u_{qn-1}, u_n) = 1$$

$\therefore$ $\delta = \gcd(u_r, u_n)$ by the claim,

establishing the lemma.

Theorem 13.3:

$$\gcd(u_m, u_n) = u_{\gcd(m,n)}$$

WLOG assume $m \geq n$.

Find $\gcd(m,n)$

$$\begin{aligned}
m &= q_1 n + r_1 \\
n &= q_2 r_1 + r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + \boxed{r_n} = \gcd(m,n) \\
r_{n-1} &= q_{n+1} r_n + 0 \quad \Rightarrow \quad r_n \mid r_{n-1}
\end{aligned}$$

$$\begin{aligned}
\gcd(u_m, u_n) &= \gcd(u_n, u_{r_1}) = \cdots = \underbrace{\gcd(u_{r_{n-1}}, u_{r_n})} \\
&= u_{r_n} \quad (\text{since } r_n \mid r_{n-1},\ u_{r_n} \mid u_{r_{n-1}} \\
&= \gcd(m,n) \qquad \text{by Thm 13.2 })
\end{aligned}$$

#4b p276 $\quad u_{n+5} \equiv 3u_n \pmod 5$

$$\begin{aligned}
u_{n+5} &= u_{n+4} + u_{n+3} \\
&= (u_{n+3} + u_{n+2}) + (u_{n+2} + u_{n+1}) \\
&= u_{n+2} + u_{n+1} + (u_{n+1} + u_n)2 + u_{n+1} \\
&= u_{n+2} + 4u_{n+1} + 2u_n \\
&= 5u_{n+1} + 3u_n
\end{aligned}$$

w/o detail ugly

$$u_{n+5} \equiv 5u_{n+1} + 3u_n \pmod 5$$
$$\equiv 3u_n \pmod 5$$

So $u_5, u_{10}, u_{15}, \ldots$ are all divisible by $5 \; (= u_5)$.

#5 Show that

$$u_1^2 + u_2^2 + \dots + u_n^2 = u_n u_{n+1}$$

[Hint: $n \geq 2$ $\quad u_n^2 = u_n u_{n+1} - u_n u_{n-1}$]

$$= u_n(\underbrace{u_{n+1} - u_{n-1}}_{= u_n})$$

$$\boxed{u_{n+1} = u_n + u_{n-1}}$$
$$\boxed{u_n = u_{n+1} - u_{n-1}}$$

$$u_1^2 = \cancel{u_1 u_2}$$
$$u_2^2 = \cancel{u_2 u_3} - \cancel{u_2 u_1}$$
$$u_3^2 = \cancel{u_3 u_4} - \cancel{u_3 u_2}$$
$$u_4^2 = u_4 u_5 - \cancel{u_4 u_3}$$
$$\vdots$$

Prove formally by induction, base case $n = 2$.

Fibonacci Nim

$n = 20$ sticks

$$\begin{array}{r} 2 \\ \hline 18 \\ 1 \\ \hline 17 \\ 2 \\ \hline 15 \\ 2 \\ \hline 13 \\ 3 \\ \hline 10 \end{array} \qquad \begin{array}{r} 10 \\ 2 \\ \hline 8 \\ 1 \\ \hline 7 \\ 2 \\ \hline 5 \\ 1 \\ \hline 4 \\ 1 \\ \hline 3 \end{array} \qquad \begin{array}{r} 3 \\ 1 \\ \hline 2 \\ 2 \\ \hline 0 \end{array}$$

I won!

\# 8 p276

u_{24} & u_{36}

Find u_k / $u_k \mid u_{24}$ and $u_k \mid u_{36}$.

Certainly $u_{12} = \gcd(u_{24}, u_{36})$ is one.

Thm 13.2: u_{mn} is divisible by u_m.

$u_1, u_2, u_3, u_4, u_6, u_{12}$

Fibonacci Nim - how does it work?

Claim - If you start w/ N non-Fibonacci, & use the strategy of always taking the smallest in the sum of non-consecutive Fibonaccis, you're guaranteed victory!

Question - If I start w/ a Fibonacci, what's the best strategy? (Are you guaranteed to lose against a savvy opponent?)