Some notes on algebraic number theory intro

Stefanus[1]

[1] Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: December 23, 2018)

Abstract

Just for fun :)

Page 6. Show that

$$f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$$

with $\{a_n\}$ Fibonacci numbers is given by

$$f(x) = \frac{1}{\sqrt{5}} \left[\exp\left(\frac{1+\sqrt{5}}{2}\ x \right) - \exp\left(\frac{1-\sqrt{5}}{2}\ x \right) \right]$$

and that

$$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

Answer. It is easier to show the latter, to show that it is a Fibonnaci number we just need to show the recurrence relation $a_n = a_{n-1} + a_{n-2}$

$$\begin{aligned}
\left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} &= \left(\frac{1+\sqrt{5}}{2} \right)^n \left(1 + \frac{1+\sqrt{5}}{2} \right) = \left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{2+1+\sqrt{5}}{2} \right) \\
&= \left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{4+2+2\sqrt{5}}{4} \right) = \left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{5+1+2\sqrt{5}}{4} \right) \\
&= \left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} \right)^2 \\
&= \left(\frac{1+\sqrt{5}}{2} \right)^{n+2}
\end{aligned}$$

ditto with the other term and we just need to check a_0, a_1 to make sure it's Fibonacci and they are the rest is straight forward.

And we can see that we cannot play this game with other numbers, if we try we will get

$$\begin{aligned}
\left(\frac{a+\sqrt{b}}{c} \right)^2 &= \left(1 + \frac{a+\sqrt{b}}{c} \right) \\
&= \left(\frac{c^2 + ac + c\sqrt{b}}{c^2} \right) \\
a^2 + 2a\sqrt{b} + b &= c^2 + ac + c\sqrt{b}
\end{aligned}$$

this means that $2a = c$ and therefore

$$\begin{aligned} a^2 + b &= c^2 + ac \\ &= 4a^2 + 2a^2 \\ \rightarrow b &= 5a^2 \end{aligned}$$

and everything will be a multiple of a so the above is the only configuration for this.

Page 11. Verify that $C(\sqrt{2}) = \{1, 2, 2, \dots\}$.

Answer. Here $C(\sqrt{2})$ is the continued fraction of $\sqrt{2}$. First let

$$\sqrt{2} = 1 + \frac{1}{1+a}$$

we now solve a by multiplying the whole thing with $a + 1$

$$\begin{aligned} (1+a)\sqrt{2} &= (1+a) + 1 \\ a(\sqrt{2} - 1) &= 2 - \sqrt{2} \\ a &= \sqrt{2} \end{aligned}$$

Therefore

$$\begin{aligned} \sqrt{2} &= 1 + \frac{1}{1+a} \\ &= 1 + \frac{1}{1+\sqrt{2}} \\ &= 1 + \frac{1}{1+1+\frac{1}{1+a}} \\ &= 1 + \frac{1}{2+\frac{1}{1+a}} \end{aligned}$$

and so on.

Page 13. Verify that $[\lambda_1, \dots, \lambda_n] = P_n/Q_n$

Answer. One thing we need to note is that

$$[\lambda_1, \dots, \lambda_n, \lambda_{n+1}] = [\lambda_1, \dots, [\lambda_n, \lambda_{n+1}]]$$

so if we replace λ_n into $[\lambda_n, \lambda_{n+1}]$ we will get

$$[[\lambda_1, \dots, \lambda_n] \rightarrow [\lambda_1, \dots, [\lambda_n, \lambda_{n+1}]] = [\lambda_1, \dots, \lambda_n, \lambda_{n+1}]$$

So now we proceed inductively, we know that up till n we have $[\lambda_1, \ldots, \lambda_n] = P_n/Q_n$ going to $n+1$ we do the above substitution $[\lambda_1, \ldots, \lambda_n] \to [\lambda_1, \ldots, [\lambda_n, \lambda_{n+1}]]$ making the same change in P_n/Q_n

$$\begin{aligned}
\frac{P_n}{Q_n} &\to \frac{[\lambda_n, \lambda_{n+1}]P_{n-1} + P_{n-2}}{[\lambda_n, \lambda_{n+1}]Q_{n-1} + Q_{n-2}} \\
&= \frac{\left(\lambda_n + \frac{1}{\lambda_{n+1}}\right) P_{n-1} + P_{n-2}}{\left(\lambda_n + \frac{1}{\lambda_{n+1}}\right) Q_{n-1} + Q_{n-2}} \\
&= \frac{\lambda_{n+1}(\lambda_n P_{n-1} + P_{n-2}) + P_{n-1}}{\lambda_{n+1}(\lambda_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} \\
&= \frac{\lambda_{n+1} P_n + P_{n-1}}{\lambda_{n+1} Q_n + Q_{n-1}} \\
&= \frac{P_{n+1}}{Q_{n+1}}
\end{aligned}$$

Page 13. Verify that $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n, n \geq 1$

Answer. Again we use induction. Assume it's true up till $n-1$ then

$$\begin{aligned}
P_n Q_{n-1} - P_{n-1} Q_n &= \lambda_n P_{n-1} Q_{n-1} + P_{n-2} Q_{n-1} - \lambda_n P_{n-1} Q_{n-1} - P_{n-1} Q_{n-2} \\
&= -(P_{n-1} Q_{n-2} - P_{n-2} Q_{n-1}) \\
&= -(-1)^{n-1} \\
&= (-1)^n
\end{aligned}$$

Page 13. Verify that $P_n Q_{n-2} - P_{n-2} Q_n = (-1)^{n-1} \lambda_n, n \geq 2$

Answer. Again we use induction. Assume it's true up till $n-1$ then

$$\begin{aligned}
P_n Q_{n-2} - P_{n-2} Q_n &= \lambda_n P_{n-1} Q_{n-2} + P_{n-2} Q_{n-2} - \lambda_n P_{n-2} Q_{n-1} - P_{n-2} Q_{n-2} \\
&= \lambda_n (P_{n-1} Q_{n-2} - P_{n-2} Q_{n-1}) \\
&= \lambda_n (-1)^{n-1}
\end{aligned}$$

using the result above.

Page 16. Verify that $(\sqrt{5}+1)/2 = [1, 1, 1, \ldots]$. In this case the sequence $\{Q_n\}$, $n \geq 0$ is the Fibonacci sequence.

Answer. Start with

$$\begin{aligned}
\frac{1+\sqrt{5}}{2} &= 1 + \frac{1}{1+a} \\
(1+a)(1+\sqrt{5}) &= 4 + 2a \\
a &= \frac{3-\sqrt{5}}{\sqrt{5}-1} \\
&= \frac{3-\sqrt{5}}{\sqrt{5}-1} \times \frac{\sqrt{5}+1}{\sqrt{5}+1} \\
&= \frac{\sqrt{5}-1}{2} \\
&= \frac{\sqrt{5}+1}{2} - 1
\end{aligned}$$

Thus

$$\begin{aligned}
\frac{1+\sqrt{5}}{2} &= 1 + \frac{1}{1+a} \\
&= 1 + \frac{1}{1 + \frac{1+\sqrt{5}}{2} - 1} \\
&= 1 + \frac{1}{\frac{1+\sqrt{5}}{2}} \\
&= 1 + \frac{1}{1 + \frac{1}{1+a}}
\end{aligned}$$

and so on.

One thing I tried that didn't work was expanding $\sqrt{5}$ and then adding 1 and dividing by 2

$$\sqrt{5} = 2 + \frac{1}{2+a}$$

we start with $2 + \dots$ because $\lfloor \sqrt{5} \rfloor = 2$ and

$$\begin{aligned}
(2+a)\sqrt{5} &= 5 + 2a \\
a(\sqrt{5}-2) &= \sqrt{5}(\sqrt{5}-2) \\
a &= \sqrt{5}
\end{aligned}$$

And thus $\sqrt{5} = [2, 4, 4, \dots]$ but adding 1 and dividing by 2 is not easy this way.

Page 23. Proposition 1.7 for a finite group G with order n and $a \in G$ we have $a^n = e$.

We can prove this without knowing lagrange's theorem. Assume the order m of a does not divide n. The cyclic group $\langle a\rangle$ forms a subgroup now take an element $b \in G$ that is not in $\langle a\rangle$ if we take $\langle a\rangle b$ we will get a whole new subset. New because if some of the elements are the same then we will have $a^h = a^l b$ which means $a^{h-l} = b$ or $e = a^{l-h}b$. In the first case this means $b \in \langle a\rangle$ which is a contradiction. In the second case since $l, h \leq m$ we have $|l - h| < m$ and so the inverse of a^{l-h} is in $\langle a\rangle$ but here b is that inverse and therefore $b \in \langle a\rangle$ again a contradiction.

But this process creates another subset with m distinct elements because if we have $a^h b = a^l b$ then we will have $a^{h-l} = e$ which is a contradiction because the order of a is m. Note that this might not be a subgroup but a subset of G.

If we repeat the process one more time with c which is not in $\langle a\rangle$ or $\langle a\rangle b$ and do $\langle a\rangle c$ we will generate another subset with m elements, the elements are all distinct just like before but they are also different from $\langle a\rangle b$ because otherwise we have $a^h c = a^l b \to c = a^{l-h}b$ but c is not in $\langle a\rangle b$.

Therefore if we repeat the process we must have $m|n$ and therefore $a^n = e$.

Page 25. Prove that if $a \in \mathbb{N}$ and $p \neq 2$ prime, $p|(a^{2n} + 1) \Rightarrow 2^{n+1}|(p - 1)$

Answer. I believe there's a typo here it should've been $a^{2^n} + 1$ instead $a^{2n} + 1$. If I were right then from Fermat's Little Theorem $p|(a^{2^n} + 1)$ means $a^{2^n} \equiv -1 \pmod{p}$. So if we square both sides

$$(a^{2^n})^2 \equiv (-1)^2 \pmod{p}$$
$$a^{2^{n+1}} \equiv 1 \pmod{p}$$

and Fermat tells us that $a^{p-1} \equiv 1$ so we have two choices either $(p-1)|2^{n+1}$ or $2^{n+1}|(p-1)$ depending on which one is bigger.

Page 25. Prove that $F_5 = 4294967297$ the fifth Fermat number is composite. $F_n = 2^{2^n} + 1$

Answer. My guess is we need to use the previous exercise. It's not an if and only if but we can try so if we can find a p such that $2^{n+1}|(p - 1)$ then maybe we can find an a such that $p|a^{2^n}$.

We now need to find which $p - 1$ is divisible by $2^{5+1} = 64$. So we want to see which

$p = 64n + 1$ is prime. We find $n = 3, 4, 7, 9, 10$ and the one with $n = 10$ is the one that divides F_5.

Page 25. Prove that $(2^{p-1} - 1)/p$ is a square only if $p = 3, 7$

Answer. Except for $p = 2$ every prime is odd therefore $p-1$ is even therefore $(2^{p-1}-1) = (2^{(p-1)/2} + 1)(2^{(p-1)/2} - 1)$.

Let's see if $2^n + 1$ can be square suppose it is then

$$\begin{aligned} 2^n + 1 &= m^2 \\ 2^n &= m^2 - 1 \\ &= (m-1)(m+1) \\ 2^n &= h(h+2), \qquad h = m - 1 \end{aligned}$$

This only works for $h = 2$ meaning $n = 3$. Now let's see if $2^n - 1$ can be square

$$2^n - 1 = m^2$$

do mod 4, $2^n - 1$ is odd if $n > 1$ therefore m is odd and $m^2 \equiv 1 \pmod 4$ but fo $n > 1$, $2^n - 1 \equiv -1 \pmod 4$ therefore it will only work if $n = 0, 1$.

Thus $2^n + 1$ can only be square if $n = 3$ and $2^n - 1$ is square only if $n = 0, 1$ therefore $(2^{p-1} - 1)/p$ is square only if $p = 3$ or 7.

Page 25. Let $a \geq 2$ an integer and p an odd prime, we have $a^{p-1} - 1 = p^e$ if and only if $a = 2$ and $p = 3$

Answer. The ($\Leftarrow$) is easy $2^2 - 1 = 3$. The other way is not quite so easy. Again for $p > 2$ we have

$$a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$$

If a is even then $a^{p-1} - 1$ is odd and if a is odd then $a^{p-1} - 1$ is even. Let $m = a^{(p-1)/2} - 1$ then what we have is $a^{p-1} - 1 = m(m + 2)$ if a is even then m and $m + 2$ are co-prime because they must be both odd and the only common factor between them must divide 2.

So if a is even then it will only work when $m = 1$ otherwise we will have more than one prime factor. And it will means that $p = 3, e = 1$ as our example above.

If a is odd then $d = \gcd(m, m+2)|2$. But since $m(m+2)$ must be even we must have m even but in that case $m(m+2)$ will have more than one prime factor unless when $m = 2$ because m even means that $m = 2h$, $m(m+2) = 4(h(h+1))$ and h and $h+1$ are co-prime so they must contain more than one prime factor except for $h = 1 \rightarrow p = 2, e = 3, a = 9$ but then p is no longer odd.

But more than that the above argument only works of p is odd because we need to split into $(a^{(p-1)/2} \pm 1)$ and $(p-1)/2$ is an integer only if p is odd but somehow it works :)