Some notes on algebraic number theory intro

Stefanus[1]

[1] Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: January 1, 2019)

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 we have

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

which works even for $p = 2$ as long as a is a square. 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 $h = 1 \to p = 2, e = 3, a = 9$ but then p is no longer odd.

Page 28. There's a typo (this book has a lot of typos) and some confusion too. On Page 23 it was said that $R - \{0\} = R^\times$. But the convention $G^\times$ is reserved for a group with inverses. So what Page 23 is saying is that if $R^\times$ happens to coincide with $R - \{0\}$ then R is a field but $R^\times$ always means a group with inverses.

The typo is $G = (\mathbb{Z}/p^{e+1}\mathbb{Z})^\times$ and $G' = (\mathbb{Z}/p^e\mathbb{Z})^\times$, they are the quotient group not the quotient ring otherwise the argument that $p \not| x$ doesn't make sense.

The argument about $G/\mathrm{Ker}f \approx G' \Rightarrow [G]/[\mathrm{Ker}f] = [G']$ is from Lagrange's Theorem. First, $[G] = [\mathrm{Ker}f][G/\mathrm{Ker}f] \to [G]/[\mathrm{Ker}f] = [G/\mathrm{Ker}f]$ but here $G/\mathrm{Ker}f \approx G'$ also here $[G]$ means the size of G.

So the last argument now makes sense, since we are dealing with the quotient group not quotient ring we have $[G] = \varphi(p^{e+1})$, $[G'] = \varphi(p^e)$.

Page 28. Prove that $(K[X])^\times = K^\times$ if K is a field

Answer. Suppose we have two polynomials

$$A = a_0 + a_1X + \cdots + a_nX^n$$
$$B = b_0 + b_1X + \cdots + b_mX^m$$

And suppose that they are inverses of one another $AB = 1, 1 \in K$ then the highest power comes from $a_nb_mX^{n+m}$ but $AB = 1$ so this means that $a_nb_m = 0$ so one of them must be zero. Say it is b_m then $B = \cdots + b_{m-1}X^{m-1}$ and then the highest power will be $a_nb_{m-1}X^{n+m-1}$ but again one of them must be zero repeating the process we get $A = a_0$ and $B = b_0$ which is what we want to show

Page 29. Prove Proposition 1.2 which is the polynomial ring version of $a = bq + r$

Answer. The uniqueness part is the easy assume there are two solutions $A = BQ_1 + R_1$, $A = BQ_2 + R_2$ then

$$(Q_1 - Q_2)B = (R_2 - R_1)$$

meaning that $B|R_2 - R_1$ but the degree of $R_2 - R_1$ is less than B so the only solution is $R_2 = R_1$.

The existence part we can do using long division but the more interesting question is suppose we have

$$X^5 + 2X^4 + 3X^3 + 3X^2 + 2X + 1 = (X^3 + X^2 + X + 1)(X^2 + X + 1)$$

here $B = (X^3 + X^2 + X + 1)$ and $Q = (X^2 + X + 1)$ now what happen if we remove the 1 from Q so that $Q = (X^2 + X)$ we will get $X^5 + 2X^4 + 2X^3 + 2X^2 + 2X$ and the remainder will be $X^3 + X^2 + 1$ but this remainder's degree is not less than B so the requirement on the degree of R is the thing keeping it unique.

Page 29. Prove Theorem 1.1. which says that for an Ideal I we have a unique P such that $I = P \cdot K[X]$

Answer. So we do what was done for integers Page 5. For now let's assume that P is monic since we can always multiply by the inverse of a_n as we are dealing with a field K. We just need to change the argument to deal with degrees of polynomials rather than numbers.

So assume that the polynomial A has degree $a \neq 0$ and is the smallest degree in I. Then $A \cdot K[X] \subseteq I$ because since I is an ideal $RI \subseteq I$ for $R \in K[X]$ and thus $RA \in I for R \in K[X]$. We can always make A monic by multiplying it by the inverse of its highest coefficient since K is a field.

Now the problem comes when there are more than one A, *i.e.* there are more than one polynomials with degree a, A_1 and A_2, but this is not so because since K is a field so like above we can make them monic.

Since I is an ideal their difference must be in I as well but their difference $A_1 - A_2$ will have a degree less than a so there must be only one A.

Now the converse, take any polynomial B in I and divide it by A, $B = AQ + R$ since B and AQ is in I then R must be in I (since it is an ideal) if $R \neq 0$ (not just the degree) then R will have a degree less than A and it's a contradiction.

Page 31. Proposition 1.14, to prove it my way I'll use this fact. Any subgroup of a cyclic group is cyclic.

Answer. To prove this is quite easy, say the cyclic group is $G = \langle x \rangle$. Let H be a subgroup of G then any element of H can be expressed as x^a for some $a \in \mathbb{Z}$. Let $H = \{x^{a_1}, x^{a_2}, \ldots, x^{x_m}\}$ the Bezout tells us that $a_1h_1 + a_2h_2 + \cdots + a_mh_m = d$ where d is the gcd of the a's. But this also means that x^d is in H but this means that every element of H is in some form of $(x^d)^l$ and therefore H is cyclic.

Page 31. The more interesting one, prove that $m = \sum_{d|m} \varphi(d)$

Answer. I think first step is to start with a cyclic group with order m, $G = \langle x \rangle$ then use the facts we know from previous theorems and propositions. $G_d = \langle x^{m/d} \rangle$ with order d and the remark in the previous paragraph shows that a cyclic group of order m has $\varphi(m)$ generators.

A cyclic group of order d has $\varphi(d)$ generators, this group has to be $\langle x^{m/d} \rangle$ the generators of this subgroup are x^h where $(h, m) = m/d$ so that its order will be $m/(h, m) = m/(m/d) = d$. And we need to make sure that any x^y where $(m, y) = m/d$ is in this subgroup. But this is easy enough to show because $y = u(m/d)$ and so $(x^{m/d})^u = x^y$ so all x^y with $(m, y) = m/d$ is in this subgroup and they are all generators.

Can a generator generate two subgroups? The answer is no if the subgroups have different orders and also from Proposition 1.14. that says that any subgroup with order d has to be G_d so generators for a subgroup can only generate that subgroup.

So if we characterize the set of numbers $S = \{1, 2, \ldots, m\}$ using their gcd with m we will cover everyone

$$S = \sum_{d|m} S_d$$

where $S_d = \{x | x \in S, \gcd(x, m) = d\}$ and each S_d has at least one element d itself. Non of the S_d overlaps because the a number cannot have two gcd's with m. And it covers all possible gcd because we cover all factors of m (including 1 and m). Therefore we have $\#S_{m/d} = \varphi(d)$ as the RHS gives the number of generators in $\langle x^{m/d} \rangle$ as explained above.

One more fact is that $\sum_{d|m} f(d) = \sum_{d|m} f(m/d)$ because we go through all factors.

So combining everything we have

$$\begin{aligned} \#S &= \sum_{d|m} \#S_d \\ &= \sum_{d|m} \#S_{m/d} \\ m &= \sum_{d|m} \varphi(d) \end{aligned}$$

Page 32. Proposition 1.16. For a finite group G of order m if for each $d|m$ there are no more than d elements of G satisfying $x^d = e$ then G is cyclic.

Answer. Cyclic means that we have only one generator so I think it's easier to prove the converse (turned out it was much harder), if G is not cyclic then there will be a $d|m$ such that more than d elements satisfy $x^d = e$.

Note that a non abelian group is non cyclic by definition (this is the contra positive of if a group is cyclic it is abelian so if it is not abelian it is not cyclic).

Let's tackle the easier case first, if G is abelian we can show the above quite easily. Note that we can have abelian groups that are non cyclic like $(\mathbb{Z}/35\mathbb{Z})^\times$.

Since G is non cyclic by assumption, we must have at least two generators who generate different sets, now the sets might overlap but they cannot be the same or one cannot be a superset of the other.

From these generators pick the one with the biggest order, say x with order h. Now take another generator y with the second biggest order l. Let $d = (h, l)$ then y^d will generate a group with order l/d. Now $1 = (l/d, h)$, if we take $z = xy^d$ then z with have an order of $h \cdot l/d$ which is bigger than h which is a contradiction because $hl/d > h$. The only way this works is if $l/d = 1$ but it's either $l = 1$ or $l = d$.

But l cannot be 1 because it is a generator with the second biggest order if $l = 1$ then x will generate the whole group and the group will be cyclic.

If $l = d$ then we have two groups with order d because $x^{h/d}$ has order d too. If the two groups with order d are not completely overlapping then we have more than d elements with $z^d = e$ if they are completely overlapping then $\langle y \rangle \subset \langle x \rangle$ which is again a contradiction because our assumption is that the generators's groups do not completely overlap.

The case for the abelian group is easy because the order of (ab) is just $\text{lcm}(|a|, |b|)$. For a non abelian group I found it much harder to show the above or maybe I'm just really dumb :) The strategy is to do a proof with contradiction, assume that for all d there are no more than d elements with $z^d = e$.

Let's start with an example. Assume $|G| = pq$ where p and q are prime. Now the order of an element cannot be pq because then the group is cyclic. So say $p > q$ pick an element, x, whose order is p. Now pick another element, y, who is not in $\langle x \rangle$. The order of y cannot be p because then we have more than p elements where $z^p = e$ so the order of y must be q.

Let's say there is still another element not covered by those two generators then its order must be either p or q but that will show that there's more than p (or q) elements with $z^p = e$ (or $z^q = e$). So the two generators must cover the whole group, let's count how many elements these two generators generate

$$1 + (p-1) + (q-1) = p + q - 1$$

the first 1 is from e, each -1 is because x and y also generate e. If we divide everything by pq we get

$$\frac{1}{p} + \frac{1}{q} - \frac{1}{pq} = -\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) + 1$$

and this ratio has to be 1 to cover all elements in the group but $(1 - 1/p) > 0$ and so the total is less than one so this means that we cannot cover the whole group which also means that there will be other elements with order p or q.

Now let's take $|G| = pqr$ then this time we have a few more things to consider. We don't need a generator with order p we can start with pq or other combinations. But again we want to know the max number of elements we can generate under the same constraints as above. So we will include all orders as long as we don't violate the contradiction assumption that for each $d|m$ there are no more than d elements with $x^d = e$.

So to maximize the number of elements generated we assume we have as many generators as possible whose subgroup they generate do not overlap. But we cannot have two generators with the same order because then we have more than p elements with $z^p = e$.

So for $|G| = pqr$ the maximum number of elements generated would be

$$1 + (p-1) + (q-1) + (r-1) + (p-1)(q-1) + (q-1)(r-1) + (p-1)(r-1)$$

some explanation, for generator with order pq the number of unique elements it generates including itself (but not including e) is $\varphi(pq) = (p-1)(q-1)$ because other elements must have order either p or q and to avoid the assumption of the contradiction we must assume that any subgroup with order p must be the same otherwise we have the $z^p = e$ situation again. And if we divide the above expression by pqr we get

$$-\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right) + 1$$

which is always less than 1. And to confirm that our calculation above is correct if we include an element with order pqr the sum would be

$$\begin{aligned} &1 + (p-1) + (q-1) + (r-1) + (p-1)(q-1) + (q-1)(r-1) + (p-1)(r-1) \\ &\quad + (p-1)(q-1)(r-1) = pqr \end{aligned}$$

and we were correct.

Another assumption we need to take care of in the above is the number of generators we included in the calculation, it cannot be greater than $|G|$. So if $|G|$ has n distinct elements than the number generators used above is $e \to 1, a_1 \to p-1, a_2 \to q-1, a_3 \to r-1, a_4 \to (p-1)(q-1), a_5 \to (q-1)(r-1), a_6 \to (p-1)(r-1)$, the notation means element a_1 generates $p-1$ unique other elements including itself and so on, so what we are doing is just summing binomial coefficients

$$\sum_{i=0}^{n-1} \binom{n}{i} = 2^n - 1$$

this is because we are just doing n choose 0 (which is the 1 generated by e) followed by n choose 1 and n choose 2 and so on what we are not doing is n choose n because then the group will be cyclic. But $2^n - 1 < |G|$ because each prime divisor of $|G|$ is at least 2.

For $|G|$ with more than 3 prime factors we get

$$-\prod_{i=1}^{n}\left(1 - \frac{1}{p_i}\right) + 1$$

and it will never be one therefore if $m = |G|$ is made up of distinct prime numbers than there is $d|m$ such that there are no more than d elements such that $x^d = e$.

If $|G|$ contains duplicate prime factors then we need to do a little modification so say we have $|G| = p^2qr$ the number of elements generated is

$$1 + (p-1) + (q-1) + (r-1) + (p-1)p + (p-1)(q-1) + (p-1)(r-1) +$$
$$(q-1)(r-1) + (p-1)p(q-1) + (p-1)p(r-1) + (p-1)(q-1)(r-1)$$

because now $\varphi(p^2q) = p(p-1)q$ and so on and if we divide the whole thing by p^2qr we get

$$-\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right) + 1$$

note that even though we have 4 prime factors $|G| = p^2qr$ the first term only has three terms and again this will not reach one, so the difference here is the total number of elements is given by

$$-\prod_{i=0}^{m}\left(1 - \frac{1}{p_i}\right) + 1$$

where m now counts the number of unique prime factors of $|G|$. So if we assume that there is no more than d elements with $x^d = e$ for each $d|m$ then we will have a contradiction thus this assumption must be wrong. So as you can see that the contrapositive is a lot more difficult to prove.

This actually works for abelian and non abelian groups what we did above was actually do number of elements generated $= \sum_{\substack{d|m \\ d\neq m}} \varphi(d)$ and so of course we cannot get 1 when we divide it by m since $m = \sum_{d|m} \varphi(d)$ and we get this identity

$$\sum_{\substack{d|m \\ d\neq m}} \frac{\varphi(d)}{m} = -\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right) + 1$$

where p_i runs through the unique prime factors of m.

Initially I was very confused by this theorem, but the main point of this theorem is that "there is no more than d elements with $x^d = e$ for each $d|m$" means that for each order d if x has order d then $H = \langle x \rangle$ contains all elements with order d.

Page 34. Proof of Proposition 1.18. Another typo $\mathbb{Z} \subset \mathbb{Q} \subset \bar{\mathbb{Z}}$ unless he means something else, if $\mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$ then $\mathbb{Q}$ cannot be a subset of $\bar{\mathbb{Z}}$ because if it is then the intersection is all of $\mathbb{Q}$. I think what he meant is that $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{Z} \subset \bar{\mathbb{Z}}$.

Note that if we define the polynomial to be non monic we do have $\mathbb{Q} \subset \bar{\mathbb{Z}}$ because for any $\frac{c}{d} \in \mathbb{Q}, c, d \in \mathbb{Z}$ we have $f(X) = dX - c$ to be the polynomial with root c/d but in the previous paragraph he set the convention that the polynomials are monic.