Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: March 1, 2016)

Abstract

Stray thoughts of a stray man. This is a collection of things that I thought was fun to do and also things that I always come back to after forgetting it :) There's no order or structure here just whatever my mind facies at the moment.

The pdf book I've been reading about elementary number theory (ent) is ent.pdf. It is written by William Stein, there are multiple versions and revisions of the book. One is called "*Primes, Congruences, and Secrets*" dated Nov 16, 2011. Another version is called "*A Computational Approach*" dated March 2007. As far as I can tell, they are pretty much the same but I'll use "*Primes, Congruences, and Secrets*" in this article.

The proofs in these books are not the easiest to understand but they are really cool. So I'll list here explanations about the proofs that hopefully clarify them.

Lemma 1.1.9 This is a really cool way to prove something. He was using the concept of (sub)sets, something seemingly unrelated to prove properties of gcd.

The goal here is to show that

$$\gcd(a,b) = \gcd(b,a) = \gcd(\pm a, \pm b) = \gcd(a, b-a) = \gcd(a, b+a)$$

The first thing he showed is that $\gcd(a,b) \leq \gcd(a,b-a)$ followed by $\gcd(a,b-a) \leq \gcd(a,b)$ which means that $\gcd(a,b) = \gcd(a,b-a)$.

To show that $\gcd(a,b) \leq \gcd(a,b-a)$ he uses the idea of a subset. He shows that every common divisor of a and b is also a common divisor of $b-a$, *i.e.* $a = dc_1, b = dc_2 \rightarrow b - a = d(c_2 - c_1)$. Now since every common divisor of a and b is also a divisor of $b-a$ this means that the common divisors of a and b is a subset of the divisor of $b-a$.

Since they are a subset $\gcd(a,b) \leq \gcd(a,b-a)$ as the max element of the subset is either the same as the max element of the superset or lower, *e.g.* consider a set $\{1,4,8,9\}$ if you form a subset of this, the maximum of this subset is 9 or lower, depending what elements you choose for the subset but it can't be higher than 9.

The next step in the proof is to show that $\gcd(a,b-a) \leq \gcd(a,b)$. He did this by replacing $a \rightarrow -a,\ b \rightarrow b-a$ such that $\gcd(a,b) \rightarrow \gcd(-a,b-a)$. He then repeats the reasoning above, every common divisor of $-a$ and $b-a$ is also a divisor of $(b-a) - (-a) = b$ this means that $\gcd(-a,b-a) \leq \gcd(-a,b)$ but $\gcd(-a,b-a) = \gcd(a,b-a),\ \gcd(-a,b) = \gcd(a,b)$. This completes the proof.

Lemma 1.1.17 This is another cool one. He uses (strong) induction in a way I'd neven seen before. Usually you use induction by proofing the link between n and $n+1$ but he doesn't. Instead he retrospects, let's see what I mean.

The goal here is to prove $\gcd(an,bn) = \gcd(a,b) \cdot |n|$ something very obvious.

He started by (implicitly) assuming that all numbers a', b' smaller than a, b, *i.e.* $a'+b' < a+b$, have this property. Note that he uses the sum of the numbers for induction instead the numbers themselves. As the base case he uses $a + b = 2$.

The proof now continues through several bridges.

1. Show that $\gcd(an, bn) = \gcd(bn, rn)$, this is achieved through Euclid's algorithm as $an = bnq + rn$.

2. Next, show that $\gcd(bn, rn) = \gcd(b, r) \cdot |n|$, how? by showing that $b + r < a + b$, why? Because if $b + r < a + b$ then the case of $\gcd(bn, rn)$ is already covered by the induction. Recall that induction assumes all pairs $b + r$ leading up to $a + b$ already have this property, so if $b + r < a + b$ then b, r is already in the induction assumption. This is why I said that he's using a strong induction.

As we have seen, the induction proof was not a typical one, we're not proving the link between n and $n+1$, he assumes that all elements less than $n+1$ are true and then show that our target is equal to one of those earlier elements. Very clever indeed.

Lemma 1.1.17, "Gangnam Style". Despite being a very clever proof I would like a simpler one :) A much simpler proof will utilize Euclid's algo

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\vdots \\ r_{m-2} &= r_{m-1} q_m + (1?) \end{aligned}$$

where if the last remainder is 1 the gcd between a and b is 1, otherwise it is r_{m-1}. If we multiply a and b by n, the multiplication will cascade down all the way

$$\begin{aligned} na &= nb \cdot q_1 + nr_1 \\ nb &= nr_1 \cdot q_2 + nr_2 \\ &\vdots \\ nr_{m-2} &= nr_{m-1} \cdot q_m + (n \cdot 1?) \end{aligned}$$

if the last remainder is n then the gcd is n since $n|nr_{m-1}$ otherwise the remainder is nr_{m-1}. Thus $\gcd(na, nb) = |n| \cdot \gcd(a, b)$.

Theorem 1.1.19 Another clever proof, another indirect one. The goal is to show that if p is prime and $p|ab$ then either $p|a$ or $p|b$.

He approaches this by showing that $p|\gcd(pb, ab)$ why? because $\gcd(pb, ab) = b\gcd(p, a) = b$. So his approach was to find "how can I represent b? are there any other forms of b that are divisible by p?" The answer of course is that $p|\gcd(pb, ab)$ and $\gcd(pb, ab)$ happens to be b itself. Nice trick.

Theorem 1.1.19, "Gangnam Style". I, on the other hand, will personally do it the other way. Starting with there was a prime p and if $p \nmid a$ and $p \nmid b$ then $p \nmid ab$, *i.e.* we turn it around, from "'if A then B" into "if not B then not A".

Say $p \nmid a$ and $p \nmid b$ and we then assume a contradiction $p|ab$. Now $p|pa$ and $p|ab$, from Lemma 1.1.17 $p|\gcd(pa, ab) \rightarrow p|a\gcd(p, b)$. Since p is prime $\gcd(p, b)$ is either p or 1. If $\gcd(p, b) = 1$ then $p|a\gcd(p, b) = p|a \cdot 1$ which is a contradiction, if $\gcd(p, b) = p$ then $p|b$ which is also a contradiction, which means that our assumption $p|ab$ is wrong, *i.e.* $p \nmid ab$.

Since $p \nmid a$ and $p \nmid b \longrightarrow p \nmid ab$ this means that $p|ab \longrightarrow p|a$ or $p|b$ with the understanding that p is prime.

Theorem 1.1.6, the proof is actually on page 10. I just want to recap the strategy he used to prove this theorem. The key is Theorem 1.1.19 but to prove 1.1.19 you need to know about gcd and its properties, they are

1. Lemma 1.1.9, for any integers a and b we have

$$\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b) = \gcd(a, b - a) = \gcd(a, b + a)$$

2. Lemma 1.1.10, suppose $a, b, n \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(a, b - an)$.

3. Proposition 1.1.11, suppose that a and b are integers with $b \neq 0$. Then there exists unique integers q and r such that $0 \leq r < |b|$ and $a = bq + r$

4. Algorithm 1.1.12 (Division Algorithm) Suppose a and b are integers with $b \neq 0$. This algorithm computes integers q and r such that $0 \leq r < |b|$ and $a = bq + r$

5. Algorithm 1.1.13 (Greatest Common Division), this is Euclid's algorithm

6. Lemma 1.1.17, for any integers a, b, n we have

$$\gcd(an, bn) = \gcd(a, b) \cdot |n|$$

7. Lemma 1.1.18, suppose $a, b, n \in \mathbb{Z}$ are such that $n|a$ and $n|b$. Then $n| \gcd(a, b)$

8. Theorem 1.1.19, let p be a prime and $a, b \in \mathbb{N}$. If $p|ab$ then $p|a$ or $p|b$

So it's nowhere near straightforward, trying to prove this theorem straightforwardly is an oxymoron.

Algorithm 1.2.3 This is actually about proof of step 2, the stopping condition. The proof of this step doesn't give any intuition as to how this is true, it basically boils down to "false assumption leads to contradictions".

There's actually a better explanation which is very intuitive. Once you come to a number that is roughly $\sim \sqrt{n}$ you know you can stop, why? The current number in question $\sqrt{n}$ is of course a prime since the non primes have been crossed off by the previous primes and their multiples. But some of the multiples of $\sqrt{n}$, *i.e.* $p\sqrt{n},\ p < \sqrt{n}$ have been crossed off by multiples of the previous lesser primes. The next thing to cross is of course $\sqrt{n} \cdot \sqrt{n}$, but this is already bigger than n, so we can stop.

The above explanation might still be confusing. Let's see it with a concrete example, for simplicity let's use the same example as in the book $n = 40$ but let's jump straight to after we've crossed off $2, 3, 5$ and their multiples. The set X is now

$$X = [7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37]$$

We now need to cross off 7 and its multiples, however,

- 7×2 was crossed off by 2×7
- 7×3 was crossed off by 3×7
- 7×4 was crossed off by 2×14
- 7×5 was crossed off by 5×7.

The next thing to cross off is then 7×7 but this is larger than n so we can immediately stop. For any other number > 7 the situation is even more dire since some of their multiples have been crossed off by the lesser primes and their square is definitely bigger than n.

Proposition 1.2.5 The goal here is to show that there are infinitely many primes in the form $4x - 1$. However the proof was a bit confusing. He started like Euclid, constructing a new number in the form

$$N = 4p_1p_2 \cdots p_n - 1$$

Notice that he began by assuming that $p_1p_2 \cdots p_n$ are primes of the form $4x - 1$. This is required as we want to show that no known prime of the form $4x - 1$ divides N, if p_i is just any prime we would only show that the new prime that divides N is not the same as any of p_i but since p_i is not of the form $4x - 1$ there might be some other primes of the form $4x - 1$ that wasn't included in constructing N. Thus the new prime factor of N is not really new, it just wan't included in constructing N.

As to why $p_i \nmid N$ is because if $p_i | N \rightarrow N = p_i m$ then

$$\begin{aligned} N = p_i m &= p_i \cdot (4 \prod_{j \neq i} p_j) - 1 \\ p_i(m - 4 \prod_{j \neq i} p_j) &= -1 \\ \rightarrow p_i &\mid -1 \end{aligned}$$

which is a contradiction (this is the reasoning used in Euclid's famous "there are infinite prime numbers" proof).

He then argues that if all prime factors of N is of the form $4x + 1$ then N will be of the form $4x + 1$ as well which is true. The mysterious phrase is then (the phrase in the "*A Computational Approach*" is even worse) "since N is odd, each prime divisor p_i is odd so there is a $p|N$ that is of the form $4x - 1$". Why not $2x + 1$? which is the most generic form of an odd number. The thing is that N is of the form $4x - 1$ so we want the product of its factors to conform to $4x - 1$. However, his requirement is actually not stringent enough (or he didn't explain it clearly enough), say that we have an odd number whose

factors are

$$(2x_1 + 1)(4x_2 - 1) = 8x_1x_2 - 2x_1 + 4x_2 - 1$$

just because one of the factor is $4x - 1$ it doesn't mean that we are guaranteed to have $N \sim 4x - 1$. What we really need (as seen from the example above) is that all other factors are of the form $4x + 1$ while at least one of them (or an odd number of them) is of the form $4x - 1$.

This is because the product of of the of x's with nothing but the 1's need to be in the form of $4x$, thus we need to have all the x's multiplied by 4 and we need an odd number of $4x - 1$ because the product of all the 1's needs to be -1.

How about the last sentence "We can repeat this process indefinitely"? Remember that the primes that construct N, *i.e.* p_i, were all of the form $4x - 1$. Since we find another one of the form $4x-1$ (as one of the factor of N) we can construct a new number $N' = 4p_1p_2 \cdots p_np_{\text{new}} - 1$ which in turn produces another prime of the form $4x - 1$ which we can use to construct another number and so on.

Problem 1.1 Warm up! :) Compute the greatest common divisor $\gcd(455, 1235)$ by hand.

I did it by hand no calculator involved :)

$$\begin{aligned} 1235 &= 455 \times 2 + 325 \\ 455 &= 325 \times 1 + 130 \\ 325 &= 130 \times 2 + 65 \\ 130 &= 65 \times 2 \end{aligned}$$

gcd is 65!

Problem 1.3 Prove that there are infinitely many primes of the form $6x - 1$.

This closely follows the proof of Proposition 1.2.5. Let

$$N = 6p_1p_2 \cdots p_n - 1$$

where p_i is of the form $6x - 1$. We know that $p_i \nmid N$. To get the form $6x - 1$ the prime factors of N has to be of the form $6x \pm 1$ and an odd number of them of them has to be

$6x-1$. Thus we have a new prime of the form $6x-1$ which we can use to construct a new Number $N' = \prod 6p_i - 1$ and the whole process repeats.

Problem 1.4 Use Theorem 1.2.10 to deduce that $\lim_{x\to\infty} \pi(x)/x = 0$.

Theorem 1.2.10 is

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1$$
$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} - 1 = 0$$

The thing I'm not sure about is whether we can do the usual algebraic manipulations with the lim involved, for example, is the following legit?

$$\lim_{x\to\infty} \left(\frac{\pi(x)}{x/\log(x)} - 1 \right) \times \frac{1}{\log(x)} = 0 \times \frac{1}{\log(x)}$$

I'm not sure if we can do the above but

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1$$
$$\lim_{x\to\infty} \pi(x) = \lim_{x\to\infty} \frac{x}{\log(x)}$$
$$\lim_{x\to\infty} \frac{1}{x} \times \pi(x) = \lim_{x\to\infty} \frac{1}{\cancel{x}} \times \frac{\cancel{x}}{\log(x)} = 0$$

I think that was legal as the first line says that $\lim_{x\to\infty} \pi(x) = \lim_{x\to\infty} x/\log(x)$, *i.e.* as x goes to ∞ the two approach the same value. This means that if we divide both sides by the same value we will still get the same limit for both sides.

Problem 1.8 (a) if $a|n$ and $b|n$ with $\gcd(a,b) = 1$, then $ab|n$

The easiest way is of course to use the fundamental theorem of arithmetic but here I try not to do that if at all possible. First $a|n \to n = aa'$, $b|n \to n = bb'$, suppose $a < b$ (we know $a \neq b$), it doesn't matter which we choose to be smaller, the argument will be the same

$$aa' = bb'$$
$$aa' = (aq + r)b'$$
$$a(a' - qb') = rb'$$

which means that $a|rb'$. We also know from Euclid's algorithm that $\gcd(b,a) = \gcd(a,r)$ but since $\gcd(a,b) = 1 \to \gcd(a,r) = 1$. We know that $a|rb'$ and obviously $a|ab'$ then

from Lemma 1.1.18 $\rightarrow a|\gcd(rb', ab')$, following the proof of Theorem 1.1.19

$$\begin{aligned} a \mid \gcd(rb', ab') \\ \gcd(ar, ab') = |b'| \cdot \gcd(r, a) = |b'| \cdot 1 \\ \rightarrow a \mid b' \end{aligned}$$

so $b' = aw \rightarrow n = bb' = (ba)w \rightarrow ab|n$ which completes the proof.

Problem 1.8 (b) if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$

Again, let's not use the fundamental theorem. Since we know that $a \neq b$, the first possibility is $a < b \rightarrow b = aq + r$

$$\begin{aligned} (aq + r)c = an \\ rc = a(n - q) \\ \rightarrow a \mid rc \end{aligned}$$

Following the footsteps of Problem 1.8 (a) above, $\gcd(b, a) = 1 = \gcd(a, r)$. Next, $a|rc$ and $a|ac$, so according to Lemma 1.1.18 $\rightarrow a|\gcd(rc, ac) = c \cdot \gcd(r, a) = c \cdot 1 = c \rightarrow a|c$.

The only other possibility is $b < a \rightarrow b = a - \Delta$

$$\begin{aligned} (a - \Delta)c = an \\ -\Delta c = a(n - c) \\ \rightarrow a \mid \Delta c \end{aligned}$$

To proceed we need to show that

$$\begin{aligned} \Delta = -b + a \\ \rightarrow \gcd(a, \Delta) = \gcd(a, -b + a) = \gcd(a, -b) = \gcd(a, b) \\ = 1 \end{aligned}$$

where we have used Lemma 1.1.9 in the second line, thus $\gcd(a, \Delta) = 1$, since $a|\Delta c$ and $a|ac$ using Lemma 1.1.18 $\rightarrow a|\gcd(\Delta c, ac) = c \cdot \gcd(\Delta, a) = c \cdot 1 = c \rightarrow a|c$.

Problem 1.9 (a) if $a|b$ and $b|c$ then $a|c$.

$$\begin{aligned} a|b \rightarrow b = am \\ b|c \rightarrow c = bn = amn \\ c = a(mn) \rightarrow a|c \end{aligned}$$

Problem 1.9 (b) if $a|b$ and $c|d$ then $ac|bd$.

$$a|b \to b = am$$
$$c|d \to d = cn$$
$$ac = (ac)(mn) \to ac|bd$$

Problem 1.9 (c) if $m \neq 0$, then $a|b$ if and only if $ma|mb$.

$$a|b \to b = aw$$
$$mb = maw \to ma|mb$$

The other way

$$ma|mb \to mb = maw \to b = aw$$
$$b = aw \to a|b$$

Problem 1.9 (c) if $d|a$ and $a \neq 0$, then $|d| \leq |a|$.

$$d|a \to a = dw \to |a| = |dw| = |d||w|$$
$$|a| = |d||w| \to |d| \leq |a|$$

Problem 1.11 (b) Fun facts! The two numbers are actually the first 27 digits of π and e and their gcd is 13. Their factors are

$$314159265358979323846264338 = 2 \times 3 \times 7 \times \mathbf{13} \times 17 \times 23 \times 53 \times 27765442739383319011$$
$$271828182845904523536028747 = \mathbf{13} \times 31 \times 14419 \times 48287851 \times 968760484921$$

Problem 1.12 (a) Suppose $a,\ b$ and n are positive integers. Prove that if $a^n|b^n$ then $a|b$.

Let's try if we can do it without the fundamental theorem, since it'll be too easy otherwise ¯\(°_o)/¯

The problem is an "if A then B" type but it also means "if not B then not A". We'll go by induction but before that, from $a^n|b^n$ we know that $a < b$ (which can be easily

proven by induction). We also know that $a|b^n$ either through Lemma 1.1.10, because $a^n|b^n \to b^n = a^n m$ and

$$\begin{aligned}
\gcd(a, b^n) &= \gcd(a, a^n m) \\
&= \gcd(a, a^n m - ad), \quad d = a^{n-1}m - 1 \\
\gcd(a, b^n) &= \gcd(a, a) = a \\
&\to a \mid b^n
\end{aligned}$$

or through $b^n = a^n m = a(a^{n-1}m) = aw \to a|b^n$ or through Problem 1.9 (a), $a|a^n$ and $a^n|b^n$ then $a|b^n$.

We now want to show that if $a \nmid b$ then $a \nmid b^n$ by induction. We start by proving the base case $a \nmid b^2$. Before we start we want to divide both a and b by $m \equiv \gcd(a, b)$ and denote them $a' = a/m$ and $b' = b/m$ where $\gcd(a', b') = 1$.

From Problem 1.9 (c) we have $a \nmid b \to a' \nmid b'$. Now what about $a'|b'^2$? Say $a'|b'^2$ then

$$\begin{aligned}
&a'|b'^2 = a'|b'b', \quad \gcd(a', b') = 1 \\
&\to a' \mid b'
\end{aligned}$$

where we have used Problem 1.8 (b). But this is a contradiction since $a' \nmid b'$, thus $a' \nmid b'^2$. Now the induction step, suppose $a' \nmid b'^n$ we want to show $a' \nmid b'^{n+1}$, assume otherwise

$$\begin{aligned}
&a'|b'^{n+1} = a'|b'b'^n, \quad \gcd(a', b') = 1 \\
&\to a' \mid b'^n
\end{aligned}$$

where we have used Problem 1.8 (b). This is a contradiction as $a' \nmid b'^n$ thus we have proved that if $a' \nmid b'$ then $a' \nmid b'^n$ where $\gcd(a', b') = 1$. In other words if $a'|b'^n$ then $a'|b'$.

Our problem states that $a^n|b^n = \cancel{m^n}a'^n|\cancel{m^n}b'^n$ where $m = \gcd(a, b)$ (we have used Problem 1.9 (c)). But $a'^n|b'^n$ means that $a'|b'^n$ (as shown above) and by the above result $a'|b'^n \to a'|b' = ma'|mb' = a|b$ using Problem 1.9 (c). This completes the proof.

I initially solved it this way

$$\begin{aligned}
b^n &= a^n m \\
m &= \left(\frac{b}{a}\right)^n
\end{aligned}$$

Since $m \in \mathbb{Z} \to b/a \in \mathbb{Z} \to b = an,\ n \in \mathbb{Z} \to a|b$. But the dodgy step is the requirement that $b/a \in \mathbb{Z}$, this smells like we are implicitly assuming the fundamental theorem as we are trying to simplify the ratio into the canonical form.

I tried many other more straightforward ways but they didn't come to anything, one of the ways was to assume $a \nmid b \to b = aq + r$ with not much luck.

Problem 1.12 (b) Suppose p is a prime and a and k are positive integers. Prove that if $p|a^k$, then $p^k|a^k$.

Again, let's try not to use the fundamental theorem. Start with $p|a^k \to p|aa^{k-1}$, we also have $p|pa^{k-1}$. From Lemma 1.1.18 $\to p|\gcd(aa^{k-1}, pa^{k-1}) = p|a^{k-1}\gcd(a,p)$. From Theorem 1.1.19 it is either $p|a^{k-1}$ or $p|\gcd(p,a)$.

Now $\gcd(p,a)$ is either 1 or p since p is prime. If $\gcd(p,a) = p$ then we are done since $p|a$ and $a|a^k$ means $p|a^k$ (see Problem 1.9 (a)). If $\gcd(p,a) = 1$ then $p|a^{k-1}$.

We now repeat the process, $p|\gcd(aa^{k-2}, pa^{k-2}) \to p|a^{k-2}$ since $\gcd(p,a) = 1$. Continuing in this path to $p|a$ we get a contradiction because we have assumed that $\gcd(p,a) = 1$, thus $\gcd(p,a) = p$ and according to Problem 1.9 (a), $p|a$ and $a|a^k$ means $p|a^k$.

Problem 1.13 (a) Prove that if a positive integer n is a perfect square, then n cannot be written in the form $4k + 3$.

Since $4k + 3$ is odd n has to be odd. In that case $n = (2x + 1)^2$

$$\begin{aligned}(2x+1)^2 &= 4x^2 + 4x + 1 \\ &= 4(x^2 + x) + 1 \\ &= 2\{2x(x+1)\} + 1\end{aligned}$$

while

$$\begin{aligned}4k + 3 &= 4k + 2 + 1 \\ &= 2(2k+1) + 1\end{aligned}$$

This means that $2x(x + 1) = 2k + 1$ which is impossible since the LHS is even while the RHS is odd.

Problem 1.13 (b) Prove that no integer in the sequence

$$11, 111, 1111, 11111, 111111, \ldots$$

is a perfect square. (Hint: $111\cdots111 = 111\cdots108 + 3 = 4k + 3$)

We just need to follow the hint :)

$$\begin{aligned}
\underbrace{111\cdots111}_{N \text{ number of 1's}} &= \sum_{i=0}^{N-1} 10^i \\
&= 11 + \sum_{i=2}^{N-1} 10^i \\
&= 11 + \sum_{i=1}^{N-2} 100^i \\
&= 4 \cdot 2 + 3 + \sum_{i=1}^{N-2} (4 \cdot 25)^i \\
&= 4 \left(2 + \sum_{i=1}^{N-2} 4^{i-1} 25^i \right) + 3 \\
&= 4k + 3
\end{aligned}$$

in the above derivation $N > 2$ for $N = 2 \rightarrow 11 = 4 \cdot 2 + 3$. From Problem 1.13 (a) we know that no perfect square is of the form $4k + 3$ and this completes the proof.

Problem 1.14 Prove that a positive integer n is prime if and only if n is not divisible by any prime p with $1 < p \leq \sqrt{n}$.

The first part is easy, if n is prime then its only factors are 1 and n thus it is not divisible by p with $1 < p \leq \sqrt{n}$.

The other way "if n is not divisible by any prime p with $1 < p \leq \sqrt{n}$ then n is prime" is a bit harder.

The proof proceeds like the field sieve algorithm. Say we list all N primes $p_i \leq \sqrt{n}$ that do not divide n sorted by $p_1 < p_2 < \cdots < p_N$. We know from the fundamental theorem that n contains prime factors that are smaller than n.

Since $p_1, p_2, \ldots, p_N$ do not divide n the next prime factor candidate will be $p_{N+1} > p_n > \sqrt{n}$. But for $n = p_{N+1}m$, m has to be $< \sqrt{n}$ and contain one of the $p_1, p_2, \ldots, p_N$, otherwise the only other option is $p_{N+1}p_{N+1} > \sqrt{n}\sqrt{n} > n$ but none of $p_1, p_2, \ldots, p_N$ divides n thus no prime divides n and n itself must be prime.

Chapter 1 Conclusion

- On the way through proving the fundamental theorem we see how important

$\gcd(na, nb) = n \cdot \gcd(a, b)$ is.

- We don't need to use the fundamental theorem as I have shown in solving the various problems above. This reiterates the idea that math is an interconnected web of theorems as mentioned by Feynman, if we don't have a theorem we can use other theorems as bridges to the one we need.

- Keen observations are a must, we need all we can get on those numbers.

++++++++++++++++++++++++++++++++++++

Example 2.1.5.

$$\mathbb{Z}/3\mathbb{Z} = \{\{\underbrace{\ldots, -3, 0, 3, \ldots}_{\text{“0”}}\}, \{\underbrace{\ldots, -2, 1, 4, \ldots}_{\text{“1”}}\}, \{\underbrace{\ldots, -1, 2, 5, \ldots}_{\text{“2”}}\}\}$$

Explanation: the set $\mathbb{Z}/3\mathbb{Z}$ only has *three* elements but each element is a set. Please do not confuse each element with an ideal, we know that the ideal

$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

because if a is an element of an ideal then $-a$ is also an element. Therefore $\{\ldots, -2, 1, 2 \ldots\}$ and $\{\ldots, -1, 2, 5 \ldots\}$ are **not** ideals.

What happens to $\mathbb{Z}/3\mathbb{Z}$ is it is a quotient of the ring $\mathbb{Z}$ by some "ideal" $n\mathbb{Z}$ (notice the quatation marks) because as we have seen that two of the sets are not ideals. What we have is shifted ideals

$$\begin{aligned}
\mathbb{Z}/3\mathbb{Z} &= \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} \\
0 + 3\mathbb{Z} &= \{\ldots, \underbrace{\mathbf{0}+-3}_{\text{-3}}, \underbrace{\mathbf{0}+0}_{\text{0}}, \underbrace{\mathbf{0}+3}_{\text{3}}, \ldots\} \\
1 + 3\mathbb{Z} &= \{\ldots, \underbrace{\mathbf{1}+-3}_{\text{-2}}, \underbrace{\mathbf{1}+0}_{\text{1}}, \underbrace{\mathbf{1}+3}_{\text{4}}, \ldots\} \\
2 + 3\mathbb{Z} &= \{\ldots, \underbrace{\mathbf{2}+-3}_{\text{-1}}, \underbrace{\mathbf{2}+0}_{\text{2}}, \underbrace{\mathbf{2}+3}_{\text{5}}, \ldots\}
\end{aligned}$$

Or in a physicist friendly way (in talking about quotient of a group), we identify each element of $\mathbb{Z}$ using $n\mathbb{Z}$, thus $0 \to 0 + n\mathbb{Z}$, etc. How about n itself? n has been covered

by $0 + n\mathbb{Z}$. So in this way $n\mathbb{Z}$ acts as a gauge transformation and each $k + n\mathbb{Z}$ is a gauge orbit.

Proposition 2.1.9 I proved this before in this document, "*A number $n \in \mathbb{Z}$ is divisible by 3 if and only if the sum of the digits of n is divisible by 3.*"

His proof boils down to

$$n = a + 10b + 100c + \cdots \equiv a + b + c + \cdots (\text{mod } 3)$$

Now why does this proof work? It says that $n = (a + b + c)(\text{mod } 3)$. The meaning of (mod 3) is that $a = b(\text{mod } 3) \rightarrow 3|a - b$ so in this case $3|n - (a + b + c)$ but since $3|n$ therefore $3|(a + b + c)$.

Definition 2.1.11 "(Complete Set of Residues). ... pairwise distinct". The name is apt since the set is the set of residues of n, *e.g.* $1, 2, 3, \ldots, n - 1$. The "pairwise distinct" phrase, I think, means that every two elements of R are not related by n, *i.e.* every two elements x_1 and x_2 of R, $n \nmid (x_1 - x_2)$.

Lemma 2.1.12,"Gangnam Style". The way I'll prove it is to show it through a contradiction. Assume that aR is not a complete set of residues modulo n, which means that there are two elements of aR, say $ax_1 - ax_2$ such that

$$n|a(x_1 - x_2)$$

since $\gcd(n, a) = 1$ from Problem 1.8 (b) we know that $n|(x_1 - x_2)$ but this is a contradiction since the elements of R are pairwise distinct. Thus aR is a complete set of residues modulo n.

Problem 2.12 Let p be prime. Prove that $\mathbb{Z}/p\mathbb{Z}$ is a field.

What is the reasoning behind this? Remember that a field is a ring where each non-zero element has an "inverse" under multiplication, *i.e.* for each element $a \neq 0$ we can find another element b such that $ab = 1$.

If q is not prime we can show that $\mathbb{Z}/q\mathbb{Z}$ is **not** a field. Here is why. For simplicity let's denote $\mathbb{Z}/q\mathbb{Z}$

$$\mathbb{Z}/q\mathbb{Z} = \{0, 1, 2, 3, \ldots, q - 1\}$$

where each number is actually $k + q\mathbb{Z}$. So, if q is not prime, at least one of the numbers in $\mathbb{Z}/q\mathbb{Z}$ less than q has to be a factor of q, let's denote this number $w,\ w < q$. Since w is a factor of $q \to q = wm$.

The identity element, 1, in the ring $\mathbb{Z}/q\mathbb{Z}$ is actually $qn + 1 = w(mn) + 1$. Now we want to find another element u such that $uw = 1 = qn + 1 = w(mn) + 1$, but this is a contradiction since $w(u - mn) = 1 \to w|1$. Thus $\mathbb{Z}/q\mathbb{Z}$ for non prime q is **not** a field.

Back to our original problem, we need to show the opposite, that for a prime p, $\mathbb{Z}/p\mathbb{Z}$ is always a field. As shown above, since none of the elements of $\mathbb{Z}/p\mathbb{Z}$ is a factor of p, this should be possible, the hard part is showing **how** this can definitely be done (answer: induction).

The trick here is to utilize the circular structure of $\mathbb{Z}/p\mathbb{Z}$ in the induction step. The base case is obviously $a \in \mathbb{Z}/p\mathbb{Z},\ a = 1$ with the inverse being itself $1 \cdot 1 = 1$. Now suppose that we have found the inverse for each non-zero element of $\mathbb{Z}/p\mathbb{Z}$ up to n, how about $v = n + 1$?

Notice that each non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is less than p. This means that we can write

$$p = vq + r$$

What we want is to just exceed p, if we add one more $v \to v(q + 1)$ and substracting p from it we get $v(q + 1) - p = v - r$. We know that $r < v$ therefore $v - r < v$ but the case of $< v$, *i.e.* all elements up to n, already has an inverse and we can use that inverse to get the inverse of v. For example $v - r = d$ and the inverse of d is y such that $dy = ps + 1 = 1$. This means that since $p = vq + r$ and $v - r = d$

$$\begin{aligned} v(q + 1) &= p + d \\ v(q + 1)y &= py + dy = py + (ps + 1) \\ v(q + 1)y &= p(y + s) + 1 \end{aligned}$$

i.e. $v(q + 1)y = 1$ and the inverse of v is $(q + 1)y$. The primality of p was needed to guarantee that $r \neq 0,\ v \nmid p$ otherwise the proof doesn't work.

$(q + 1)y$ is generally not the "smallest" inverse of v but we can of course bring it back

to be $< p$ by substracting it by $pt \to v((q+1)y - pt) = p(y + s - tv) + 1 = 1$ for some t such that $0 < (q+1)y - pt < p$.

Now, we are dealing with $k + n\mathbb{Z}$. If the element we are inspecting is $> p$ or < 0 we can still repeat the same argument but this time instead of just exceeding p we want to exceed $|np|$ with $|n|$ the smallest number such that $|np| > |v|$.

Notice that in the above argument, we can identify $v(q+1) = d$ because of the circular structure of $\mathbb{Z}/p\mathbb{Z}$ which also allows us to utilize previously discovered inverses. Let's see this with a concrete example using $\mathbb{Z}/7\mathbb{Z}$ and pick from it the element $v = 3$ (lucky seven meet holy trinity).

$$7 = 3 \times 2 + 1$$

Adding one more 3 and substracting 7

$$\begin{aligned}((3 \times 2) + 3) - 7 &= 3 - 1 \\ &= 2\end{aligned}$$

But in the induction process leading up to 3 we have found the inverse for 2 which is 4, $2 \cdot 4 = 8 = 1$. Thus the inverse of 3 is $(2+1) \cdot 4 = 12 \to 3 \times 12 = 36 = 7 \cdot 5 + 1$.

Some sidenote, we can of course use the above method to get the inverse of 2 from the inverse of 1 but it can actually be computed a lot easier. In the case of 2 the inverse is y such that $2y = pn + 1$. We want $pn + 1$ to be even and unless p is 2, p is always odd. Therefore any odd n will do ($n = 1$ is a very good choice) and y is just $(p+1)/2$ while the case of $p = 2$ is trivial since the only members of $\mathbb{Z}/2\mathbb{Z}$ are $\{0, 1\}$.

In conclusion we have done a 2-in-1 combo deal. We have proven that if p is not prime then $\mathbb{Z}/p\mathbb{Z}$ is a not field, in other words if $\mathbb{Z}/p\mathbb{Z}$ is a field then p is prime and we have proven that if p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field. Therefore we have proven a much stronger statement, *p is prime if and only if $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Definition 2.1.16. Be careful about the reasoning in this proof, especially the following statement

There are only finitely many residue classes modulo n, so we must eventually nd two integers i, j with $i < j$ such that

$$x^j \equiv x^i (\text{mod } n).$$

What he was saying is not that the series x^j will produce all remainders of n but that at some point the remainder will repeat, *e.g.* $x^i = nq + r,\ x^j = nq' + r'$ where $r' = r$. It doesn't mean that that we will have all remainders $0, 1, \ldots, n-1$ of n.

Theorem 2.1.20. The proof is similar to Lemma 2.1.12. If two elements of xP are congruent, *i.e.* $xa = xa'(\text{mod } n)$ then since $\gcd(x, n) = 1$ according to Proposition 2.1.10 we can divide both sides $\cancel{x}a = \cancel{x}a'(\text{mod } n)$.

But since all elements of P are distinct $a = a'$. Meaning xP has the same number of elements as P and they are all distinct.

Note that this doesn't mean that $xa = a(\text{mod } n)$!

Proposition 2.1.22. In the proof of Wilson's theorem the enigmatic statement

If $a \in \{1, 2, ..., p-1\}$, then the equation

$$ax \equiv 1(\text{mod } p)$$

has a unique solution $a' \in \{1, 2, ..., p-1\}$.

The above statement is from Exercise 2.12, *i.e.* if p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is a field every element has an inverse. The set $\{1, 2, ..., p-1\}$ is just the lift of $\mathbb{Z}/p\mathbb{Z}$ thus each element has an inverse as well.

"Multiplying both sides by $p-1$ proves that $(p-1)! \equiv 1(\text{mod } n)$". Note that

$$\begin{aligned} 1(\text{mod } n) &= 1 + pm \\ \rightarrow (p-1) \times \{1(\text{mod } n)\} &= (p-1)(1+pm) \\ &= -1 + p(pm + 1 - m) \\ (p-1)\{1(\text{mod } n)\} &= -1(\text{mod } n) \end{aligned}$$

Another mysterious statement is "so that $p \geq 4$ is a composite number", what happens to 3? Well 3 was the example on page 27.

There are a couple keen observations in this proof

- $l|(p-1)!$, this is because $l|p$ so $l < p$ and $(p-1)! = 1 \cdot 2 \cdot 3 \ldots (p-1)$ since it lists all numbers between 0 and p, it must contain l.

- "a prime cannot divide a number a and also divide $a+1$"

Theorem 2.2.2. In the proof we need to substract both sides of $a + tm \equiv b (\text{mod } n)$. We can always add and substract both sides of a congruence since if $a \equiv b (\text{mod } n)$ then $n|(a - b) \rightarrow n|((a + \Delta) - (b + \Delta))$.

Multiplication is a bit trickier if $a \equiv b (\text{mod } n)$ then $ca \equiv cb (\text{mod } n)$. We can of course divide both sides with c even if $c \nmid n$. However, we can't just factor out both sides in general.