# Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: April 12, 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 1.1.9, lowbrow version**. The way I'd prove this is straighforward, *i.e.* proof by contradiction. Assume $d = \gcd(a,b) \neq d' = \gcd(a,b-a)$. There are then only two choices, either $d > d'$ or $d < d'$. Start with $d > d'$. Now since $d|a$ and $d|b \rightarrow d|b-a$ this means that $d$ is a common divisor of $a$ and $b-a$ which is a contradiction since $d > d'$,

*i.e.* no other common divisor should be larger than $d'$, the *greatest* common divisor of $a$ and $b-a$.

The other way around, $d < d'$, is also a contradiction. Because $d'|a$ and $d'|b-a \rightarrow d'|b$, so here we find a common divisor $d'$ of $a, b$ that is greater than the *greatest* common divisor $d$! Thus $d$ must be equal to $d'$.

**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, lowbrow version**. Despite being a very clever proof I would like a simpler one :) A much simpler proof will utilize Euclid's algo

$$a = bq_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$\vdots$$

$$r_{m-2} = r_{m-1} q_m + (1?)$$

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, lowbrow version**. 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,

- $7 \times 2$ was crossed off by $2 \times 7$
- $7 \times 3$ was crossed off by $3 \times 7$
- $7 \times 4$ was crossed off by $2 \times 14$
- $7 \times 5$ was crossed off by $5 \times 7$.

The next thing to cross off is then $7 \times 7$ 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

$$N = 4p_1 p_2 \cdots p_n - 1$$

Notice that he began by assuming that $p_1 p_2 \cdots p_n$ 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 $\infty$ 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

$$\begin{aligned} aa' &= bb' \\ aa' &= (aq+r)b' \\ a(a'-qb') &= rb' \end{aligned}$$

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

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

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 $a < b \rightarrow b = aq + r$

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

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 $b < a \rightarrow b = a - \Delta$

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

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 $a|c$.

$$a|b \rightarrow b = am$$
$$b|c \rightarrow c = bn = amn$$
$$c = a(mn) \rightarrow a|c$$

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

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

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

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

The other way

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

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

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

**Problem 1.11 (b)** Fun facts! The two numbers are actually the first 27 digits of $\pi$ 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

$$b^n = a^n m$$
$$m = \left(\frac{b}{a}\right)^n$$

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 $N = 2 \to 11 = 4\cdot 2 + 3$. 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

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

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

$$n = a + 10b + 100c + \cdots \equiv a + b + c + \cdots \pmod 3$$

Now why does this proof work? It says that $n = (a + b + c) \pmod 3$. The meaning of $\pmod 3$ is that $a = b \pmod 3 \to 3|a - b$ 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, lowvrow version**. 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. Also, $(q + 1)y$ cannot be 0 (mod $p$) because otherwise $v(pv') = p(y + s) + 1 \to p(vv' - (y + s)) = 1 \to p|1$ which is a contradiction.

$(q+1)y$ is generally not the "smallest" inverse of $v$ but we can of course bring it back to be $< p$ by substracting it by $pt \rightarrow v((q+1)y - pt) = p(y + s - tv) + 1 = 1$ 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 $\pm|np|$ with $\pm|n|$ 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 $(2+1) \cdot 4 = 12 \rightarrow 3 \times 12 = 36 = 7 \cdot 5 + 1$.

The last thing to show is that if all there inverses are unique. Say two elements $a$ and $b$ have the same inverse $c$

$$\begin{aligned}ac &\equiv 1 \pmod{p} \\ bc &\equiv 1 \pmod{p} \\ \rightarrow c(a-b) &\equiv 0 \pmod{p}\end{aligned}$$

but since $c$ is not zero (see comment above) then $a = b$. Thus all inverses are unique.

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.*

On the other hand, if $n$ is not prime things can still be salvage (a bit). We remove the elements $a$ of $\mathbb{Z}/n\mathbb{Z}$ that have $\gcd(a, n) \neq 1$. However, even though the surviving elements all have inverses, as we shall see, the set is no longer a field since it is no longer closed under addition. Now, why are the left over terms invertible? Bezout's lemma, *i.e.* for any two numbers $a$ and $n$ and their gcd $d = \gcd(a, n) = 1$

$$am + ny = 1$$

which is also a consequence of the ideals, $a\mathbb{Z} + n\mathbb{Z} = 1\mathbb{Z}$. Therefore, $m$ is the inverse of $a$ and any elements with gcd = 1 w.r.t $n$ will have an inverse as well.

**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

$$x^j \equiv x^i \pmod{n}.$$

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.* $xa = xa' \pmod{n}$ then since $\gcd(x, n) = 1$ according to Proposition 2.1.10 we can divide both sides $\cancel{x}a = \cancel{x}a' \pmod{n}$.

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 $xa = a \pmod{n}$!

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

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

$$ax \equiv 1 \pmod{p}$$

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. Another crucial ingredient is that all inverses are unique such that the number of inverses are the same as the number of residues, *i.e.* we can cover all the numbers in $(p-1)! = 1 \cdot 2 \cdot 3 \ldots p-1$ and therefore pair up a residue with its inverse.

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

$$\begin{aligned} 1 \pmod{n} &\equiv 1 + pm \\ \rightarrow (p-1) \times \{1 \pmod{n}\} &\equiv (p-1)(1+pm) \\ &\equiv -1 + p(pm + 1 - m) \\ (p-1)\{1 \pmod{n}\} &\equiv -1 \pmod{n} \end{aligned}$$

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 $a+1$"

Wilson's theorem can also be stated in a different way stating that there are arbitrarily large gaps between successive primes, *i.e.* for any positive integer $n$ there is a sequence of $n$ consecutive composite integers. The above statement can be proven rather easily (if you know the answer). What we want is a series of consecutive composite integers.

The most composite integer is $n!$ since it has all factors from 1 to $n$. A keen observation

shows that

$$\begin{aligned} 1|(n!+1) \\ 2|(n!+2) \\ 3|(n!+3) \\ \vdots \\ n|(n!+n) \end{aligned}$$

However, we do not want $1|(n!+1)$ since 1 divides anything. We can therefore shifts everything by one

$$\begin{aligned} 2|((n+1)!+2) \\ 3|((n+1)!+3) \\ \vdots \\ n+1|((n+1)!+(n+1)) \end{aligned}$$

where we now have $n$ consecutive composite integers $(n+1)!+2, \ldots, (n+1)!+(n+1)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

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

Multiplication is a bit trickier if $a \equiv b \pmod{n}$ then $ca \equiv cb \pmod{n}$. 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.

**Eq. 2.2.2** $p$ has to be prime otherwise it won't work, *e.g.* $p = 4$, $\varphi(4) = 2$ but $4 - 4/4 = 3$.

**Page 36**. "Note: it is easiest to square 49 by working modulo 4 and 25 and using the Chinese remainder Theorem".

Chinese Remainder Theorem in this case is

$$\begin{aligned} x &\equiv 49^2 \pmod{4} \\ x &\equiv 49^2 \pmod{25} \\ x &\equiv x' \pmod{4 \cdot 25} \end{aligned}$$

$49 \equiv 1 \pmod 4$ and $49 \equiv 24 \pmod{25} = -1 \pmod{25}$, thus

$$\begin{aligned} 1 + t \cdot 4 &\equiv 1 \pmod{25} \\ 4t &= (1-1) \pmod{25} = 0 \pmod{25} \\ t &= 25 \\ \rightarrow x &= 101 = 1 \pmod{4 \cdot 25} \end{aligned}$$

and so $49^2 \equiv 1 \pmod{100}$.

**Proposition 2.2.7**. Note that this proposition only works if $\gcd(m, n) = 1$ otherwise you'll get weird results! Also for **Equation 2.2.2**, $p$ is prime.

**Theorem 2.4.1**. There's a typo in the proof. Instead of "follows from Proposition 2.1.22" it should've followed from Theorem 2.1.20 where $x^{\varphi(n)} \equiv 1 \pmod n$ since for a prime number $n$, $\varphi(n) = n - 1$.

**Section 2.5**. "The structure of of $(\mathbb{Z}/p\mathbb{Z})^*$ ..... this implies that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group".

A cyclic group is a group that can be generated from just one element of the group. The term cyclic here refers to taking powers of a single element. For example for $(\mathbb{Z}/3\mathbb{Z})^* = \{1, 2\}$, 1 can't obviously generate the whole group but 2 can since $2^1 = 2$ and $2^2 = 4 \equiv 1 \pmod 3$.

**Proposition 2.5.3**. Note that this only applies to fields. See the last paragraph in the proof, especially this sentence "since $\beta - \alpha \neq 0$ and $k$ is a field, we have $g(\beta) = 0$.". This is because every element in a field (other than zero) has an inverse such that

$$\begin{aligned} (\beta - \alpha)g(\beta) &= 0 \\ (\beta - \alpha)^{-1}(\beta - \alpha)g(\beta) &= (\beta - \alpha) \cdot 0 \\ g(\beta) &= 0 \end{aligned}$$

**Theorem 2.5.8**. My first question when I saw the proof was that why can't one of the roots of $x^{q_i^{n_i}} - 1$ that is not a root of $x^{q_i^{n_i-1}} - 1$ be a root of say $x^{q_i^{n_i-k}}$ for $1 < k < n_i - 1$? *e.g.* $\alpha$ is a root of $x^{q_i^{n_i}} - 1 = 0$ but it's not a root of $x^{q_i^{n_i-1}} - 1 = 0$ but $\alpha$ can still be a root of $x^{q_i^{n_i-k}} - 1 = 0$, right?

Well, it can't be because $q_i^{n_i-k} | q_i^{n_i-1}$. So since $\alpha^{q_i^{n_i-k}} - 1 = 0 \rightarrow \alpha^{q_i^{n_i-k}} = 1$

$$\begin{aligned} x^{q_i^{n_i-1}} - 1 &= 0 \\ \left(x^{q_i^{n_i-k}}\right)^{q_i^{k-1}} - 1 &= 0 \\ \left(\alpha^{q_i^{n_i-k}}\right)^{q_i^{k-1}} - 1 &= 0 \\ (1)^{q_i^{k-1}} - 1 &= 0 \\ 1 - 1 &= 0 \end{aligned}$$

*i.e.* any roots of $x^{q_i^{n_i-k}} - 1$ are automatically roots of $x^{q_i^{n_i-1}} - 1$ thus a root of $x^{q_i^{n_i}} - 1$ that is not a root of $x^{q_i^{n_i-1}} - 1$ is really a new root!

**Proposition 2.5.12**. An additive order modulo $n$ is the smallest positive $x$ such that $ax \equiv 0 \pmod{n}$.

**Problem 2.1**. Prove that for any positive integer $n$, the set $(\mathbb{Z}/n\mathbb{Z})^*$ under multiplication modulo $n$ is a group.

Remember that $(\mathbb{Z}/n\mathbb{Z})^*$ is the unit of $\mathbb{Z}/n\mathbb{Z}$, *i.e.* any element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is $0 < a < n$ and $\gcd(a, n) = 1$. To show that $(\mathbb{Z}/n\mathbb{Z})^*$ in a group under multiplication $\pmod{n}$ we first need to show that it is closed.

Say we have two elements $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ if their product $(ab) < n$ then we are done because $\gcd(ab, n) = 1$ as $\gcd(a, n) = \gcd(b, n) = 1$. However, if $(ab) > n$ we can proceed as so, first $ab = nq + r$ with $0 < r < n$ ($r$ can't be zero since $n|ab$ otherwise).

We now utilize Bezout's lemma, *i.e.* for $p, q \in \mathbb{Z}$, $d|g \iff ps + qt = g$ where $d = \gcd(p, q)$. We know that $\gcd(ab, n) = 1$ therefore

$$\begin{aligned} (ab)s + nt &= 1 \\ (nq + r)s + nt &= 1 \\ rs + n(t + qs) &= 1 \end{aligned}$$

and by Bezout's lemma $\gcd(r, n) = 1$ and since $0 < r < n$, $r \in (\mathbb{Z}/n\mathbb{Z})^*$. So we have shown that multiplication $\pmod{n}$ is closed.

We now need to show that every element of $(\mathbb{Z}/n\mathbb{Z})^*$ has an inverse. From Bezout's

lemma, for every element $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $as + nt = 1$

$$\begin{aligned} nt &= 1 - as \\ \rightarrow n &\mid 1 - as \\ \rightarrow as &\equiv 1 \pmod{n} \end{aligned}$$

and therefore $s$ in the inverse of $a$ but since $as + nt = 1$ it also means that $\gcd(s, n) = 1$, *i.e.* $s \in (\mathbb{Z}/n\mathbb{Z})^*$. (If $s$ is less than zero or greater than $n$ we can always bring it back within $(0, n)$ by $s = nq' + r' \rightarrow s \equiv r' \pmod{n}$) And so we have an inverse for every element of $(\mathbb{Z}/n\mathbb{Z})^*$.

The other properties of a group can be easily proven:

- $(\mathbb{Z}/n\mathbb{Z})^*$ has an identity element as $1 \in (\mathbb{Z}/n\mathbb{Z})^*$.
- $a, b, c \in (\mathbb{Z}/n\mathbb{Z})^*$ then $(ab)c = a(bc)$. This is obvious since the group action is multiplication $\pmod{n}$.

**Problem 2.4**. Prove that if $a$ and $b$ are integers and $p$ is prime, then $(a+b)^p \equiv a^p + b^p \pmod{p}$. You may assume that the binomial coefficient

$$\frac{p!}{r!(p-r)!}$$

is an integer.

The problem is actually equivalent to show that the binomial coefficient $p!/r!(p-r)!$ is divisible by $p$ if $p$ is prime. The requirement that $p$ is prime is a must otherwise it won't work, *e.g.* $\binom{4}{2} = 6$ and it is not divisible by 4.

To show that $\binom{p}{r}$ is an integer we need to inductively use Pascal identity, $\binom{p}{k} = \binom{p-1}{k-1} + \binom{p-1}{k}$, and the fact that $\binom{p}{0} = \binom{p}{p} = 1$.

But once it is established that $\binom{p}{r}$ is an integer we can proceed swimmingly

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = \frac{p(p-1)\dots(p-r-1)}{r!}$$

Since $\binom{p}{r}$ is an integer it means that $r!|p(p-1)\dots(p-r-1)$ but since $\gcd(r!, p) = 1$ ($p$ is prime) this means that $r!|(p-1)\dots(p-r-1) \rightarrow (p-1)\dots(p-r-1) = (r!)q$ and

therefore

$$\begin{aligned}\binom{p}{r} &= \frac{p(p-1)\dots(p-r-1)}{r!} = p \cdot \frac{(p-1)\dots(p-r-1)}{r!} \\ &= pq\end{aligned}$$

which means that $\binom{p}{q} = 0 \pmod{p}$, provided $\binom{p}{q} > 1$. And this completes the proof.

**Problem 2.5**. (a) Prove that if $x, y$ is a solution to $ax + by = d$, with $d = \gcd(a, b)$, then for all $c \in \mathbb{Z}$,

$$x_0 = x + c \cdot \frac{b}{d}, \qquad y_0 = y - c \cdot \frac{a}{d} \tag{2.6.1}$$

is also a solution to $ax + by = d$.

(b) Find two distinct solutions to $2261x + 1275y = 17$.

(c) Prove that all solutions are of the form (2.6.1) for some $c$.

For (a) we just need to substitute $x_0, y_0$ into $ax + by = d$

$$\begin{aligned}ax_0 + by_0 &= a\left(x + c \cdot \frac{b}{d}\right) + b\left(y - c \cdot \frac{a}{d}\right) \\ &= ax + by + c \cdot \left(\frac{a\cancel{b}}{\cancel{d}} - \frac{b\cancel{a}}{\cancel{d}}\right) \\ &= ax + by \\ &= d\end{aligned}$$

For (b) One set of solutions is $x = 22, y = -39$ and another is $x = 997, y = -1768$.

For (c), say we have another solution $ax' + by' = d$, take their difference w.r.t $ax + by = d$, *i.e.*

$$\begin{aligned}ax' + by' - ax + by &= a(x' - x) + b(y' - y) \\ 0 &= a(x' - x) + b(y' - y) \\ \rightarrow a(x' - x) &= b(y - y') \\ \cancel{d}a'(x' - x) &= \cancel{d}b'(y - y')\end{aligned}$$

which means that $a' | b'(y - y')$ but since $\gcd(a', b') = 1$, $a' | (y - y')$ or in other words $y - y' = a'q$ for some integer $q$. Rearranging $y' = y - a'q$.

Looking the other way, it also means that $b' | a'(x' - x)$ and since $\gcd(b', a') = 1$, $b' | (x' - x)$, which means that $x' - x = b'p$ for some integer $p$.

But we have a constraint for $p$ because

$$a'(x'-x) = b'(y-y'), \quad y-y' = a'q$$
$$a'(b'p) = b'(a'q)$$

that is $p = q$. Therefore, $x' = x + b'q$ and this completes the proof (once me rename $q$ as $c$ and $a', b'$ as $a/d, b/d$ respectively).

**Problem 2.6**. Let $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ be a quadratic polynomial with integer coefficients, for example, $f(x) = x^2 + x + 6$. Formulate a conjecture about when the set

$$\{f(n) : n \in \mathbb{Z} \text{ and } f(n) \text{ is prime}\}$$

is infinite. Give numerical evidence that supports your conjecture.

Well, first $b$ must not be zero because otherwise $f(x) = x^2 + ax = x(x+a) \to x|f(x)$ for which $f(x)$ can only be prime if $x = 1$.

Fine, so $b \neq 0$, but for some $a$ and $b$ we can factor $f(x) = (x + x_1)(x + x_2)$ where $x_1 + x_2 = a$ and $x_1 x_2 = b$. But again, this is bad news, as $f(x)$ would not be prime. To make sure this doesn't happen $b$ must be prime or 1.

Let's take the easier route, $b = 1$ such that $f(x) = x(x+a) + 1$ so as long as $x$ is even we have a chance for $f(x)$ to be prime. And from Wilson's theorem, Proposition 2.1.22, we require that $(x(x+a))! \equiv -1 \pmod{(x(x+a)+1)}$.

Actually there's a way to increase the probability that $x(x+a)+1$ will keep producing prime numbers (intermittently and) indefinitely such that the set we are interested in is infinite.

We can set $a = 0$ such that $f(x) = x^2 + 1$. Why might this work? it is actually related to my version of the generalized Euclid's proof that there are infinitely many prime numbers.

Let's see how this works. Say we scan $x$ from $x = 1$ to infinity and beyond. Everytime $x = p_1 \dots p_n$ for some $n$

$$f(x) = (p_1 \dots p_n)^2 + 1$$

then $f(x)$ either contains a new prime or is itself prime since if it contains $p_j, 1 \leq j \leq n$ then $p_j|1$ which is a contradiction. The only caveat is that $f(x)$ itself might not be prime

which is why this is only a conjecture :) although in that case we can flip $b \to -1$

$$f(x) = (p_1 \dots p_n)^2 - 1$$

since by the same argument the above should also produce new primes indefinitely.

For other choices of $b > 1$ and $b$ is prime we have $f(x) = x(x+a) + b$ and as long as $b \neq 2$ and $x$ is even we have a chance to have $f(x)$ as prime, if $b = 2$ then $x(x+a)$ must be odd. We can also flip the sign of $b$ if things don't work out :)

Another idea is maybe something like an extended Chinese remainder theorem

$$\begin{aligned} x^2 + ax + b &\equiv 0 \pmod{p_1} \\ x^2 + ax + b &\equiv 0 \pmod{p_2} \\ &\vdots \\ x^2 + ax + b &\equiv 0 \pmod{p_n} \end{aligned}$$

Although I don't know how this would work since $x$ is squared.

**Problem 2.7**. Find four complete sets of residues modulo 7, where the $i$th set satisfies the $i$th condition: (1) nonnegative, (2) odd, (3) even, (4) prime.

(1) complete residues, nonnegative $\{0, 1, 2, 3, 4, 5, 6\}$

(2) complete residues, odd, we need to change each even number in (1) into an odd one which can be easily done by adding (or subtracting) 7 such that $\{7, 1, 9, 3, 11, 5, 13\}$

(3) complete residues, even, this time we need to add 7 to the odd ones in (1), $\{0, 8, 2, 10, 4, 12, 6\}$

(4) complete residues, prime, this one is a bit tricky, we need to add 7 until a number becomes prime, $\{7, 29, 2, 3, 11, 5, 13\}$ where $29 = 1 + 7 \cdot 4$.

**Problem 2.8**. Find rules in the spirit of Proposition 2.1.9 for divisibility of an integer by 5, 9, and 11, and prove each of these rules using arithmetic modulo a suitable $n$.

The case for 11 will covered below in Problem 2.9. The the other two cases, denote

$$n = a + b10 + c100 + \dots$$

For the case of 5, this is easy since any number other than 5 will have

$$b10 \equiv c100 \equiv \dots \equiv 0 \pmod{5}$$

since $10^n,\ n > 0 \rightarrow 10^n \equiv 0 \pmod 5$, thus

$$n \equiv a \pmod 5$$

and since $5|n \rightarrow n \equiv 0 \pmod 5$, $a$ has to be either 0 or 5.

For the case of 9

$$\begin{aligned} a + b10 + c100 + \ldots &= a + b + c + \cdots + b9 + c99 + \ldots \\ &\equiv a + b + c + \ldots \pmod 9 \end{aligned}$$

Therefore $a + b + c + \ldots$ must be a multiple of 9.

**Problem 2.9**. (*) (The following problem is from the 1998 Putnam Competition.) Define a sequence of decimal integers $a_n$ as follows: $a_1 = 0,\ a_2 = 1$, and $a_{n+2}$ is obtained by writing the digits of $a_{n+1}$ immediately followed by those of $a_n$. For example, $a_3 = 10,\ a_4 = 101$, and $a_5 = 10110$. Determine the $n$ such that $a_n$ is a multiple of 11, as follows:

(a) Find the smallest integer $n > 1$ such that $a_n$ is divisible by 11.

(b) Prove that $a_n$ is divisible by 11 if and only if $n \equiv 1 \pmod 6$.

First, what is the requirement that a number is a multiple of 11? It's that the sum of the digit multiplied by alternating power of -1 is zero, *i.e.* if the number we're interested in is

$$n = a + b10 + c100 + d1000 + \ldots$$

then a - b + c - d + $\ldots = 0$, why? because

$$\begin{aligned} 10 &= 11 - 1 \\ 100 &= 110 - 10 \\ &= 110 - (11 - 1) \\ &= 110 - 11 + 1 \\ 1000 &= 1100 - 100 \\ &= 1100 - (110 - 11 + 1) \\ &= 1100 - 110 + 11 - 1 \end{aligned}$$

et cetera, thus

$$\begin{aligned} n &= a + b10 + c100 + d1000 + \dots \\ &= a + b(11-1) + c(110 - 11 + 1) + d(1100 - 110 + 11 - 1) + \dots \\ &= a - b + c - d + \dots \pmod{11} \\ 0 &= a - b + c - d + \dots \pmod{11} \end{aligned}$$

the last line is because $11|n \to n = 0 \pmod{11}$, and so the alternate sum of the digits of the number must be zero for the number to be a multiple of 11.

Let's list the first few $a$'s and their digits' alternate sum

- $a_1 = 0 \to 0, \quad 11|a_1$
- $a_2 = 1 \to 1, \quad 11 \nmid a_2$
- $a_3 = 10 \to -1, \quad 11 \nmid a_3$
- $a_4 = 101 \to 2, \quad 11 \nmid a_4$
- $a_5 = 10110 \to 1, \quad 11 \nmid a_5$
- $a_6 = 10110101 \to 1, \quad 11 \nmid a_6$
- $a_7 = 1011010110110 \to 0, \quad 11|a_7$

so the smallest $n > 1$ such that $11|a_n$ is $n = 7$.

The number of digits of $a_i$ is the $i^{\text{th}}$ fibonacci number.

**Problem 2.10**. Find an integer $x$ such that $37x \equiv 1 \pmod{101}$.

We use Euclid's gcd algorithm to find the solution of Bezout's lemma $37x + 101y = 1$

$$\begin{aligned} \underline{101} &= \underline{37} \cdot 2 + \underline{27} & \underline{27} &= \phantom{-}1 \cdot \underline{101} - 2 \cdot \underline{37} \\ \underline{37} &= \underline{27} \cdot 1 + \underline{10} & \underline{10} &= -1 \cdot \underline{101} + 3 \cdot \underline{37} \\ \underline{27} &= \underline{10} \cdot 2 + \underline{7} & \underline{7} &= \phantom{-}3 \cdot \underline{101} - 8 \cdot \underline{37} \\ \underline{10} &= \underline{7} \cdot 1 \ + \underline{3} & \underline{3} &= -4 \cdot \underline{101} + 11 \cdot \underline{37} \\ \underline{7} &= \underline{3} \cdot 2 \ + \underline{1} & \underline{1} &= \phantom{-}11 \cdot \underline{101} - 30 \cdot \underline{37} \end{aligned}$$

Therefore $x = -30$.

**Problem 2.11**. What is the order of 2 modulo 17?

The order of a number is the smallest positive $m$ such that $2^m \equiv 1 \pmod{17}$. We can just try different numbers by brute force but an astute observer will observe that $2^4 = 16 \equiv -1 \pmod{17}$ and $1 = (-1)^2 = (2^4)^2 \equiv 2^8 \pmod{17}$. Thus the order of 2 modulo 17 is 8.

**Problem 2.13**. Find an $x \in \mathbb{Z}$ such that $x \equiv 4 \pmod{17}$ and $x \equiv 3 \pmod{23}$.

We use Theorem 2.2.2 to solve Chinese remainder theorem

$$\begin{aligned} x = -4 + t \cdot 17 &\equiv 3 \pmod{23} \\ 17t &\equiv 7 \pmod{23} \\ t &= 18 \\ \rightarrow x = -4 + 306 &= 302 \end{aligned}$$

to solve the above we first need the inverse of $17 \pmod{23}$ which can be computed by the extended gcd of 17 and 23. Once we find that we just multiply the inverse to both sides. Or you can just try the numbers between $1 \ldots 22$ one at a time :)

**Problem 2.14**. Prove that if $n > 4$ is composite then

$$(n-1)! \equiv 0 \pmod{n}$$

First if $n = 4$, $(n-1)! = 3! = 6$ and 6 is not $0 \pmod{n}$. For the rest, we use our awesomesauce friend the fundamental theorem of arithmetic.

Write $n$ as

$$n = \prod_{i=1}^{M} p_i^{\alpha_i}$$

where each $p_i$ is distinct. We can now pick and choose :) Pick any $p$ you want, say $p_j$. Now, pull out $p_j$ out of $n$ such that $n = p_j n'$.

Now, if $p_j \neq n'$, since $p_j$ and $n'$ are both less than $n$, they are included in $(n-1)!$ (remember that $(n-1)!$ is a product of *all* numbers less than $n$). Thus, since $(n-1)!$ contains $n$ as a factor, $(n-1)! \equiv 0 \pmod{n}$.

When $n' = p_j$, the above argument fails since $(n-1)!$ contains all numbers less than $n$ only *once*. However, it can still be remedied. Let $m = p_j(p_j - 1) = p_j(n' - 1) \neq n$

and since $n' - 1 < n \to m < n$ both $m$ and $p_j$ are both contained as factors in $(n-1)!$ and $p_j n' | (n-1)! \to n | (n-1)!$. The only way it doesn't work is if $n' = 2$ because then $m$ is just $p_j$ which affirms the fact that $n > 4$ for the above assertion to be true. This completes the proof.

**Problem 2.15**. For what values of $n$ is $\varphi(n)$ odd?

Again, here we are going to call upon our awesomesauce friend da fundamental theorem. Recall Proposition 2.2.7 which states that if $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. Next, every number is a (unique) product of primes

$$n = \prod_{i=1}^{M} p_i^{\alpha_i}$$

where each $p_i$ is distinct. Thus

$$\varphi(n) = \prod_{i=1}^{M} \varphi(p_i^{\alpha_i})$$

For all primes $p > 2$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, see Eq. 2.2.2, which is even (since $p$ is odd) while $\varphi(2^\alpha) = 2^{\alpha-1}$ which also means that only when $\alpha = 1$ is $\varphi(2)$ odd.

Therefore, $\varphi(n)$ is only odd if and only if $n = 2$ (and also for $n = 1$ but that one is trivial since the only member of $\mathbb{Z}/1\mathbb{Z}$ and $(\mathbb{Z}/1\mathbb{Z})^*$ is 1 which is also equal to $0 \pmod 1$).

**Problem 2.17**. Seven competitive math students try to share a huge hoard of stolen math books equally between themselves. Unfortunately, six books are left over, and in the fight over them, one math student is expelled. The remaining six math students, still unable to share the math books equally since two are left over, again fight, and another is expelled. When the remaining five share the books, one book is left over, and it is only after yet another math student is expelled that an equal sharing is possible. What is the minimum number of books that allows this to happen?

The above is actually a Chinese remainder problem with the following setting

$$x \equiv 6 \pmod 7$$
$$x \equiv 2 \pmod 6$$
$$x \equiv 1 \pmod 5$$
$$x \equiv 0 \pmod 4$$

We first solve the first 2, using proof of Theorem 2.2.2 $x = 6 + t \cdot 7 \equiv 2 \pmod 6$, $7t \equiv -4 \pmod 6 \equiv 2 \pmod 6$, so $t = 2$ and $x = 6 + 2 \cdot 7 = 20$. This solution is not unique as any other $x' \equiv 20 \pmod{7 \cdot 6}$ is also a solution. We have now reduced the problem to

$$\begin{aligned} x &\equiv 20 \pmod{42} \\ x &\equiv 1 \pmod 5 \\ x &\equiv 0 \pmod 4 \end{aligned}$$

Repeating the process $x = 20 + t \cdot 42 \equiv 1 \pmod 5 \to t \cdot 42 \equiv 1 \pmod 5$ since $5|20$, thus $t = 3$ and so $x = 20 + 3 \cdot 42 = 146$.

The last thing to do is to make it conform to $x \equiv 0 \pmod 4$. This is the trickiest part since now $\gcd(42 \cdot 5, 4) = 2 \neq 1$ and Theorem 2.2.2 needs $\gcd(m, n) = 1$, here $m = 42 \cdot 5 = 210$ and $n = 4$. The situation we have now is

$$\begin{aligned} x &\equiv 146 \pmod{210} \\ x &\equiv 0 \pmod 4 \end{aligned}$$

The solution using Theorem 2.2.2 is

$$\begin{aligned} x = 146 + t \cdot 210 &\equiv 0 \pmod 4 \\ t \cdot 210 &\equiv -146 \pmod 4 \\ 210t &\equiv 2 \pmod 4 \end{aligned}$$

Although $\gcd(42 \cdot 5, 4) = 2 \neq 1$, according to Proposition 2.1.15, since $\gcd(42 \cdot 5, 4) = 2$ divides 2, this equation has a solution $t = 1$ with $x = 356$.

The problem is now making sure that 356 is the smallest solution. In the proof of Theorem 2.2.2, the solution of Chinese remainder theorem is unique up to $\pmod{mn}$ which means that we can always substract $mn$ from the solution to get the smallest one. However, the proof requires $\gcd(m, n) = 1$, here $\gcd(210, 4) = 2$. Let's modify the proof then.

Suppose that $x$ and $y$ solve both congruences. Then $z = xy$ satisfies $z \equiv 0 \pmod m$ and $z \equiv 0 \pmod n$, so $m|z$ and $n|z$. Since $\gcd(n, m) \neq 1$, it follows that $\operatorname{lcm}(n, m)|z$, so $x \equiv y \pmod{\operatorname{lcm}(n, m)}$.

Here $\text{lcm}(210, 4) = 420$ and it is greater than 356, therefore 356 is the smallest solution. Math students are not very bright after all, they should've stolen 356 iPhones instead of math books :)

**Problem 2.18**. Show that if $p$ is a positive integer such that both $p$ and $p^2 + 2$ are prime, then $p = 3$.

I tried to show that the fact that $p$ and $p^2+2$ are prime implies $p = 3$ and it didn't work out too well. The reason it didn't work out well is because the tools we have to show that a number is prime are Wilson's theorem (Proposition 2.1.22) and the pseudoprimality test (Theorem 2.4.1). Both are unwieldy as Wilson involves factorial while pesudoprimality involves all numbers.

A better approach is to flip the statement, *i.e.* if $p \neq 3$ then $p$ is not prime OR $p^2 + 2$ is not prime (we can't have both to be prime) which is the solution given in the book.

However, it is not impossible to be pigheadded and go ahead with a direct deduction from the if clause. An astute observer will notice that $2 = \varphi(3)$ such that

$$p^2 + 2 \Longrightarrow p^{\varphi(3)} + \varphi(3)$$

Note that from Theorem 2.1.20 (Euler's Theorem), $x^{\varphi(p)} \equiv 1 \pmod{p}$ when $\gcd(x, p) = 1$. But since 3 is prime $\gcd(x, 3) = 1$ for any nonzero $x$ other than 3. Therefore, for any $x > 0,\ x \neq 3$

$$\begin{aligned} x^{\varphi(3)} + \varphi(3) &\equiv (1 + 3 - 1) \pmod{3} \\ &\equiv 0 \pmod{3} \\ x^{\varphi(3)} + \varphi(3) &= 3n \end{aligned}$$

Since $x^{\varphi(3)} + \varphi(3)$ is prime, $n = 1$ is a must. But then $x = 1$ is the only solution and it is not prime. Therefore $x = 3$. Note that we did not even assume that 3 meets the criterion, we just show that if there's only viable candidate, it has to be 3 :)

The problem can then be generalized, if $x, p$ are prime and $x^{n\varphi(p)} + \varphi(p),\ n > 0$ is also prime, then $x = p$. The proof of this more general statement is the same as above. Since for $x \neq p$, $x^{n\varphi(p)} = 1 \pmod{p}$ and $\varphi(p) = p - 1$, $x^{n\varphi(p)} + \varphi(p) = 0 \pmod{p}$ and $x = 1$, a contradiction, therefore $x = p$.

Initially, I tried generalizing this into, $p$ and $p^2+(p-1)$, *e.g.* $p=5$ with $p^2+(5-1)=29$ where both are primes. However, for $p=7$, $p^2+6=55$ is not prime. The problem is that $5^2+6=31,\ 19^2+6=367$ are also prime.

**Problem 2.19**. Let $\varphi : N \to N$ be the Euler $\varphi$ function.

(a) Find all natural numbers $n$ such that $\varphi(n)=1$.

(b) Do there exist natural numbers $m$ and $n$ such that $\varphi(mn) \neq \varphi(m)\cdot\varphi(n)$?

(a) From problem 2.15 we know that $\varphi(n)=1$ only for $n=1,2$.

(b) As long as $\gcd(m,n) \neq 1$, $\varphi(mn) \neq \varphi(m)\cdot\varphi(n)$, as shown by the derivations leading to Proposition 2.2.7, *e.g.* $m=2, n=4$, $\varphi(2\cdot 4)=4$ while $\varphi(2)=1$ and $\varphi(4)=2,\ \varphi(2)\cdot\varphi(4)=2\neq\varphi(2\cdot 4)=4$.

**Problem 2.20**. Find a formula for $\varphi(n)$ directly in terms of the prime factorization of $n$.

According to the fundamental theorem of arithmetic

$$n=\prod_{i=1}^{N} p_i^{\alpha_i}$$
$$\varphi(n)=\prod_{i=1}^{N}\varphi(p_i^{\alpha_i})$$
$$\varphi(n)=\prod_{i=1}^{N} p_i^{\alpha_i-1}(p_1-1)$$

we can use Proposition 2.2.7 because each prime factors are obviously co-prime to one another (obviously).

**Problem 2.23**. Find all four solutions to the equation

$$x^2-1\equiv 0 \pmod{35}.$$

We know that 1 and $35-1\equiv -1 \pmod{35}$ are roots of $x^2-1\equiv 0 \pmod{35}$ and all roots must have gcd 1 with 35, the other two roots (by the slow way of elimination) are 6 and 29.

**Problem 2.24**. Prove that for any positive integer $n$ the fraction $(12n+1)/(30n+2)$ is in reduced form.

Reduced form means that $\gcd(12n+1, 30n+2) = 1$ (we cannot simplify it further). Say $d = \gcd(12n+1, 30n+2)$

$$\begin{aligned} 12n+1 &= da \\ 30n+3 &= db \\ \rightarrow \frac{12\cancel{n}}{30\cancel{n}} &= \frac{da-1}{db-2} \\ \frac{2}{5} &= \frac{da-1}{db-2} \\ 2db-4 &= 5da-5 \\ d(2b-5a) &= -1 \\ \rightarrow d &\mid -1 \end{aligned}$$

which means that $d = 1$ and the fraction is indeed in reduced form.

**Problem 2.25**. Suppose $a$ and $b$ are positive integers.

(a) Prove that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

(b) Does it matter if 2 is replaced by an arbitrary prime $p$?

(c) What if 2 is replaced by an arbitrary positive integer $n$?

First, assume without loss of generality $b > a,\ b = aq_0 + r_0$ ($b = a$ is obvious), we then use Lemma 1.1.9, $\gcd(a, b) = \gcd(a, b-a)$

$$\begin{aligned} \gcd(2^a - 1, 2^b - 1) &= \gcd(2^a - 1, 2^b - 1 - 2^a + 1) \\ &= \gcd(2^a - 1, 2^a(2^{b-a} - 1)) \end{aligned}$$

But we also know that $\gcd(2^a - 1, 2^a) = 1$ because two consecutive numbers cannot have gcd larger than 1 because

$$\begin{aligned} d|a \qquad d|a+1 \\ d|(a+1-a) \rightarrow d|1 \\ \rightarrow d = 1 \end{aligned}$$

Now since $\gcd(2^a - 1, 2^a) = 1$

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^a - 1, 2^{b-a} - 1)$$

We can then repeat the process $\gcd(2^a-1, 2^{b-a}-1) = \gcd(2^a-1, 2^a(2^{b-a}-1)) = \gcd(2^a-1, 2^{b-2a}-1)$, doing this $q_0 = \lfloor b/a \rfloor$ times we will get

$$\gcd(2^a-1, 2^b-1) = \gcd(2^a-1, 2^{b-aq_0}-1) = \gcd(2^a-1, 2^{r_0}-1)$$

where $r_0 = b \mod a$. Since $0 \leq r_0 < a$, we now swap the role of $a \leftrightarrow r_0$ and do the same thing

$$\begin{aligned}\gcd(2^a-1, 2^{r_0}-1) = \gcd(2^{r_0}-1, 2^a-1) &= \gcd(2^{r_0}-1, 2^a-1-2^{r_0}+1) \\ &= \gcd(2^{r_0}-1, 2^{r_0}(2^{a-r_0}-1)) \\ &= \gcd(2^{r_0}-1, 2^{a-r_0}-1)\end{aligned}$$

We can again repeat this $q_1 = \lfloor a/r_0 \rfloor$ times until we get

$$\gcd(2^{r_0}-1, 2^a-1) = \gcd(2^{r_0}-1, 2^{a-r_0q_1}-1) = \gcd(2^{r_0}-1, 2^{r_1}-1)$$

where $r_1 = a \mod r_0$. We are thus just following the steps of Euclid's gcd algorithm

$$\begin{aligned}\gcd(2^a-1, 2^b-1) &= \gcd(2^a-1, 2^{r_0}-1), \quad b = aq_0 + r_0 \\ \gcd(2^{r_0}-1, 2^a-1) &= \gcd(2^{r_0}-1, 2^{r_1}-1), \quad a = r_0q_1 + r_1 \\ \gcd(2^{r_1}-1, 2^{r_0}-1) &= \gcd(2^{r_1}-1, 2^{r_2}-1), \quad r_0 = r_1q_2 + r_2 \\ &\vdots \\ \gcd(2^{r_{n-1}}-1, 2^{r_{n-2}}-1) &= \gcd(2^{r_{n-1}}-1, 2^d-1), \quad r_{n-2} = r_{n-1}q_n + d \\ \gcd(2^d-1, 2^{r_{n-1}}-1) &= \gcd(2^d-1, 2^{dq_1}-1), \quad r_{n-1} = dq_1\end{aligned}$$

where $d = \gcd(a, b)$. If we repeat the same process on the last equality $q_1$ times

$$\begin{aligned}\gcd(2^d-1, 2^{dq_1}-1) &= \gcd(2^d-1, 2^{dq_1-dq_1}-1) \\ &= \gcd(2^d-1, 2^0-1) = \gcd(2^d-1, 0) \\ &= 2^d-1 = 2^{\gcd(a,b)}-1 \\ \gcd(2^a-1, 2^b-1) &= 2^{\gcd(a,b)}-1\end{aligned}$$

This completes the proof of (a). For (b) and (c), it is obvious from the above derivation that 2 can be substituted with any number.

**Problem 2.26**. For every positive integer $b$, show that there exists a positive integer $n$ such that the polynomial $x^2 - 1 \in (\mathbb{Z}/n\mathbb{Z})[x]$ has at least $b$ roots.

From my first misadventure I gathered the following facts about roots of $x^2 - 1 = 0 \pmod{n}$. First of all, the roots of $x^2 - 1$, denote them $\beta \to \beta^2 - 1 \equiv \pmod{n}$ satisfy $\gcd(\beta, n) = 1$ because otherwise say $d = \gcd(\beta, n) > 1,\ \beta = d\beta',\ n = dn'$

$$\begin{aligned} \beta^2 - 1 &\equiv 0 \pmod{n} \\ \beta^2 - 1 &= 0 + ny \\ \beta^2 - ny &= 1 \\ d(\beta'\beta - n'y') &= 1 \\ \to d &\mid 1 \end{aligned}$$

which is a contradiction. Or you can just use Bezout's lemma, since $\beta^2 \equiv 1 \pmod{n}$

$$\begin{aligned} \beta^2 &= 1 + ny \\ \beta \cdot \beta - n \cdot y &= 1 \end{aligned}$$

therefore $\gcd(\beta, n) = 1$.

Second, since $x^2 - 1 = (x - 1)(x + 1)$, $x = 1$ and $x = -1 = n - 1 \pmod{n}$ are automatically solutions.

Third, once you have two solutions $\alpha, \beta$ (not equal to 1 of course) you can get a third one because

$$\begin{aligned} \alpha^2 \cdot \beta^2 &\equiv 1 \cdot 1 \pmod{n} \\ (\alpha\beta)^2 &\equiv 1 \pmod{n} \end{aligned}$$

and $\alpha\beta$ cannot be equivalent to $\alpha$ or $\beta$ because otherwise

$$\begin{aligned} \alpha\cancel{\beta} &\equiv \cancel{\beta} \pmod{n} \\ \alpha &\equiv 1 \pmod{n} \end{aligned}$$

which is a contradiction (the same argument works for $\alpha\beta \equiv \alpha \pmod{n} \to \beta \equiv 1 \pmod{n}$). In the above argument we can cancel $\alpha$ or $\beta$ from both sides because $\gcd(\alpha, n) =$

$\gcd(\beta, n) = 1$. But you cannot continue this process indefinitely as multiplying the new solution with $\alpha$ or $\beta$ produces

$$\alpha \cdot \alpha\beta = (\alpha^2)\beta \equiv 1 \cdot \beta \pmod{n}$$
$$\alpha^2\beta \equiv \beta \pmod{n}$$

so we are not getting any new solution (the same thing happens if you multiply $\beta$ with the new solution $\alpha\beta$ you'll just get $\alpha$).

Other than the above items, I didn't see any way to prove the number of solutions of a polynomial $\mod n$ (especially when $n$ is not prime).

The way to prove that we can find $n$ such that $x^2 - 1$ has at least $b$ solutions is to use something called the Chinese remainder map. Consider a number, any number $x$, we can represent this number in the following way

$$\begin{aligned} x &\equiv x_1 \pmod{n_1} \\ x &\equiv x_2 \pmod{n_2} \\ &\vdots \\ x &\equiv x_{123} \pmod{n_{123}} \\ &\vdots \\ x &\equiv x_M \pmod{n_M} \end{aligned}$$

where $x_1 = x \mod n_i$, *i.e.* it is just the remainder of $x$, and $x$ is unique up to

$$x \equiv x' \pmod{n_1 \cdot n_2 \ldots n_{123} \ldots n_M}$$

provided that all the $n_i$'s are c relatively prime to one another.

We can now solve this problem. First, find $b$ numbers of distinct primes $p_1, \ldots, p_b$ (we can do this since Euclid has proven that there are infinitely many prime numbers). Now, we multiply all those $b$ prime numbers into $n = p_1 \cdot \cdots \cdot p_b$ and we want to solve $x^2 - 1 \equiv \pmod{n}$.

There is of course at least one solution to $x^2 - 1 \equiv 0 \pmod{n}$, *e.g.* $x = 1$, let's denote this solution $\beta \to \beta^2 - 1 \equiv 0 \pmod{n}$. It is more helpful to denote $\alpha = \beta^2$, therefore if

we represent $\alpha$ using Chinese remainder map

$$\begin{aligned}\alpha_i &\equiv \beta_i^2 \pmod{p_i} \\ &\equiv (\pm\beta_i)^2 \pmod{p_i}\end{aligned}$$

since $(-\beta_i)^2 = (+\beta_i)^2$. We can thus choose whether we want to include the minus sign of **each** $\beta_i$ and presto we have $2^b$ distinct $\beta$'s, *i.e.* $2^b$ distinct roots of $x^2 - 1$. The only trick here is that $p_i > 2$ because $\mathbb{Z}/2\mathbb{Z}$ only has 1 "element" so to say, *i.e.* $-1 \equiv +1 \pmod 2$, thus $\pm\beta_i = \beta$, altering the minus sign doesn't produce a new solution. Let's see this with an example.

Say $b = 2$, $p_1 = 2,\ p_2 = 3$, we now want to solve $x^2 - 1 \equiv 0 \pmod 6$. We know that 1 (mod 6) is a solution, *i.e.* $\alpha = 1$, which means that

$$\begin{aligned}\alpha &\equiv 1 \pmod 2, \quad \alpha_1 = 1 \\ \alpha &\equiv 1 \pmod 3, \quad \alpha_2 = 1 \\ \alpha_1 &\equiv (\pm 1)^2 \pmod 2 \\ \alpha_2 &\equiv (\pm 1)^2 \pmod 3\end{aligned}$$

We now have $2^2 = 4$ choices for $\beta = (\beta_1, \beta_2) = (+1, +1),\ (-1, +1),\ (+1, -1),\ (-1, -1)$

$$\begin{aligned}(+1, +1) &\to \beta = 1 \pmod 6 \\ (-1, +1) &\to \beta = 1 \pmod 6 \\ (+1, -1) &\to \beta = 5 \pmod 6 \\ (-1, -1) &\to \beta = 5 \pmod 6\end{aligned}$$

Oops, we only get *two* distinct solutions, had we started with $p_1 = 3,\ p_2 = 5$ instead, we would have gotten

$$\begin{aligned}\alpha_1 &\equiv (\pm 1)^2 \pmod 3 \\ \alpha_2 &\equiv (\pm 1)^2 \pmod 5 \\ (+1, +1) &\to \beta = 1 \pmod{15} \\ (-1, +1) &\to \beta = 4 \pmod{15} \\ (+1, -1) &\to \beta = 11 \pmod{15} \\ (-1, -1) &\to \beta = 14 \pmod{15}\end{aligned}$$

*four* distinct $\beta$'s, *i.e.* four distinct roots instead of just two.

Our proposed solution above is actually an overkill, we do not need $2^b$ solutions, we just need $b$ solutions, so we only need $\lceil \log_2(b) \rceil$ distinct prime numbers (each $> 2$).

**Problem 2.27**. (a) Prove that there is no primitive root modulo $2^n$ for any $n \geq 3$. (b) (*) Prove that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is generated by $-1$ and 5.

For part(a) we just need to follow the hint. We will need to use induction, but to avoid notational clutter, I'll just show a specific case instead of the generic case in the induction step.

From the hint we know that all elements of $(\mathbb{Z}/8\mathbb{Z})^*$ have multiplicative order of 2. Now take for example $2^4 = 16$, $\varphi(16) = 8$. Assume that the order of $x \in (\mathbb{Z}/16\mathbb{Z})^*$ is 8, *i.e.* $x^8 \equiv 1 \pmod{16}$.

Since the order of $x \pmod{16}$ is 8, $x^4, x^2, x \not\equiv 1 \pmod{16}$. There is something we can say about $x^2$, we know that $x^2 \not\equiv 1 \pmod{8}$, why? because if it is

$$\begin{aligned} x^2 &\equiv 1 \pmod{8} \\ &= 1 + 8n \\ x^4 &= (1+8n)^2 = 1 + 16n + 64n^2 \\ x^4 &\equiv 1 \pmod{16} \end{aligned}$$

which is a contradiction since the order of $x \pmod{16}$ is 8. Since $x \neq 1$, and thanks to Euler's theorem $x^{\varphi(8)} = x^4 \equiv 1 \pmod{8}$, the order of $x \pmod{8}$ is 4. But we know that the order of any $x \in (\mathbb{Z}/8\mathbb{Z})^*$ is 2. Thus the order of $x \pmod{16}$ cannot be 8, whatever $x$ is and hence $(\mathbb{Z}/16\mathbb{Z})^*$ does not have a primitive root. It is then obvious that we can generalize the above argument for a general the inductive step by replacing 8 with $2^n$ and 16 with $2^{n+1}$.

For part (b), there are many things we need to consider. We know that the elements of $(\mathbb{Z}/2^n\mathbb{Z})^*$ are just positive odd numbers $< 2^n$. By a generator the question hints that we can make any element of $(\mathbb{Z}/2^n\mathbb{Z})^*$ by multiplying 5 and $-1$ arbitrary times, *i.e.* the group operation is multiplication $\mod 2^n$ and therefore any element of $(\mathbb{Z}/2^n\mathbb{Z})^*$ can be generated from $(-1)^a 5^b$ for some $a, b$.

A cursory observation shows that there is a pattern on $5^q \mod 2^n$ as shown in the

TABLE I

| $q$ | $5^q$ | $5^q \mod 2^2$ | $5^q \mod 2^3$ | $5^q \mod 2^4$ | $5^q \mod 2^5$ | $5^q \mod 2^6$ |
|---|---|---|---|---|---|---|
| 1 | 5 | **1** | 5 | 5 | 5 | 5 |
| 2 | 25 | **1** | **1** | 9 | 25 | 25 |
| 3 | 125 | **1** | 5 | 13 | 29 | 61 |
| 4 | 625 | **1** | **1** | **1** | 17 | 49 |
| 5 | 3125 | **1** | 5 | 5 | 21 | 53 |
| 6 | 15625 | **1** | **1** | 9 | 9 | 9 |
| 7 | 78125 | **1** | 5 | 13 | 13 | 45 |
| 8 | 390625 | **1** | **1** | **1** | **1** | 33 |
| 9 | 1953125 | **1** | 5 | 5 | 5 | 37 |
| 10 | 9765625 | **1** | **1** | 9 | 25 | 57 |
| 11 | 48828125 | **1** | 5 | 13 | 29 | 29 |
| 12 | 244140625 | **1** | **1** | **1** | 17 | 17 |
| 13 | 1220703125 | **1** | 5 | 5 | 21 | 21 |
| 14 | 6103515625 | **1** | **1** | 9 | 9 | 41 |
| 15 | 30517578125 | **1** | 5 | 13 | 13 | 13 |
| 16 | 152587890625 | **1** | **1** | **1** | **1** | **1** |

following table

There is a compelling pattern from the above table, the order of $5 \mod 2^n$ is $2^{n-2}$. This has a serious implication. Take for example the phase from $2^3 \to 2^4$, $625 \mod 8 = 625 \mod 16 = 1$ while $25 \mod 8 \neq 25 \mod 16$. This is because

$$\begin{aligned} 25 &= 1 + 8u \\ 25 &= 9 + 16v = (1+8) + 2 \cdot 8v \\ &= 1 + 8(2v+1) \\ \to u &= 2v + 1 \end{aligned}$$

while

$$625 = 1 + 8r$$
$$625 = 1 + 16s$$
$$\rightarrow r = 2s$$

This says that at the order $q$ of 5 for a particular $2^n$ the quotient $\lfloor 5^q/2^n \rfloor$ is always odd

$$\frac{5^{2^{n-2}} - 1}{2^n} = \text{odd}$$

But this all makes sense, every number is either even or odd, say

$$5^M \equiv r \pmod{2^N}$$
$$5^M = 2^N L + r$$

if $L$ is odd

$$5^M = 2^N(2U + 1) + r = 2^{N+1}U + (2^N + r)$$
$$5^M \equiv (2^N + r) \pmod{2^{N+1}}$$

if $L$ is even

$$5^M = 2^N(2U) + r = 2^{N+1}U + r$$
$$5^M \equiv r \pmod{2^{N+1}}$$

We are now ready to prove Problem 2.27(b) by utilizing induction. First, we fix $n$ and show that the quotient $\lfloor 5^{qm}/2^n \rfloor$ where $5^{qm} \equiv 1 \pmod{2^n}$ oscillates between odd and even as we ascendingly traverse through different values of $m = 1 \ldots \infty$ with $m = 1$ (which means $q$ is the order of 5 $\mod 2^n$) having an odd quotient. We then use induction to prove that this patterns continues as we increase $n$.

To setup the induction proof we set $n = 2,\ 2^n = 4$. The order of 5 $\mod 4$ is obviously 1 and

$$5 = 2^2 \cdot 1 + 1$$

Thus the quotient $\lfloor 5/2^2 \rfloor = 1$ is odd and we have met the prerequisite of an odd quotient. We now move on to the oscillating pattern. Even though we have fixed $n = 2$, it is constructive to be more generic.

Let's denote the order of $5 \pmod{2^n}$ as $q$ and the quotient $\lfloor 5^q/2^n \rfloor = k$. In the above example, $q = 1$, $n = 2$, and $k = 1$. The thing we need here is that $k$ is odd. To proceed we need a fact about the multiplicative order of a number.

**Proposition 2.27.(b).1** $x^m \equiv 1 \pmod{n}$ if and only if $q|m$ where $q$ is the (multiplicative) order of $x \pmod{n}$.

*Proof.* Say $q \nmid m$, this means that $m = qs + r$ and

$$x^m = x^{qs+r} = (x^q)^s \; x^r$$
$$1 \pmod{n} \equiv 1 \cdot x^r$$

but we know that $0 \leq r < q$ and $q$ is the *smallest* power such that $x^q \equiv 1 \pmod{n}$, thus the only way for it to be consistent is if $r = 0$ which in turn means that $q|m$. So we have proven that if $x^m \equiv 1 \pmod{n}$ then $q|m$.

The other way is obvious, if $q|m$ then $m = qs$, therefore

$$\begin{aligned} x^m &= x^{qs} = (x^q)^s \\ &\equiv 1^s \pmod{n} \\ x^m &\equiv 1 \pmod{n} \end{aligned}$$

This completes our proof.

We now resume our earlier proof. From our proposition above, for $5^y \equiv 1 \pmod{2^n}$ to be true, $y = qm$. We now list $1 \pmod{2^n}$ in ascending power of 5, note that $5^{qm} = (5^q)^m$

$$\begin{array}{lllll} (5^q)^1 & = 1 + A & & & = 1 + 2^n \cdot \text{odd} \\ (5^q)^2 & = 1 + 2A + A^2 & = 1 + A(2 + A) & & = 1 + 2^n \cdot \text{even} \\ (5^q)^3 & = 1 + 3A + 3A^2 + A^3 & = 1 + A(3 + 3A + A^2) & & = 1 + 2^n \cdot \text{odd} \\ (5^q)^4 & = 1 + 4A + 6A^2 + 4A^3 + A^4 & = 1 + A(4 + 6A + 4A^2 + A^3) & & = 1 + 2^n \cdot \text{even} \\ & \vdots & & & \\ (5^q)^m & = 1 + mA + m_1A^2 + \cdots + A^m & = 1 + A(m + m_1A + \cdots + A^m) & & \end{array}$$

where we have denoted $A = 2^n k$ to avoid clutter.

Some points to take note. One, the coefficient of $A^0$ in the bracket $(m+m_1A+\cdots+A^{m_0})$ is always the exponent $m$ as dictated by binomial expansion. Two, each term in bracket has $A$ as a factor and therefore even, except for $m$. Three, the sum of odd and even

is odd and since all the terms in bracket except for $m$ is guaranteed to be even, the even/oddness of the sum of all the terms inside the bracket is determined by $m$. Lastly, since $A = 2^n k$ and $k$ is odd, the even/oddness of the quotient $\lfloor 5^{qm}/2^n \rfloor$ is determined by the even/oddness of the bracket.

Since the sequence of the coefficients of $A^0$ in brackets is just the sequence of natural numbers, the quotient $\lfloor 5^{qm}/2^n \rfloor$ oscillates between odd and even, starting with odd since $k$ is odd. This completes the first part of our proof.

The induction itself involves varying $n$. We have proven above that for the case of $n = 2,\ 2^n = 4$ the order of 5 $\mod 4$ is $2^{n-2} = 1$. There are several intermediate steps we need to establish to complete this proof

- Our inductive assumption is that $\mod 2^n$ has the oscillating pattern as described above and the order $q_n$ of 5 $\mod 2^n$ is $q_n = 2^{n-2}$.

- First, we want to show that if $\mod 2^n$ has the oscillating pattern as described above, $\mod 2^{n+1}$ will also have the same oscillating pattern (with a lower frequency and an odd first quotient), this is to ensure the continual survival of our inductive step.

- We want to show that the order of 5 $\mod 2^{n+1}$ is $2q_n$ where $q_n$ is the order of 5 $\mod 2^n$.

- Combining the above two results, and knowing that $q = 1$ for $n = 2,\ 2^n = 4$, shows that the order of 5 $\mod 2^z$ is $2^{z-2}$.

- Since the above pattern repeats for the inductive step, the conclusion that the order of 5 $\mod 2^z$ is $2^{z-2}$ holds for any$z$. This will only show that $5^z$ covers half of the elements of $(\mathbb{Z}/2^n\mathbb{Z})^*$, remember that $(\mathbb{Z}/2^n\mathbb{Z})^*$ has $2^{n-1}$ elements.

- We then show that $-(5^h)$ generates the other half of $(\mathbb{Z}/2^n\mathbb{Z})^*$ and this would complete our proof that 5 and $-1$ generate $(\mathbb{Z}/2^n\mathbb{Z})^*$.

We now proceed to prove our first item in the preceding list. By assumption we know that up to $n$, the quotient $\lfloor 5^{q_n m_n}/2^n \rfloor$ oscillates between odd and even where $q_n$ is the

order of 5 $\mod 2^n$, also $5^{q_n} = 1 + A_n$ where $A_n = 2^n k_n$. We know that the quotient $k_n = \lfloor 5^{q_n}/2^n \rfloor$ is odd and therefore

$$\begin{aligned} 5^{q_n} &= 2^n k_n + 1 \\ &= 2^n(2l_n + 1) + 1 \\ &= 2^{n+1} l_n + (2^n + 1) \\ 5^{q_n} &\equiv (2^n + 1) \pmod{2^{n+1}} \not\equiv 1 \pmod{2^{n+1}} \end{aligned}$$

Thus the order of 5 $\mod 2^{n+1}$ is not $q_n$. For the even quotients, we can pull out the factor 2 such that

$$\begin{array}{rcl} (5^{q_n})^2 = (5^{2q_n})^1 & = & 1 + 2A_n + A_n^2 = 1 + 2A_n(1 + A_n/2) \\ (5^{q_n})^4 = (5^{2q_n})^2 & = & 1 + 4A_n + 6A_n^2 + 4A_n^3 + A_n^4 = 1 + 2A_n(2 + 3A_n + 2A_n^2 + A_n^3/2) \\ (5^{q_n})^6 = (5^{2q_n})^3 & = & 1 + 6A_n + 15A_n^2 + \cdots + A_n^6 = 1 + 2A_n(3 + 15A_n/2 + \cdots + A_n^5/2) \\ (5^{q_n})^8 = (5^{2q_n})^4 & = & 1 + 8A_n + 28A_n^2 + \cdots + A_n^8 = 1 + 2A_n(4 + 14A_n + \cdots + A_n^8/2) \\ \vdots & & \\ (5^{q_n})^m = (5^{2q_n})^{m/2} & = & 1 + mA_n + m_1 A_n^2 + \cdots + A_n^m = 1 + 2A_n(m/2 + m_1 A_n/2 + \cdots + A_n^m/2) \end{array}$$

since $2A_n = 2^{n+1}k_n$, $5^{2q_n} \equiv 1 \pmod{2^{n+1}}$. Even though we pulled out a factor of 2, $A/2$ is still even since $n > 2$, $2^{n-1} = 2g$ thus just like before the quotients $\lfloor 5^{(2q_n)d}/2^{n+1} \rfloor$ oscillates between odd and even as we traverse $d$ monotonically. The first quotient is $1 + A_n/2$ which is odd plus even which is odd, therefore we met all the criteria of having oscillating quotients with the first on being odd.

But we have jumped the gun by claiming that $2q_n$ is the first one, *i.e.* the order of 5 mod $2^{n+1}$ is $2q_n$. We need to demonstrate this explicitly, which is the next item in the list.

This is actually quite straightforward, we know from Euler's theorem that $x^{\varphi(n)} \equiv 1 \pmod{n}$. Here we have $5^{\varphi(2^{n+1})} \equiv 1 \pmod{2^{n+1}}$, with $\varphi(2^{n+1}) = 2^n$.

Now, we have previously shown that $5^{q_n} \equiv (2^n + 1) \pmod{2^{n+1}} \not\equiv 1 \pmod{2^{n+1}}$, combined with the inductive assumption that $q_n = 2^{n-2}$ this means that $5^{2^m} \not\equiv 1 \pmod{2^{n+1}}$ for $m \leq n - 2$ because otherwise we will infract Proposition 2.27.(b).1.

But from Euler's theorem we know that $q_{n+1}$ has to be $2^u$, and we have shown that $5^{2^m} \not\equiv 1 \pmod{2^{n+1}}$ for $m \leq n - 2$ while showing that $5^{2^{2q_n}} = 5^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$,

thus the order of 5 $\mod 2^{n+1}$ has to be $q_{n+1} = 2q_n = 2^{n-1}$. This completes step 2 of the induction proof.

We have therefore successfully shown that the order of 5 $\mod 2^z$ is $2^{z-2}$ for any$z > 2$. The next major task is to show that $-(5^h)$ generates the other half of $(\mathbb{Z}/2^n\mathbb{Z})^*$.

This turns out to be quite tricky. The point here is that we must make sure that $-(5^a)$ are all distinct from $+(5^b)$ for any positive integer $a, b$. And they all are, this is why. Suppose some $-(5^a) \equiv +(5^b) \pmod{2^n}$

$$\begin{aligned} 5^b &\equiv -(5^a) \pmod{2^n} \\ 5^b + 5^a &\equiv 0 \pmod{2^n} \\ 5^b + 5^a &= 2^n s \end{aligned}$$

A crucial observation we need is that the difference between any two powers of 5 is

$$\begin{aligned} 5^u - 5^v &= (2^n q_u + r_u) - (2^n q_v + r_v) \\ 5^v(5^{u-v} - 1) &= 2^n(q_u - q_v) + (r_u - r_v) \\ 5^v(5-1)(5^{u-v-1} + \cdots + 5 + 1) &= 2^n(q_u - q_v) + (r_u - r_v) \\ 4 \cdot 5^v(5^{u-v-1} + \cdots + 5 + 1) &= 4 \cdot 2^{n-2}(q_u - q_v) + (r_u - r_v) \\ &\to 4 \mid (r_u - r_v) \end{aligned}$$

So the difference between any two $5^a$ and $5^b$, $\mod 2^n$, is a multiple of 4. And we know, thanks to Euler's theorem, that one of those remainders is obviously 1, we can therefore write

$$\begin{aligned} 5^b + 5^a &= 2^n s \\ 2^n q_a + r_a + 2^n q_b + r_b &= 2^n s \\ (1 + 4h_a) + (1 + 4h_b) &= 2^n \Delta, \qquad \Delta = s - q_a - q_b \\ 2(1 + 2(h_a + h_b)) &= 2^n \Delta \\ 1 + 2(h_a + h_b) &= 2^{n-1} \Delta \\ &\to 2 \mid 1 \end{aligned}$$

which is a contradiction and since $-(5^h)$ is just the negative of $5^h$, $-(5^h) \mod 2^n$, $1 \leq hq_n$, are all distinct. So we have shown that indeed $-(5^h)$ generates the other half of $(\mathbb{Z}/2^n\mathbb{Z})^*$.

And we have arrived, plugging in our base case $n = 2, 2^n = 4$ and letting the inductive machinery takes over, we see that we have proven that 5 and $-1$ generate $(\mathbb{Z}/2^n\mathbb{Z})^*$ for $n \geq 2$.

Some interesting point. There's a version of this proof on Victor Soup's book that is way more elegant than mine. Also, 3 and $-1$ also actually generate $(\mathbb{Z}/2^n\mathbb{Z})^*$ (as well, 9, 11,13, and so on). There's a something peculiar about 3 but we will discuss that when we discuss the solution for 2.28 because they are related (by blood?).

**Problem 2.28**. Let $p$ be an odd prime.

(a) (*) Prove that there is a primitive root modulo $p^2$ . (Hint: Use that if $a, b$ have orders $n, m$, with $\gcd(n, m) = 1$, then $ab$ has order $nm$.)

(b) Prove that for any $n$, there is a primitive root modulo $p^n$.

(c) Explicitly find a primitive root modulo 125.

First of all, the hint is quite misleading. Now we know that $\varphi(p^2) = p(p-1)$. In the proof of the existence of a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$, the author uses the fact that we can decompose $(p-1)$ into its prime factors and by using the fact that $x^n - 1$ always have exactly $n$ roots we can construct a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$.

The problem here is that $p^2$ is no longer prime, thus we don't know how many roots $x^n - 1$ has. The best I could do was proof that $x^2 - 1$ has exactly 2 roots (true for $p^n$ as well not just $p^2$)

$$x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p^n}$$
$$(x-1)(x+1) = p^n w$$

Now since $p$ is prime it's either $p|(x-1)$ or $p|(x+1)$ since there are $n$ of them we have $p^a|(x-1)$ or $p^b|(x+1)$ with $a + b = n$.

If $b = 0$ then $x - 1 \equiv 0 \pmod{p^n} \to x \equiv 1 \pmod{p^n}$, the other extreme $a = 0$ means that $x \equiv -1 \pmod{p^n}$. How about the middle ground?

$$x + 1 = p^b u$$
$$x - 1 = p^a s$$
$$(x+1) - (x-1) = 2 = p^a(p^{b-a}u - s)$$
$$\to p \mid 2$$

which is a contradiction unless $p = 2$ (but we are talking about ). Therefore there are only 2 roots $\pm 1$. We also know that $x^{\varphi(p^n)} - 1$ has exactly $\varphi(p^n)$ roots (from Euler's theorem), however

$$x^{\varphi(p^n)} - 1 = (x^2 - 1)(x^{\varphi(p^n)/2} + \cdots + 1)$$

therefore $(x^{\varphi(p^n)/2} + \cdots + 1)$ has exactly $\varphi(p^n) - 2$ roots. Note that $2|\varphi(p^n)$ since $\varphi(p^n) = p^{n-1}(p-1)$ and $p - 1$ is even for $p > 2$.

But that was as far as I could go, there was nothing else I could do about it. The hint actually pertains to finding 2 numbers, one with the order $(p-1)$ while the other with the order of $p^{n-1}$. We need this segregation since as the hint states, the orders must have gcd of 1.

The key now is to find a number inside $(\mathbb{Z}/p^n\mathbb{Z})^*$ that has an order $(p-1)$. This is *very* tricky. The way I proceeded was suppose we have a number $x$ that has an order $a$ mod $m$ and another order $b \mod n$, what can we say about the order of $x \mod (mn)$? Well

$$\begin{aligned} x^y &\equiv 1 \pmod{mn} \\ &= 1 + mn \cdot k \\ &= 1 + m(nk) \\ &= 1 + n(mk) \\ x^y &\equiv 1 \pmod{m} \\ x^y &\equiv 1 \pmod{n} \end{aligned}$$

Therefore, from Proposition 2.27.(b).1, $a|y$ and $b|y$, denote the $z = \text{lcm}(a, b)$, then $y = zc$. Now we apply this to our problem at hand. Here we are interested in $p^2$, therefore $m = p$ and $n = p$ while $a = b = p - 1$, *i.e.* $x$ is a primitive root $\mod p$.

In this case $\text{lcm}(p-1, p-1) = p - 1$, therefore $y = (p-1)c$ and

$$\begin{aligned} x^{(p-1)c} &\equiv 1 \pmod{p^2} \\ (x^c)^{p-1} &\equiv 1 \pmod{p^2} \end{aligned}$$

Therefore $x^c$ has the order $p - 1 \mod p^2$. This can of course be easily generalized to $p^n$.

So we have found the number with order $p-1$, we now need to find a number with order $p^{n-1}$. The proof of this is similar to the solution to problem 2.27.

In our earlier solution we started with a number whose remainder is always 1, that was our base case. The only thing is that we started with $2^2$ instead of $2^1$. Here we want to start with $p^1$ and then proceed with the same inductive process.

Instead of 5 the number we want to choose is $x = 1 + p$

$$
\begin{array}{lll}
(x^q)^1 &= 1 + P & = 1 + p^n \cdot [P] \\
(x^q)^2 &= 1 + 2P + P^2 & = 1 + P(2 + P) \qquad = 1 + p^n \cdot \not[P \\
(x^q)^3 &= 1 + 3P + 3P^2 + P^3 & = 1 + P(3 + P + P^2) \qquad = 1 + p^n \cdot \not[P \\
&\vdots & \\
(x^q)^p &= 1 + pP + p_1P^2 + \cdots + P^p & = 1 + P(p + p_1P + \cdots + P^p) \qquad = 1 + p^n \cdot [P] \\
&\vdots & \\
(x^q)^{pm} &= 1 + pmP + m_1P^2 + \cdots + P^{pm} & = 1 + P(pm + m_1P + \cdots + P^{pm}) \qquad = 1 + p^n \cdot [P]
\end{array}
$$

Some explanation is in order here. First the symbol $[P]$ means divisible by $p$ while $\not[P$ means indivisible by $p$.

So it is very much like problem 2.27, the sum of the terms in bracket is either divisible by $p$ or not divisible by $p$. Since $p = 2$ in problem 2.27, we characterized them even and odd. Here we can see that it oscillates when we hit an exponent that is divisible by $p$, but since $p$ was just 2 in problem 2.27, it oscillated every other step.

Since $P = p^n k$ the sum of the terms in bracket is divisible by $p$ only if the coefficient of $P^0$ is divisible by $p$, this is true because $p$ is prime. And since $P = p^n k$ with $p \nmid k$, the quotient is divisible by $p$ only if the bracket is.

The base case here is simpler, $n = 1,\ p^n = p$, such that $P = p \cdot 1$, $k = 1$ and therefore not divisible by $p$. Thus we have shown that the base case meets all the criteria with the order of $1 + p$ is just $p^{n-1} = p^0 = 1$.

We now proceed to the inductive step and it is very similar to problem 2.27 by just

replacing 2 with $p$

$$\begin{aligned}
(x^{q_n})^p &= (x^{pq_n})^1 &&= 1 + pP_n + \cdots + P_n^p &&= 1 + pP_n(1 + \ldots + P_n^p/p) \\
(x^{q_n})^{2p} &= (x^{pq_n})^2 &&= 1 + 2pP_n + \cdots + P_n^{2p} &&= 1 + pP_n(2 + \cdots + P_n^{2p}/p) \\
&\vdots \\
(x^{q_n})^{pp} &= (x^{pq_n})^p &&= 1 + ppP_n + \cdots + P_n^{pp} &&= 1 + pP_n(p + \cdots + P_n^{pp}/p) \\
&\vdots \\
(x^{q_n})^{ppm} &= (x^{pq_n})^{pm} &&= 1 + ppmP_n + \cdots + P_n^{ppm} &&= 1 + pP_n(mp + \cdots + P_n^{ppm}/p)
\end{aligned}$$

We see that again we have the oscillation every time the exponent of $x^{pq_n}$ hits a multiple of $p$. We also know that

$$(x^{q_n})^w \not\equiv 1 \pmod{p^{n+1}}, \quad p \nmid w$$

This is because

$$\begin{aligned}
(x^{q_n})^w &= 1 + p^n \not{R} \\
&= 1 + p^n(ps + t), \qquad 1 \le t < p \\
&= (1 + t) + p^{n+1}s \\
(x^{q_n})^w &\equiv (1 + t) \pmod{p^{n+1}}
\end{aligned}$$

The next argument is similar to the one in Problem 2.27 but more complicated. We know that $q_n = p^{n-1}$ and $\varphi(p^{n+1}) = p^n(p-1)$.

We have shown that $(x^{q_n})^1 = x^{p^{n-1}} \not\equiv 1 \pmod{p^{n+1}}$ and by Proposition 2.27.(b).1 this means that $x^{p^m} \not\equiv 1 \pmod{p^{n+1}}$ for all $0 < m < n-1$.

But now we need to take care of the cases for $x^{p^m h}$ where $h|(p-1)$, $0 < m < n-1$. First

$$\begin{aligned}
x^{p^{n-1}(p-1)} &= x^{p^n - p^{n-1}} = x^{p^n} x^{-p^{n-1}} \\
&\equiv (1 \pmod{p^{n+1}})((1+t)^{-1} \pmod{p^{n+1}}), \quad 0 < t < p \\
x^{p^{n-1}(p-1)} &\equiv (1+t)^{-1} \pmod{p^{n+1}} \not\equiv 1 \pmod{p^{n+1}}
\end{aligned}$$

where $(1+t)^{-1}$ is the "inverse" of $1+t$ such that $(1+t)^{-1}(1+t) = 1$ and it is obvious that $(1+t)^{-1} \not\equiv 1 \pmod{p^{n+1}}$. The existence of an inverse is guaranteed since $(\mathbb{Z}/p^n\mathbb{Z})^*$ is a group.

With this result it is true that $x^{p^m h} \not\equiv 1 \pmod{p^{n+1}}$, $0 < m < n-1,\ h|(p-1)$ because otherwise it would violate Proposition 2.2.7.(b).1. We have therefore shown that the order of $x$ is $pq_n = p^n \mod p^{n+1}$.

We have shown that for our base case of $x = 1 + p$ and $(\mathbb{Z}/p^1\mathbb{Z})^*$, $q_1 = p^0 = 1$ and the quotients oscillates as shown above, going through the inductive motion we have therefore shown that $1 + p$ has the order $p^{n-1} \mod p^n$.

The primitive root is therefore given by $(1+p)d^c$ where $d$ is a primitive root of $(\mathbb{Z}/p^1\mathbb{Z})^*$ and $c$ is $y/(p-1)$ where $y$ is the order of $d \mod p^n$.

A primitive root of $125 = 5^3$ is therefore given by $(1 + 5)d^c$. First we need to find a primitive root of $(\mathbb{Z}/5\mathbb{Z})^*$ and one of those roots is $d = 3$ (the other is $d = 2$). We now need to find the order of $3 \mod 5^3$ and it is (believe it or not) $y = 100$. Therefore $c = y/(p-1) = 100/4 = 25$.

A primitive root is then $6 \cdot 3^2 5 \equiv 33 \pmod{125}$. Had we chosen $d = 2$ we would get $y = 100$, $c = 25$ with a primitive root of $92 \pmod{125}$. But wait a minute, since the order of 2 and 3 are $100 = 5^2(5-1)$, they themselves are primitive roots, so we have found 4 of them in this exercise :)

Some comments, we could have chosen $x = 1 - p$ instead of $1 + p$.

Why can't we use the above strategy for problem 2.27, the problem lies in the base case

$$(3)^2 \ = \ (3^2)^1 \ = \ 1 + 2A + A^2 \ = \ 1 + 2A(1 + A/2)$$

$3 = 1 + 2$, therefore $A = 2$ and $1 + A/2 = 2$ an even number where it's supposed to be odd. It is indeed a heavy burden to be the first among infinitely many primes :)

We can still show that 3 is a generator but we need to tweak the proof a bit. Hence we start with $5 = 1 + 2^2$ and $\mod 2^2$ instead. However, by the above argument $1 - 2^2$ also works but this is just $-3$ and since the other generator is $-1$, 3 is also a generator.

We want to show that something has the order $p^{n-1}$.

The only way the above fails is if $A = 2$ because

$$\begin{aligned} 1 + 2A(1 + A/2) &= 1 + 2 \cdot 2(1 + 2/2) \\ &= 1 + 2^2(1 + 1) \\ &= 1 + 2^2 \cdot \text{even} \end{aligned}$$

We need $-1$ because 5 only covers half of $(\mathbb{Z}/2^n\mathbb{Z})^*$.

Another fact about $5^q \mod 2^n$, when we increase $q \to q+1$ the remainder of $5^q$ always changes because otherwise

$$\begin{aligned} 5^q &= 2^n q + r \\ 5^{q+1} &= 2^n(5q) + 5r \end{aligned}$$

If $5r < 2^n$ then $5^q \mod 2^n \neq 5^{q+1} \mod 2^n$ if $5r > 2^n$, $5r = 2^n + r'$, therefore $5^{q+1} \equiv r' \pmod{2^n}$. If $r = r'$

$$\begin{aligned} 5r &= 2^n + r' = 2^n + r \\ 4r &= 2^n \\ r &= 2^{n-2} \end{aligned}$$

Thus

$$\begin{aligned} 5^q &= 2^n q + r \\ &= 2^n q + 2^{n-2} \\ &= 2^{n-2}(2^2 q + 1) \\ \to 2 &\mid 5^q \end{aligned}$$

which is a contradiction and thus every time we increase $q$ the remainder changes, except for $n = 2$ where $5^q \mod 2^2$ is always 1.