Alternative Proofs and Solutions to Exercises in Elementary Number Theory (Part I)

Stefanus[1]

[1] Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: May 19, 2016)

Abstract

This is a (not so) short study guide (for newcomers to number theory like me) to accompany William Stein's "Elementary Number Theory" book. Here I give alternative proofs to theorems/lemmas/propositions in the book (when possible) and extra explanations as well. I included some interesting findings I discovered by myself that were not mentioned in the book. Lastly, solutions to exercises are provided in as many details as possible in the hope that any TA/student can get help whenever they're stuck. (Part I contains Chapter 1-3 of the book).

Chapter 1

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

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

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, 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.

However, there is another way to prove the fundamental theorem, my way :)

Lowbrow version of proof. Instead of using gcd (greatest common divisor) I'll use lcm (least common multiple). First, I need to show that every common multiple of two numbers is itself a multiple of the least common multiple.

Proof. Assume otherwise, denote the least common multiple of two numbers a and b is denoted L and another common multiple M (larger than L obviously since L is the *least*

common multiple) we assume M is not a multiple of L and $M > L$. Now we do some arithmetic :)

$$M - L = R_0$$

we know that because $a, b|M$ and $a, b|L \longrightarrow a, b|R_0$, which means that R_0 is also a common multiple of a, b. But since L is the *least* common multiple of a and b, $R_0 > L$. We can further deduce that $R_0 > 0$ since $M > L$. We also know that $L \nmid R_0$ because if R_0 is a multiple of L then M must be a multiple of L too.

But this also means that we can repeat the process

$$R_0 - L = R_1$$

with the same conclusion for R_1, it is a common multiple of a, b which is not a multiple of L and $R_1 > L$. We can then repeat it, and repeat it infinitely many times, which becomes *"reductio ad absurdum* since we start with two *finite* numbers M and L. Thus any common multiple of two numbers must be a multiple of their least common multiples.

The above proof can also be done using a more orthodox number theory stuff, *i.e.* the proposition that for $a, b \in \mathbb{Z},\ a > b$ there exist unique q, r such that $a = bq + r$ where $0 \leq r < b$ and $q > 0$. Therefore

$$M = Lq + r$$

but because $a, b|M$ and $a, b|L \longrightarrow a, b|r$ and since $0 \leq r < L$, r is a common multiple of a and b that is smaller than the least common multiple, which is a contradiction.

Now, if a and b were primes it can be shown that $L = ab$. A word of caution, you can't say that since a, b are primes the only factors of ab are $1, a, b$ therefore their lcm must be ab. This is circular reasoning. We want to show that any number can be factorized into a unique set of primes, however, we haven't shown that that is the case yet.

To show that L is ab we need to use the above result. We know that since ab is a common multiple of a and b it has to be a multiple of L

$$ab = Lq$$

but $L = an$ since $a, b|L$ and so

$$\cancel{a}b = \cancel{a}nq$$

$$b = nq$$

since b is prime n, q must be $1, b$, the question is which one is which? n can't be one since then $L = a$ which is a contradiction, therefore $q = 1, n = b$ and thus $L = ab$.

We have therefore shown that the least common multiple of two primes is the product of those two. This combined with the fact that any common multiple is a multiple of the least common multiple are the only ingredients we need to prove the fundamental theorem of arithmetic.

Now, to the fundamental theorem. Suppose we can factor a number N into two different factorization

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

where p_i, q_j are all primes. We will show that $m = n$ (the same number of factors for both sides) and that the p's are equal to the q's.

First, $N = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ means that N is a common multiple of p_1 and q_1 and since they are both primes N must be a multiple of $p_1 q_1$ therefore

$$N = \cancel{p_1} q_1 R_{p_1} = \cancel{p_1} p_2 \dots p_n$$

$$q_1 R_{p_1} = p_2 \dots p_n$$

where R_{p_1} is just some integer. But the above result means that $N_{p_1} = q_1 R_{p_1} = p_2 \dots p_n$ is a common multiple of q_1 and p_2 and since they are both primes N_{p_1} must be a multiple of $p_2 q_1$ therefore

$$N_{p_1} = \cancel{p_2} q_1 R_{p_2} = \cancel{p_2} p_3 \dots p_n$$

$$q_1 R_{p_2} = p_3 \dots p_n$$

We can then repeat the process until $q_1 R_{p_{n-1}} = p_n$, since both q_1 and p_n are prime the only solution is to have $R_{p_{n-1}} = 1$ and $q_1 = p_n$, we can therefore factor them out from the equation

$$p_1 p_2 \dots \cancel{p_n} = \cancel{q_1} q_2 \dots q_m$$

$$\rightarrow p_1 p_2 \dots p_{n-1} = q_2 q_3 \dots q_m$$

We can now repeat the procedure above to get $q_2 = p_{n-1}$ and so on.

Now if $m \neq n$ we will be in trouble sooner or later because one side will be left with just 1

$$p_1 p_2 \dots p_k = 1 \quad \text{if } n > m$$
$$1 = q_j q_{j+1} \dots q_n \quad \text{if } n < m$$

which is again a contradiction since p's and q's are all prime numbers. The only way out is to have $m = n$ (the number of prime factors are the same) but that means p's and q's constitute the same set of prime numbers. We therefore have the result that the prime factors of any number is unique which is the fundamental theorem of arithmetic. As a bonus, our procedure above also demonstrates that the prime factors is unique up to an ordering since we can choose any p and q to begin with. $\mathcal{Q.E.D}$:)

Theorem 1.2.1 (Euclid). *There are infinitely many primes.*

I tried proving this my own way and I couldn't get very far from the original proof. It somehow must contain the product of all primes, no matter how you spin it. Here's the best I could get. My proof utilizes contradictions. If there are only a finite number of primes, say $\{p_1, p_2, \dots, p_N\}$ then any number $> p_N$ will have one of those primes as a factor. However, this generates a few contradictions, they are

1. Choose a number $> p_N$, *e.g.* $n = p_N p_{N-1} \dots p_{i+1} + p_i \dots p_1$, this number clearly does *not* have $p_j, 1 \leq j \leq N$ as a factor otherwise

$$p_j m = p_N p_{N-1} \dots p_{i+1} + p_i \dots p_1$$
$$p_j(m - p_N p_{N-1} \dots p_{i+1}/p_j) = p_i \dots p_1$$
$$\rightarrow p_j \mid p_i \dots p_1$$

   which is a contradiction (in the above example we have assumed that $j > i$, if not we just moved the other term to the left hand side with the same conclusion).

2. Like Euclid, construct $n = p_1 p_2 \dots p_N$, then $n \pm 1$ will have $\gcd(n, n \pm 1) = 1$. However, all three numbers $n-1, n, n+1$ are greater then p_N, moreover n contains all prime numbers as factors and $n \pm 1$ contains at least one of those primes, thus their gcd should not be 1, a contradiction.

3. Again, construct $n = p_1 p_2 \dots p_N$, the Euler's function $\varphi(n)$ defined in chapter 2 counts the number of numbers that have gcd 1 with respect to n. However, since there are only a finite number of primes any number $> p_N$ must have one of those primes as a factor and since n contains all of those primes any number $w > p_N$ will have $\gcd(w, n) \neq 1$. This also applies to n^2, therefore the number of numbers that have gcd 1 w.r.t. to n and n^2 are the same, *i.e.* $\varphi(n) = \varphi(n^2)$. This is a contradiction as φ is multiplicative which is shown in Chapter 2.

Note that the above arguments didn't give you clues on how to produce new primes from old ones, they are merely showing what contradictions result from assuming that there are only finitely many primes.

Alternatively, we can generalize Euclid's proof of $p_1 \dots p_n + 1$ further, resulting in other ways to produce primes from known ones.

The key is to include all previously known primes, if there's a prime we exclude the proof will not succeed. So here we go. Let's take a look of the following

$$S = p_1 + p_2 \dots p_n$$

where $p_1 \dots p_n$ are all the known primes we have. This means that S must contain a new prime as its factor. Otherwise, if p_1 is a factor of S

$$\begin{aligned} S - p_1 = p_2 \dots p_n, \quad S = p_1 S' \\ p_1(S' - 1) = p_2 \dots p_n \\ \rightarrow p_1 \mid p_2 \dots p_n \end{aligned}$$

which is a contradiction as $p_2, p_3, \dots, p_n$ are all primes. The same happens if $p_j | S,\ j \neq 1$, *e.g.*

$$\begin{aligned} S - p_2 \dots p_n = p_1, \quad S = p_{13} S' \\ p_{13}(S' - p_2 \dots p_{12} p_{14} \dots p_n) = p_1 \\ \rightarrow p_{13} \mid p_1 \end{aligned}$$

which is also a contradiction since p_1 is prime. We can generalize this further into something like $S = p_1 \dots p_k + p_{k+1} \dots p_n$ and the proof above still goes through. Basically we

just need to group the known primes we have into 2, create the product for each group and add them. Finally, we can even take this further by raising the primes into arbitrary powers (and setting arbitrary sign for each term)

$$S = \pm \prod_{i=1}^{l} p_i^{\alpha_i} \mp \prod_{j=l+1}^{n} p_j^{\alpha_j}$$

OR

$$S = \pm 1 \mp \prod_{i=1}^{n} p_i^{\alpha_i}$$

The above two arrangements still produce a new prime factor for S following the same argument as before.

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.

Chapter 2

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 $a = b \pmod 3 \rightarrow 3|a - b$ 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, lowbrow 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.

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

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

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 $n|(a-b) \rightarrow n|((a+\Delta)-(b+\Delta)) = n|(a-b)$.

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.

Lowbrow version. Let's start with $\varphi(n = pq)$ where p, q are distinct primes. We want to count the number of numbers between $1, \ldots, pq$ that have gcd $= 1$ with pq.

A straightforward counting approach will work for pq but not for more complicated products like $pqrstvw\ldots$ LOL

An easier way to do it is to start this way. Say we have $n = n'q$ where n' is a product of *distinct* primes and we know what $\varphi(n')$ is.

For me it's easier to see the problem this way. First, let's organize the numbers from $1, \ldots, n$ into

$$\underbrace{1, \ldots, n'-1}_{S_1},\ n'\ , \underbrace{n'+1, \ldots, n'+(n'-1)}_{S_2},\ 2n'\ , \ldots, \underbrace{(q-1)n'+1, \ldots, (q-1)n'+(n'-1)}_{S_q},\ n'q$$

Note that different S's are separated by mutiples of n' therefore they are congruent to one another. Because they are congruent, a number that is co-prime to n' in one S is also co-prime to n' in another S', see Lemma 1.1.9 and Lemma 1.1.10.

Now for each set S_i there are $\#(\mathbb{Z}/n'\mathbb{Z})^*$ numbers that have gcd $= 1$ with n' and there are q numbers of S's. We then throw away any number a between $1, \ldots, n$ that have $\gcd(a, n') \neq 1$ and we are left with $m = \varphi(n') \cdot q$ numbers.

Now we would like to throw away numbers that are mutiples of q from $1, \ldots, n$. We need to be careful here, some of them are already thrown away. Any number dq where $\gcd(d, n') \neq 1$ were already thrown away. Therefore only multiples of q with hq where $h < n'$ and $\gcd(h, n') = 1$ are still left. How about $h > n'$, that wouldn't work since then $hq > n$.

How many $h < n'$ and $\gcd(h, n') = 1$ are there? The answer is $\varphi(n')$. Therefore

$$\begin{aligned}\varphi(n) &= \varphi(n')q - \varphi(n') \\ &= \varphi(n')(q-1) \\ \varphi(n) &= \varphi(n')\varphi(q)\end{aligned}$$

Therefore, starting with $n = p$ we can (inductively) show that any product of distinct primes

$$n = \prod_i^N p_i \to \varphi(n) = \prod_i^N \varphi(p_i)$$

Now, what happens if n is not a product of *distinct* primes but instead contains duplicates of primes?

Start with $n = n'q$ and $n' = mq$ and thus $n = mq^2$. We already know $\varphi(n')$ and we want to use this info to calculate $\varphi(n = n'q)$. We again represent the number between $1, \ldots, mq^2$ in the following similar manner

$$\underbrace{1, \ldots, mq}_{S_1}, \ \underbrace{mq+1, \ldots, mq+mq}_{S_2}, \ \ldots \ , \underbrace{mq(q-1)+1, \ldots, mq(q-1)+mq}_{S_q}$$

Just like before each set S is congruent to another as they are separated by multiples of $mq = n'$. Therefore a number that is co-prime to n' in one S is also co-prime to n' in another S, see Lemma 1.1.9 and Lemma 1.1.10.

Now, we remove all numbers in each S that are not co-prime to n' thus leaving only $\varphi(n')$ numbers in each S. By doing so we have also removed all numbers that are not

co-prime to q since $n' = mq$ and we are done. We have $q\varphi(n')$ numbers that are co-prime to $n = mq^2$.

By doing this inductively we have shown that $\varphi(n = ab)$ is multiplicative, $\varphi(ab) = \varphi(a)\varphi(b)$, as long as $\gcd(a, b) = 1$.

Lesson learned. My first attempt was to show this by directly counting the numbers that are co-prime to n. At first glance, there are

$$pq - \frac{pq}{p} - \frac{pq}{q}$$

co-prime numbers, *e.g.* for $n = 3 \cdot 5 = 15$, there are $\frac{15}{3} = 5$ multiples of 3 and $\frac{15}{5} = 3$ multiples of 5. However, we are overcounting by one because then we include $n = 15$ itself twice, once for the multiples of 3 and another for the multiple of 5. Therefore $\varphi(n = pq)$ is

$$\begin{aligned}
\varphi(pq) &= pq - \frac{pq}{p} - \frac{pq}{q} + 1 \\
&= pq - (q + p) + 1 \\
&= (p - 1)(q - 1) \\
\varphi(pq) &= \varphi(p)\varphi(q)
\end{aligned}$$

What if $n = pqr$, well first we remove the usual suspects

$$pqr - \frac{pqr}{p} - \frac{pqr}{q} - \frac{pqr}{r}$$

But then we are overcounting things again. First, when we are throwing away multiples of p we include all multiples of pq as well and there are r of them and multiples of pr and there are q of them, this is what the $-\frac{pqr}{p}$ is for.

But when we are throwing away multiples of q by $-\frac{pqr}{q}$, we are throwing away multiples of pq and multiples of qr. However, multiples of pq are already substracted when we are delaing with mutiples of p, therefore we need to restore $+r$ to $\varphi(pqr)$.

Next, we get rid of multiples of r, but again we are throwing away mutiples of pr that have been counted when dealing with multiples of p, since there are q of them we need to add $+q$ to $\varphi(pqr)$. Lastly we get rid of multiples of qr but these are already accounted for when dealing with multiples of q, since there are p of them we need to restore $+p$ to $\varphi(pqr)$.

However, we have a problem. The one number we need to take note of is pqr itself. Note that we restored multiples of r *twice* by adding $+q$ and $+p$. Hwever, we are again overcounting as each of those restorations recounts pqr so we need to substract 1 from it and

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

The above explanation might be confusing so let's see it in action through an example $\varphi(3 \cdot 5 \cdot 7)$. In this example we start with $3 \cdot 5 \cdot 7 = 105$ numbers. We first get rid of multiples of 3 by substracting $\frac{105}{3} = 35$ numbers from the 105 numbers.

Next we remove multiples of 5 by substracting $\frac{105}{5} = 21$ numbers from the $(105-35) = 70$ numbers we have left. However, the following numbers were already removed by removing multiples of 3, $\{15, 30, 45, 60, 75, 90, 105\}$, they are multiples of $3 \cdot 5$ and there are 7 of them so we need to add back 7, *i.e.* $105 - 35 - 21 + 7$.

Then we remove any multiples of 7 by substracting $\frac{105}{7} = 15$. These 15 numbers are

$$7, 14, \cancel{21}, 28, 35, \cancel{42}, 49, 56, \cancel{63}, 70, 77, \cancel{84}, 91, 98, \cancel{105}$$

However, $\{21, 42, 63, 84, 105\}$ were already removed as part of multiples of $3 \cdot 7$ and there are 5 of them (as shown as crossed out numbers above). Therefore we need to substract $15 - 5$ instead of 15, $105 - 35 - 21 + 7 - (15 - 5) = 105 - 35 - 21 - 15 + 7 + 5$.

Another set of numbers that have already been removed are multiples of $5 \cdot 7$, $\{35, 70, 105\}$ (shown as crossed of numbers below) when we removed multiples of 5, there are 3 of them.

$$7, 14, 28, \cancel{35}, 49, 56, \cancel{70}, 77, 91, 98$$

However, we have already restored the count for 105 when we added back $+5$. So we cannot just add $+3$ we need to add $+3-1$ and the final tally is $105-35-21-15+7+5+3-1$.

This direct counting method gets very complicated once we have more than three distinct primes, thus not tenable as a generic proof. And of course the bijective map

proof given in the book is the most elegant of all but it doesn't mean that it cannot be proven from basic principles :)

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 $2^2 = 4 \equiv 1 \pmod{3}$.

Definition 2.5.1. Primitive root. The thing about primitive root is that it is the generator of the group, *i.e.* say g is a primitive root modulo an odd prime p, the order of g is $\varphi(p) = p - 1$. Therefore, any element $a \in \mathbb{Z}/p\mathbb{Z}$ is

$$a \equiv g^m \pmod{p}$$

The question is now whether we can reverse the statement

$$g \stackrel{?}{\equiv} a^n \pmod{p}$$

The answer is it depends, if a is also a primitive root then yes, otherwise the answer is no because otherwise we can express any other element of $\mathbb{Z}/p\mathbb{Z}$ in terms of a, *i.e.* $b \equiv g^u \pmod{p} \equiv a^{nu} \pmod{p}$.

Inverse Primitive Root

Taking this further, is there an inverse primitive root? *i.e.* a number that can be expressed as a power of *every* other number, except for 1 and 0.

$$d \equiv b_i^{m_i} \pmod{p} \quad \text{for all } b_i \in \mathbb{Z}/p\mathbb{Z}, \quad b_i \neq 0, 1$$

of course, d itself should not be 1. For example for $\mathbb{Z}/5\mathbb{Z}$, 4 is this number as

$$4 \equiv 2^2 \pmod{5}$$
$$4 \equiv 3^2 \pmod{5}$$

For one thing, exponentiating $p-1$ only gets you $p-1$ and 1 since $p-1 \equiv -1 \pmod{p}$. Therefore, the only candidate for the inverse primitive root is $p-1$.

If $a^m \equiv -1 \pmod{p}$ then $a^{2m} \equiv 1 \pmod{p}$ and $\gcd(2m, p-1) = d$ where d is the multiplicative order of a modulo p.

Well, let's think about it for a bit. Say a number a satisfies the following

$$\begin{aligned} a^m &\equiv -1 \pmod{p} \\ \rightarrow a^{2m} &\equiv 1 \pmod{p} \end{aligned}$$

where m is the smallest number that the above is true. Therefore, the order of a has to be even. Conversely, if the order of a is odd, then there's no m such that $a^m \equiv -1 \pmod{p}$ because if there is then the order of a would be even, which is a contradiction.

Therefore, there exists an inverse primitive root if and only if every number $1 < a < p-1$ has an even multiplicative order modulo p. Note that, for a primitive root g, $g^{(p-1)/2} \equiv -1 \pmod{p}$ is guaranteed as $p-1$ is even for an odd prime.

From the proof of Theorem 2.5.8, the existence of primitive roots modulo an odd prime p, we know that we can find a number a with $p_i^{n_i}$ as its order where

$$p - 1 = \prod_i^N p_i^{n_i}$$

where p_i is a prime factor of $p-1$. Therefore there is an inverse primitive root modulo p *if and only if* $p - 1 = 2^n$.

Proof. $p - 1 = 2^n$ means that $\varphi(p) = 2^n$. Therefore the order of any $a \in \mathbb{Z}/p\mathbb{Z}$ is a factor of 2^n, see Proposition 2.27.(b).1, *i.e.* every number has an even order. Therefore $a^{d/2} \equiv -1 \pmod{p}$. Why? Note that $x^2 - 1 \equiv 0 \pmod{p}$ only has two solutions $+1$ and -1, $+1$ isn't legit because then that means $a^{d/2} \equiv 1 \pmod{p}$ but the order of a is d, then -1 it is :) As a side note, this also means that the only element of $\mathbb{Z}/p\mathbb{Z}$ that has an order of 2 is $-1 \pmod{p}$. This completes the proof.

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

$$(\beta - \alpha)g(\beta) = 0$$
$$(\beta - \alpha)^{-1}(\beta - \alpha)g(\beta) = (\beta - \alpha) \cdot 0$$
$$g(\beta) = 0$$

Lemma 2.5.7. It is very curious that the whole thing depends *only* on the *orders* of a and b and not on a and b themselves. Think about it, what happens if $ab \equiv 1 \pmod{n}$?, *i.e.* b and a are inverses of one another. In this case the order of (ab) is obviously 1 since $ab \equiv 1 \pmod{n}$. However, it turns out that

Proposition 2.5.7.1 The order of an inverse $b = a^{-1}$ of an element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is the same as the order of a.

Proof. This proposition can be easily proven if $(\mathbb{Z}/n\mathbb{Z})^*$ contains primitive roots. Say g is a primitive root of $(\mathbb{Z}/n\mathbb{Z})^*$ and $a \equiv g^m \pmod{n}$. According to Proposition 2.5.12.4 the inverse of a is given by $a^{-1} = b \equiv g^{\varphi(n)-m} \pmod{n}$.

Furthermore, according to Proposition 2.5.12.3, the order of a is given by $\varphi(n)/\gcd(\varphi(n), m)$ while the order of its inverse, b, is given by $\varphi(n)/\gcd(\varphi(n), \varphi(n)-m)$. However, according to Lemma 1.1.9

$$\gcd(\varphi(n), m) = \gcd(\varphi(n), -m) = \gcd(\varphi(n), -m + \varphi(n))$$

Therefore, the orders of a and b are the same.

What if $(\mathbb{Z}/n\mathbb{Z})^*$ does not contain primitive roots? The proof is quite simple and generic (it applies also for unit groups with primitive roots), it uses the usual trick in quantum mechanics, inserting identity over and over again :)

We know that $ab \equiv 1 \pmod{n}$, say the order of a is d and we multiply take ab to the d^{th} power

$$(ab)^d = \underbrace{bbb\cdots bbb}_{d \text{ numbers of } b\text{'s}} \times \underbrace{aaa\cdots aaa}_{d \text{ numbers of } a\text{'s}}$$
$$1 \pmod{n} \equiv \underbrace{bbb\cdots bbb}_{d \text{ numbers of } b\text{'s}} \times 1 \pmod{n}$$
$$\rightarrow b^d \equiv 1 \pmod{n}$$

note that $ab \equiv 1$ thus $(ab)^d \equiv 1$. So the order of b must be a divisor of d. What if the order of b, say u, is smaller than d, then

$$\begin{aligned}
(ab)^d &= a^d b^d \\
&= a^d (b^u) b^{d-u} \\
1 &\equiv a^d (1) b^{d-u} \pmod{n} \\
&\equiv a^u (ab)^{d-u} \pmod{n} \\
&\equiv a^u (1) \pmod{n} \\
\to 1 \pmod{n} &\equiv a^u
\end{aligned}$$

But this is a contradiction as $u < d$ and the order of a is d. Therefore, the order of $b = a^{-1}$ must be d as well.

Corollary 2.5.7.1.1 If $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $ab \equiv 1 \pmod{n}$ then a and b generate the same subset of $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. Say the the order of a (and that of b) is d, note that

$$\begin{aligned}
a^d &\equiv 1 \pmod{n} \\
(a^{d-1})a &\equiv 1 \pmod{n}
\end{aligned}$$

Therefore a^{d-1} must be an inverse of a and thus $a^{d-1} \equiv b \pmod{n}$. This is guaranteed by the way of Bezout's

$$ab' + ny = 1$$

and according to Problem 2.5 (a) any $b' = b + c \cdot (n/h)$ with $h = \gcd(a, n)$ will satisfy the above Bezout equation. But $h = \gcd(a, n) = 1$ therefore $b' = b + cn \equiv b \pmod{n}$, *i.e.* any inverse of a must be equivalent to $b \pmod{n}$.

Since $a^{d-1} \equiv b \pmod{n}$ by the same reasoning it is also true that $b^{d-1} \equiv a \pmod{n}$ we have

$$b^k \equiv (a^{d-1})^k \qquad a^l \equiv (b^{d-1})^l$$

for any k, l. Thus we can express any power of a in terms of b and any power of b in terms of a and since both a and b have the same order they must generate the same subset of $(\mathbb{Z}/n\mathbb{Z})^*$.

As to Lemma 2.5.7 itself, there's no guarantee what the order of ab is if the $\gcd(r, s) \neq 1$, for example the order of 4 modulo 13 is 6 and the order of 7 modulo 13 is 12, the order of $4 \cdot 7$ modulo 7 is 12, on the other hand the order of 3 modulo 13 is 3 while the order of $4 \cdot 3$ modulo 13 is 2.

Lowbrow proof of Lemma 2.5.7 Say that the order of ab is q where $q|rs$

$$(ab)^q \equiv 1 \pmod{n}$$
$$(a^q)(b^q) \equiv 1 \pmod{n}$$

Therefore a^q and b^q are inverses of one another and according to Proposition 2.5.7.1 above the order of a^q must be the same as that of b^q, let's denote this order y

$$(a^q)^y = a^{qy} \equiv 1 \pmod{n}$$
$$(b^q)^y = b^{qy} \equiv 1 \pmod{n}$$

Since the order of a is r and the order of b is s it must be that

$$r|qy \rightarrow qy = rz$$
$$s|qy \rightarrow qy = sh$$
$$rz = sh$$

Since $\gcd(r, s) = 1$ it means that $s|z,\ z = sz'$ and $r|h,\ h = rh'$, *i.e.*

$$rsz' = srh'$$
$$\rightarrow z' = h'$$

which in turn means that $qy = rsz'$ where z' is any positive integer. But y, as a multiplicative order, is the smallest positive integer such that $(a^q)^y \equiv (b^q)^y \equiv 1 \pmod{n}$. The smallest y would mean that $z' = 1$ and $qy = rs$.

Now we know that, $q|rs$, say that $q = r's',\ r'|r,\ s'|s$ then according to Corollary 2.5.12.3.1 the order of $a^{r's'}$ is $r/\gcd(r, r's') = r/r'$, the same follows for $b^q = b^{r's'}$, its order is given by $s/\gcd(s, r's') = s/s'$

But from our result above qy must be equal to rs here $qy = r's's/s' = r's$ or $qy = r's'r/r' = rs'$ which is a contradict on unless $r' = r$ and $s' = s$ or in other words $q = rs$. This completes the proof.

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.* α 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 α 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 $\alpha^{q_i^{n_i-k}} - 1 = 0 \to \alpha^{q_i^{n_i-k}} = 1$

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

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 $ax \equiv 0 \pmod{n}$. The order we've been talking about in this chapter is multiplicative order.

Lowbrow version of the proof. This whole business about nested φ can be explained without group theory. First we need to show that different primitive roots are related in a certain way.

Properties of Primitive Roots

Proposition 2.5.12.1. Any two primitive roots, $g, \tilde{g}$, modulo n are related through

$$\tilde{g} \equiv g^d \pmod{n}$$

where $\gcd(d, \varphi(n)) = 1$. Moreover, since $\varphi(n)$ is always even for $n > 2$, d is always odd.

Proof. We know that a primitive root, g , is a generator of $\mathbb{Z}/n\mathbb{Z}$. Therefore, if there is another primitive root, $\tilde{g}$, it must be that $\tilde{g} \equiv g^d \pmod{n}$.

Say $\gcd(d, \varphi(n)) = w$ thus

$$\begin{aligned} \tilde{g}^{\varphi(n)/w} &\equiv (g^d)^{\varphi(n)/w} \pmod{n} \\ &\equiv g^{d'\varphi(n)} \pmod{n}, \quad d = d'w \\ \rightarrow \tilde{g}^{\varphi(n)/w} &\equiv 1 \pmod{n} \end{aligned}$$

which is a contradiction as the order of $\tilde{g}$ is $\varphi(n)$. Therefore $\gcd(d, \varphi(n)) = 1$.

Proposition 2.5.12.2. g is a primitive root modulo n if and only if $g^d \pmod{n}$ is also a primitive root modulo n where $\gcd(d, \varphi(n)) = 1$.

Proof. First, suppose that g is a primitive root, now assume that $k = g^d \pmod{n}$ is not a primitive root, therefore

$$k^u = (g^d)^u \equiv 1 \pmod{n}$$

where $u|\varphi(n)$ as shown in Proposition 2.27.(b).1. but this is a contradiction as $ud < \varphi(n)$ and the order of g is $\varphi(n)$.

Now conversely, suppose $g^d \pmod{n}$ **is** a primitive root. We know from Euler's theorem that $g^{\varphi(n)} \equiv 1 \pmod{n}$ and according to Proposition 2.27.(b).1 the order of g must divide $\varphi(n)$, let's denote the order of g as $h \rightarrow g^h \equiv 1 \pmod{n}$. Therefore

$$(g^h)^d = (g^d)^h \equiv 1 \pmod{n}$$

However, the order of g^d is $\varphi(n)$, thus h must be $\varphi(n)$ but in that case since h is the order of g, it has be be a primitive root as well.

Proposition 2.5.12.3. If $(\mathbb{Z}/nZ)^*$ contains a primitive root, g, then the order of an element $a \equiv g^m \pmod{n}$ is given by $\varphi(n)/\gcd(\varphi(n), m)$.

Proof. Say the order of $a \equiv g^m \pmod{n}$ is f therefore

$$a^f \equiv g^{mf} \pmod{n} \equiv 1 \pmod{n}$$

Therefore $\varphi(n)|mf$ since g is a primitive root. If $\gcd(\varphi(n), m) = 1$ then the smallest f is $\varphi(n)$ itself and in that case we have another primitive root. If $h = \gcd(\varphi(n), m) \neq 1$ then the smallest f is obviously $\varphi(n)/h$.

Corollary 2.5.12.3.1. Say a is not a primitive root and $b \equiv a^k \pmod{n}$ and the order of a is d, therefore the order of b is $d/\gcd(d, k)$. The proof follows closely to the

one above by replacing g with a. We can also prove this by expressing a in terms of a primitive root g and using the identity

$$\gcd(a, bc) = \gcd(a, b) \cdot \gcd\left(\frac{a}{\gcd(a, b)}, c\right)$$

Corollary 2.5.12.3.2. If there's a prmitive root, then it means that the only number with order 2 is $g^{\varphi(n)/2} \pmod{n}$. This is because say

$$\varphi(n) = 2_2^n \cdot \prod_i^N p_i^{n_i}$$

where each prime $p > 2$ and they are all distinct. For $\gcd(d, \varphi(n)) = \varphi(n)/2$, d must be

$$d = k \cdot 2^{n_2 - 1} \cdot \prod_i^N p_i^{n_i}$$

but $d < \varphi(n)$ thus $k = 1$ and that's the only value for d.

However, we also know that the order of -1 modulo n is 2, since there's only 1 number with an order of 2 this means that $g^{\varphi(n)/2} \equiv -1 \pmod{n}$. The only exception to this is $\mathbb{Z}/2\mathbb{Z}$ since the only element is $1 \equiv -1 \pmod{2}$ (hence 4-1 has an order of 1 modulo 2).

Note that just because each number in $(\mathbb{Z}/n\mathbb{Z})^*$ can be expressed as $a \equiv g^d \pmod{n}$ with unique d it doesn't mean that the order of a number given by $\varphi(n)/\gcd(\varphi(n), d)$ is unique. This is because two distinct numbers $f \neq h$ can have the same gcd with a third number $\gcd(f, j) = \gcd(h, j)$.

Corollary 2.5.12.3.3. Non-primitive roots of a unit group are generators of a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. Say a is not a primitive root of $(\mathbb{Z}/n\mathbb{Z})^*$ and the order of a is $d < \varphi(n)$. We can list all powers of a

$$a,\ a^2,\ \ldots\ , a^d \equiv 1 \pmod{n}$$

For the above set to be a group each element must have an inverse and of course it does since the inverse of $a^y,\ y < d$ is just a^{d-y}. The identity element is also included in the set by default. Next we need to show that it is closed under multiplication modulo n which it is since $a^z \cdot a^x = a^{x+y} \equiv a^{((a+y) \mod d)} \pmod{n}$. So every non-primitive root is a generator of a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

And following Proposition 2.5.12.1, each a^y where $\gcd(d, y) = 1$ is also a generator of the subgroup.

For example, in $(\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ we have the following

$$1 \rightarrow \{1\} \qquad 2 \rightarrow \{2, 4, 8, 1\} \qquad 4 \rightarrow \{4, 1\} \qquad 7 \rightarrow \{7, 4, 13, 1\}$$
$$8 \rightarrow \{8, 4, 2, 1\} \qquad 11 \rightarrow \{11, 1\} \qquad 13 \rightarrow \{13, 4, 7, 1\} \qquad 14 \rightarrow \{14, 1\}$$

what the above means is that for example 2 generates $\{2, 4, 8, 1\}$ and so on. Thus the collection $\{2, 7, 11, 14\}$ are the generators of $(\mathbb{Z}/15\mathbb{Z})^*$ we can of course make other choices as well like $\{8, 11, 13, 14\}$.

Corollary 2.5.12.3.4. If a unit group $(\mathbb{Z}/n\mathbb{Z})^*$ has primitive roots then for each (not necessarily prime) factor q of $\varphi(n)$ we can find an element $(\mathbb{Z}/n\mathbb{Z})^*$ whose order is q.

Proof. Say q is a factor of $\varphi(n)$ such that $\varphi(n) = qq'$ then according to Proposition 2.5.12.3 $g^{q'}$ will have an order q modulo n.

Corollary 2.5.12.3.5. For any unit group $(\mathbb{Z}/n\mathbb{Z})^*$ we can find an element of the group whose order is a factor of $\varphi(n)$ (with certain restrictions).

Proof. The proof lies in the hands of the Chinese :) We need Chinese remainder theorem for this one. First we decompose $\varphi(n)$ into its primal constituents

$$n = \prod_i^N p_i^{n_i} \qquad\qquad \varphi(n) = \prod_i^N p_i^{n_i - 1}(p_i - 1)$$

where each p_i is a *distinct* prime number. We now utilize Chinese remainder theorem to do work for us. Say we want a number with order $w = \prod_i q_i^{u_i}$ where each w is a factor of $\varphi(n)$. If, w is a factor of just one of the $\varphi(p_i^{n_i})$ we just set up the following Chinese remainder map

$$\begin{aligned}
x &\equiv 1 \pmod{p_1^{n_1}} \\
&\vdots \\
x &\equiv g_i^{\varphi(p_i^{n_i})/w} \pmod{p_i^{n_i}} \\
&\vdots \\
x &\equiv 1 \pmod{p_N^{n_N}}
\end{aligned}$$

Since each p_i is a distinct prime, $\gcd(p_i^{n_i}, p_j^{n_j}) = 1$ for any $i \neq j$ thus Chinese remainder theorem guarantees that we can find such an x. Also from Corollary 2.5.12.3.4, $g^{\varphi(p_i^{n_i})/w}$

(mod $p_i^{n_i}$) is guaranteed to have an order of w modulo $p_i^{n_i}$. While x has an order of 1 modulo $p_{j\neq i}^{n_{j\neq i}}$ since x is just 1 for modulo $p_{j\neq i}^{n_{j\neq i}}$.

We now need to show that x has an order of w modulo n. Thanks to Proposition 2.29.1 which will be proven later, the order of x modulo n, let's denote it o_x, is given by the least common factor of its each order modulo $p_k^{n_k}$

$$o_x = \text{lcm}(1, 1, 1, \ldots, w, \ldots, 1) = w$$

Thus x has an order of w modulo n.

If w has factors from disparates $\varphi(p_i^{n_i})$'s, we need to split w into w_i's such that each w_i is co-prime to one another (this is to make sure the lcm works as intended) and set up the following Chinese remainder map

$$\begin{aligned}
x &\equiv g_1^{\varphi(p_1^{n_1})/w_1} \pmod{p_1^{n_1}} \\
&\vdots \\
x &\equiv g_i^{\varphi(p_i^{n_i})/w_i} \pmod{p_i^{n_i}} \\
&\vdots \\
x &\equiv 1 \pmod{p_N^{n_N}}
\end{aligned}$$

the order of x modulo n will then be given by

$$o_x = \text{lcm}(w_1, w_2, w_3, \ldots, w_i, \ldots, 1) = w_1 \cdot w_2 \cdot w_3 \ldots w_i \cdot 1 \cdot \cdots \cdot 1 = w$$

Since we can always find such an x therefore for every factor w of $\varphi(n)$, we can find a number such that its order modulo n is w.

The only restriction is when one of the p_i's is 2 because $\mathbb{Z}/2^n\mathbb{Z}$ does not have primitive roots for $n \geq 3$. However, $\mathbb{Z}/2^n\mathbb{Z}$ still has $(5, -1)$ as generators (and other numbers as well), with 5 having an order 2^{n-2}. And since every $(p_i - 1)$ is even the order w modulo n we can get is at most $2^{n-2}\tilde{w}$ where $\tilde{w}$ doesn't contain any factor of 2.

Proposition 2.5.12.4. If $(\mathbb{Z}/nZ)^*$ contains a primitive root, g, then the inverse of an element $a \equiv g^m \pmod{n}$ is given by $a^{-1} \equiv g^{\varphi(n)-m} \pmod{n}$.

Proof. Say $b = a^{-1}$, since g is a primitive root, $b \equiv g^l \pmod{n}$ then

$$\begin{aligned} ab &\equiv g^m b \pmod{n} \\ &\equiv g^m g^l \pmod{n} \\ 1 \pmod{n} &\equiv g^{m+l} \pmod{n} \end{aligned}$$

Thus $m + l = y \cdot \varphi(n) \to l = y\varphi(n) - m$ where y is a positive integer. However, if $y > 1$

$$\begin{aligned} g^{y\varphi(n)-m} &= g^{(y-1)\varphi(n)} \cdot g^{\varphi(n)-m} \\ g^{(y-1)\varphi(n)} \cdot g^{\varphi(n)-m} &\equiv 1 \cdot g^{\varphi(n)-m} \pmod{n} \\ \to g^{y\varphi(n)-m} &\equiv g^{\varphi(n)-m} \pmod{n} \end{aligned}$$

Therefore $a^{-1} \equiv g^{\varphi(n)-m} \pmod{n}$.

Note that the case of $\mathbb{Z}/pZ$ where p is prime is unique as $\mathbb{Z}/pZ = (\mathbb{Z}/pZ)^*$. Thus the primitive roots generate both the unit group and the field itself. For others, things are not so rosy and the primitive roots only generate the unit group **NOT** the ring itself.

We can now proceed to prove **Proposition 2.5.12**. Let's list the powers of g, a primitive root modulo n

$$g, g^2, g^3, \ldots, g^{\varphi(n)}$$

According to Proposition 2.5.12.2 any g^d where $\gcd(d, \varphi(n)) = 1$ is a primitive root. Now how many such d's are there? Well, the answer is of course $\varphi(\varphi(n))$ since by definition $\varphi(n)$ counts the number of numbers, a's, greater than 0 that have $\gcd(n, a) = 1$. This completes the proof.

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

$$(ab)s + nt = 1$$
$$(nq + r)s + nt = 1$$
$$rs + n(t + qs) = 1$$

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

$$nt = 1 - as$$
$$\to n \mid 1 - as$$
$$\to as \equiv 1 \pmod n$$

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 $s = nq' + r' \ \to \ s \equiv r' \pmod n$) 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 2.2. Compute the following gcds using Algorithm 1.1.13:

$$\gcd(15, 35) \quad \gcd(247, 299) \quad \gcd(51, 897) \quad \gcd(136, 304)$$

This is nothing but an application of Euclid's algorithm

$$\begin{aligned} \underline{35} &= 2 \cdot \underline{15} + 5 \\ 15 &= 3 \cdot 5 \end{aligned} \qquad \begin{aligned} \underline{299} &= 1 \cdot \underline{247} + 52 \\ 247 &= 4 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 \end{aligned} \qquad \begin{aligned} \underline{897} &= 17 \cdot \underline{51} + 30 \\ 51 &= 1 \cdot 30 + 21 \\ 30 &= 1 \cdot 21 + 9 \\ 21 &= 2 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 \end{aligned} \qquad \begin{aligned} \underline{304} &= 2 \cdot \underline{136} + 32 \\ 136 &= 4 \cdot 32 + 8 \\ 32 &= 4 \cdot 8 \end{aligned}$$

Therefore $\gcd(15, 35) = 5$, $\gcd(247, 299) = 13$, $\gcd(51, 897) = 3$, $\gcd(136, 304) = 8$.

Problem 2.3. Use Algorithm 2.3.7 to find $x, y \in \mathbb{Z}$ such that $2261x + 1275y = 17$.

Algorithm 2.3.7 is

1. [Initialize] Set $x = 1, y = 0, r = 0, s = 1$.
2. [Finished?] If $b = 0$, set $g = a$ and terminate.
3. [Quotient and Remainder] Use Algorithm 1.1.12 to write $a = qb + c$ with $0c < b$.
4. [Shift] Set $(a, b, r, s, x, y) = (b, c, x - qr, y - qs, r, s)$ and go to Step 2.

Here $a = 2261, b = 1275$, $x = 1, y = 0, r = 0, s = 1$, let's crank it through

$$\begin{aligned}
2261 &= 1 \cdot 1275 + 986, \quad q = 1 \\
(a, b, r, s, x, y) &= (1275, 986, 1 - 1 \cdot 0, 0 - 1 \cdot 1, 0, 1) \\
(a, b, r, s, x, y) &= (1275, 986, 1, -1, 0, 1) \\
1275 &= 1 \cdot 986 + 289, \quad q = 1 \\
(a, b, r, s, x, y) &= (986, 289, 0 - 1 \cdot 1, 1 - 1(-1), 1, -1) \\
(a, b, r, s, x, y) &= (986, 289, -1, 2, 1, -1) \\
986 &= 3 \cdot 289 + 119, \quad q = 3 \\
(a, b, r, s, x, y) &= (289, 119, 1 - 3(-1), -1 - 3 \cdot 2, -1, 2) \\
(a, b, r, s, x, y) &= (289, 119, 4, -7, -1, 2) \\
289 &= 2 \cdot 119 + 51, \quad q = 2 \\
(a, b, r, s, x, y) &= (119, 51, -1 - 2 \cdot 4, 2 - 2(-7), 4, -7) \\
(a, b, r, s, x, y) &= (119, 51, -9, 16, 4, -7) \\
119 &= 2 \cdot 51 + 17, \quad q = 2 \\
(a, b, r, s, x, y) &= (51, 17, 4 - 2(-9), -7 - 2 \cdot 16, -9, 16) \\
(a, b, r, s, x, y) &= (51, 17, 22, -39, -9, 16) \\
51 &= 3 \cdot 17, \quad q = 3 \\
(a, b, r, s, x, y) &= (17, 0, -9 - 3 \cdot 22, 16 - 3(-39), 22, -39) \\
(a, b, r, s, x, y) &= (17, 0, -75, 133, 22, -39)
\end{aligned}$$

$b = 0$ so it's done. Therefore $x = 22,\ y = -39$.

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 $c \in \mathbb{Z}$,

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

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.*

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

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

$$\begin{aligned} a'(x' - x) = b'(y - y'), \quad y - y' = a'q \\ a'(b'p) = b'(a'q) \end{aligned}$$

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 ith set satisfies the ith 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 $10^n,\ n > 0 \to 10^n \equiv 0 \pmod{5}$, thus

$$n \equiv a \pmod{5}$$

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

For the case of 9

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

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

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

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.

TABLE I: The first few a's and their properties

Index	String	Alternate Sum	Divisibility by 11
a_1	0	0	$11 \nmid a_1$
a_2	1	1	$11 \nmid a_2$
a_3	10	-1	$11 \nmid a_3$
a_4	101	2	$11 \nmid a_4$
a_5	10110	1	$11 \nmid a_5$
a_6	10110101	1	$11 \nmid a_6$
a_7	1011010110110	0	$11 \mid a_7$
a_8	101101011011010110101	1	$11 \nmid a_8$

Let's list the first few a's and their digits' alternate sum, see table. I so the smallest $n > 1$ such that $11|a_n$ is $n = 7$. Here I have included a_8 as well as we will need this for part (b).

For part (b) we just need to use induction. An important fact about a string of zeros and ones, say we have a random string A

$$\mathrm{A} = 10111010101 \ldots 01010$$

and the alternate sum of the digits of A is *non zero*. We can shift A to the left by any arbitrary digits into

$$\mathrm{A}' = 10111010101 \ldots 01010 \ldots 000000000$$

and the alternate sum of the digits of A$'$ will still be non zero, what we'll get is at most a sign flip of the alternate sum. This is because every time we shift by one digit each 1 will flip its sign but if their sum wasn't zero, it will still not be zero. On the other hand, if the alternate sum of the digits of A is zero, it will remain zero no matter how many times we shift A.

Another important fact is that if we have two strings of ones and zeros, A and B, the alternate sum of the digits of concatenated string AB or BA is zero if and only

TABLE II: The second iteration of the string pattern

Actual Index	Relative Index	String	Alternate Sum
a_7	$\tilde{a}_1$	A	0
a_8	$\tilde{a}_2$	B	1
a_9	$\tilde{a}_3$	B A	-1
a_{10}	$\tilde{a}_4$	B A B	2
a_{11}	$\tilde{a}_5$	B A B B A	1
a_{12}	$\tilde{a}_6$	B A B B A B A B	1
a_{13}	$\tilde{a}_7$	B A B B A B A B B A B B A	0
a_{14}	$\tilde{a}_8$	B A B B A B A B B A B B A B A B B A B A B	1

if the alternate sum of A and the alternate sum of B are independently zero. This is a consequence of the above fact. And since this is true, it is also true if concatenate multiple A's and B's.

One last crucial ingredient, the length of a_7 and a_8, we need both lengths to be odd, since a's are nothing but Fibonacci sequence, the lengths are 1,1,2,3,5,8,13,21, so a_7 is 13 characters long while a_8 is 21 characters long.

We can now start constructing our induction proof. We use as the base case $a_1, a_2, \ldots, a_8$ from part (a). To simplify things we will denote A = a_7 and B = a_8 and we continue the sequence as shown in Table. II. This is where we need both a_7 and a_8 to be odd characters long. This way we can think of A and B as just single digits. Here's why. Say A is **even** characters long with alternate sum of 1 and B odd characters long with alternate sum of 0, A B B A will have an alternate sum of 2 while 1001 ($= - + - +$) should have an alternate sum of 0.

This is because the A on the left (**A**BBA) has been shifted odd + odd + even = even digits, thus its alternate sum stays the same, had A had odd characters, the higher **A**BBA will be shifted by odd + odd + odd = odd digits and hence the alternate sum of ABBA will be zero.

It is now obvious that the pattern repeats. To continue let's denote C = $\tilde{a}_7$ = B A B

TABLE III: The next iteration of the string pattern

Actual Index	Relative Index	String	Alternate Sum
a_{13}	$\tilde{a}_1$	C	0
a_{14}	$\tilde{a}_2$	D	1
a_{15}	$\tilde{a}_3$	D C	-1
a_{16}	$\tilde{a}_4$	D C D	2
a_{17}	$\tilde{a}_5$	D C D D C	1
a_{18}	$\tilde{a}_6$	D C D D C D C D	1
a_{19}	$\tilde{a}_7$	D C D D C D C D D C D D C	0
a_{20}	$\tilde{a}_8$	D C D D C D C D D C D D C D C D D C D C D	1

B A B A B B A B B A with its alternate sum of 0 and D = $\tilde{a}_8$ = B A B B A B A B B A B B A B A B B A B A B with its alternate sum of 1. We now need to make sure that the string length of C and D are both odd. Well, they are guaranteed to be odd because $\tilde{a}_7$ has an odd number of substrings and each substring has an odd number of characters, odd $\times$ odd = odd, the same is true with $\tilde{a}_8$. So we can continue the sequence we will get the exact same sequence as shown in Table. III We can continue this pattern for eternity :) The key observation is the two facts mentioned above that the alternate sum of a string only flips sign if we shift the string and the fact that the string length of a_7 and a_8 is odd. Therefore a_n is divisible by 11 if and only if $n \equiv 1 \pmod 6$.

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 $37x + 101y = 1$

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

Therefore $x = -30 \equiv (101 - 30) \equiv 71 \pmod{101}$.

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 2.12 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 $q \rightarrow q = wm$.

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 $w(u - mn) = 1 \rightarrow w|1$. 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 $v \rightarrow v(q + 1)$ 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 $0 \pmod p$ because otherwise $v(pv')=p(y+s)+1\rightarrow p(vv'-(y+s))=1\rightarrow p|1$ 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 side note, 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.

I solved Problem 2.12 way early in the chapter when it was first mentioned and hence it didn't occur to me that you can just use Bezout's lemma to prove it, but hey, it's still a solution :)

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 (mod 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 (mod 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 $n' - 1 < n \rightarrow m < n$ both m and p_j are both contained as factors in $(n-1)!$ and $p_j n' | (n-1)! \rightarrow n | (n-1)!$. 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 2.16. (a) Prove that φ is multiplicative as follows. Suppose m, n are positive integers and $\gcd(m,n) = 1$. Show that the natural map $\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is an injective homomorphism of rings, hence bijective by counting, then look at unit groups.

(b) Prove conversely that if $\gcd(m,n) > 1$, then the natural map $\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not an isomorphism.

From Lemma 2.2.5 the map is

$$\psi(c) = (c \bmod m, c \bmod n)$$

This problem is slightly different from the proof of Lemma 2.2.5, there we were dealing with units not rings. The proof will follow the proof of Lemma 2.2.5 very closely (basically copy and paste with some modification).

We first show that ψ is injective (means one-to-one but doesn't mean that every element in the target space has a pre-image). If $\psi(c) = \psi(c_0)$, then $m|cc_0$ and $n|cc_0$, so $nm|cc_0$ because $\gcd(n,m) = 1$. Thus $c = c_0$ as elements of $\mathbb{Z}/mn\mathbb{Z}$.

Next we show that ψ is surjective (onto, *i.e.* every element on the target space has a pre-image) that every element of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is of the form $\psi(c)$ for some c.

This is where we deviate from the original proof, Theorem 2.2.2 (Chinese remainder theorem) didn't require $\gcd(a, m) = 1$ or $\gcd(b, n) = 1$. Therefore Theorem 2.2.2 implies that there exists c with $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$ and therefore ψ is surjective. Hence ψ is bijective.

Now since unit groups $(\mathbb{Z}/w\mathbb{Z})^*$ is a subset of $\mathbb{Z}/w\mathbb{Z}$ a bijective map ψ on a subset is still bijective. This completes the proof.

For part (b) we just need to go back to the first part of the proof of (a). If $\psi(c) = \psi(c_0)$, then $m|cc_0$ and $n|cc_0$, but since $\gcd(n, m) > 1$ it is only guaranteed that $\text{lcm}(n, m)|cc_0$. This is not enough to definitely show that the map is no longer injective.

However, we can construct a counter example. Let $d = \gcd(m, n),\ m' = m/d,\ n' = n/d$ and

$$c = x + m'dn'$$
$$c_0 = x$$

To make sure that $c \neq c_0$ we need $x < mn - m'dn'$ such that $c, c_0 < mn$, we also need $x < m, n$. These latter requirements are needed such that $c \bmod m = c_0 \bmod m$ and $c \bmod n = c_0 \bmod n$.

There is a number that satisfy all the above requirements, $x = 1$. It is guaranteed to be $< mn - m'dn'$ because $mn/m'dn' = d,\ mn - m'dn' = (d-1)m'dn'$ and by definition $d = \gcd(m, n) > 1$. Also, $1 \bmod w = 1$ for any $w > 1$. Therefore

$$\begin{aligned} c = 1 + mn/d \quad & c_0 = 1 \\ \psi(c) &= (c \bmod m, c \bmod n) = (1, 1) \\ \psi(c_0) &= (c_0 \bmod m, c_0 \bmod n) = (1, 1) \\ \rightarrow \psi(c) &= \psi(c_0) \end{aligned}$$

Therefore since $c \not\equiv c_0 \pmod{mn}$ the map is not one-to-one.

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

$$\begin{aligned} x &\equiv 6 \pmod 7 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 0 \pmod 4 \end{aligned}$$

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 $x = 20 + t \cdot 42 \equiv 1 \pmod 5 \rightarrow t \cdot 42 \equiv 1 \pmod 5$ 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 $\operatorname{lcm}(210,4)=420$ 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 φ 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 2.21. (a) Prove that if $\varphi : G \to H$ is a group homomorphism, then $\ker(\varphi)$ is a subgroup of G.

(b) Prove that $\ker(\varphi)$ is normal, i.e., if $a \in G$ and $b \in \ker(\varphi)$, then $a^{-1}ba \in \ker(\varphi)$.

Some background info. The kernel of a homomorphism is the set of pre-images of the identity element, loosely the set of $\varphi^{-1}(e)$ where e is identity element in the target space.

Next, a map $\varphi : G \to H$ is a homomorphism if

- $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$
- $\varphi(e) = e$
- $\varphi(g^{-1}) = (\varphi(g))^{-1}$

First order of business is to prove that $\ker(\varphi)$ forms a subgroup, *i.e.* it must meet all the criteria of a group

- Existence of an identity element, since $\varphi(e) = e$, $e \in \ker(\phi)$, remember that we can loosely think of kernel as $\varphi^{-1}(e)$
- Closure of product, since we are talking about kernel, we are just interested in the pre-images of the identity e. Suppose $\varphi(a) = e$ and $\varphi(b) = e$, *i.e.* $a, b \in \ker(\phi)$, since φ is a homomorphism $\varphi(ab) = \varphi(a)\varphi(b) = e \cdot e = e$, therefore $a \cdot b \in \ker(\phi)$
- Existence of inverse. Suppose $a \in \ker(\varphi)$, since φ is a homomorphism $\varphi(a^{-1}) = (\varphi(a))^{-1} = (e)^{-1} = e$. Therefore $a^{-1} \in \ker(\varphi)$.

For part (b) since φ is a homomorphism

$$\begin{aligned}
\varphi(a^{-1}ba) &= \varphi(a^{-1})\varphi(b)\varphi(a), \quad b \in \ker(\varphi) \to \varphi(b) = e \\
&= (\varphi(a))^{-1}\ e\ \varphi(a) \\
&= (\varphi(a))^{-1}\varphi(a))e \\
&= e \cdot e \\
&= e
\end{aligned}$$

Therefore $a^{-1}ba \in \ker(\varphi)$ and $\ker(\varphi)$ is normal.

Problem 2.22. Is the set $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ with binary operation multiplication modulo 5 a group?

Well, it is not because of the element 0, it has no inverse :)

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 α, β (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 α or β 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 $\alpha\beta \equiv \alpha \pmod{n} \rightarrow \beta \equiv 1 \pmod{n}$). In the above argument we can cancel α or β from both sides because $\gcd(\alpha, n) = \gcd(\beta, n) = 1$. But you cannot continue this process indefinitely as multiplying the new solution with α or β produces

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

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

Fourth, $x^2 \equiv 1 \pmod{n}$ means that the order of x is 2 or a factor of 2, *i.e.* the order of x is either 2 or 1. Now, from Proposition 2.5.12.4 if there is a primitive root then the only number with order 2 is $g^{\varphi(n)/2}$ which is $-1 \pmod{n}$, see Corollary 2.5.12.3.2. Thus we must find a number n such that $(\mathbb{Z}/n\mathbb{Z})^*$ does **not** have a primitive root.

I feel that this problem is very tricky I don't know why Stein doesn't mark it as difficult with an asterisk or maybe I just missed something very obvious.

My way to solve the problem (quite crudely) is as follows. First,

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

where $m = x - 1$. We now construct the following, first choose $n = p_1 p_2 p_3 \dots p_N$ where each p is a *distinct* prime > 2 and $N \geq 3$.

Now, $m(m+2) \equiv 0 \pmod{n}$ means that $m(m+2) = ns$. So we just need to spread the factors of n into m and $m+2$.

Next choose one prime factor p_i from n and set $w = p_i$ and then set $v = n/p_i$ (so v contains all other prime factors of n) which also means that $\gcd(w, v) = 1$. Now from

Bezout's lemma we can find two numbers k, l such that

$$wk + vl = 1$$

$$2wk + 2vl = 2$$

Now one of k, l must be negative as w, v are both positive. Say k is positive then

$$2wk = 2 + 2v|l|$$

Now if we multiply

$$\begin{aligned} 2wk \cdot 2v|l| &= 2\cancel{p_i}k \cdot 2\left(\frac{n}{\cancel{p_i}}\right)|l| \\ &= n(4k|l|) \\ 2wk \cdot 2v|l| &\equiv 0 \pmod{n} \end{aligned}$$

so we can set $m = 2v|l| = x - 1,\ m + 2 = 2wk,\ x = 2v|l| + 1$ and $x^2 \equiv 1 \pmod{n}$. If k is negative and l is positive we just set $m = 2w|k|$ instead. Note that the pair $(2wk, 2vl)$corresponds to only **one** value of x.

What happens if we choose another prime factor of n? Say $w' = p_j$ and $v' = n/p_j,\ j \neq i$. Just like before $2w'k' + 2v'l' = 2$. We can show that $2wk \not\equiv 2w'k' \pmod{n}$ because otherwise

$$\begin{aligned} 2w'k' &= 2wk + nt \\ &= p_i\left(2k + \frac{n}{p_i}t\right) \end{aligned}$$

note that $w = p_i$. This means that either $p_i | w'$ or $p_i | k'$ but this is a contradiction since $w' = p_j$ is a different prime from p_i and Bezout tells us that $w'k' + v'l' = 1$ means not only $\gcd(w', v') = 1$ but also $\gcd(k', v') = 1$ and note that $v' = n/p_j = p_i q$ and since $\gcd(k', v') = 1$ this means that $p_i \nmid k'$.

Now what about $2w'k'$ and $2vl$?

$$\begin{aligned} 2w'k' &= 2vl + nt, \quad v = \frac{n}{p_i} = p_j p_o u \\ 2\cancel{p_j}k' &= \cancel{p_j}p_o\left(2ul + \frac{n}{p_j p_o}t\right) \\ 2k' &= p_o\left(2ul + \frac{n}{p_j p_o}t\right) \end{aligned}$$

Since each $p > 2$ it means $p_o | k'$ but just like before $\gcd(k', v') = 1$ and $v' = n/p_j = p_o y$ translates to $p_o \nmid k'$. So this ends up in a contradiction as well.

Next we check $2v'l'$ and $2wk$

$$
\begin{aligned}
2wk &= 2v'l' + nt, \quad v' = \frac{n}{p_j} = p_i p_o u \\
2\cancel{p_i}k &= \cancel{p_i} p_o \left(2ul + \frac{n}{p_i p_o} t \right) \\
2k &= p_o \left(2ul + \frac{n}{p_j p_o} t \right) \\
\rightarrow p_o &\mid k
\end{aligned}
$$

Just like before $wk + vl = 1$ means that $\gcd(k, v) = \gcd(k, p_o y) = 1$ so $p_o | k$ is a contradiction.

The last case is $2v'l'$ and $2vl$

$$
\begin{aligned}
2vl &= 2v'l' + nt \\
\frac{\cancel{n}}{p_i}(2l) &= \frac{\cancel{n}}{p_j}(2l') + \cancel{n}t \\
p_j(2l) &= p_i((2l') + p_j t) \\
\rightarrow p_i &\mid l
\end{aligned}
$$

But $wk + vl = 1$ means that $\gcd(w, l) = \gcd(p_i, l) = 1$, thus $p_i | l$ is a contradiction.

We have thus shown that each p generates a distinct solution to $x^2 - 1 \equiv 0 \pmod{n}$. To get b solutions we just need to set N, the number of prime factors, to $N = b + 3$. This guarantees at least b solutions.

The above might be a bit confusing so let's do some example. Say $n = 3 \cdot 5 \cdot 7$, we have three distinct prime factors. We now go Bezout

$$
\begin{aligned}
3(12) + 5 \cdot 7(-1) &= 1 & 5(-4) + 3 \cdot 7(1) &= 1 & 7(-2) + 3 \cdot 5(1) &= 1 \\
m = 2(5 \cdot 7) &\equiv 70 & m = 2(5 \cdot 4) &\equiv 40 & m = 2(7 \cdot 2) &\equiv 28 \\
x = m + 1 &\equiv 71 & x = m + 1 &\equiv 41 & x = m + 1 &\equiv 29
\end{aligned}
$$

to avoid clutter I shortened $\equiv \pmod{n}$ to just $\equiv$. Thus in the case of $n = 3 \cdot 5 \cdot 7 = 105$ we have found three roots of $x^2 - 1 \equiv 0 \pmod{105}$, they are $29, 41, 71$ we still have ± 1 as roots of course.

A more elegant 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 (as shown by Victor Soup). 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 α 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** β_i and presto we have 2^b distinct β'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 β'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 modulo 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 modulo 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 modulo 8 has to be 4. But we know that the order of any $x \in (\mathbb{Z}/8\mathbb{Z})^*$ is 2. Thus the order of x modulo 16 cannot be 8, whatever x is and $(\mathbb{Z}/16\mathbb{Z})^*$ does not have a primitive root. It is then obvious that we can generalize the above argument for the general 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 modulo 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 Table.IV.

There is a compelling pattern in Table. IV, the order of 5 modulo 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

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

TABLE IV

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**

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 modulo 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 modulo 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 modulo 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 modulo 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.

As a side note, an interesting (or not) fact about 5^q modulo 2^n I found while solving this problem is that when we increase $q \to q + 1$ the remainder always changes. Here's why,

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

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. The above proof also applies when we replace $1 + p$ for 5 and p^n for 2^n where p is an odd prime since the logic is the same.

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 $5^{qm} = (5^q)^m$

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

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

Some points to consider. 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 modulo 4 is $2^{n-2} = 1$. There are several intermediate steps we need to establish to complete this proof

- Our inductive assumption is that $5^w \equiv 1 \pmod{2^n}$ has the oscillating pattern as described above where the order q_n of 5 modulo 2^n is $q_n = 2^{n-2}$ and the first quotient is odd.

- First, we want to show that if $5^w \equiv 1 \pmod{2^n}$ has the oscillating pattern as described above, $5^w \equiv \pmod{2^{n+1}}$ 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 eould like the first quotient to be odd to make sure that it doesn't remain 1 when we increase $n \to n+1$.

- We want to show that the order of 5 modulo 2^{n+1} is $2q_n$ where q_n is the order of 5 modulo 2^n.
- Combining the above two results, and knowing that $q = 1$ for $n = 2,\ 2^n = 4$, shows that the order of 5 modulo 2^z is 2^{z-2}.
- Since the above pattern repeats for the inductive step, the conclusion that the order of 5 modulo 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 modulo 2^n, also $5^{q_n} = 1 + A_n$ where $A_n = 2^n k_n$. By our inductive assumption the first 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 modulo 2^{n+1} is not q_n. For the even quotients, we can pull out the factor 2 such that

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

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 = odd, therefore we met all the criteria of having oscillating quotients with the first one being odd.

But we might have jumped the gun by claiming that $2q_n$ is the order of 5 modulo 2^{n+1}. 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 $5^{2q_n} = 5^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$, thus the order of 5 modulo 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 $+(5^b) \equiv -(5^a) \pmod{2^n}$

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

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

multiple of 4

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

So the difference between any two remainders of 5^a and 5^b, modulo 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. Therefore, since $-(5^h)$ are just the negative of 5^h, $-(5^h) \pmod{2^n}$ with $1 \leq h \leq q_n$ are all distinct from $+(5^b) \pmod{2^n}$. This also means that there are no $-(5^f) \equiv -(5^g) \pmod{2^n}, 1 \leq f, g \leq q_n,\ f \neq g$, because otherwise $(5^f) \equiv (5^g) \pmod{2^n}$ which means that $5^{|f-g|} \equiv 1 \pmod{2^n},\ |f-g| < q_n$, a contradiction since q_n is the order of 5 modulo 2^n. So we have indeed shown that $-(5^h)$ 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 as 11, 13, 19, 21, 29 and so on as we shall see in a bit). 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.

Personally speaking, the hint is quite misleading. 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 prove that $x^2 - 1$ modulo p^2 has exactly 2 roots (true for modulo p^n as well not just modulo 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 an odd p). Therefore there are only 2 roots $x = \pm 1$. 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 any prime $p > 2$.

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 modulo m and another order b modulo n, what can we say about the order of x modulo (mn)? Well, say that y is the order of x modulo mn

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

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 modulo 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 $p-1$ modulo p^2. This can of course be easily generalized to p^n.

So we have found the number with order $p-1$ modulo p^n, we now need to find a number with order p^{n-1} modulo p^n. 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 modulo 2^2 instead of modulo 2^1. Here we want to start with modulo p^1 and then proceed with the same inductive process.

Instead of 5 the number we choose is $x = 1 + p$ which is the most obvious choice. Again, for future use, I use a more generalized notation just like in Problem 2.27 and like Problem 2.27 we start listing the powers of x^q

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

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 quotient is divisible by p only if the coefficient of P^0 is divisible by p, this is true assuming $\gcd(k, p) = 1$. The base case here is $n = 1,\ p^n = p$, such that $P = p \cdot 1,\ k = 1 \rightarrow \gcd(k, p) = 1$ and therefore the quotient is not divisible by p. Thus we have shown that the base case meets all the criteria with the order of $1 + p$ modulo p being $p^{n-1} = p^0 = 1$.

We now proceed to the inductive step very similar to problem 2.27 by just replacing 2 with p. The inductive assumption is that the quotient oscillates between non-divisible and divisible by p and the first quotient is non-divisible by p. From the above discussion, all the quotients that are non divisible by p have $x^{q_n w}$ with $p \nmid w$

$$\begin{aligned}
x^{q_n w} &= 1 + p^n g, \quad p \nmid g \rightarrow g = pq + r,\ 0 < r < p \\
&= 1 + p^n(pq + r) \\
&= (1 + r) + p^{n+1} q \\
x^{q_n w} &\equiv (1 + r) \pmod{p^{n+1}} \not\equiv 1 \pmod{p^{n+1}}
\end{aligned}$$

While for the quotients that are divisible by 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 just like before we have the oscillation of the quotient $\lfloor x^{(pq_n)pm}/p^{n+1} \rfloor$ every time the exponent of (x^{pq_n}) hits a multiple of p. Now we need to show that the order of x modulo p^{n+1} is pq_n. The argument needed is similar to the one in Problem 2.27 but a bit 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 $h|(p-1)$, $0 < m < n-1$. Thanks to Proposition 2.27.(b).1 this ain't so. Because $\gcd(p-1, p) = 1$. You see, if $x^{p^m h} \equiv 1 \pmod{p^{n+1}}$ then by our beloved proposition $p^m h | p^{n+1} \to h | p^v$ but $\gcd(h, p) = \gcd(p-1, p) = 1$ means it ain't so.

We can show it more explicitly

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

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 $x^{p^m h} \not\equiv 1 \pmod{p^{n+1}}$, $0 < m < n-1$, $h|(p-1)$ we have therefore shown that the order of x modulo p^{n+1} is $pq_n = p^n$.

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 with the first one being non-divisible by p, going

through the inductive motion we have therefore shown that $1 + p$ has the order p^{n-1} modulo 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 modulo 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 modulo 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 $1+p$ and everything would just work out the same but in this case we will find another primitive root.

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

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

$3 = 1 + A$, $A = 2$ 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, we just need to start with 2^3 as the base case instead because $3^2 = 1 + 2^3$ since $3^2 = 1 + 2^2 2$ has an even quotient, something we don't want. 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.

Generalized moral of the story. The main points of the proof of Problem 2.28 is to setup a very obvious base case, find a number that has an order $1 = p^{n-1}$, therefore $n = 1$, and has a quotient that is not divisible by p such that when we go from modulo p^n to p^{n+1} the order of x is guaranteed to change, the most obvious choice is then $x = 1+p \equiv 1 \pmod{p}$. But that is not the only choice, a more general choice would be

$$x = 1 \pm |a|p \equiv 1 \pmod{p}$$

where $\gcd(a,p)=1$. This way the order of x is $p^{n-1}=p^0=1$ and its quotient is not divisible by p. Another obvious result is that the quotient oscillates

$$\begin{aligned} x^m &= (1\pm|a|p)^m = 1\pm m|a|p + m_1p^2 + \cdots \pm |a|^m p^m \\ &= 1\pm|a|p\cdot p(m/p + m_1p + \cdots \pm |a|^m p^{m-1}) \end{aligned}$$

as just like discussed previously whether the quotient of x^m is divisible by p or not depends on whether m is divisible by p or not (since $\gcd(a,p)=1$).

However, this strategy is problematic when $p=2$. The case for $p=2$ turns out to be a lot more interesting as we shall soon see. Well for one thing $\mathbb{Z}/2^n\mathbb{Z},\ n\geq 3$ has no primitive roots. Thus we are not looking for something that has an order of 2^{n-1}. Another is the case of $x=3=1+2$ as explained above. Luckily, $x=3$ works for modulo 2^3

$$\begin{aligned} x &= 1+2 \equiv 3 \pmod 8 \\ x^2 &= 1+8 \equiv 1 \pmod 8 \end{aligned}$$

However, it is harder to generalize $x=1+2\rightarrow x=1\pm|a|2$

$$\begin{aligned} x &= 1\pm 2|a| &&\not\equiv 1 \pmod 8 \\ x^2 &= 1\pm 4|a|+4a^2 &&\equiv 1 \pmod 8 \end{aligned}$$

Or in other words we must satisfy the following

$$\begin{aligned} \pm 2a &\neq 8u & \qquad 4a(\pm 1+a) &= 8k \\ a &\neq \mp 4u & a(\pm 1+a) &= 2k \end{aligned}$$

This means that a must be odd. Assume $a=2v+1$ the condition that $x=1\pm 2(2v+1)$ translates to

$$x=\begin{cases} 1+2(2v+1) \rightarrow 2(2v+1)\neq 8u \\ 1-2(2v+1) \rightarrow -4v \neq 8u \end{cases}$$

So if we choose the plus sign we can choose any odd number for a while if we choose the negative sign we must choose $a=2v+1$ with an odd v and that will guarantee that $-4v\not\equiv 1 \pmod 8$.

With this choice

$$x^2=\begin{cases} (1+2(2v+1))^2 = 1+8(2v^2+3v+1) \\ (1-2(2v+1))^2 = 1+8(v+2v^2) \end{cases}$$

We need $2v^2+3v+1$ to be odd, therefore v must be even, while an odd v guarantees that $v+2v^2$ is odd. Therefore,the generalization of $x = 1+2$ is

$$x = \begin{cases} 1+2(4u+1) &= 8u+3 \\ 1-2(4u+3) &= -8u-5 \end{cases}$$

Barring the difficulties we have with $x = 3$, the order we want is 2^{n-2} instead of 2^{n-1}. The easiest choice is to find a number that has the order $1 = 2^{n-2} \rightarrow n = 2$, therefore $x = 1+2^2 \equiv 1 \pmod{2^2}$. Just like before the generalization is then obvious

$$x = 1 \pm |2u+1|2^2 \equiv 1 \pmod{2^2}$$

$2u+1$ guarantees $\gcd(2u+1, 2) = 1$. Now we can see how we can get other generators, if we choose $x = 1+2(4u+1)$ we get $11, 19, 27, 35, 43, 51, 59, \ldots$. And if we choose $x = 1+|a|2^2$ we get $13, 21, 29, 37, 45, 53, 61, \ldots$.

The only thing left to show is that with this choice $+(x^a) \not\equiv -(x^b) \pmod{2^n}$. The proof is not as straightforward as the one for $x = 5$. To start, assume that $+(x^a) \equiv -(x^b) \pmod{2^n}$

$$\begin{aligned} x^a \equiv -(x^b) \pmod{2^n} &= -(x^b) + 2^n G \\ x^a + x^b &= 2^n G \\ x^a(x^{b-a}+1) &= 2^n G \\ \rightarrow x^{b-a} &\equiv -1 \pmod{2^n} \end{aligned}$$

We will limit $0 \leq a, b \leq q$ where $q = 2^{n-2}$ is the order of x modulo 2^n as shown above. This restriction is sufficient since the pattern will repeat for $a, b > q$.

We also know that $-(x^q) \equiv -1 \pmod{2^n}$ therefore

$$\begin{aligned} x^q = x^{b-a}x^{q-(b-a)} &\equiv 1 \pmod{2^n} \\ -(x^q)x^{q-(b-a)} &\equiv 1 \pmod{2^n}, \quad \text{Let } c = q-(b-a) \\ -(x^q x^c) &\equiv 1 \pmod{2^n} \\ x^q(-(x^c)) &\equiv 1 \pmod{2^n} \\ \rightarrow x^c &\equiv -1 \pmod{2^n} \end{aligned}$$

Going to the last line we used the fact that $x^q \equiv 1 \pmod{2^n}$. So we have $x^c \equiv x^{b-a} \equiv -1 \pmod{2^n}$. However, $c = q - (b-a)$, therefore, it must be true that $x^{|(q-(b-a))-(b-a)|} \equiv 1 \pmod{2^n}$.

If $q - (b-a) \neq (b-a)$ this will result in x having an order (modulo 2^n) smaller than q, which is a contradiction. The only way out is to have $q - (b-a) = (b-a)$ which translates to $(b-a) = q/2 = 2^{n-3}$. However, this also leads to another contradiction.

Note that $x^{2^{n-3}} \equiv 1 \pmod{2^{n-1}}$, which is the basis of our inductive reasoning and it also has an odd quotient

$$\begin{aligned} x^{2^{n-3}} &= 1 + 2^{n-1}(2m+1) \\ &\equiv (1 + 2^{n-1}) \pmod{2^n} \end{aligned}$$

It is therefore impossible to have $(1 + 2^{n-1}) \equiv -1 \pmod{2^n}$ because otherwise

$$\begin{aligned} 1 + 2^{n-1} &= 2^n g - 1 \\ 2(1 + 2^{n-2}) &= 2^n g \\ &\rightarrow 2 \mid (1 + 2^{n-2}) \end{aligned}$$

which is a contradiction (note that $n \geq 3$). The only case we need to tackle is the base case $n = 3$ since obviously there is no such thing as modulo 2^{n-1} for the base case. But our base case is simple, the order of x modulo 2^3 is just $q = 2$, therefore $(b-a) = q/2 = 1$ and by construction we know that $x^1 \not\equiv -1 \pmod{2^3}$.

Therefore, there is no a, b such that $+(x^a) \equiv -(x^b) \pmod{2^n}$ which means that the following are the generators of $(\mathbb{Z}/2^n\mathbb{Z}),\ n \geq 3$

$$-1 \qquad \text{and} \qquad x = \begin{cases} 1 + 2(4u+1) \\ 1 - 2(4u+3) \\ 1 \pm |2u+1|2^2 \end{cases}$$

with $u \geq 0$. Some might ask as to why we want to generalize $1 + p \rightarrow 1 \pm |a|p$. Apart from its pedagogical value, it might also helps us find other primitive roots modulo p^n. In conclusion, the trick is to find a base case with oscillating quotient and an "odd" first quotient. Also, although the method above is not elegant (it's rather crude even) yet it is also very effective, especially when finding other generators modulo 2^n.

Problem 2.29. (*) In terms of the prime factorization of n, characterize the integers n such that there is a primitive root modulo n.

For consistency and to avoid confusion I will rename $n \to w$ since we have used n in Problem 2.28 as the power of p, thus the number we are interested here is w.

First suppose we pick a number x and two other numbers m, n with $\gcd(m, n) = 1$, the orders of x are given by

$$\begin{aligned} x^a &\equiv 1 \pmod{m} \\ x^b &\equiv 1 \pmod{n} \end{aligned}$$

Denote $\text{lcm}(a, b) = d$, it is then true that

$$\begin{aligned} x^d &\equiv 1 \pmod{m} \\ &= 1 + mu \\ x^d &\equiv 1 \pmod{n} \\ &= 1 + nv \end{aligned}$$

Furthermore

$$\begin{aligned} x^d &= x^d \\ 1 + mu &= 1 + nv \\ mu &= nv \end{aligned}$$

Since $\gcd(m, n) = 1$ this means that $n|u$ and $m|v \to mu = nv = mns$, thus

$$\begin{aligned} x^d &= 1 + mns \\ &\equiv 1 \pmod{mn} \end{aligned}$$

We know that the order of x modulo mn must be divisible by a and b and $d = \text{lcm}(a, b)$ is the smallest number that is divisible by a and b, therefore $x^d \equiv 1 \pmod{mn}$ means that the order of x modulo mn is indeed $d = \text{lcm}(a, b)$. Therefore,

Proposition 2.29.1. The order of x modulo mn where $\gcd(m, n) = 1$ is given by $\text{lcm}(a, b)$ where a is the order of x modulo m and b is the order of x modulo n.

TABLE V

$w = \prod_1^z$	$p_1^{n_1}$	$p_2^{n_2}$	$p_3^{n_3}$	$\ldots$	$p_z^{n_z}$
$\varphi(p_i^{n_i}) =$	$p_1^{n_1-1}(p_1-1)$	$p_2^{n_2-1}(p_2-1)$	$p_3^{n_3-1}(p_3-1)$	$\ldots$	$p_z^{n_z-1}(p_z-1)$
	$x^{a_1} \equiv 1 \pmod{p_1^{n_1}}$	$x^{a_2} \equiv 1 \pmod{p_2^{n_2}}$	$x^{a_3} \equiv 1 \pmod{p_3^{n_3}}$	$\ldots$	$x^{a_z} \equiv 1 \pmod{p_z^{n_z}}$
	$a_1 \mid (p_1^{n_1-1}(p_1-1))$	$a_2 \mid (p_2^{n_2-1}(p_2-1))$	$a_3 \mid (p_3^{n_3-1}(p_3-1))$	$\ldots$	$a_z \mid (p_z^{n_z-1}(p_z-1))$

We now use this result to characterize the primitive roots of w based on its prime factorization. Thanks to Euclid, every number w can be factorized into

$$\begin{aligned} w &= p_1^{n_1} p_2^{n_2} p_3^{n_3} \ldots p_z^{n_z} \\ &= \prod_{i=1}^{z} p_i^{n_i} \\ \rightarrow \varphi(n) &= \prod_{i=1}^{z} p_i^{n_i-1}(p_i-1) \end{aligned}$$

We now list every number $1 < x < w$ for each distinct $\pmod{p_i^{n_i}}$, where a_i is the order of each x modulo $p_i^{n_i}$ where each a_i is limited by Euler's theorem to be $a_i \mid (p_i^{n_i-1}(p_i-1))$, see Table. V As shown above, the order of x modulo w is given by

$$x^{\mathrm{lcm}(a_1,a_2,\ldots,a_z)} \equiv 1 \pmod{p_1^{n_1} p_2^{n_2} \ldots p_z^{n_z}}$$

since $\gcd(p_i^{n_i}, p_j^{n_j}) = 1$ for any i, j. For x to be a primitive root of n we need

$$\mathrm{lcm}(a_1, a_2, \ldots, a_z) = p_1^{n_1-1}(p_1-1) p_2^{n_2-1}(p_2-1) \ldots p_z^{n_z-1}(p_z-1)$$

Now since each $a_i \mid (p_i^{n_i-1}(p_i-1))$, for the above requirement to hold it has to be that each $a_i = (p_i^{n_i-1}(p_i-1))$. However, $2 \mid (p_i-1)$ for every $p_i \neq 2$, therefore

$$\mathrm{lcm}(a_1, a_2, \ldots, a_z) \leq p_1^{n_1-1}(p_1-1) p_2^{n_2-1}(p_2-1) \ldots p_z^{n_z-1}(p_z-1)$$

All is not lost, hope, though frail, is hard to kill :) Say one of the p's is 2, $\varphi(2) = 1$, thus if $p \neq 2$ then $w = 2p^z,\ \varphi(w = 2p^z) = 1 \cdot \varphi(p^z)$ and therefore w have primitive roots (here z can be zero of course). Another obvious solution is $w = p^z$ which we proved in Problem 2.28. And from Problem 2.27 $w = 4$ will have primitive roots as well and those are the only 3 cases where w will have primitive roots :)

My initial approach in solving this problem was actually to construct much like what we did with Problem 2.28, this turned out to be unprofitable. The difference here is that we have extra primes involved but we can easily use the construction method in Problem 2.28 to find a number with order $p_i^{n_i-1}$.

To illustrate this better let's just assume that w only contains two distinct primes $w = p_1^{n_1}p_2^{n_2}$. We will still use induction but this time we vary n_i one at a time, first we vary n_1 while keeping n_2 fixed, prove it by induction and then we vary n_2 while keeping n_1 fixed and prove the induction for n_2.

First, the number we want is $x = 1 + p_2^{n_2}p_1 = 1 + P$ and here $P = p_2^{n_2}p_1k$, $k = 1$, just like last time

$$\begin{aligned}
(x^q)^1 &= 1 + P &&= 1 + P(1) &&= 1 + p_2^{n_2}p_1^n \cdot [P] \\
(x^q)^2 &= 1 + 2P + P^2 &&= 1 + P(2 + P) &&= 1 + p_2^{n_2}p_1^n \cdot \not{R} \\
(x^q)^3 &= 1 + 3P + 3P^2 + P^3 &&= 1 + P(3 + P + P^2) &&= 1 + p_2^{n_2}p_1^n \cdot \not{R} \\
&\vdots \\
(x^q)^{p_1} &= 1 + p_1P + p'P^2 + \cdots + P^{p_1} &&= 1 + P(p_1 + p'P + \cdots + P^{p_1}) &&= 1 + p_2^{n_2}p_1^n \cdot [P] \\
&\vdots \\
(x^q)^{p_1m} &= 1 + p_1mP + m_1P^2 + \cdots + P^{p_1m} &&= 1 + P(p_1m + m_1P + \cdots + P^{p_1m}) &&= 1 + p_2^{n_2}p_1^n \cdot [P]
\end{aligned}$$

And we see the same pattern. The argument holds because $\gcd(p_1, p_2) = 1$, therefore whether the sum of the terms in bracket is divisible by p_1 or not depends entirely on the coefficient of P^0 and the quotient $\lfloor (x^q)^{p_1m}/p_2^{n_2}p_1^n \rfloor$ is either divisible by p_1 or not depending on whether the bracket is divisible by p_1 or not.

It is now obvious that $1 + p_2^{n_2}p_1$ has an order of $p_1^{n_1-1}$ modulo $p_1^{n_1}p_2^{n_2}$ and of course conversely $1 + p_1^{n_1}p_2$ has the order of $p_2^{n_2-1}$ modulo $p_1^{n_1}p_2^{n_2}$. So in general

$$x = 1 + p_i \prod_{j \neq i} p_j^{n_j} \text{ has the order of } p_i^{n_i-1} \text{ modulo } \prod_l p_l^{n_l}$$

However, this strategy is not beneficial in solving Problem 2.29 since it is hard to deal with numbers that have an order of $(p_i - 1)$. The difficulty is due to the fact that $2|(p_i - 1)$ so even if I found disparate numbers with order $(p_i - 1)$ I cannot just multiply all of them to get a primitive root since $\gcd(p_i - 1, p_j - 1) \geq 2$. And this prompted me to find another strategy which resulted in the above solution.

Problem 2.30 Compute the last two digits of 3^{45}.

First, we need to find the (multiplicative) order of 3 modulo 100 which is 20, thus

$$3^{45} \equiv 3^5 \pmod{100} \equiv 43 \pmod{100}$$

Thus the last two digits of 3^{45} is '43'.

Problem 2.31. Find the integer a such that $0 \leq a < 113$ and

$$102^{70} + 1 \equiv a^{37} \pmod{113}.$$

The order of 102 modulo 113 is 56 so

$$\begin{aligned} 102^{70} &\equiv 102^{14} \pmod{113} \\ &\equiv 98 \pmod{113} \end{aligned}$$

and therefore

$$\begin{aligned} 102^{70} + 1 \equiv 98 + 1 \equiv a^{37} \pmod{113} \\ a^{37} \equiv 99 \pmod{113} \end{aligned}$$

The order of 99 modulo 113 is 28 so $a^{37 \cdot 28} \equiv 1 \pmod{113}$. Note that 113 is prime so $\varphi(113) = 112$ and an order of a number must be a divisor of 112. However $\gcd(37, 112) = 1$ then it must be that

$$\begin{aligned} a^{37 \cdot 28} &\equiv 1 \pmod{113} \\ \rightarrow (a^{28})^{37} &\equiv 1 \pmod{113} \\ a^{28} &\equiv 1 \pmod{113} \end{aligned}$$

Thus we just need to find a number whose order modulo 113 is 28 and that number is $a = 60$.

Problem 2.32. Find the proportion of primes $p < 1000$ such that 2 is a primitive root modulo p.

Using a small C code I found 67 primes out of 169 (39.64%) that have 2 as a primitive root, they are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467,

491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709, 757, 773, 787, 797, 821, 827, 829, 853, 859, 877, 883, 907, 941, 947.

Increasing the limit to $p < 10,000$ gets us 470 out of 1229 (38.24 %) and for $p < 100,000$, it is 3603 out of 9592 (37.56%) and lastly for $p < 1,000,000$ it is 29341 out of 78498 (37.38%). So it is slowly decreasing.

Problem 2.33. Find a prime p such that the smallest primitive root modulo p is 37.

I don't know any clever way to do this. The problem is that even if I know that 37 is a primitive root I don't know any good way of telling if it is the *smallest* primitive root. So I wrote a small C code to find primes who have 37 as its smallest primitive root, they are

36721	51361	63361	97441	129529	132169	171889
190537	201769	314161	333791	343081	387721	422231
493919	496609	515761	529489	532009	532561	557041
596569	600601	618719	619921	628319	629281	631991
662281	663127	687289	704719	711959	720359	739201
751969	774601	783721	828601	840839	859031	890111
907369	1006799	1092961	1102201	1183199	1195489	1210609
1233241	1257721	1266841	1295809	1353791	1405681	1427281
1433041	1445161	1450849	1453321	1463641	1497271	1500071
1522249	1560409	1567729	1570631	1602169	1622041	1622209

and many more :) but since the above list was generated in order 36721 is the smallest prime to have 37 as its smallest primitive root.

Chapter 3

Page 51. "3. Then, $ang \equiv n \pmod{p}$, so everyone knows Nikita's secret key n, and hence can easily compute the shared secret s."

A bit more explanation will be helpful here. First From step 2, which is Bezout's

lemma we have

$$\begin{aligned} ag + bp &= 1 \\ n \times (ag + bp) &= n \\ nag &= n - nbp \\ \rightarrow agn &\equiv n \pmod{p} \end{aligned}$$

What we have is $gn \pmod{p}$ which is part of the public key. From Bezout's lemma we calculated a, therefore we just need to multiply $a \times gn \equiv n \pmod{p}$ and we would have found n.

Algorithm 3.4.5 "(Probabilistic Algorithm to Factor n)." Some explanation is needed here, especially in the probabilistic part and the top part of page 65.

First, this method is probabilistic in two ways, one by choosing random a's to test whether $a^{m/2}$ is equivalent to $1 \pmod{n}$ or not. Next, once we shoce those random a's everything seems to be deterministic. However, the probabilistic portion is in the "three possibilities for these signs" at the bottom of page 64. It is that sometimes (not all of the time)

$$a^{m/2} \equiv -1 \pmod{p} \qquad \text{and} \qquad a^{m/2} \equiv -1 \pmod{q}$$

But what's wrong with this? we can still say

$$p | a^{m/2} + 1 \qquad \text{but} \qquad q | a^{m/2} + 1$$

But that's a problem because then $pq | a^{m/2} + 1$ and $\gcd(a^{m/2} - 1, pq) = pq$ which doesn't give us the factorization of $n = pq$ into p or q. Thus in the explanation at the top of page 65, he could've just used

$$p \nmid a^{m/2} + 1 \qquad \text{but} \qquad q | a^{m/2} + 1$$

and we will get $\gcd(a^{m/2} + 1, pq) = q$. So the lesson here is that we want $a^{m/2}$ to have *different* values modulo p from modulo q. This is why $a^{m/2} \equiv +1 \pmod{p}$ **and** $a^{m/2} \equiv +1 \pmod{q}$ is a bad thing.

Definition 3.4.7. "if there exists a single a such that $a^{m/2} \not\equiv 1 \pmod{n}$, then half the a have this property, since then $a \rightarrow a^{m/2}$ is a surjective homomorphism $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow \{\pm 1\}$

and the kernel has index 2". At first I didn't understand why half the a have this property even if the map is surjective.

Surjective just means onto, *i.e.* all elements in the target space are covered, but it doesn't say anything about the distribution of the pre-images, like how many of them map to $+1$ and how many to -1. Before continuing, let's review some basic definitions

The index of H in G, denoted $|G : H|$, is the number of cosets of H in G. A coset is defined as

- left coset of H in G is the set $g * H$ where $g \in G$
- right coset of H in G is the set $H * g$ where $g \in G$

where $*$ is the group operation.

For example, let $G = \mathbb{Z}$, *i.e.* G is the group of all integers under *addition*, let $H = 2\mathbb{Z}$ be the group of all even integers under *addition*. There are only *two* cosets of H. One is H itself which is just $0 * H = 0 + H$ and another is $1 * H = 1 + H$ which is the group of odd integers under addition. How about $5 * H = 5 + H$, well $5 + H$ results in the same set as $1 + H$, so it's already covered. The same for $4 + H = 0 + H = H$. Thus the index of H in this case is 2 since there are only 2 cosets of H in G.

Back to our earlier discussion, I think this half and half business has something to do with Lagrange's theorem and the fact that if G and H are groups and $\varphi : G \to H$ is a homomorphism, then the index of the kernel of φ in G is equal to the order of the image:

$$|G : \ker(\varphi)| = |\text{im } \varphi|.$$

In our case at hand, $G = (\mathbb{Z}/n\mathbb{Z})^*$, while $\varphi : a \to a^{m/2} \pmod n \to \pm 1$, *i.e.* the image of φ, which is H is just $\equiv 1 \pmod n \to +1$ or $\not\equiv 1 \pmod n \to -1$, so we denote them ± 1. Thus $|\text{im } \varphi|$ is just 2.

However, this fact alone is not enough. We need Lagrange's theorem that states, if G and H are finite groups, then the index of H in G is equal to the quotient of the orders of the two groups:

$$|G : H| = \frac{|G|}{|H|}$$

note that order is just the number of elements of the group.

Therefore

$$\begin{aligned} |G : \ker(\varphi)| &= 2 \\ |G : \ker(\varphi)| &= \frac{|G|}{|\ker(\varphi)|} \\ \rightarrow \frac{|G|}{|\ker(\varphi)|} &= 2 \\ |\ker(\varphi)| &= \frac{|G|}{2} \end{aligned}$$

and half of $G = (\mathbb{Z}/n\mathbb{Z})^*$ have $a^{m/2} \not\equiv 1 \pmod{n}$.

Some cautionary tales. At first glance it seems that every map that maps to $\{\pm 1\}$ seems to result in a kernel with image of 2 because if we follow the above recipe

$$\begin{aligned} |G : \ker(\varphi)| &= 2 \\ |G : \ker(\varphi)| &= \frac{|G|}{|\ker(\varphi)|} \\ \rightarrow \frac{|G|}{|\ker(\varphi)|} &= 2 \\ |\ker(\varphi)| &= \frac{|G|}{2} \end{aligned}$$

However, this is only true if φ is a homomorphism. For example if we arbitrarily map $\mathbb{Z}/7\mathbb{Z}$ as $1 \rightarrow +1$ and the rest to -1 the map is no longer homomorphic. For example

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

However

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

a contradiction since φ is no longer homomorphic, *i.e.* $\varphi(a \cdot b) \neq \varphi(a)\varphi(b)$. The above

difficulty can be (seemingly) overcome if we map to $\{0,1\}$ instead of $\{\pm 1\}$, for example

$$\begin{aligned}\varphi(1\cdot 2\cdot 3) &= \varphi(1)\varphi(2)\varphi(3)\\ &= (+1)(0)(0)\\ &= 0\\ \varphi(1\cdot 2\cdot 3) &= \varphi(1)\varphi(2\cdot 3)\\ &= (+1)(0)\\ &= 0\end{aligned}$$

So it seems that it is consistent, however, 0 doesn't have an inverse, thus $\{0,1\}$ is no longer a group. So be careful in applying the above reasoning to any binary mapping!

Comments. Just a short comment on Section 3.4 "Attacking RSA". If we already know $\varphi(n)$ or even d, why do we need to factorize n? We can straightforwardly decrypt the message ¯\(°_o)/¯

Problem 3.1. This problem concerns encoding phrases using numbers using the encoding of Section 3.3.2. What is the longest that an arbitrary sequence of letters (no spaces) can be if it must fit in a number that is less than 10^{20}?

We have 26 characters to encode A, ..., Z thus we can encode as a number in base 26. However, if we do this the character Z will be 26 and it will coincide with the second character in the sequence, therefore we still need to use base 27.

The longest sequence of letter we can encode is therefore

$$\lfloor \log_{27}(10^{20}) \rfloor = 13$$

The floor is to ensure that we have enough space for all 13 characters.

Problem 3.2. Suppose Michael creates an RSA cryptosystem with a very large modulus n for which the factorization of n cannot be found in a reasonable amount of time. Suppose that Nikita sends messages to Michael by representing each alphabetic character as an integer between 0 and 26 (A corresponds to 1, B to 2, etc., and a space to 0), then encrypts each number *separately* using Michaels RSA cryptosystem. Is this method secure? Explain your answer.

This method is not too secure as eavesdroppers can see repeating numbers being sent by Nikita and they might be able to figure out a dictionary between the plain text alphabets and the encrypted alphabets.

Problem 3.3. For any $n \in N$, let $\sigma(n)$ be the sum of the divisors of n; for example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(10) = 1 + 2 + 5 + 10 = 18$. Suppose that $n = pqr$ with $p,\ q$, and r distinct primes. Devise an "efficient" algorithm that given $n,\ \varphi(n)$ and $\sigma(n)$, computes the factorization of n. For example, if $n = 105$, then $p = 3,\ q = 5$, and $r = 7$, so the input to the algorithm would be

$$n = 105,\ \varphi(n) = 48,\ \text{and } \sigma(n) = 192,$$

and the output would be 3, 5, and 7.

Well, we follow closely the strategy of Section 3.4.1 "Factoring n Given $varphi(n)$". First we express

$$\begin{aligned}
\varphi(n) &= \varphi(pqr) \\
&= (p-1)(q-1)(r-1) \\
&= pqr - pq - pr - qr + p + q + r - 1 \\
\sigma(n) &= pqr + pq + pr + qr + p + q + r + 1
\end{aligned}$$

Therefore

$$\begin{aligned}
\sigma(n) + \varphi(n) &= pqr + p + q + r \\
\rightarrow p + q + r &= \sigma(n) + \varphi(n) - n \\
\sigma(n) - \varphi(n) &= 2(pq + pr + qr) + 2 \\
\rightarrow pq + pr + qr &= \frac{\sigma(n) - \varphi(n)}{2} - 1
\end{aligned}$$

We also know that

$$\begin{aligned}
(x-p)(x-q)(x-r) &= x^3 - x^2(p+q+r) + x(pq+pr+qr) - pqr \\
&= x^3 - x^2(\sigma(n) + \varphi(n) - n) + x\left(\frac{\sigma(n) - \varphi(n)}{2} - 1\right) - n
\end{aligned}$$

We therefore setup a cubic polynomial with the above coefficients and solve it using the cubic formula.

One comment about the cubic formula. The first thing it does is to depress the equation to get rid of x^2. This turns our to be a general strategy for any polynomial. What we usually do to solve the quadratic equation is to complete the square. This is actually the "wrong" thing to do. What we actually want is to get rid of the x term, which is the same as completing the square for the quadratic case.

However, this strategy of completing the square cannot be extended to completing the cube, for one

$$x^3 = a \to x = a^{1/3}$$
$$x^2 = a \to x = \pm a^{1/2}$$

even if we can complete the cube we only get one solution instead of three, while completing the square guarantees that we have two solutions. So just like the adage, "One man's treasure is another man's trash" :) A point of view that works very well for one particular problem hinders us from solving another problem.

Problem 3.4. You and Nikita wish to agree on a secret key using the Diffe-Hellman key exchange. Nikita announces that $p = 3793$ and $g = 7$. Nikita secretly chooses a number $n < p$ and tells you that $g^n \equiv 454 \pmod{p}$. You choose the random number $m = 1208$. What is the secret key?

The secret key in this case is $g^{nm} \pmod{p} \equiv (g^n)^m \pmod{p}$

$$\begin{aligned} g^n &\equiv 454 \pmod{p} \\ (g^n)^m &\equiv (454)^m \pmod{p} \\ (g^n)^{1208} &\equiv (454)^{1208} \pmod{p} \\ &\equiv 2156 \pmod{3793} \end{aligned}$$

Problem 3.5. You see Michael and Nikita agree on a secret key using the Diffe-Hellman key exchange. Michael and Nikita choose $p = 97$ and $g = 5$. Nikita chooses a random number n and tells Michael that $g^n \equiv 3 \pmod{97}$, and Michael chooses a random number m and tells Nikita that $g^m \equiv 7 \pmod{97}$. Brute force crack their code: What is the secret key that Nikita and Michael agree upon? What is n? What is m?

By brute force $n = 70$, $m = 31$, therefore $g^{31 \cdot 70} \equiv 44 \pmod{97}$.

Problem 3.6. In this problem, you will"crack" an RSA cryptosystem. What is the secret decoding number d for the RSA cryptosystem with public key $(n, e) = (5352381469067, 4240501142039)$?

Using brute force factorization method we get $n = 141307 \cdot 37877681$. Using the Fermat's method, Section 3.4.2, took around 15 times longer.

We now need to find d where

$$ed \equiv 1 \pmod{\varphi(n)}$$

where $\varphi(n) = (p-1)(q-1) = 5352343450080$. We use Algorithm 2.3.7, which is Bezout's Lemma to calculate d

$$\begin{aligned} & ed + \varphi(n)y = 1 \\ & \qquad \rightarrow d = -156721461241 \equiv 5195621988839 \pmod{5352343450080} \end{aligned}$$

We should check that we have the correct d, *i.e.* $ed - 1$ must be divisible by $p - 1$ and $q - 1$, and in this case it is.

Problem 3.7. Nikita creates an RSA cryptosystem with public key

$$(n, e) = (1433811615146881, 329222149569169).$$

In the following two problems, show the steps you take to factor n. (Don't simply factor n directly using a computer.)

(a) Somehow you discover that $d = 116439879930113$. Show how to use the probabilistic algorithm of Section 3.4.3 to factor n.

(b) In part (a) you found that the factors p and q of n are very close. Show how to use the Fermat Factorization Method of Section 3.4.2 to factor n.

Part (a), first, we need

$$m = ed - 1 = 383345875661677416927794860 96$$

This number turns out to be too big for a 64-bit integer, thus I couldn't use my C code to do it. I ended up using maxima, the functions needed are 'power_mod(a,m,n)' another somewhat related one is 'zn_power(a,n)'.

This problem turned out to be a little tricky. I initially chose $a = 2$ just like the example in Section 3.4.3. However, this only gave $a^{m/2} \equiv -1 \pmod{p}$ and $a^{m/2} \equiv -1 \pmod{q}$ when $a^{m/2} \not\equiv 1 \pmod{n}$, no luck, other primes like 5, 11, 13 are in the same boat. Thus this strategy is really probabilistic.

However, $a = 5$ works, we keep dividing m by 2 until we get

$$\begin{aligned} m/2 &= 47918234457709677115974357 62 \\ \rightarrow 5^{m/2} &\equiv 597421503155725 \pmod{n} \not\equiv 1 \pmod{n} \\ \gcd(597421503155725 - 1, n) &= 37865717 \end{aligned}$$

The other prime factor of n is then $n/37865717 = 37865693$.

For part(b), Fermat's method was far quicker (by at least 400,000 times) than brute force factorization, where $p = 37865717$ and $q = 37865693$ because it only needs *one* iteration.

$$\begin{aligned} t &= \lceil \sqrt{n} \rceil = 37865705 \\ t^2 - n &= = s^2 = 144 \\ \rightarrow s &= 12 \end{aligned}$$

Therefore $p = t + s = 37865717$ and $q = t - s = 37865693$.

Chapter 4

Some general comments. In dealing with congruences one must be careful. For example, 5 being a prime number can certainly **not** be a square. However,

$$7^2 \equiv 5 \pmod{11}$$

This cyclic nature sometimes confuses people :)

Definition 4.1.2. The example right after this definition. $\left(\frac{5}{5}\right) = 1$. I believe this is wrong because $\gcd(5, 5) = 5 \neq 1$ and as such it should be that $\left(\frac{5}{5}\right) = 0$.

Lemma 4.1.4. There are some nice things that can be said about $\mathbb{Z}/p\mathbb{Z}$ when p is an odd prime and $p = 2^n + 1$.

Proposition 4.1.4.1. If p is an odd prime and $p = 2^n + 1$ then all primitive roots of $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic non residues and non-primitive roots are all quadratic residues. In other words, exactly half of $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues while the other half are not.

Proof. From Proposition 2.5.12.2 we know that when g is a primitive root, all g^d with $\gcd(d, \varphi(p)) = 1$ are also primitive roots.

And each primitive root is of course a quadratic non residue because from the proof of Lemma 4.1.4 we know that any primitive root with an odd power is a quadratic non residue. Or more explicitly, $x^2 - 1$ only has ± 1 as solutions and $x = g^{\varphi(p)/2}$ where g is *any* primitive root is of course a solution since $(g^{\varphi(p)/2})^2 \equiv 1$. However, since g is a primitive root we cannot have $g^{\varphi(p)/2} \equiv +1$ cause then its order will be $\varphi(p)/2$ which is a contradiction. So since the only other solution to $x^2 - 1$ is -1 then $g^{\varphi(p)/2} \equiv -1$.

So we have shown that *all* primitive roots are quadratic non-residues. How about the non primitive roots? Well, again from Proposition 2.5.12.2, the non primitive roots are the ones with g^h where $\gcd(h, \varphi(p) \neq 1$. Since $\varphi(p) = 2^n$, h has to be even. And from the proof of Lemma 4.1.4, any g^{2m} is a quadratic residue, thus in this case the non-primitive roots are all quadratic residues. This completes the proof.

Proposition 4.2.1, lowbrow version. Euler's Criterion. This can be proven in a more down to earth manner. The most obvious way is to use the proof of Lemma 4.1.4. There it was shown that all quadratic residue is of the form g^{2m} where g is a primitive root. Therefore,

$$(g^{2m})^{(p-1)/2} = g^{m(p-1)} \equiv 1 \pmod{p}$$

thanks to Euler's theorem 2.1.20 $a^{\varphi(p)} \equiv 1 \pmod{p}$.

Or in more details, my lowbrow proof is as follows. First, if $a \equiv b^2 \pmod{p}$ then

$$\begin{aligned} a^{(p-1)/2} &\equiv (b^2)^{(p-1)/2} \pmod{p} \\ &\equiv b^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

thanks again to Euler's theorem. We now need to prove the converse, if $a^{(p-1)/2} \equiv 1 \pmod{p}$ then since p is an odd prime, the existence of a primitive root is guaranteed,

therefore we can express $a \equiv g^m \pmod{p}$ and

$$a^{(p-1)/2} \equiv (g^m)^{(p-1)/2} \pmod{p}$$

Now if m is odd, $m = 2y + 1$ we get

$$\begin{aligned}(g^m)^{(p-1)/2} &\equiv (g^{2y+1})^{(p-1)/2} \pmod{p} \\ &\equiv g^{y(p-1)} g^{(p-1)/2} \pmod{p} \\ &\equiv 1 \cdot g^{(p-1)/2} \pmod{p}\end{aligned}$$

Since g is a primitive root $g^{(p-1)/2} \not\equiv 1 \pmod{p}$. Hence if m is odd we get

$$\begin{aligned}a^{(p-1)/2} &\equiv (g^{2y+1})^{(p-1)/2} \pmod{p} \\ a^{(p-1)/2} &\not\equiv 1 \pmod{p}\end{aligned}$$

which is a contradiction, therefore m has to be even, $m = 2y$ but then $a \equiv g^{2y} \pmod{p}$ and from the proof of Lemma 4.1.4 g^{2y} is a quadratic residue. This completes the proof.

Proof of Proposition 4.2.1. " Since the kernel of a homomorphism is a group, and the order of a subgroup divides the order of the group, we have either $\ker(\varphi) = \ker(\psi)$ or $\varphi = 1$."

Some explanation, the order of a group is the size of a group. Next, since $\ker(\psi)$ is a (normal) subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, see Problem 2.21, it is true that $\#(\mathbb{Z}/p\mathbb{Z})^* = d \cdot \#\ker(\psi)$ as the order of a subgroup divides the order of the group.

But it is also true that $\ker(\varphi) \subset \ker(\psi)$, thus $\#\ker(\varphi) \leq \#\ker(\psi)$ therefore if $\#\ker(\psi) > \#\ker(\varphi)$ then $d < 2 \rightarrow d = 1$ and $\#(\mathbb{Z}/p\mathbb{Z})^* = \#\ker(\psi)$. While if $\#\ker(\varphi) = \#\ker(\psi)$ then $\#(\mathbb{Z}/p\mathbb{Z})^* = 2 \cdot \#\ker(\psi)$.

Now $\#(\mathbb{Z}/p\mathbb{Z})^* = \#\ker(\psi)$, means that the kernel of ψ is the entire group $(\mathbb{Z}/p\mathbb{Z})^*$ which means that ψ maps every member of $(\mathbb{Z}/p\mathbb{Z})^*$ to 1, *i.e.* $\psi(a) = a^{(p-1)/2} = 1$. At first I thought $\varphi = 1$ means that φ is the identity operator :)

Corollary 4.2.3. The proof mentions " This follows from Proposition 4.2.1 and the fact that the polynomial $x^2 - 1$ has no roots besides $+1$ and -1".

I'll show explicitly how it follows from the fact that $x^2 - 1$ has no roots besides $+1$ and -1.

If $x^2 \not\equiv a \pmod{p}$ then it also means that $a \not\equiv x^2 \pmod{p}$, which is to say that a is a quadratic nonresidue. Thus from Proposition 4.2.1 $a^{(p-1)/2} \not\equiv 1 \pmod{}$. Now, from Euler's theorem we have

$$a^{p-1} \equiv 1 \pmod{p}$$

Therefore we can rewrite $x^2 \equiv 1 \pmod{p}$ as

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \\ \rightarrow x^2 &\equiv a^{p-1} \pmod{p} \end{aligned}$$

Taking the "squre root" of both sides

$$x = \pm 1 \equiv a^{(p-1)/2} \pmod{p}$$

We know that x is either $+1$ or -1 therefore

$$a^{(p-1)/2} \equiv \begin{cases} +1 \pmod{p} \\ -1 \pmod{p} \end{cases}$$

But from Proposition 4.2.1 $a^{(p-1)/2} \equiv 1 \pmod{p}$ means that a is a quadratic residue, which is a contradiction and hence $a^{(p-1)/2} \equiv -1 \pmod{p}$.

The converse is straighforward, if $a^{(p-1)/2} \equiv -1 \pmod{p}$, from Proposition 4.2.1 it follows that a is a quadratic nonresidue and therefore $x^2 \equiv a \pmod{p}$ has no solution.

Proof of Lemma 4.3.1. A clarification of the proof of this Lemma. First, this Lemma wants to map $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ to $(-p/2, p/2)$. But we are not using *all* numbers between $(-p/2, p/2)$ as the image. We are only using *half* of them obviously as $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ is just half of the complete set of residues of p.

Therefore the statement "No number $1, 2, \ldots, \frac{p-1}{2}$ appears more than once, with **either choice of sign**". Say two elements of S, ka mapped to $|d|$ and ja mapped to $-|d|$, therefore

$$\begin{aligned} |d| + (-|d|) &\equiv 0 \pmod{p} \\ ka + ja &\equiv 0 \pmod{p} \end{aligned}$$

which was proven to be a contradiction in the text.

This whole business of proving Lemma 4.3.1 can actually be done more clearly using Lemma 2.1.12. Note that $-a\frac{p-1}{2}, \ldots, 0, \ldots, \frac{p-1}{2}a$ is a complete set of residue according to Lemma 2.1.12 because $a \not\equiv 0 \pmod{p} \rightarrow \gcd(a, p) = 1$ as p is prime.

Let's denote

$$\begin{aligned} A^+ &= \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\} \\ A^- &= \{-a, -2a, -3a, \ldots, -\frac{p-1}{2}a\} \\ A &= \{-a\frac{p-1}{2}, \ldots, -a, 0, a, \ldots, \frac{p-1}{2}a\} = \{A^-, 0, A^+\} \\ O &= \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\} \end{aligned}$$

i.e. $A = aO$. Thanks to Lemma 2.1.12 there is a one to one (and onto) mapping between A and O. To prove Lemma 4.3.1 we want to map $S = A^+$ to O, let's call this bijective mapping $f(A) : A \rightarrow O$, $f(A^+) = O^+ \subset O$, $f(A^-) = O^- \subset O$.

It is now straightforward to show that "No number $1, 2, \ldots, \frac{p-1}{2}$ appears more than once, with **either choice of sign**" in O^+. First, assume there are duplicate entries with a positive relative sign d, d in O^+. This is a blatant contradiction as f is a bijective mapping as required by Lemma 21.12.

Next, say there are duplicate entries with a relative negative sign $d, -d \in f(A^+)$, then there will be no bijective mapping between A and O. First the mapping between A and O is just a reduction modulo p which means that $\tilde{a} \equiv \tilde{o} \pmod{p}$ where $\tilde{a} \in A$ and $\tilde{o} = f(\tilde{a}) \in O$. Therefore

$$\begin{aligned} \tilde{a} &\equiv \tilde{o} \pmod{p} \\ -\tilde{a} &\equiv -\tilde{o} \pmod{p} \\ \rightarrow f(A^-) &= -f(A^+), \quad \text{note that } A^- = -A^+ \end{aligned}$$

Hence $d, -d$ will be in the image of A^- as well. This is a contradiction as the overlap between $f(A^+) \cap f(A^-) = \{d, -d\}$ means that $\#\{f(A^-), f(0), f(A^+)\} < \#O$.

I chose to use Lemma 2.1.12 to make sure that the map between $S = A^+$ and O^+ is guaranteed to exist, that's all.

Page 78. Proof of Proposition 4.3.4.

I would like to explain the set I which is a union of many intervals. What we want to achieve here is to list all numbers that are equivalent to $(-\frac{p}{2}, 0)$ modulo p. If we just take the numbers between $(0, p)$ the ones that are in $(-\frac{p}{2}, 0)$ are obviously $(\frac{p}{2}, p)$.

If we go to the next interval $(p, 2p)$ the ones that are in $(-\frac{p}{2}, 0)$ are then $(p + \frac{p}{2}, 2p)$. Thus $(-\frac{p}{2}, 0)$ are represented by $((m - \frac{1}{2})p, mp)$.

Page 78. "Next suppose that $b = \frac{1}{2}(a - 1)$".

The next equation seems to be wrong, for example "$\frac{a-1}{2}p + \frac{p}{2} = \frac{p-1+a}{2}$". The thing is $\frac{a-1}{2}p + \frac{p}{2} = \frac{pa}{2}$.

I don't understand why he suddenly adds $\frac{p}{2}$ to bp. The last number in I is bp. However, this is what I could figure out.

$$bp + \frac{p}{2} = \frac{pa}{2}$$

and $\frac{pa}{2} > \frac{(p-1)a}{2}$. However, the integers between $(bp, \frac{pa}{2})$ are all $(0, +\frac{p}{2})$ modulo p. This is because $bp \equiv 0 \pmod{p}$ and $bp + \frac{p}{2} \equiv \frac{p}{2} \pmod{p}$.

Therefore, the numbers in S that are between $(bp, \frac{pa}{2})$ are all between $(0, +\frac{p}{2})$, *i.e.* they're all on the *positive* half of $(-\frac{p}{2}, +\frac{p}{2})$ while the numbers in S that are between $((b - \frac{1}{2})p, bp)$ will be in the *negative* half of $(-\frac{p}{2}, +\frac{p}{2})$.

Page 80. Proof of Proposition 4.3.5. "The possibilities for r are 1, 3, 5, 7."

Where did we get these possibilities? Note that $p = 8c+r \to p \equiv r \pmod{8}$. Therefore r is $0 \leq r \leq 7$. However p is a prime and thus $2,\ 4,\ 6$ are disallowed because, say $r = 6$

$$\begin{aligned} p &\equiv 6 \pmod{8} \\ &= 6 + 8n = 2(3 + 4n) \\ \to 2 &\mid p \end{aligned}$$

which is a contradiction. So any even r is disallowed, only odd ones are possible.

Page 81. "Next suppose that $p \not\equiv q \pmod{4}$, so $p \equiv q \pmod{4}$".

This means that either the difference of two odd primes is a multiple of 4 or the sum of two odd primes is a multiple of 4. To prove this express an odd prime as

$$p \equiv u \pmod{4}$$

where $0 \leq u \leq 3$. Now u must be either 1 or 3 because if u is 0 or 2 then p would be an even number and not prime, *i.e.*

$$\begin{aligned} p &\equiv 2 \pmod 4 \\ &= 2 + 4n = 2(1 + 2n) \\ \rightarrow 2 &\mid p \end{aligned}$$

Thus if two odd primes are both equivalent to $1 \pmod 4$ or $3 \pmod 4$ then their difference would be a multiple of 4 and if one of them is $1 \pmod 4$ and the other is $3 \pmod 4$ then their sum will be a multiple of 4.

Page 81. "the last equality is because $\frac{p1}{2}$ is even if and only if $\frac{q1}{2}$ is even"

If $p \equiv q \pmod 4$ then $\frac{p-1}{2}$ is even if and only if $\frac{q-1}{2}$ is even because

$$\begin{aligned} p &\equiv q \pmod 4 \\ &= q + 4n \\ \rightarrow \frac{p-1}{2} &= \frac{(q-1)}{2} + \frac{4n}{2} \end{aligned}$$

Since $\frac{4n}{2}$ is always even, thus if $\frac{(q-1)}{2}$ is even the LHS is also even and if $\frac{(q-1)}{2}$ is odd then the LHS is also odd.

On the other hand if $p \equiv -q \pmod 4$ then

$$\begin{aligned} p &\equiv -q \pmod 4 \\ p + q &= 4n \\ (p-1) + (q-1) &= 4n - 2 \\ \frac{p-1}{2} + \frac{(q-1)}{2} &= \frac{4n-2}{2} \\ \rightarrow \frac{p-1}{2} + \frac{(q-1)}{2} &= 2n - 1 \end{aligned}$$

Since $2n - 1$ is odd the LHS has to be odd as well, *i.e.* one of $\frac{(q-1)}{2}$ and $\frac{(p-1)}{2}$ has to be odd and the other must be even. Therefore $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ has to be even.