MONT Typos and Corrections

Aditya Khurmi *

Last Updated: March 29, 2022

There are minor typos, which include small things like grammatical errors or mathematical errors which can be easily guessed as being typos. Then there are major typos which are big typos that change the problem/statement. These are marked with **!!!**

All typos are in red color, while corrections (such as deletion of a problem) are written normally in black. One common typo appearing a lot is changing ".

P.g. 16 We finish this discussion with a list of properties, some of which we discussed above, and some others, which I leave as exercises to prove.

P.g. 17 For 2 fixed integers x, y, prove that

$$x - y \mid x^n - y^n$$

for any positive integer n. (Hint: Long division)

P.g. 19 So, for instance, you can factorize 45 as $3^2 \times 5$ but not in any other way.

P.g. 19 Theorem 1.5.1 (Divisibility in Sets). Let a, b be two positive integers. Then

$$a \mid b \Leftrightarrow A \subseteq B.$$

P.g. 23 **!!!** (Add a problem)
Prove that if p is a prime with $p \mid ab$, then $p \mid a$ or $p \mid b$. In particular $p \mid a^2$, then $p \mid a$.
This is an incredibly useful property. In fact, this property is equivalent to p being a prime, and so very strong.

P.g. 24 $\gcd(440, 124) = \gcd(124, 68) = \gcd(68, 56) = \gcd(56, 12) = \gcd(12, 8) = \gcd(8, 4) = 4$.

P.g. 27 Further, we write, say 514567, as

P.g. 31 **!!!** Now, since $aq + a > b$, hence $a > b - aq = r$.

P.g. 31 This is possible if $d \mid m, n$

P.g. 31 We present the most natural way to approach this question

P.g. 31 Hence, we would at the end have $g = a^{\gcd(m,n)} - 1$.

P.g. 31 This is hard to think of, so I suggest you take some examples (such as $(m, n) = (15, 4)$) and convince yourself. (basically delete "see")

P.g. 31 we will see such similar themes in the Constructions chapter

P.g. 34 (more of a Latex error) So, the above gcd equals $\gcd(a + b, p)$, which is either 1 or p.

P.g. 35 However, in this case $\text{lcm}(a, b, c) = abc$.

P.g. 37 This is exactly identical to the problem

P.g. 38 **!!!** Assume $\mathcal{S}$ has at least 2 elements (since $\phi, \{a\}$ are working sets), since otherwise the condition is useless. Observe that the arithmetic mean of $b, 2a - b$ is a.

P.g. 40 **!!!** Problem 1.12.8 (Russia 2001 grade 11 Day 2/2). Let a, b be distinct naturals

P.g. 41 **!!!** (All Russian Olympiad 2017 Day1 Grade 10 P5). Suppose n is a composite positive integer. Let $1 < a_1 < a_2 < \cdots < a_k < n$ be all the divisors of n. It is known, that $a_1 + 1, ..., a_k + 1$ are all divisors for some m (except $1, m$). Find all such n.

P.g. 41 Problem 1.12.13 (IMO 2002/4)

*Contact me at adityak1135@gmail.com

P.g. 41 Indian National Mathematical Olympiad

P.g. 46 **Problem 2.1.3.** Show that the set of integers a such that $a \equiv 0 \pmod{n}$ is the set of multiples of n.

P.g. 47 In Divisibility, we studied the multiplication table, which was the first column

P.g. 47 The three columns above are called the 3 "residue classes" modulo 3. In general we have the following:

P.g. 47 Guess why the above classes are called "residue" classes.

P.g. 50 **Question 2.5.1.** *What's the period?*

P.g. 50 $a_i \equiv a_j \pmod{p} \implies a(i-j) \equiv 0 \pmod{p} \implies p \mid a(i-j)$.

P.g. 51 Now, $\gcd((p-1)!, p) = 1$, hence we can divide both the sides by $(p-1)!$ by Problem 2.4.8. Hence $a^{p-1} \equiv 1 \pmod{p}$.

P.g. 51 Don't forget the "relatively prime" part of the theorem.

P.g. 52 Now let's look at the definition of "equal sets" in Theorem 2.5.1.

P.g. 52 **!!!** $\frac{20}{46} \equiv \frac{-1}{4} \equiv 5 \pmod{7}$

P.g. 55 $2 \cdot 3 \cdot 4 \cdots 9 = (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) = 1 \cdot 1 \cdot 1 \cdot 1 \equiv 1 \pmod{11}$.

P.g. 61 Example 2.12.1, Let a, m, n be integers. Suppose d satisfies

P.g. 61 this was Problem 2.4.8

P.g. 61 (delete "to") Now, the d contributes only $\gcd(d, n)$ in this divisibility.

P.g. 62 If we think of $\mathbb{F}_p$ as a "structure", i.e. a system of certain numbers, then this identity holds over this system.

P.g. 64

$$2 \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv -\sum_{i=1}^{p-1} \frac{1}{i^2} \pmod{p}.$$

P.g. 65

$$\begin{aligned} \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{(p-1)^2} &\equiv +(1^2 + 2^2 + \cdots + (p-1)^2) \\ &= +\frac{(p-1)p(2p-1)}{6} \pmod{p}, \end{aligned}$$

P.g. 65 note where we use $=$ and where $\equiv$, denoting where we used algebraic facts vs number theoretic facts

P.g. 66 (delete an extra "if") So if we can show the sequence $\langle a_i \rangle$ eventually becomes constant ...

P.g. 67 $a + b + c \geq 3c + 3d \geq 3d$.

P.g. 69 So this problem is screaming at us to try to do what he did, show that the "set" is infinite; in his case the set of primes, and in our case the set M.

P.g. 71 Regional Mathematical Olympiad

P.g. 72 **!!!** every positive integer has at least as many divisors of the form $4k+1$ as divisors of the form $4k+3$

P.g. 75 **!!!** However, there are some technical details you need to know to fully appreciate the proof, so you can find it in the special section of the chapter: Modular Arithmetic Advanced.

P.g. 79 Because of the 2 in $2\sqrt{n}$, we feel some pairing type argument might be involved in the proof.

P.g. 79 Indeed, if $d \mid n$, then $(n/d) \mid n$. too.

P.g. 81 There are thus $\varphi(m)$ numbers in each row coprime to m.

P.g. 82 Use the integral test to show that $\zeta(s)$ converges if and only if $s > 1$. In particular, show that $\zeta(1)$ diverges.

P.g. 83 The product somehow balances out each others' growth).

P.g. 84 This function is very useful because of the following 2 properties:

P.g. 85 We observe the sum with indices varying over $d \mid n$ are a common theme in multiplicative functions.

P.g. 86 (Delete the 5th point "$\mu * 1 = \delta$.")

P.g. 87 (delete "us find")
This is a very useful fact, and can help us ~~find the~~ invert the equation we wanted to!

P.g. 88 (Delete the 2 extra "in general"s)
In general, all the fractions would appear ~~in general~~ in the double sum in Equation 3.2 ~~in general~~ for any n.

P.g. 89 **!!!** The idea in Example 3.4.2 is the fact the following:

$$\left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\} = \left\{\left\{\frac{k}{d} : 1 \leq k \leq d, \gcd(k,d) = 1\right\} : d \mid n\right\}.$$

P.g. 89 Is this the same proof as the one we gave here: 3.3.1?

P.g. 89 (in the footnote) Technically this isn't an Arithmetic Function since they are $\mathbb{R} \to \mathbb{Z}$. However, I still cover them in this chapter.

P.g. 89 The graph suggests why it is called the "floor function"

P.g. 90 For negative, it's not exactly the decimal part, but its complementary.

P.g. 90 The definitions give the following properties

P.g. 90 Remove the PreRMO problem.

P.g. 95 (Delete "One useful lemma we obtain this way is")

P.g. 96 So it suffices to show $d(n+1) > a_n$ and $d(n+1) < a_n$ both hold infinitely often (why?).

P.g. 96 (Latex error) Hence, $d(n+1) > \max\{d(1), \ldots d(n)\} \geq a_n$, as desired.

P.g. 96 **!!!** Here, the rows and columns are $1, 2, \ldots, n$, and an element (i, j) is 1 if i is a multiple of j, and 0 otherwise.

P.g. 96 **!!!** Fix a column say the ith one. Then, the number of 1s here is $\left\lfloor \frac{n}{i} \right\rfloor$.

P.g. 96 **!!!** Next, if we fix a row, say the ith one, then the number of 1s here is the number of divisors of i (why?).

P.g. 97 **!!!** Now, suppose in our table, instead of writing 1s, we write the multiple, i.e. the (i, j) element is j if i is a multiple of j, and 0 otherwise. So, the table for $n = 8$ now is

	1	2	3	4	5	6	7	8
1	1	0	0	0	0	0	0	0
2	1	2	0	0	0	0	0	0
3	1	0	3	0	0	0	0	0
4	1	2	0	4	0	0	0	0
5	1	0	0	0	5	0	0	0
6	1	2	3	0	0	6	0	0
7	1	0	0	0	0	0	7	0
8	1	2	0	4	0	0	0	8

If we fix a column, then the sum of the elements is

$$\mathcal{S} = 1\left\lfloor \frac{n}{1} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + \cdots + n\left\lfloor \frac{n}{n} \right\rfloor.$$

If we fix a row first, we get

$$\mathcal{S} = \sigma(1) + \sigma(2) + \cdots + \sigma(n).$$

P.g. 97 **!!!** The function $d(n)$ doesn't have a nice formula, and is far from continuous. It is very large at some points and very small at just the next input. However, the average function

$$f(n) = \frac{d(1) + \cdots + d(n)}{n}$$

is more stable. Show that $\log n - 1 \leq f(n) \leq \log n + 1$. In other words, $f(n) = \Theta(\log n)$, i.e. it behaves like $\log n$.

P.g. 101 (Start the "Practice Problems" section on a new page.)

P.g. 105 For instance, the equation $x^2 + y^2 = 2$.

P.g. 106 So, two integers multiply to give 12.

P.g. 107 Of course the above is a variant of Simon's identity, however still very useful.

P.g. 108 (delete "of") So, the number of solution equals the number of divisors ~~of~~ d.

P.g. 108 Example 4.2.6 (INMO 1990/2)

P.g. 109 Clearly $(k, -k)$ always works, so suppose $x + y \neq 0$.

P.g. 109 Delete: Further, we rejected the possibility of $x + y = 0$ above. In fact, any $(k, -k)$ works too.

P.g. 110 $\frac{1}{2} \cdot \frac{2}{3} \cdots \frac{32}{33} \cdot \frac{34}{35} \cdots \frac{39}{40} \cdot \frac{66}{67} = \frac{17}{670} = \frac{51}{2010}$.

P.g. 110 Modular methods to restraint variables is often a complete solution, but often nothing more than one important step.

P.g. 112 (Delete "Of course" in last para)

P.g. 112 Other such unproved theorems written off by him were eventually proven, however this one was stuck harder in the path of mathematicians than others.

P.g. 114 So if $c + b = x^2, c - b = y^2$, then $c = (x^2 + y^2)/2$ and b= $(x^2 - y^2)/2$.

P.g. 114 thus $a = 2mn$, as desired.

P.g. 114 **!!!** (Add the following intro before the first example):

Infinite Descent is a technique that is used widely in all areas of mathematics. The idea is simple: Suppose x_0 satisfies a property P. Then you show that so does some other x_1, and repeat the process on x_1 to get another working x_2, and eventually you get an infinite chain

$$x_0 \to x_1 \to x_2 \to \dots$$

of numbers satisfying property P. The most common form of argument proceeds by showing $x_0 > x_1$, which then gives $x_1 > x_2$ and so on. If you can show that $x_i \in \mathbb{Z}$ always, and that only positive numbers satisfy P, then you have a contradiction. (why?)

There are many variants of the argument above, which basically induce an infinite chain and show that this must be impossible. At heart, an infinite descent argument can be translated into an argument involving the extremal principle (by saying pick the smallest x satisfying property P), however infinite descents are easier to motivate.

Let's try an example problem:

P.g. 114 If you have a sharp eye, you will observe that this is the same format as the equation before!

P.g. 115 The interesting part is, for each solution we can go to a new solution, and the new solution is "smaller" than the previous one.

P.g. 115 (16,4, 12)

P.g. 115 (delete "hence")

However, since each time we get a solution over non-negative integers, ~~hence~~ we can't go down forever!

P.g. 115 Clearly, however $S \geq 0$ so it can't go on decreasing forever.

The idea is that in each process we get closer to $(0, 0, 0)$, either from the left side or the right side. Using the monovariant $S = |x| + |y| + |z|$ is just a formalization of this intuition.

P.g. 115 **!!!** $a_i + a_{i+1} + a_{i+2} + a_{i+3} + a_{i+4} \equiv a_i - a_{i+1} + a_{i+2} - a_{i+3} + a_{i+4} = 0 \pmod 2$.

P.g. 115 Hence, for every i, (a_i, a_{i+5}) have the same parity.

P.g. 115 (Delete "so is")

So, Also, if $a - b + c - d + e = 0$, then ~~so is~~ $a/2 - b/2 + c/2 - d/2 + e/2 = 0$.

P.g. 116 **!!!** (Complete the following intro before the first example)

Vieta Jumping is a technique which is nothing but a derivative of infinite descent, albeit a useful one. Officially, this first spread in use after the IMO 1988, wherein the infamous IMO 1988/6 used this technique. Legend has it that the IMO jury couldn't solve the problem when they were presented with it, however some students did!

It is best understood by examples, so let's take a look, starting with the IMO 1988 problem itself:

P.g. 118 Then, if we have a lattice point $(x, y) \in \mathcal{H}$, then by Vieta the point $(ky - x, y)$ is also a lattice point on $\mathcal{H}$. Further, we can show that $ky - x < x$ and so the x coordinate is lower.

P.g. 118 In retrospect, we realize that we can shorten some of our work.

P.g. 118 If at this point, we have $x > b$, then we repeat everything we just did and get to (a, b) from (x, b), since a is the other root of the quadratic x forms.

P.g. 119 Then, once we show $x \leq a$ is a positive integer, so that (x, b) is also a valid pair, we say that $x + b < a + b$, which contradicts the minimality. From here on, we will use either descent or the extremal principle to phrase our argument, depending on which one is easier.

P.g. 120 !!! (Delete part in red) holds ~~unless $(a, b) = (2, 1)$ (why?). If $(a, b) = (2, 1)$, then $k = 6/2 = 3$, as desired. So suppose not~~

P.g. 127 !!! In Problem 4.9.1, change the equation to

$$x^2y + y^2z + z^2x = 3xyz.$$

P.g. 133 At the end of the day, solving some sort of equation is one of the key goals of a mathematician. That is what led them to discover $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. This is what we have done in the last chapter on modular arithmetic too. For instance, in solving the equation $ax - b \equiv 0 \pmod{p}$, we were led to the concept of inverses.

P.g. 133 One of the equations that led humanity to discover irrationals was $x^2 = 2$.

P.g. 134 Now let's consider the equation that led humans to discover the complex numbers: $x^2 = 1$.

P.g. 134 So, $x^2 \equiv -1 \pmod{5}$ has the solutions $x \equiv 2, 3$.

P.g. 135 $x^2 \equiv -1 \pmod{p} \implies (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.

P.g. 136 For instance, when $p = 5$, we have $1^2 \equiv 1, 4^2 \equiv 1 \pmod{5}$.

P.g. 136 Let me give you some better examples:

P.g. 138 Then $2^{2^n} \equiv -1 \pmod{p}$, which shows $2^{2^{n+1}} \equiv 1 \pmod{p}$.

P.g. 138 Suppose $\text{ord}_p(2) = 2^k$ with $k \leq n$.

P.g. 139 Primitive roots "generate" all residues and give us a better control over them in many scenarios. Let's see them in action now.

P.g. 140 (Delete the following line):
~~Also, this is an important result so remember this.~~

P.g. 142 !!! (Add the line in red:)
Clearly if m were a prime, then the above would imply $m|(x - 1)$ or $m|(x + 1)$, the former being the one we would want. However, m can't be a prime (why?), so we must try something else. We have a complete characterization of when a primitive root exists, so why not use that?

P.g. 143 (In Lemma 5.8.1)

$$x \mid y^z + 1.$$

P.g. 143 (and nothing more, so this condition is useless now, i.e. we can't extract any more information from here).

P.g. 144 This problem, just like the previous one, is tricky despite having a simple solution.

P.g. 147 Problem 5.9.2 Show that any odd prime factor q of $p^p - 1$ is $\equiv 1 \pmod{p}$.

P.g. 150 Here's the reason: go back and take a look at the proof we had given while discussing this originally in Example 2.12.3.

P.g. 151 Write $n = 231_{(5)}$ and $m = 23_{(5)}$.

P.g. 151 (Delete "Doing this, we would get" and replace by:)
Comparing the coefficient of X^{66} on the LHS and RHS then gives

P.g. 153 Let $f \in \mathbb{F}_p[X]$ have m distinct roots

P.g. 154 !!! If $m = 1$, then we are done.

P.g. 154 (since we assumed roots to be distinct.)

P.g. 154 Consider the following three polynomials:

P.g. 154 $g(x) = x^2 - 5x \in (\mathbb{Z}/6\mathbb{Z})[X]$

P.g. 154 So the degree of $h(x)$ above, for example, is not defined (since it is the zero polynomial).

P.g. 155 !!! (Change last line of proof of Lagrange's Theorem)
However, this is impossible as $g(x_{k+1}) \neq 0$ (why?). Hence we are done.

P.g. 157 then we can write any integer n as

$$n = \prod_{i \geq 0} p_i^{\nu_{p_i}(n)} = p_1^{\nu_{p_1}(n)} p_2^{\nu_{p_2}(n)} \dots$$

P.g. 157 Let's now present one property which is going to be themost important result related to ν_p :

P.g. 157 The idea is to use ν_p to remove the divisibility relation.

P.g. 158 (Delete "Conclude" in (b))

P.g. 158 (Delete "We can similarly get $\nu_p(x \div y) = m - n$.")

P.g. 158 To overcome this, we generalize p-adic valuation:

P.g. 159 So it is possible the $(a + b)$ term also contributes a power of p, and so we might have $\nu_p(x + y) > \min\{\nu_p(x), \nu_p(y)\}$. Hence in general we have the following lemma:

P.g. 159 We have said "equality holds if" not "if and only if".

P.g. 160 **!!!** (In the Proof of Example 6.1.1)

$$b = p^{xn+y}\ell, \quad 1 \leq y \leq n - 1.$$

P.g. 162 and we are done. (Recall Problem 3.5.2)

P.g. 162 But this is clear (for instance by assuming without loss of generality that $x \geq y \geq z$).

P.g. 164 $\nu_3(4^3 - 1) = \nu_3(63) = \nu_3(3^2 \times 7) = 2$.

P.g. 164 Instead of actually calculating the value of $4^{27} - 1$,

P.g. 166 **!!!** Prove that for any natural n,

$$\nu_3(2^{3^n} + 1) = n+1.$$

P.g. 166 **!!!** (LTE for addition) Let $p > 2$ be a prime and $a, b \in \mathbb{Z}$ be coprime to p such that $p \mid a+b$.

P.g. 167 "Clearly, a = 1 works since then $4(1n + 1) = 8$ for all n, which is a cube. Now, we will show this is the only possibility." The proof we gave follows after this. Don't miss this "obvious" statement and lose marks!

P.g. 169 Example 6.6.1 (Paul Erdös)

P.g. 170 **!!!** If $\nu_p(x) = y$, think of x as p^y, not as cp^y.

P.g. 170 **!!!** In this case, if $\nu_p(a^x + b^y + c^z) \geq 0$, we must have that $\nu_p(b^y) = \nu_p(c^z)$

P.g. 170 **!!!** Hence, $y\nu_p(b) = z\nu_p(c)$. If $\gcd(y, z) = d$ and $y = y^*d, z = z^*d$, then we must have $\nu_p(b) = kz^*$ and $\nu_p(c) = ky^*$ for some k. Hence,

$$\nu_p(a) = -(\nu_p(b) + \nu_p(c)) = -k(z^* + y^*).$$

Hence $\nu_p(a)$ is always divisible by $(z^* + y^*) > 1$, which is independent of p.

P.g. 172 Delete Problem 6.7.3 and Problem 6.7.5.

P.g. 174 China TST 2 2016/4

P.g. 176 The proof dwells a lot upon many properties of Cyclotomic Polynomials, a topic we avoid in this book.

P.g. 177 Then $p \nmid 2^n - 1$, so $p|2^n + 1$.

P.g. 179 If you want to know the reason really bad, then it's because $\mathbb{N}$ is not a "commutative ring" (A "structure" from abstract algebra. So ignore if you haven't heard this before), while $\mathbf{R}[X]$ is defined for commutative rings $\mathbf{R}$.

P.g. 180 It, however, is incredibly useful, and finds applications outside maths too. For instance:

P.g. 181 $F(X) = G(X)Q(X) + R(X)$,

P.g. 181 we can't divide by a non-zero integer and always expect to get an integer.

This property of rationals is also seen in $\mathbb{F}_p$; if we divide two non-zero elements of $\mathbb{F}_p$, we still get an element in $\mathbb{F}_p$. Thus, Euclid's Division Lemma also holds true in $\mathbb{F}_p[X]$. This was used in the special section of the chapter Modular Arithmetic Advanced.

P.g. 182 Well, we can also say it is $2(x^2 + 2)$ since each constant divides a polynomial in $\mathbb{Q}[X]$.

P.g. 182 $\gcd(F(x), G(x)) = \gcd(R(x), G(x))$.

P.g. 183 **!!!** (Add question:)

Show that if $P(q) = 0$ for a reduced rational q and $P \in \mathbb{Z}[X]$, then the denominator of q must divide the leading coefficient of $P(x)$. (This is also a part of the rational root theorem)

P.g. 184 **!!!** hence this polynomial is reducible over $\mathbb{R}[X]$. Also note the non-units part. So $5x^2 - 10 = 5(x^2 - 2)$ is still considered irreducible in $\mathbf{R}[X]$ (unless $\mathbf{R} = \mathbb{Z}$).

P.g. 185 Also, $(x-z)(x-\bar{z}) = x^2 - (z+\bar{z}) + z\bar{z} = x^2 - 2\Re(z)x + |z|^2 \in \mathbb{R}[X]$.

P.g. 185 **!!!** Theorem 7.1.8 (Fundamental Theorem of Algebra). Every polynomial of degree at least 3 in $\mathbb{R}[X]$ is reducible into linear and quadratic factors in $\mathbb{R}[X]$.

P.g. 185 Now since at least one of c_1, c_2 is greater than 1 (why?), hence there is a prime p dividing c_1c_2.

P.g. 185 **!!!** (Add the following line at the end)
Compare the coefficients of x^{n+m} in $(c_1c_2)f = (c_1g)(c_2h)$. On the left side, it is k_{n+m} (which is divisible by p), while on the right side it is a_nb_m. So $p \mid a_n$ or $p \mid b_m$, say the former.

P.g. 186 **!!!** So pick the largest $0 \le i \le n$ and $0 \le j \le m$ such that $p \nmid a_i, b_j$.

P.g. 186 So, identical polynomials means "exactly the same", i.e. carbon copies. The important point in the definition is that it says the coefficients are same, and says nothing about the values. We say that they are formally" equal ("formal" in context of polynomial is used for coefficients)

P.g. 187 Each term serves as an "indicator term"

P.g. 187 **!!!** $P(x) = 2 \cdot \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 3 \cdot \frac{(x-3)(x-4)(x-1)}{(2-3)(2-4)(2-1)} + 4 \cdot \frac{(x-4)(x-1)(x-2)}{(3-4)(3-1)(3-2)} + 5 \cdot \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}$.

P.g. 188 **!!!** $P(2) = 0 + 3 \cdot \frac{(2-3)(2-4)(2-1)}{(2-3)(2-4)(2-1)} + 0 + 0 = 3$.

P.g. 188 It can be viewed as a generalization of the facts that two points uniquely determine a straight line, and intuitively follows since a degree n polynomial has $n+1$ coefficients, and hence $n+1$ degrees of freedom.

P.g. 191 Comment 7.3.1: Alternatively, since $a \equiv b \pmod{(a-b)}$, hence

$$P(a) = c_na^n + c_{n-1}a^{n-1} + \cdots + c_0 \equiv c_nb^n + c_{n-1}b^{n-1} + \cdots + c_0 = P(b) \pmod{(a-b)}.$$

P.g. 191 In Lemma 7.3.2, $P(m) \equiv P(n) \pmod{a}$.

P.g. 191 But then $a - b = |a-b| = |c-a| = a - c$ implies $b = c$, and hence $c = P(b) = P(c) = a$ too. Thus $a = b = c$, contradicting the fact that a, b, c were distinct.

P.g. 192 Comment 7.3.2: Once we took a prime $p \mid f(2^t)$,

P.g. 192 We basically used the periodic property to add a "degree of freedom", which is always very helpful.

P.g. 192 **!!!** Definition 7.4.2. For any polynomial $p \in \mathbb{Z}[X]$, the set of primes dividing some element of $\mathcal{F}(p)$ is denoted by $\mathfrak{P}(p)$ and call it the prime set of p. So $\mathfrak{P}(p) = \{q : q \text{ prime}, q \mid p(n) \text{ for some } n \in \mathbb{Z}\}$.

P.g. 193 Example 7.4.2 For which polynomials $f \in \mathbb{Z}[X]$ does $\{f(0), f(1), \ldots, f(p-1)\}$ form a complete residue class modulo p for all sufficiently large primes p?

P.g. 193 **!!!** So define the polynomial $g(x) = \frac{f(x)}{x} \in \mathbb{Z}[X]$ and note that g satisfies the same hypothesis as f so we can repeat the argument on g.

P.g. 194 The proof is a fun application of the periodicity lemma that I leave as an exercise

P.g. 202 (Add bullets to problem)
Problem 7.7.17 (2020 Korean MO winter camp Test 1 P3). Find all integer coefficient polynomials Q such that

- $Q(n) \ge 1 \ \forall n \in \mathbb{Z}_+$.
- $Q(mn)$ and $Q(m)Q(n)$ have the same number of prime divisors for all $m, n \in \mathbb{Z}_+$

P.g. 203 not "the number"

P.g. 204 Remember how we talked about the "defining polynomial"

P.g. 204 To avoid this dumb situation, we keep the "defining" polynomial monic

P.g. 204 The answer to the question is explained by our intuition of the "smallest defining polynomial". So the reason is: consider $f(x) = x - \sqrt{2}$. This does not have integer coefficients.

P.g. 206 (Delete "in Olympiads":)
There are two main properties that make these very useful ~~in Olympiads~~

P.g. 208 It is now easy to see that this happens if and only if $a_0 = \cdots = a_{p-1}$, as desired.

P.g. 209 **!!!** (Add proof of Kronecker's Theorem)

P.g. 212 Problem 8.1.2. Show that the product of quadratic residues mod p is -1 if $p \equiv 1 \pmod 4$ and $+1$ otherwise.

P.g. 213 **!!!** (note here that we are dealing with non-zero quadratic residues)

P.g. 213 since the "same category idea" is everywhere

P.g. 214 Using the Legendre's symbol, we basically have converted the English question "is x a quadratic residue" to a mathematical expression.

P.g. 214 !!! Prove that for a prime $p > 3$, the smallest quadratic nonresidue is smaller than $\sqrt{p}+1$.

P.g. 214 !!! The idea is simple, pick the smallest quadratic nonresidue r, and try to show $r < \sqrt{p}$ (we only consider $\sqrt{p}$ instead of $\sqrt{p}+1$ for now).

P.g. 215 !!! If we try to mend this idea, we look at numbers of the form $r, 2r, \ldots, (r-1)r, r^2$.

$\vdots$

Hence, we get $p + r > ra > p$. Hence, $ra \mod p$ lies in $\{1, 2, \ldots, r-1\}$, which means it must be a QR, a contradiction (if $a \neq r$)!

However, if $a = r$, then $p + r > r^2$ implies $r < \frac{1}{2}\left(\sqrt{4p+1}+1\right) < \sqrt{p}+1$, and so we are done in this case too.

P.g. 215 "crosses" p

P.g. 215 We will see a generalization of this result in the chapter "Constructions."

P.g. 215 Explain the significance of "reciprocity" in the theorem's name.

P.g. 216 It is given as an exercise problem (with solution) in the chapter "Constructions".

P.g. 217 (Latex error) $(-1)^{\frac{5-1}{2}} \cdot (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}} \left(\frac{5}{3}\right)$

P.g. 218 Just recall that $\{an + b\}$ forms a complete residue class mod p if $\gcd(a, p) = 1$. So

P.g. 218 We need a more general method. So let's try to find one.

P.g. 220 !!! Corollary 8.4.1. Let p be an odd prime and a, b be integers both coprime to p. Then

$$\sum_{i=0}^{p} \left(\frac{an^2 + b}{p}\right) = -\left(\frac{a}{p}\right).$$

P.g. 220 Problem 8.5.1. Use the method from Example 8.1.1 to show that $x^2 + y^2 - 1 \equiv 0 \pmod{p}$ always has a solution $x, y \in \mathbb{F}_p$.

P.g. 223 Clearly we can assume that $\gcd(x, y, z) = 1$.

P.g. 224 !!! In particular, $5^m - 1$ is square free for primes > 2 (why?)

P.g. 237 !!!

$$\begin{array}{cccc} 0^0 & 1^1 & \ldots & (p-1)^0 \\ p^1 & (p+1)^2 & \ldots & (2p-1)^1 \\ (2p)^2 & (2p+1)^3 & \ldots & (3p-1)^2 \\ (3p)^3 & (3p+1)^4 & \ldots & (4p-1)^3 \\ \vdots & \vdots & \ddots & \vdots \end{array}$$

Also, the numbers with exponent 1 in the list are $p^1, (2p-1)^1, (3p-2)^1, \ldots$

P.g. 255 is the trivial solution $a_1 = a_2 = \cdots = a_n = 0$.

P.g. 256 The numbers $\{1, i\}$ are independent, and so are $\{1, \sqrt{3}\}$. Here's an exercise: Show that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ are independent.

P.g. 256 The classic proof of that is the "reductio-ad absurdum" method.

P.g. 257 Since surds modulo p keep changing ~~on changing p~~, there is no direct way to do this.

P.g. 257 !!! Add conjuagte lemma to explain properly: "Also, the other roots of $P(x)$ (the conjugates of B) are also integer mod p by the lemma"

P.g. 259 Show that $n = |\mathcal{S}_p| = 1$.

P.g. 266 !!! Fix $i < j$. How many values of k satisfy $a_i + ki \equiv a_j + kj \pmod{p}$?

P.g. 269 279. Write $d = \gcd(xy + 1, xy + x + 2) = \gcd(x + 1, y - 1)$ so that $xy + 1 = du^2, xy + x + 2 = dv^2, x + 1 = da, y - 1 = db$.

P.g. 270 320. If $p \mid q - 1$, try to find a suitable a such that $x^{-1} + 1 \equiv a \pmod{q}$ gives the result.

P.g. 272 (change variable α to avoid confusion) 377. Write $p + m - 1 = p^\beta$ and use $p^\beta + m - 1 \mid n$.

P.g. 280 Let $s = 2^\alpha 5^\beta \gamma$, where γ is coprime to 10.

P.g. 281 So $z_1^n \equiv z_2^n \equiv x \pmod{p}$ and $z_1^n \equiv z_2^n \equiv y \pmod{p}$.

P.g. 282 Since $n < p$, hence $p \nmid n$ meaning that the right side of the above expression is non-zero, and hence $x_1 + \cdots + x_n \not\equiv 0 \pmod{p}$. Now the above holds for *all* $a \in \mathcal{S}_p$, which is impossible since $a \equiv -n \cdot (x_1 + \cdots + x_n)^{-1}+1 \pmod{p}$ is unique.

P.g. 283 ~~(Outline of a more Number Theoretic Approach)~~ The above was, in heart, a combinatorial solution. However, we can use number-theoretic esti- mates too.

P.g. 284 **!!!** However, we know $\varphi(n) \geq \sqrt{n}$ for $n \neq 2, 6$. Now linear growth is faster than logarithmic growth. Hence $c(\log n)^2 < \sqrt{n}$ for large enough n, and we have our contradiction.

P.g. 286 Solution 4.9.9 (EGMO 2013/4)

P.g. 289 If $k = 4$, then $(x, y) = (1, 1)$ works and we get

P.g. 293 China TST 2 2016/4

P.g. 295 **!!!** ... we find

$$\begin{aligned} n\nu_p(a_{n+1}) &\leq n\nu_p(C) + \nu_p(a_1) + \nu_p(a_2) + \cdots + \nu_p(a_n) \\ &\leq n\nu_p(C) + \nu_p(a_1) + (\nu_p(a_1) + \mathbb{H}_1\nu_p(C)) + \cdots + (\nu_p(a_1) + \mathbb{H}_{n-1}\nu_p(C)) \\ &= n\nu_p(a_1) + (n + \mathbb{H}_1 + \cdots + \mathbb{H}_{n-1})\,\nu_p(C). \end{aligned}$$

and hence

$$\begin{aligned} \nu_p(a_{n+1}) - \nu_p(a_1) &\leq \frac{1}{n}\left(n + \left(\frac{1}{1}\right) + \cdots + \left(\frac{1}{1} + \cdots + \frac{1}{n-1}\right)\right)\nu_p(C) \\ &= \frac{1}{n}\left(\left(1 + \underbrace{\frac{1}{2} + \frac{1}{2}}_{2} + \cdots + \underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{n}\right) + \left(\frac{1}{1}\right) + \cdots + \left(\frac{1}{1} + \cdots + \frac{1}{n-1}\right)\right)\nu_p(C) \\ &= \frac{1}{n}\left(n \cdot \frac{1}{1} + n \cdot \frac{1}{2} + \cdots + n \cdot \frac{1}{n}\right)\nu_p(C) = \mathbb{H}_n\nu_p(C). \end{aligned}$$

P.g. 298 **!!!** But $R(m^{c-2} \cdot m)$ and $R(m^{c-2})R(m)$ have the same prime divisors, and since $R(m^{c-2}) > 1$, hence $R(m^{c-1})$ has at least as many prime divisors as $R(m)$. So, $R(m^{c-1})$ and $R(m)$ have the same divisors.

So from every $R(m^{2^k})$ we can induct down to prove the claim.

P.g. 299 Clearly we just have to show that 3 is a quadratic nonresidue.