Chapter 1

Divisibility

1.1 Definitions and Propositions

Let us start by defining *remainder*.

Definition 1.1. When an integer b is divided by another integer a, we can write $b = aq + r$ where q can be any integer. In this case, r is called the *remainder* of the division.

However, if we choose q such that $0 \leq r < |b|$, then r is called the *minimum remainder*.

At times, it is convenient to carry out the division so that b is as close as possible to an integral multiple of a. Then we can write $b = aq + r$, with $|r| \leq |\frac{b}{2}|$ for some integer q. In this case, r is called the *minimum absolute remainder*.

Here, note that, if b is odd, we will have a unique r. But if b and a both are even, there can be two possible cases for r. For example, if $b = 20$ and $a = 8$ then $20 = 8 \cdot 2 + 4$ and $20 = 3 \cdot 8 - 4$. In both cases, $|r| = 4$. To force r to be unique in this case, we will take the r with $r > 0$. Therefore, $20 = 2 \cdot 8 + 4$ would be accepted as the minimum absolute remainder.

Unless we state it explicitly, by remainder we will mean minimum remainder since it is unique, which we will prove later.

Now, if we divide 4 by 2, we get a remainder 0. In this case, we say that 4 is *divisible* by 2 and write it as $2|4$.

Definition 1.2. Let a and b be two integers. If b leaves a remainder 0 upon division by a, or equivalently, if there is an integer k for which $b = ak$, we write $a|b$ [1] and say that

- b is *divisible* by a,
- a *divides* b,
- a is a *divisor* (or a *factor*) of b,

[1] Some authors and problem setters use the notation $b \vdots a$ instead of $a|b$, but it is not as common.

- b is a *multiple* of a.

Likewise, $a \nmid b$ denotes that b is not divisible by a.

The number a is called a *proper divisor* of b if $|a| < |b|$ [2].

Example. $4|20$ and $5|20$ but $11 \nmid 20$.

Again, 1 is a divisor of any positive integer.

Take $23 = 5 \cdot 2 + 13$, so we can say 13 is a remainder of 23 upon division by 5 but not a minimum remainder. If we write it as $23 = 5 \cdot 4 + 3$, then 3 is the minimum remainder. And if we write it as $23 = 5 \cdot 5 + (-2)$ then -2 is the minimum absolute remainder.

You can also try to make sense of it this way: 8 divides 40 because 40 has every factor that 8 has in it. In other words, if 8 had a factor which was not a factor of 40, 40 would not be divisible by 8. For example, 42 does not have the factor 4, which is a factor of 8, therefore $8 \nmid 42$. Now, see that if we divide 20 by 4, we get a *quotient* 5, i.e., $\frac{20}{4} = 5$. So, whenever $a|b$ for integers a, b, we have $\frac{b}{a} = k$ where k will be some integer. If $a \nmid b$, then k will not be an integer.

We will define primes and composite numbers now.

Definition 1.3 (Prime and Composite Numbers). An integer $n > 1$ is called *prime* if it has exactly two distinct divisors – 1 and n itself. A number greater than 1 which is not a prime is *composite*. In other words, an integer n is composite if a positive integer greater than 1 and smaller than n divides n.

Note. When we say a is a divisor of b, unless otherwise stated, we usually mean a is a positive divisor of b. This is distinguished because negative divisors exist as well.

1 is neither prime nor composite. Actually, the above definition for primes and composite numbers applies only for *positive* integers – negative numbers are not included in this definition.

The following example clarifies the definition of primes and composite numbers.

Example. 11 is a prime because no positive integer greater than 1 and less than 11 divides it. Similarly $2, 3, 29$ are primes but 169 (divisible by 13) or 1001 (why?) are composites. 2 is the only even prime (why?).

Definition 1.4 (Parity). Parity is the property of an integer being *even* or *odd*. An even number is defined as the integers divisible by 2 and an odd number are the ones which are not.

Example. 2 and 4 have the same parity, they are both even. 5 and 10 are of different parity, 5 is odd and 10 is even.

The following note is seemingly obvious, but it is useful in many cases when solving a number theory problem.

[2] $|a|$ is the value of a i.e. $|-5| = 5$ and $|5| = 5$

Note. If we add or subtract two numbers of the same parity, the result is even. Conversely, the result of addition or subtraction of two numbers with different parity is always an odd number. Using these two facts, you can easily find many properties of integers related to parity. For instance, we can say that if we add or subtract an even number to or from a positive integer n, the parity does not change; i.e., parity remains *invariant*. Moreover, any odd multiple of n has the same parity as n. Another example is that if you raise an integer to a power, its parity does not change.

We usually deal only with positive integers in divisibility relations. However, sometimes negative integers or zero also come into play.

The following propositions are the basic facts related to divisibility. Many readers may find them trivial but we provide an outline of a proof so that early problem solvers have an idea about how intuition works when trying to prove something in number theory.

Proposition 1.1 (Basic Properties of Divisibility). *Let a, b, and c be three integers. Then*

1. *$a|0$.*
2. *$a|a$.*
3. *$1|a$ and $-1|a$.*
4. *If $0|a$, then $a = 0$.*
5. *If $a|b$, then $a|-b$, $-a|b$, and $-a|-b$.*
6. *If $a|b$, then $a|bk$ for all integers k.*
7. *If $a|b$, then $ak|bk$ for all integers k.*
8. *If $ak|bk$ for some non-zero integer k, then $a|b$.*
9. *If $a|b$ and $b|c$, then $a|c$.*

   Keith Conrad states this as a mantra: A factor of a factor is a factor.
10. *If $a|b$ and b is non-zero, then $|b| \geq |a|$. In other words, if $a|b$ and $|a| > |b|$, then we have $b = 0$.*
11. *If $a|b$, then $a^n|b^n$ for all non-negative integers n.*
12. *If $a^n|b^n$ for some positive integer n, then $a|b$.*

Most of these properties are trivial and we do not provide proofs for them. However, they come handy in many situations so we suggest you to keep them in the back of your mind. Here, we prove the rest of the given properties.

Proof.

Part 4. $0|a$ means that $a = 0k$ for some integer k. So $a = 0$.

Part 6. $a|b$ means that $b = aq$ for some q. Multiply both sides of this equation by k to get $bk = akq = aq'$. Therefore $a|bk$.

Part 9. $a|b$ and $b|c$, so $b = aq_1$ and $c = bq_2$ for some integers q_1, q_2. Combine these two equations to get $c = aq_1q_2 = aq$ and thus $a|c$.

Part 10. $a|b$, so $b = ak$ for some integer k. Rewrite this equation in absolute value terms: $|b| = |ak| = |a| \cdot |k|$. Since k is a non-zero integer, the smallest value for $|k|$ is 1, so $|b| = |a| \cdot |k| \geq |a|$.

Part 12. A proof will be explained later in Section (1.4).

□

The next property is pretty important, and so we express it in a separate proposition.

Proposition 1.2. *If $a|b$ and $b|a$, then $|a| = |b|$ or $a = \pm b$.*

Proof. The proof is quite simple using part 10 of the previous propositions. Namely, we get $|b| \geq |a|$ and $|a| \geq |b|$, which means $|a| = |b|$ or $a = \pm b$.

□

The idea behind this proposition comes handy when you want to prove that two expressions are equal. If you can show that both of the expressions divide the other one, along with both of them are positive, you can directly imply they are equal.

Proposition 1.3. *For fixed positive integers a and b, there are unique integers q and r so that $b = aq + r$ with $0 \leq r < a$. In other words, minimum remainder is unique.*

Proof. Ruling out the case $r = 0$ is easy: just notice that $a|b$.

In other case, $a \nmid b$, so b must have a nonzero remainder upon division by a, say r. Now, how do we prove that this r indeed is unique? Though this is obvious, here is a rigorous proof. Assume to the contrary that, there are q', r' so that,

$$b = aq + r = aq' + r'$$

This implies $a(q - q') = r' - r$, which shows that $r' - r$ is divisible by a. Is it possible? The answer is clearly no. Because r' and r both are less than a, hence $|r' - r| < a$. Thus, we must have $|r' - r| = 0$ i.e. $r' = r$. This means two remainders must be same, that is this remainder is unique, so is the quotient.

□

Now, take the following two divisibilities: $4|20$ and $4|16$; do we have $4|20 + 16$?

Proposition 1.4. *If $a|b$ and $a|c$ then $a|bx + cy$ where x, y are arbitrary integers. Specially, $a|b \pm ak, a|b + c, a|b - c$ are useful.*

Proof. Since $a|b$, we can say there is an integer k so that $b = ak$. Similarly, there is an integer l so that $c = al$. Therefore,

$$bx + cy = akx + aly = a(kx + ly),$$

which is certainly divisible by a since it has a factor a in it, multiplied by $kx + ly$, which is an integer.

□

Note. Here, x and y can be negative integers as well. That's how negative integers may come into play even when we start off with positive integers.

If you have reached this point, congratulations! You have learned important theorems in divisibility by now. We will provide some propositions about prime numbers in the following.

Proposition 1.5. *If n is an integer greater than 1, then it has a prime divisor.*

Proof. If n itself is a prime, we are done. So, assume it is not. Since in this case n is composite, it has a proper divisor, i.e., there is an integer greater than 1 and less than n which divides n. Let's call this divisor d. Now, if d is not a prime, then d has a divisor too. We can continue like this until we reach a point where d does not have a proper divisor greater than 1. We know, by definition, that only a prime number does not have a proper divisor other than 1. Therefore, that divisor must be a prime.

□

This proposition forces the following:

Corollary 1.1. *If n is a positive integer, then the smallest divisor of n is a prime if and only if $n > 1$.*

The next proposition is called the Euclid's lemma.

Proposition 1.6 (Euclid's Lemma). *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

You should be able to prove it yourself by now.

Proposition 1.7. *Every composite n has a prime factor less than or equal to $\sqrt{n}$.*

Proof. Since n is composite, it has a prime factor. Now, *consider the smallest prime factor p of n* and write $n = pk$. Of course $p \leq k$, because otherwise according to Corollary (1.1), the smallest prime factor would be k or some of its divisors. So,

$$n = pk \geq p^2$$

which in turn implies $p \leq \sqrt{n}$, which proves our claim.

□

This proposition is quite useful to test if a number is prime or not. It implies that we just have to check if n is divisible by any of the primes less than or equal to $\sqrt{n}$. If it is, then it is not a prime. Check this with some simulations by hand, say for $11, 25, 479$. But the test can be quite lengthy and tedious if n is too large and its smallest prime factor is really large. If you want to test your patience or just curious how lengthy this test can be, take the number 357879581 and try finding its smallest prime divisor. Just don't curse us in the process. ☻

Definition 1.5 (Prime Factorization). Prime factorization is the process of finding all the prime factors of a positive integer, if it has any.

Every positive integer greater than 1 has a prime factorization, which gives birth to a very important theorem.

Finally, we state the *Fundamental Theorem of Arithmetic*.

Theorem 1.1 (Fundamental Theorem of Arithmetic). *Every positive integer n can be written as a product of primes in a unique way. We write this factorization as:*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{1.1}$$

where $p_1, p_2, \ldots p_k$ are different primes and $e_1, e_2, \cdots e_k$ are their powers. Using product notation, we can write equation (1.1) as:

$$n = \prod_{i=1}^{k} p_i^{e_i} = \prod_{p|n} p^e$$

where p runs through different primes dividing n and e is the maximum power of p that divides n.[3]

Example. Try to understand the following examples and match them with the factorization representation. $12 = 2^2 \cdot 3$ (here $p_1 = 2, e_1 = 2, p_2 = 3, e_2 = 1$ and $k = 2$) and $180 = 2^2 \cdot 3^2 \cdot 5$ ($p_1 = 2, e_1 = 2, p_2 = 3, e_2 = 2, p_3 = 5, e_3 = 1$). This representation is unique for $n > 1$ no matter in what order you factor out the primes. Also, note that all the powers are positive. We could bring primes with power 0 but that doesn't change the product, so we avoid it for simplicity. To find this factorization of any number, just keep dividing that number by any prime factor if it has one. Also, try to gain a perspective of how this is used in solving problems, even though we will show how it comes into the play later.

Note. In the product $n = \prod_{i=1}^{k} p_i^{e_i}$, k is the number of distinct prime factors of n. For example, for $n = 12$, $k = 2$ since 12 has only two distinct prime factors 2 and 3. If $n = 180$, then $k = 3$ since n has three prime factors $2, 3, 5$. But how do we prove that this factorization must be unique if we do not consider order of primes? Think the opposite: what if the factorization is not unique? And try to find a contradiction.

As explained above, one way to factorize a number n is to divide it by all primes less than $\sqrt{n}$. Dividing a number by another would be pretty boring for large numbers. In order to simplify the process, next section provides some rules for divisibility by some specific numbers like $3, 5, 7, 11$, etc. You may already have come across some of these rules.

1.1.1. Divisibility By Certain Numbers

Here we provide some divisibility criteria without proof. You should try and see if you can to prove them. In the following, by *last digit*, we mean the rightmost digit.

Divisibility by 2. A number is divisible by 2 if and only if its last digit is even (one of $0, 2, 4, 6, 8$).

[3] Make sure you understand the notations $\sum$ and $\prod$ well.

Divisibility by 3. A number is divisible by 3 if and only if the sum of digits of the number is divisible by 3.

Example. Take the number 951 which has a sum of digits $9+5+1 = 15$, divisible by 3. According to our claim, 951 should be divisible by 3 and indeed it is: $951 = 3 \cdot 317$.

Divisibility by 4. A number is divisible by 4 if and only if the number formed by its last two digits is divisible by 4.

Example. 2023902348 has the last two digits 4 and 8 which make the number formed by its last two digits 48. Since 48 is divisible by 4, the number 2023902348 is divisible by 4.

Divisibility by 5. A number is divisible by 5 if and only if it has 0 or 5 as last digit.

Divisibility by 6. A number is divisible by 6 if and only if it is even and divisible by 3 (why?).

Divisibility by 7. A number is divisible by 7 if and only if the difference of the number formed by the last three digits and the rest of digits is divisible by 7.

Example. Take the number 13111. To see if it is divisible by 7 or not, first separate the number into two parts: Form a number with last three digits and another with the other part. In this case, we have 111 and 13. Their difference is 98, which is divisible by 7. According to the rule of divisibility by 7, this number is divisible by 7.

Divisibility by 8. A number is divisible by 8 if and only if the number formed by its last three digits is divisible by 8.

Divisibility by 9. A number is divisible by 9 if and only if the sum of its digits is divisible by 9.

If you have a curious mind, you should already notice a pattern in the divisibility rules for $2, 4$, and 8. For 2, we only check the last digit. For 4, we check the last two digits and for 8, the last three digits. Do you see the pattern now? $2 = 2^1, 4 = 2^2$ and $8 = 2^3$. You can easily check that the same is true if we take $16 = 2^4$. Then it's enough to test the number formed by last 4 digits. We can generalize this result for 2^k.

Proposition 1.8 (Divisibility by 2^k). *A number is divisible by 2^k if and only if the number formed by the last k digits is divisible by 2^k.*

Hint. To prove this one, let the number be $x = \overline{x_n x_{n-1} \dots x_k x_{k-1} \dots x_2 x_1}$, where $x_1, x_2, \dots x_n$ are its digits. Note that

$$\begin{aligned} x &= \overline{x_n x_{n-1} \dots x_{k+1} \underbrace{000 \dots 0}_{k \text{ times}}} + \overline{x_k x_{k-1} \dots x_2 x_1} \\ &= 10^k \cdot \overline{x_n x_{n-1} \dots x_{k+1}} + \overline{x_k x_{k-1} \dots x_2 x_1}. \end{aligned}$$

Divisibility by 11. A number is divisible by 11 if and only if the difference of sums of alternating digits is divisible by 11.

Example. Take 12047816. The sum of digits in even places is $2+4+8+6=20$ and sum of digits in odd places $1+0+7+1=9$. Their difference is $20-9=11$, which is divisible by 11. The number $12047816 = 11 \cdot 1095256$ indeed is divisible by 11.

Divisibility by 13. A number is divisible by 13 if and only if the result of addition of four times the last digit and the the number formed by rest of the digits is divisible by 13.

Example.

$$\begin{aligned} 8658 &\implies 865 + 4 \cdot 8 = 897 \\ 897 &\implies 89 + 4 \cdot 7 = 117 \\ 117 &\implies 11 + 4 \cdot 7 = 39. \end{aligned}$$

And $39 = 13 \cdot 3$, so 858 is divisible by 13.

Divisibility by 17. A number is divisible by 17 if and only if the result of subtraction of five times the last digit from the number formed by rest of the digits is divisible by 17.

Example.

$$\begin{aligned} 11322 &\implies 1132 - 5 \cdot 2 = 1122 \\ 1122 &\implies 112 - 5 \cdot 2 = 102 \\ 102 &\implies 10 - 5 \cdot 2 = 0. \end{aligned}$$

So 11322 is divisible by 17.

Divisibility by 19. A number is divisible by 19 if and only if the result of addition of two times the last digit and the the number formed by rest of the digits is divisible by 19.

Example.

$$\begin{aligned} 12654 &\implies 1265 + 2 \cdot 4 = 1273 \\ 1273 &\implies 127 + 2 \cdot 3 = 133 \\ 133 &\implies 13 + 2 \cdot 3 = 19. \end{aligned}$$

Therefore 12654 is divisible by 19.

It would be an excellent exercise for you to prove them yourself. But you will probably need some more knowledge, and quite often this kind of facts can be proved with

1.2 GCD-LCM

Take two numbers 18 and 27 and consider all of their divisors. Now if you keep only the ones which show up in both lists and discard others, you should be left with $1, 3, 9$. 9 is the largest among these common divisors. We call it the *greatest common divisor* of 18 and 27. Let's do the opposite now. This time we take the multiples of 18 and 27. The list of multiples of 18 is $18, 36, 54, 72, 90, 108, \ldots$ and the list for 27 is $27, 54, 81, 108, \ldots$. The common multiples of 18 and 27 are $54, 108, \ldots$. But the smallest of them is 54, which we call the *least common multiple* of 18 and 27.

Definition 1.6 (GCD and LCM). For two integers a and b which are not zero at the same time, the greatest common divisor of a and b or simply $\gcd(a, b)$ is the greatest positive integer which divides both a and b. For brevity, we denote this by (a, b) in this book.

The least common multiple of a and b or shortly $\text{lcm}(a, b)$ is the smallest positive integer that is divisible by both a and b. Again, for brevity, we denote this by $[a, b]$ in this book.

The concept of gcd and lcm is the same for more than 2 integers. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is the largest positive integer which divides them all. We denote this by $(a_1, a_2, \ldots, a_n)$. We can define $[a_1, a_2, \ldots, a_n]$ in a similar way.

Example. $(18, 27) = 9$ and $[18, 27] = 54$.

Example. $(18, 27, 36) = 9$ and $[18, 27, 36] = 108$.

Note. The above definition of gcd is equivalent to the following: In order to show that (a, b) equals g, prove that d divides both a and b, and if there is a positive integer c for which $c|a$ and $c|b$, then $g \geq c$. The same approach can be used to find the lcm: In order to show that $[a, b]$ equals ℓ, prove that ℓ is divisible both a and b and then show that if there is a positive integer c for which $a|c$ and $b|c$, then $c \geq \ell$.

The the following proposition can be inferred from the definition.

Proposition 1.9 (GCD and LCM Properties). *Let a and b be two positive integers. The following statements are true:*

1. $(a, b) = (b, a) = (a, -b) = (-a, -b)$ *and* $[a, b] = [b, a] = [a, -b] = [-a, -b]$.
2. $(a, 0) = a$ *and* $[a, 0] = 0$, $(a, 1) = 1$ *and* $[a, 1] = a$.
3. $(a, a) = [a, a] = a$.
4. $[a, b] \geq (a, b)$.
5. $a|b$ *if and only if* $(a, b) = a$ *and* $[a, b] = b$.
6. *For any integer* k, $(a, b + ak) = (a, b)$ *and* $(ka, kb) = k(a, b)$. *Furthermore,* $[ka, kb] = k[a, b]$.
7. *For any non-negative integer* n, *we have* $(a^n, b^n) = ((a, b))^n$ *and* $[a^n, b^n] = ([a, b])^n$
8. *For any integers* x, y, *we have* $(a, b)|ax + by$.
9. *If* p *is a prime divisor of* a *or* b, *then* $p|[a, b]$.
10. *For any prime divisor* p *of* (a, b), *we have* $p|a$ *and* $p|b$.
11. *If* p *is a prime, then*

$$(a, p) = \begin{cases} p, & \text{if } p|a \\ 1, & \text{otherwise} \end{cases}$$

The proof for all parts is pretty easy, so try them yourself. We only provide a hint for part 4: use part 10 of Proposition (1.1).

We are now able to prove part 12 of Theorem (1.1).

Example. Assume that $a^n|b^n$ for some positive integer n. Then by part 5 of Proposition (1.9), we have $(a^n, b^n) = a^n$. Let $g = (a, b)$, and so $g^n = (a^n, b^n)$. This means that $(a^n, b^n) = a^n = g^n$, and therefore $a = g = (a, b)$. Using the same part of Proposition (1.9), we get $a|b$. The proof is complete.

The following proposition is the stronger version of the note mentioned after the definition of gcd and lcm, which is indeed very useful.

Proposition 1.10. *For positive integers a, b, and c, if $c|a$ and $c|b$, then $c|(a, b)$. Analogously, if $a|c$ and $b|c$ then $[a, b]|c$.*

A common mistake is that if $a|n$ and $b|n$, then we have $ab|n$, which is wrong. Try to find some counterexamples to see why.

Definition 1.7. Two positive integers are *co-prime* or *relatively prime to each other* if their greatest common divisor is 1. We shall use $a \perp b$ to denote that $(a, b) = 1$, i.e., a and b are co-prime.

Example. $3 \perp 4$, but $4 \not\perp 6$ since 2 divides both 4 and 6.

The following proposition explains some theorems related to co-prime integers. Try to prove them as an exercise.

Proposition 1.11. *Let a, b and c be three integers. Then*

1. *If $a \perp b$, $a|c$ and $b|c$, then $ab|c$.*
2. *If $a \perp b$ and $a|bc$, then $a|c$.*
3. *If $a \perp b$ and $a \perp c$, then $a \perp bc$.*
4. *If $a \perp b$, then $a^m \perp b^n$ for all non-negative integers m, n.*
5. *If $a \perp b$, then $[a, b] = ab$.*
6. *If $a \perp b$, then $(a, bc) = (a, c)$.*
7. *If p and q are distinct primes, then $p \perp q$.*

Note. Part 2 is really useful in solving problems. It is actually the general form of Proposition (1.6). Sometimes, people make the mistake of writing $a|bc$ implies $a|b$ or $a|c$, which is not true unless a is a prime (this is stated in Proposition (1.6)). A proof will be provided for the general form of part 5.

How can we calculate (a, b) if a and b are given? There are two ways to do that. Here is the first (and also the simpler) one.

Proposition 1.12 (Euclidean Algorithm). *Let a and b be two positive integers with $a = bq + r$, where $0 \leq r < b$. Then $(a, b) = (a, r)$.*

Proof. Let $g = (a, b)$. We already know that $g|a$ and $g|b$. Since $b = aq + r$, $g|aq + r$. But $g|a$ implies $g|aq$ [4]. Now, as we established before in divisibility propositions, we can subtract two divisibility relations and find $g|aq + r - aq$, or $g|r$. This means that g divides r too, i.e., the greatest common divisor is a divisor r too. We want to show that $g = (a, r)$; and so there is only one thing remained to prove: if there exists some c for which $c|a$ and $c|r$, then $g \geq c$. We will prove that if such c exists, then $c|g$, which is a stronger argument. Note that $c|a$ gives $c|aq$, and thus $c|aq + r = b$. From Proposition (1.10) we see that $c|(a, b) = g$. The proof is complete.

Thus, it is enough to find (a, r) instead of (a, b). Note that finding (a, r) is easier because r is smaller than b.

□

Corollary 1.2. Let n, a, and b be positive integers such that $n|a - b$. Then $(n, a) = (n, b)$.

Proof. If $n|a - b$ then $a - b = nk$ for some integer k. Now, since $a = b + nk$, using Euclidean algorithm, $(n, a) = (n, b)$.

□

To make sense of this, see a simulation of this algorithm below[5].

Example. Let's find $(112, 20)$. Since $112 = 20 \cdot 5 + 12$, we have $(112, 20) = (20, 12)$. Now, because $20 = 12 \cdot 1 + 8$, $(12, 20) = (12, 8) = (8, 4) = (4, 0)$ and $(4, 0)$ is 4 according to previous propositions. So, $(20, 112) = 4$. You can test this algorithm for some more values of (a, b). If you understood the process correctly, you'll know that the algorithm terminates when one of a or b becomes 0.

The other way of finding the greatest common divisor relies on factorization. We provide an example for this method before stating the related proposition so that you can see what is happening.

Example. First prime factorize both 20 and 112.

$$20 = 2^2 \cdot 5, 112 = 2^4 \cdot 7$$

You can easily find that since the prime factor 5 does not appear in the factoring of 112, 5 cannot appear in $(20, 112)$. For the same reason, 7 will not appear in the gcd as well. In other words, we just have to consider the primes that are in both 112 and 20. Now, we are left with the only prime 2. The highest power of 2 in 112 is 4; but in 20, it is 2. Therefore $(20, 112)$, cannot have a power of 2 greater than 2 (the minimum of 4 and 2); otherwise, it will not divide 20. Since we are looking for the greatest common divisor, we will certainly take 2^2 and because there are no other common primes that divide both numbers, we have $(112, 20) = 2^2$.

This method works also for the least common multiple:

[4] note the multiplication; we will discuss more about such divisibility techniques later while solving problems

[5] An algorithm means a set of operations in a certain process to solve a problem or to find something

Example. Since $180 = 2^2 \cdot 3^2 \cdot 5^1$ and $105 = 3^1 \cdot 5^1 \cdot 7^1$, we have $(180, 105) = 3^1 \cdot 5^1 = 15$. We can find $[a, b]$ in similarly. We will just take the maximum value of the powers. For this specific example, $[180, 105] = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7$. Because since $[180, 105]$ is divisible by both 180 and 105, every prime power that divides one of them must also divide this lcm value.

Do the simulation for a few more examples to convince yourself. Meanwhile, let's formalize this process.

Proposition 1.13. *If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$, where p_i are primes and $e_i, f_i \geq 0$ are integers for $1 \leq i \leq k$, then:* [6]

$$(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$
$$[a, b] = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

Using product notation,

$$(a, b) = \prod_{i=1}^{k} p_i^{\min(e_i, f_i)}$$
$$[a, b] = \prod_{i=1}^{k} p_i^{\max(e_i, f_i)}$$

This idea can be generalized for finding gcd or lcm of n integers. Just factorize the numbers and select the proper powers of primes. The next proposition is pretty useful in a number of number theory problems.

Proposition 1.14. *For two integers a and b with $g = (a, b)$, there exist integers m and n such that $a = gm$ and $b = gn$. Moreover, $m \perp n$, i.e., m and n share no factor other than 1.*

Note. Integers m and n exist because $g|a$ and $g|b$. But why are m and n co-prime? This is true because if there were any other common factor between m and n, that would have been included in g too. Otherwise, g could not remain the greatest common divisor since we can make a bigger one multiplying that common factor with g. We can think of m and n as the *uncommon* part between a and b. For example, $(18, 27) = 9$ and $18 = 9 \cdot 2, 27 = 9 \cdot 3$. Now, 9 is the largest common part. Here, 2 is the uncommon part from 18 which 27 does not have besides 9, and 3 is the uncommon part of 27 which 18 does not have besides 9. Thinking about m, n in this way may make more sense to you. Thinking similarly, you should be able make sense of the next proposition.

Proposition 1.15. *Let $g = (a, b)$ and $\ell = [a, b]$. If $a = gm$ and $b = gn$ with $(m, n) = 1$, then $\ell = gmn$.*

The next proposition is well-known and useful in many cases.

[6] Try to find out why $e_i \geq 0$ whereas we consider only $e_i \geq 1$ when we discussed prime factorization first.

Proposition 1.16. *Let $g = (a, b)$ and $\ell = [a, b]$. Then $ab = g\ell$. In words, the product of two positive integers is equal to the product of their greatest common divisor and least common multiple.*

We can prove it in a couple of ways but here are two proofs. Also, note that this can be used to find least common multiple of two numbers.

First proof. As the previous proposition says, we can write $a = gm, b = gn$ with $(m, n) = 1$. Therefore $ab = gm \cdot gn = g^2mn$. On the other hand, $gl = g \cdot gmn = g^2mn$. □

The following proof uses prime factorization and is somewhat more rigorous. But we are showing it later because the previous one makes more sense. Even though it is uglier, it shows how to invoke prime factorization to prove something.

Second Proof (Using Prime Factorization). Assume that we have the prime factorization of a and b.

$$a = p_1^{e_1} \cdots p_k^{e_k},$$
$$b = p_1^{f_1} \cdots p_k^{f_k}.$$

Now, can you understand the simple fact that $\min(x, y) + \max(x, y) = x + y$? If so, then the proof should be clear to you. It is because we have

$$ab = p_1^{e_1} \cdots p_k^{e_k} \cdot p_1^{f_1} \cdots p_k^{f_k} = p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}.$$

On the other hand, from Proposition (1.13),

$$\begin{aligned}(a, b) \cdot [a, b] &= p_1^{\min(e_1)} \cdots p_k^{\min(e_k)} \cdot p_1^{\max(e_1,f_1)} \cdots p_k^{\max(e_k,f_k)} \\ &= p_1^{\min(e_1,f_1)+\max(e_1+f_1)} \cdots p_k^{\min(e_k,f_k)+\max(e_k,f_k)} \\ &= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k} \\ &= ab.\end{aligned}$$

□

Question. Must $abc = (a, b, c) \cdot [a, b, c]$ hold? If not, why?

1.3 Numerical Systems

1.3.1. Introduction

There is a rumor that **Pascal** once promised 1000000 dollars to anyone who marries his daughter. Later, when her husband asked for money, Pascal gave him only 64 dollars. Poor guy! If you got the joke, you're probably good with bases. If not, don't worry, keep reading and you will get the point.

In daily mathematics, meaning the math you face in real life, you always express your numbers in decimal system. That is, when you say you have 15 apples, you are using base 10 without mentioning it. So, the question is, what is this *base* actually? Let's start with a simple example.

Example. Consider the number 573. Have you ever thought why we write digits in this way to denote a number? The reason is that every digit in the number represents the coefficient of a power of ten. That is,

$$573 = 5 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0.$$

Rigorously talking, each integer has to be written in a *base* for it to makes sense. For example, the number 15 has different values when expressed in base 6 and in base 10. Actually, $(15)_6 = (11)_{10}$ – so you can see how important base is.

All of our calculations in daily life are done in base 10, which is called the *decimal system*. However, this does not mean that we cannot present numbers in any other bases different from 10. Probably you have already figured out that in a base there are some *digits*. These digits run from 0 to the integer just before the base. For this reason, in base 10 the digits are $0, 1, \ldots, 9$. So, in base b the digits will be $0, 1, \ldots, b-1$. Observe the base-10 representation of 573 in the example above again. The rightmost digit is multiplied by 1 (that means, it is as it is). The digit left to it is multiplied by 10 (reason why it is called the *tenth digit*). The next digit is multiplied by 100 (the *hundredth digit*) and so on. In simpler words, each time we go left, we multiply the multiplier by 10. If it were base b instead of base 10, we would multiply by b each time. So, the multipliers would be $1, b, b^2, \ldots$ and so on. Now, you should understand the formal representation of an integer in base b, where we assume the base to be $b > 1$. Note that it is pointless to take base 1 since we don't have any meaningful digit (recall that, 0 is not a meaningful digit).

Definition 1.8 (Base b representation). In a numeral system, the number x and its *base* $b > 1$ are written together as $(x)_b$. If the digits of an n-digits number x are represented as $\overline{x_{n-1}x_{n-2}\ldots x_0}$, then

$$(x)_b = (\overline{x_{n-1}x_{n-2}\ldots x_1x_0})_b = b^{n-1}x_{n-1} + b^{n-2}x_{n-2} + \cdots + b^1x_1 + x_0,$$

where $x_0, x_1, \ldots, x_{n-1}$ are non-negative integers less than b (do you understand why?).

We usually draw a line over a number to denote it is being represented in base b. The base is written in the subscript, while the digits are inside the bracket to clarify it is not a product. An important thing to note is the fact that x_{n-1} is always non-zero, because if it is 0, then there is no point in keeping this as the leftmost digit. So we can remove this digit until we get a nonzero digit as the leftmost digit. The rightmost digit of x is denoted by x_0, and it is called the *least significant digit* of x. Analogously, the leftmost digit, x_n, is called the *most significant digit* of x. You should already be able to guess why! See that the rightmost digit has multiplier 1, and so contributes the least. The largest digit 9 contributes 9 if it is in the rightmost position. On the other hand, if 1 is the leftmost digit (say thousandth), then it has multiplier (you can think of it as a weight in this regard as well) 1000, which is a lot more than 9. So, 1 contributes the most, and naturally it is the most significant one. Same explanation applies for the least significant digit.

Example. The number $(327)_8$ is calculated as

$$(327)_8 = 3 \cdot 8^2 + 2 \cdot 8 + 7 = 215.$$

Note. When the base is absent in a representation, it is regarded to be 10 by default.

Different bases are used in different systems. For example, in computer science, it's conventional to represent the numbers in base 16 or 8. Another example is base 60 which was used by ancient Summerians in the 3rd millennium BC. In order to avoid repeating these numbers, we use a specific name for these popular bases. You can find a list of such names in the following table.

Base	**System Name**
2	Binary
3	Ternary
4	Quaternary
8	Octal
10	Decimal
16	Hexadecimal
36	Hexatrigesimal
60	Sexagesimal

1.3.2. Base Conversion

After defining bases, the first problem that we face is defining the relationship between the numbers in different bases. We can only understand the meaning of numbers when they are represented in decimal system. For example, you may have no clue about the real value of $(1234)_5$, but you surely know what is 1234 (remember when we do not write the base, it means it is 10).

Conversion from base b to base 10

In order to understand the meaning of numbers (their value), we need to convert them to a number in base 10. In the previous given example, we showed how to convert $(327)_8$ to base 10. The process of converting base $b < 10$ to base 10 is directly resulted from the Definition (1.8). However, we have an issue when converting bases $b > 10$ to base 10. Before stating the process of conversion, think about this: What happens if the base, b, is greater than 10? Then we have a problem in representing the digits. For example, in the *hexadecimal system*, with base of 16, the digits must be less than 16. So we should be able to represent digits 10 to 15 in hexadecimal system. But how is it possible to have a two-digits number as one digit in an hexadecimal number? In order to avoid the confusion, we use the following notation for digits bigger than ten:

$$10 = \texttt{A}, \quad 11 = \texttt{B}, \quad 12 = \texttt{C}, \quad 13 = \texttt{D}, \quad 14 = \texttt{E}, \quad 15 = \texttt{F}.$$

Example.

$$\begin{aligned}(2\texttt{FE}05)_{16} &= 2\cdot 16^4 + 15\cdot 16^3 + 14\cdot 16^2 + 0\cdot 16 + 5\\ &= 131,072 + 61,440 + 3,584 + 5\\ &= 196,101.\end{aligned}$$

You have now learned how to convert numbers in any base to a number in base 10. The next step is the opposite act: converting numbers in decimal system to other bases. You probably know how to do this, but we are going to introduce a systematic method for it.

Conversion from base 10 to base b

The simplest way of converting a decimal number to other bases is to use the traditional division. Before explaining the method, let us discuss the fundamentals of this method.

We want to convert the number y in decimal system to base b, which is, we want to write y as $(\overline{x_n x_{n-1}\dots x_1 x_0})_b$ so that $x_0, x_1, \dots x_n$ are the digits of y when represented in base b. From previous sections, we know that y can be written as

$$y = b^n x_n + b^{n-1}x_{n-1} + \cdots + b^1 x_1 + x_0, \tag{1.2}$$

where $0 \le x_i < b$ for $0 \le i \le n$. Our aim is to find the value of x_i's. The idea is to repeatedly divide y by b. Re-write the Equation (1.2) as

$$y = b\cdot \underbrace{\left(b^{n-1}x_n + b^{n-2}x_{n-1} + \cdots + x_1\right)}_{y_1} + x_0.$$

We have written y as $y = by_1 + x_0$, which means that the remainder of y when divided by b is x_0. So the rightmost digit of y in base b, which here is x_0, is the remainder of y when divided by b! As you can see, we are simply using the division theorem here, so bases relate to divisibility after all!

To find the next digit x_1, we have to divide the quotient of the above division, y_1, by b. The reason is simple: re-write y_1 as

$$y_1 = b\cdot \underbrace{\left(b^{n-2}x_n + b^{n-3}x_{n-1} + \cdots + x_2\right)}_{y_2} + x_1.$$

Therefore, x_1 is the remainder of y_1 when divided by b. We can find the next digit x_2 by finding the remainder of y_2 when divided by b. The digits $x_3, x_4, \dots, x_{n-1}$ can be found similarly by continuing this process. The leftmost digit, x_n, is the **quotient** of the last division because we no longer can divide it by b (since the digits are all less than b).

Don't worry if you did not fully understand the explained method. We will clarify it by stating a few examples.

Example. Let's find the representation of 215 in base 8 and base 2. Let's start with base 8 first. We start the process by dividing the given number by 8. The remainder of this division is the rightmost digit of 215 in base 8. Then we divide the quotient by

8 again. The remainder of this division is the digit before the rightmost one. Since the quotient of this division is less than 8, the process is over:

$$\begin{array}{r|l} 215 & 8 \\ \hline -16 & 26 \\ \hline 55 & \\ -48 & \\ \hline 7 & \end{array} \qquad \begin{array}{r|l} 26 & 8 \\ \hline -24 & 3 \\ \hline 2 & \end{array}$$

Thus $215 = (327)_8$ which matches the result in previous section. Let's find 215 in base 2 now:

$$\begin{array}{r|l} 215 & 2 \\ \hline -2 & 107 \\ \hline 01 & \\ -0 & \\ \hline 15 & \\ -14 & \\ \hline 1 & \end{array} \quad \begin{array}{r|l} 107 & 2 \\ \hline -10 & 53 \\ \hline 07 & \\ -6 & \\ \hline 1 & \end{array} \quad \begin{array}{r|l} 53 & 2 \\ \hline -4 & 26 \\ \hline 13 & \\ -12 & \\ \hline 1 & \end{array} \quad \begin{array}{r|l} 26 & 2 \\ \hline -2 & 13 \\ \hline 06 & \\ -6 & \\ \hline 0 & \end{array} \quad \begin{array}{r|l} 13 & 2 \\ \hline -12 & 6 \\ \hline 1 & \end{array} \quad \begin{array}{r|l} 6 & 2 \\ \hline -6 & 3 \\ \hline 0 & \end{array} \quad \begin{array}{r|l} 3 & 2 \\ \hline -2 & 1 \\ \hline 1 & \end{array}$$

Reading from right to left, the quotient of the first division is the leftmost digit, and the remainders of divisions form the other digits. So, the result is $(11010111)_2$.

Example. Assume we want to convert the number $196,101$ to base 16.

$$\begin{array}{r|l} 196101 & 16 \\ \hline -16 & 12256 \\ \hline 36 & \\ -32 & \\ \hline 41 & \\ -32 & \\ \hline 90 & \\ -80 & \\ \hline 101 & \\ -96 & \\ \hline 5 & \end{array} \quad \begin{array}{r|l} 12256 & 16 \\ \hline -112 & 766 \\ \hline 105 & \\ -96 & \\ \hline 96 & \\ -96 & \\ \hline 0 & \end{array} \quad \begin{array}{r|l} 766 & 16 \\ \hline -64 & 47 \\ \hline 126 & \\ -112 & \\ \hline 14 & \end{array} \quad \begin{array}{r|l} 47 & 16 \\ \hline -32 & 2 \\ \hline 15 & \end{array}$$

If you write down the divisions like we did, you can see that the last quotient is the most significant digit and the remainders of the divisions (from right to left) are the other digits (As you move from the last remainder to the first one, the significance of the digits decreases). Finally, writing 15 as `F` and 14 as `E`, we have

$$196,101 = (2\texttt{FE}05)_{16}.$$

Conversion of other bases

Assume that we want to convert a number in base 2 to base 8. How should it be done? One approach is to convert the number to base 10 first, and then convert it to base 8. You should be able to do this procedure by now. However, we prefer to do the conversion in one step, if possible, rather than two steps.

Let $x = (\overline{a_n a_{n-1} \dots a_1 a_0})_2$ be our binary number, where $a_i = 0$ or 1 for $0 \le i \le n$. Assume that we have converted this number to base 8, and the result is $x = (\overline{b_m b_{m-1} \dots b_1 b_0})_8$, where $0 \le b_j \le 7$ for $0 \le j \le m$. Our aim is to find the relation between a_i and b_j. It might seem a bit difficult to find a relation, but it will be clear if you write the expansion of x in both bases. Starting with base 2, we can represent x as

$$x = 2^n a_n + 2^{n-1} a_{n-1} + \dots + 2^1 a_1 + a_0.$$

Start grouping a_i digits in groups of 3, starting at the right. For convenience, assume that $n+1$ is divisible by 3 (note that there are $n+1$ digits $a_0, a_1, \dots, a_n$ and we are grouping them in groups of 3). Other cases when number of digits is not divisible by 3 will be discussed later. Then

$$\begin{aligned} x &= \left(2^n a_n + 2^{n-1} a_{n-1} + 2^{n-2} a_{n-2}\right) + \left(2^{n-3} a_{n-3} + 2^{n-4} a_{n-4} + 2^{n-5} a_{n-5}\right) + \dots + \left(2^2 a_2 + 2^1 a_1 + a_0\right) \\ &= 2^{n-2}\left(2^2 a_n + 2a_{n-1} + a_{n-2}\right) + 2^{n-5}\left(2^2 a_{n-3} + 2a_{n-4} + a_{n-5}\right) + \dots + 2^0\left(2^2 a_2 + 2a_1 + a_0\right) \\ &= 8^{\frac{n-2}{3}} \underbrace{\left(2^2 a_n + 2a_{n-1} + a_{n-2}\right)}_{b_m} + 8^{\frac{n-5}{3}} \underbrace{\left(2^2 a_{n-3} + 2a_{n-4} + a_{n-5}\right)}_{b_{m-1}} + \dots + 8^0 \underbrace{\left(2^2 a_2 + 2a_1 + a_0\right)}_{b_0}. \end{aligned}$$

Note that the number $2^2 a_i + 2a_{i-1} + a_{i-2}$ is actually $(\overline{a_i a_{i-1} a_{i-2}})_2$, and so it is a non-negative integer less than or equal to $(\overline{111})_2 = 7$. This means that $2^2 a_i + 2a_{i-1} + a_{i-2}$ is acceptable as a digit in base 8! (Remember that digits in base b should be less than b and non-negative). Now look at the last line of the above equations. It is of the form $8^m b_m + 8^{m-1} b_{m-1} + \dots + 8b_1 + b_0$, so we have found a relation:

$$m = \frac{n-2}{3}, \quad b_j = 2^2 a_{3j+2} + 2a_{3j+1} + a_{3j} = (\overline{a_{3j+2} a_{3j+1} a_{3j}})_2 \text{ for } 0 \le j \le m.$$

Remember that we first assumed the number of digits of the binary number is divisible by 3 so that we can group them. What if number of digits is not divisible by 3? It's not a problem. Put one or two zeros at the left of the binary number and make the number of digits divisible by 3, then continue the process!

The above result looks a bit scary, but it is really simple in plain English, explained in the following theorem.

Theorem 1.2 (Base 2 to 8 Conversion Rule). *To convert a binary number to base 8 directly, start grouping the 0 and 1 digits of the number in groups of 3. If number of digits of the binary number is not divisible by 3, put one or two zeros at the left of the number to make it so, and then group the digits. Then convert each of these groups into one octal digit and rewrite the number. Conversion is done.*

Example. Let us convert $(\overline{1010011010})_2$ to base 8. Number of digits is 10, which is not divisible by 3. So we add two zeros to the left and start the process with the number

$(\overline{001010011010})_2$. Now

$$(\overline{001})_2 = (\mathbf{1})_8, (\overline{010})_2 = (\mathbf{2})_8, (\overline{011})_2 = (\mathbf{3})_8, (\overline{010})_2 = (\mathbf{2})_8.$$

Thus $(\overline{001010011010})_2 = (\overline{1232})_8$.

Conversion from base 8 to base 2 is conversely and easily done. For the sake of completeness, we include it here.

Theorem 1.3 (Base 8 to 2 Conversion Rule). *To convert an octal number to base 2 directly, convert each digit to base 2 and rewrite the number. Conversion is done.*

You can convert a binary number to base 16 by just grouping the digits into groups of 4 and convert each group to a hexadecimal number. In general, one can use a similar approach to convert a binary number to base 2^n. However, the cases where n is larger than 4 are rarely used.

Similar approaches can be used for conversion between other numbers as well. For example, to convert base 3 to base 9, one should start grouping the digits in groups of 2 and then do the conversion. The theorems are pretty similar to the above and we are not including them here.

1.4 Theorems In Divisibility

You should always keep some simple things in mind like parity and greatest common divisor. The reader should also bear this in mind that in no way these are the only theorems or facts one need in order to solve problems. Rather, they are posed here just as a starting point when solving problems. By all honesty, the authors believe the reader should start problem solving without even learning any theorems. But the ones provided here are almost trivial or easy to prove facts. So, it should not affect the way someone can think.

We start with a very basic but useful fact. This result can be used in solving many problems.

Theorem 1.4. *Two integers a and b are of the same parity if and only if their sum and difference is even. Equivalently, they are of different parity if their sum and difference is odd.*

Corollary 1.3. *One of a and b is even (odd) if and only if $a \pm b$ is odd.*

Theorem 1.5. *Every positive integer n can be written in the form $n = 2^k s$ where k is a non-negative integer and s is an odd integer.*

Note. Here, k is the largest power of 2 that divides n, therefore s must be odd. s is the largest odd divisor of n. Note that if n is odd, then $k = 0$ and $s = n$.

Actually, one can write any integer n as $n = p^k s$ where p is a prime, k is non-negative, and $(s, p) = 1$. The case $p = 2$ is usually used in problem solving (and sometimes even in some combinatorics problems).

Theorem 1.6. *Every integer n can be written as ab where $a \perp b$.*

Corollary 1.4. *If n is composite, then n can be written as ab where $a \perp b$ and $a, b > 1$.*

Theorem 1.7. *$(n-1)!$ is divisible by n if and only if $n > 4$ is a composite integer or $n = 1$.*

Proof. The case $n = 1$ is trivial. For $n = 2, 3, 4$ we can check by hand. For $n > 4$, if n is a prime, n does not share a factor with any of $1, 2, \ldots, n-1$. So n does not divide their product $(n-1)!$. If n is composite, we can write $n = ab$ such that $a, b > 1$ and $a \neq b$. Since $a \neq b$ and $(n-1)!$ contains both a and b in the product, $ab|(n-1)!$.

□

Theorem 1.8 (Four Numbers Theorem). *Let a, b, c, and d be four positive integers such that $ab = cd$. There exist four positive integers r, s, t and u so that*

$$a = rs, b = tu, c = rt, d = su.$$

Proof. Let $(a, c) = g_1$, then by Proposition (1.14), there exist integers x_1 and y_1 such that $a = g_1 x_1$ and $c = g_1 y_1$ with $x_1 \perp y_1$. Also, let $(b, d) = g_2$, then there exist integers x_2 and y_2 such that $b = g_2 x_2$, and $d = g_2 y_2$ with $x_2 \perp y_2$. Substitute these equations into the given equation $ab = cd$ to get

$$g_1 g_2 x_1 x_2 = g_1 g_2 y_1 y_2$$
$$x_1 x_2 = y_1 y_2.$$

We claim that $x_1 = y_2$ and $x_2 = y_1$. To prove this claim, we use a trick. See that $x_1 x_2 = y_1 y_2$ means that $x_1 | y_1 y_2$. The second part of Proposition (1.11) tells us that since $x_1 \perp y_1$ and $x_1 | y_1 y_2$, then $x_1 | y_2$. The trick comes handy in here. Use analogous reasons to show that $y_2 | x_1$ and so by Proposition (1.2), $x_1 = y_2$. One can similarly show that $x_2 = y_1$. Now compare the theorem's parameters with the ones we just used and take $r = g_1, s = x_1, t = x_2$, and $u = g_2$. The proof is complete.

□

The following theorems enable us to consider prime factorization in many cases while solving a problem.

Theorem 1.9. *For positive integers a, b, n, and e, suppose that $a \perp b$ and $ab = n^e$. Then there exist positive integers x and y such that $a = x^e$ and $b = y^e$. In other words, if product of two co-prime positive integers is a perfect e^{th} power, then both of them should be perfect e^{th} powers.*

Proof. Let's consider the prime factorization of a and b as the following.

$$a = p_1^{e_1} \cdots p_k^{e_k},$$
$$b = q_1^{f_1} \cdots q_\ell^{f_\ell},$$

and so

$$ab = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell}.$$

From uniqueness of prime factorization, n must have only primes $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ as prime factor. Let,

$$n = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_\ell^{b_\ell} \implies n^e = p_1^{a_1 e} \cdots p_k^{a_k e} q_1^{b_1 e} \cdots q_\ell^{b_\ell e}.$$

Since $ab = n^e$, we get

$$p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell} = p_1^{a_1 e} \cdots p_k^{a_k e} q_1^{b_1 e} \cdots q_\ell^{b_\ell e}.$$

The exponents of the primes in both sides must be equal. Therefore, $e_1 = a_1 e, \ldots, e_k = a_k e$ and $f_1 = b_1 e, \ldots, f_\ell = b_\ell e$. But then,

$$a = \left(p_1^{a_1} \cdots p_k^{a_k}\right)^e,$$
$$b = \left(q_1^{b_1} \cdots q_\ell^{b_\ell}\right)^e.$$

proving the claim.

□

Note. You should think about why we considered the prime factorization and try to understand what led us into that way of thinking.

Corollary 1.5. *If a and b are relatively prime positive integers such that ab is a perfect square, then a and b both are perfect squares.*

Theorem 1.10. *Let a, b, and c be positive integers such that $ab = c^2$. There exist integers g, u, v with $u \perp v$ so that*

$$a = gu^2, b = gv^2, c = guv.$$

Proof. Let $g = (a, b)$. Then there exist co-prime integers x and y such that $a = gx$ and $b = gy$. Then $g^2xy = c^2$, so $g^2|c^2$ or, $g|c$ (see the example provided right after Proposition (1.9) for a proof). We can assume that $c = gk$. Substituting this into the equation, $k^2 = xy$ with $x \perp y$. From Corollary (1.5), there exist integers u and v such that $x = u^2$ and $y = v^2$. Thus, $a = gu^2, b = gv^2$, and $c = guv$.

□

The previous two theorems are useful in many situations. However, in order to use these theorems (and many more theorems in general), you need to know how to properly factorize expressions. We have already discussed a couple of important identities in Chapter (**??**). Besides those techniques, we introduce a simple but really useful method for factorization: **Simon's Favorite Factorization Trick**[7], or **SFFT** in brief.

[7]Named after Simon Rubinstein-Salzedo, a member of AoPS.

Proposition 1.17 (SFFT). *For any real numbers x, y, j, and k, the following relation holds*

$$xy + xk + yj + jk = (x + j)(y + k).$$

Two special common cases are: $xy + x + y + 1 = (x + 1)(y + 1)$ and $xy - x - y + 1 = (x - 1)(y - 1)$.

Let's see the motivation behind this trick. Once Mr. Simon was studying number theory, he found this problem: find all positive integers x and y such that $xy - x + y = 49$. Simon probably hates expressions of this form because he cannot factorize them. However, if he adds -1 to both sides this equation, he finds the nice and factored form $(x + 1)(y - 1) = 48$ which is much easier to solve than the original equation (it's just case work). If you look closely, SFFT is inspired by the so called **Completing the Square Method**:

$$x^2 + kx + \frac{k^2}{4} = \left(x + \frac{k}{2}\right)^2.$$

In fact, the act of adding jk to $xy + xk + yj$ in order to be able to factor it could be called **completing the rectangle** in analogy to the famous *completing the square* trick.

Theorem 1.11. *If N is the least common multiple of positive integers upto n, that is, $N = [1, 2, \ldots, n]$, then for a prime p, the maximum integer α for which $p^\alpha | N$ is the unique nonnegative integer α so that $p^\alpha \leq n < p^{\alpha+1}$. In other words, if p_i is a prime less than or equal to n, and for that prime, α_i is the unique integer such that $p_i^{\alpha_i} \leq n < p_i^{\alpha_i+1}$ then,*

$$N = p_1^{\alpha_1} \cdots p_k^{\alpha_i}.$$

We can write α_i in terms of n and p_i using logarithm. Actually, α_i is the greatest nonnegative integer less than or equal to $\log_{p_i}(n)$.

The proof in fact follows from the definition of least common multiple. Try some examples yourself and prove it. Also, we often use this kind of argument using logarithm to find some boundaries in some problems.

The next definition doesn't actually belong here, but we will introduce it anyway for our convenience.

Definition 1.9. Let n be a positive integer and let p be a prime. The maximum integer α for which $p^\alpha | n$ is denoted by $\alpha = v_p(n)$. We also write this as $p^\alpha \| n$.

You will see the usage of this notation in the whole book (and specially in Chapter (**??**)).

Theorem 1.12. *The square of every odd integer leaves a remainder of 1 when divided by 8.*

Proof. We can write each odd integer n in the form $n = 2k - 1$ for some $k \in \mathbb{N}$. Then

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

Since one of k or $k-1$ must be even (why?) we can write $k(k-1) = 2\ell$. Then $n^2 = 8\ell + 1$, and so n^2 leaves a remainder 1 when divided by 8.

□

Theorem 1.13. *Every number of the form $4k+3$ has at least one prime factor of the form $4k+3$.*

Proof. The idea comes from the fact that if we multiply two numbers of the form $4k+1$, say $4a+1$ and $4b+1$, the result will be

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1,$$

which is, again, of the form $4k+1$. Clearly, all prime factors of a number n of the form $4k+3$ are odd, and therefore is either of the form $4k+1$ or $4k+3$. If all prime factors of n are of the form $4k+1$, then by the logic represented in above lines, any product of powers of these primes, including n, should be of the form $4k+1$. So, we get a contradiction and there exists at least one prime factor of n which is of the form $4k+3$.

□

The following theorem needs mere insight.

Theorem 1.14. *The number of solutions to the equation*

$$xy = n$$

in positive integers is $\tau(n)$, where $\tau(n)$ is the number of positive divisors of n.

Example. $\tau(6) = 4$ since 6 is divisible by $1, 2, 3$, and 6. If you look carefully, you can see how the positive integer solutions to $xy = 6$ are related to divisors of 6.

We will study $\tau(n)$ in details in Chapter (**??**).

Theorem 1.15. *Every prime greater than 3 is either of the form $6k+1$ or of the form $6k-1$.*

Proof. We can write an integer in exactly one of the following forms:

$$6k-2, 6k-1, 6k, 6k+1, 6k+2, 6k+3.$$

Numbers of the form $6k-2, 6k+2, 6k, 6k+3$ cannot be prime because the first two are divisible by 2 and the last two are divisible by 3. Thus, if n is a prime, it must be either $6k-1$ or $6k+1$.

□

Using the above theorem, we can prove the following theorem.

Theorem 1.16. *For a prime $p > 3$, $24|p^2 - 1$.*

Proof. We can assume $p = 6k \pm 1$ for some integer k. So

$$\begin{aligned} p^2 &= (6k \pm 1)^2 \\ &= 36k^2 \pm 12k + 1 \\ &= 12k(3k \pm 1) + 1 \end{aligned}$$

Note that $k + 3k \pm 1$ is odd. Therefore, they are of different parity and $k(3k \pm 1)$ is divisible by 2. Let $k(3k \pm 1) = 2\ell$, then $p^2 = 24\ell + 1$, or $p^2 - 1 = 24\ell$, which proves the theorem.

□

Theorem 1.17. *If the sum of two positive integers is a prime, they are co-prime to each other.*

Proof. Assume that $a + b = p$ where p is a prime. If $(a, b) = g$ then $a = gx, b = gy$ with $x \perp y$. So

$$\begin{aligned} p &= a + b \\ &= g(x + y), \end{aligned}$$

which means g divides p. The possible values of g are 1 and p. But it can't be p since then $x + y = 1$ would lead to one of x or y being 0. Thus $(a, b) = g = 1$.

□

Theorem 1.18. *For all positive integer n,*

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

If n is odd, $a^n + b^n = a^n - (-b)^n$, so,

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \cdots + b^{n-1}).$$

Proof. We can just use induction on n, but we will try to avoid using induction as much as possible.

$$S = a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$$

Then, $aS = a^n + a^{n-1}b + \cdots + b^{n-1}a$ and $bS = a^{n-1}b + a^{n-2}b^2 + \cdots + b^n$. Subtract them and we get

$$(a - b)S = a^n - b^n$$

so we are done.

□

Corollary 1.6. *$a - b$ divides $a^n - b^n$ for all positive integer n.*

Corollary 1.7. *$a + b$ divides $a^n + b^n$ for all odd n.*

Theorem 1.19. *$a^m - 1 | a^n - 1$ if and only if $m|n$.*

Proof. We will first show that if $m|n$, then $a^m - 1 | a^n - 1$. Note that $m|n$ means that there exists a positive integer h such that $n = mh$, and so

$$a^n - 1 = a^{mh} - 1 = (a^m)^h - 1.$$

Let $x = a^m$. By corollary (1.6), $x - 1 = a^m - 1$ divides $x^h - 1 = a^n - 1$ as desired.

Now, let us show the other side. If $a^m - 1 | a^n - 1$, then

$$a^m - 1 | a^n - 1 - (a^m - 1) = a^n - a^m = a^m(a^{n-m} - 1).$$

But $a^n - 1 \perp a^m$. Therefore, $a^n - 1 | a^{n-m} - 1$. We repeat the same process, and get $a^n - 1 | a^{n-2m} - 1$. This suggest us to take $n = mq + r$ so that $0 \leq r < m$. Then, we will have $a^n - 1 | a^{n-mq} - 1 = a^r - 1$. Evidently, $a^r - 1 < a^m - 1 \leq a^n - 1$ which forces $a^r - 1 = 0$. So $r = 0$ and $n = mq$, which means that $m|n$.

□

Theorem 1.20. *If $a^k - 1$ is a prime for positive integers a and $k > 1$, then $a = 2$ and k must be a prime.*

Proof. As we already know,

$$a^k - 1 = (a - 1)(a^{k-1} + \ldots + 1)$$

If $a > 2$, then $a - 1$ will divide $a^k - 1$ which is absurd because $a^k - 1$ is a prime. So, a must be 2. If $k = p\ell$ for some prime p and $\ell > 1$, then we have,

$$a^k - 1 = (a^p)^\ell - 1 = (a^p - 1)\left(a^{p(\ell-1)} + \cdots + 1\right)$$

which would, again, be impossible. Therefore, k must be a prime too.

□

Remark. The numbers of the form $2^n - 1$ are called *Mersenne numbers* and denoted by M_n. So, if M_n is a prime, then n must also be a prime.

Theorem 1.21. *If $a^n + 1$ is a prime for odd n, then a is even and $n = 2^k$.*

The proof is same as the previous one, so we leave it to the reader.

The next theorem is a very useful tool.

Theorem 1.22. *For two positive integers a and b, if $a \perp b$, then*

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}.$$

Notice the proof of this theorem. Here, we will use Euclidean algorithm but the idea is applicable in many cases.

Proof. If $m = n$, the result is trivial since both sides are $a^m - b^m$. So, we can take $m > n$ without loss of generality[8]. If $m = n + k$ where $k \in \mathbb{N}$, then

$$\begin{aligned} a^m - b^m &= a^{n+k} - b^{n+k} \\ &= a^n(a^k - b^k) + b^k(a^n - b^n) \end{aligned}$$

Thus, $(a^m - b^m, a^n - b^n) = (a^n(a^k - b^k) + b^k(a^n - b^n), a^n - b^n) = (a^n(a^k - b^k), a^n - b^n)$. Since $a \perp b$, $a^n \perp a^n - b^n$ (why?). This gives us

$$(a^m - b^m, a^n - b^n) = (a^n - b^n, a^k - b^k)$$

Note that, this is the descending step of Euclidean algorithm! If we do the same process again, we would eventually reach (m, n) in the exponent.

□

The proof of the following useful theorem shows you how the second part of proposition (1.11) comes handy. Remember $\binom{n}{k}$ is the *binomial coefficient* and

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Theorem 1.23. *n is a prime if and only if n divides $\binom{n}{k}$ for all $0 < k < n$.*

For now, we will be proving only the first part.

Proof. From identity (**??**) we already know that

$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Obviously, the right side is divisible by p, so must be the left side. From the definition of prime numbers, $p \perp k$. So, by the second part of the previous proposition, we can say p must divide $\binom{p}{k}$.

□

1.5 Solved Problems

Well, now that we have a basic understanding of how divisibility relations work, we should see how we can apply those propositions to solve problems. Let's start with some really easy problems so that readers have a firm idea about how to approach a problem in order to solve it. Then we will gradually discuss less easier problems. But right now, we won't dive into that hard problems.

Problem 1.1. Find all positive integers n so that n divides $n + 3$.

[8] Wherever there is symmetry, don't forget to use this trick!

This can be solved in a variety of ways. But before we solve this, I want to share some experience. This may not directly help readers understand how to solve the problem but it may help them understand how different people think when they encounter a problem. I went to a remote area in winter, 2014-15. The students were just a regular batch of students who barely had the idea of problem solving. After showing them some basic facts about divisibility, I threw this problem at them. Here is how they approached it – most of them started calculating by hand for which numbers this is true. But not all of them could understand that it won't work in general for all numbers even if they found some initial solutions. One or two of them got that if n divides $n+3$, then $n+3$ is at least twice n. But $n+3$ doesn't increase as quickly as $2n$ which leads to a solution. Another student solved this the old fashioned way, like the division process that's taught in sixth or seventh grade here. And he found out that n must divide 3. Other than those few students, most of them got that $n = 1$ and $n = 3$ work but couldn't quite get why other numbers don't. Well, that's the most difficult part of solving a number theory problem. Whenever you encounter a number theory problem, at first you can make some assumptions. Most of the times our observations are true, but in many cases there are counter-examples or some trick cases where our assumption may be wrong. That's why we have to prove something whenever we make some claim that's not known beforehand. The same goes for theorems which are not well known. You may know theorems that seem well known to you but there may be other problem solvers who don't know what exactly you are talking about. Usually, this assumption is wrong, whatever the problem - be it number theory, algebra, or geometry.

Also, whenever you read a solution, instead of just understanding the solution, try to understand the motivation behind the idea. Now let's get back to the problem.

Solution (Old-fashioned Way). Since $n|n+3$, the fraction $\dfrac{n+3}{n} = 1+\dfrac{3}{n}$ is a positive integer. This shows that $\dfrac{3}{n}$ must be an integer i.e. n divides 3.

Solution (A Smarter Way). We know that if $a|b$ and $a|c$, then $a|b-c$. But how can we know what to subtract? See that the right side of $n|n+3$ has a variable n which is the main problem. So we need to remove it somehow. That's where divisibility rules come into play. Since $n|n$, we can now subtract $n|(n+3)-n = 3$ or $n|3$. In words, n is a divisor of 3 which has namely two divisors 1 and 3. Thus, n can be 1 or 3.

Solution (Another Smart Solution). Again, if $a|b$, $b \geq a$ if both are positive integers. Now, since $n+3$ can't be equal to n, if it has to be divisible by n, it must be at least twice n i.e. $n+3 \geq 2n$. This forces $3 \geq n$ or n is one of $1, 2$, or 3. There are only three values so we can check them by hand and get the answer.

Note the difference between the first and second solution. There are pretty much no differences other than the fact that the latter is more systematic. And you will find that solving problems this way is particularly useful in Olympiads.

For now, we will keep the use of inequality in store. Let's twist up the left and right hand sides more. And assume that the intended number is a positive integer unless stated explicitly.

Problem 1.2. Find all n so that $n|2n+3$.

Solution. This time we have to remove n like before, but notice that there is an extra 2 attached.

But we can overcome this easily: just see that $n|2n$ and then it's the same as the previous problem: $n|2n+3-2n=3$.

Problem 1.3. Find all n so that $n+1|3n+4$.

Solution. What about this one? The left side contains more than just a n, but it still is no big problem at all. We have $n+1|3(n+1)=3n+3$ and it is given that $n+1|3n+4$. Thus, $n+1|3n+4-(3n+3)=1$ which means $n+1$ must be 1. This is impossible because $n+1$ is a positive integer greater than 1.

Note. We have to check for all the divisors of the right side in order to find valid solutions or we have to be smart about it.

Try to do the following one yourself before reading the solution.

Problem 1.4. Find all $n \in \mathbb{N}$ which satisfies $4n+2|6n+5$.

Solution. What should we do now? There are coefficients on both sides of divisibility now. Still it can be overridden but it is a bit tricky. See that $4n+2|3(4n+2)=12n+6$ and also $4n+2|2(6n+5)=12n+10$. Now that the coefficients are matched, we can subtract and get this $4n+2|12n+10-(12n+6)=4$. So, $4n+2$ must be one of $1, 2$, or 4 which is not possible unless $n=0$.

Note. If you haven't noticed already, this idea can be generalized to find the solutions of $an+b|cn+d$. Then what shall we multiply both sides with? **Hint:** does this have anything to do with the lcm of a and c? And why a and c? If you don't still get it, consult the next problem.

Problem 1.5. Find all positive integer n for which $8n+9|12n+5$.

Solution. Our working principle is: we want to eliminate the variables on the right side so we get a numeric value. In order to do that we shall match the coefficients on both sides. Since coefficients must be equal, the minimum working value will be the lcm of 8 and 12, which is $[8,12]=24$. Now, to make the left side coefficient 24, we have to multiply $8n+9$ by $\frac{24}{8}=3$ and $12n+5$ needs to be multiplied by $\frac{24}{12}=2$. Therefore, we get

$$8n+9|3(8n+9)=24n+27$$
$$8n+9|2(12n+5)=24n+10$$

Thus, $8n+9|24n+27-(24n+10)=17$ and $8n+9$ can be one of 1 or 17. If $8n+9=1$, we don't have a valid solution. If $8n+9=17$, we get $n=1$.

Problem 1.6 (Dhaka Divisional Olympiad, 2010). Find all positive integers greater for which divides $n+4$ and $n+12$ for some positive integer n.

Solution. You should already get that it's wise to assume the positive integer that satisfies the condition yourself, let's call it d. Then using divisibility rules, $d|n+4$ and $d|n+12$. Immediately we have $d|n+12-(n+4)=8$ and so d can be one of $\{1,2,4,8\}$. Since d must be greater than 1, we get $d=2,4$, or 8.

Problem 1.7. Find all prime p so that $9p+1$ is a prime too.

Solution. This can be done easily using parity issues. When you encounter a problem with primes(especially if you are asked to find a prime), it may be helpful to separate the problem into two cases. First case: $p=2$. We can see that this works here. Now p is odd. It should tell you that as p is odd then $9p+1$ is even. And since $9p+1>2$ and even, it is divisible by 2, so not prime.

Problem 1.8. Find all n so that $7n+1|8n+55$.

Problem 1.9. Since $[8,7]=56$ and $\dfrac{56}{7}=8$, first we get $7n+1|8(7n+1)=56n+8$. For the right side, since $\dfrac{56}{8}=7$, $8n+55|7(8n+55)=56n+385$. So $7n+1|56n+385-(56n+8)$ or $7n+1|377$. Now, we have to find divisors of 377. When you are stuck with finding divisors, instead of trying random numbers or testing the numbers $2,3,4,5,\ldots$ serially if they divide 377, let's try a cooler approach which reduces out effort significantly. Remember Proposition (1.7) which said that if n is composite, i.e., if it has a divisor greater than 1, then it must have a prime factor less than or equal to $\sqrt{n}$. In other words, we are interested in finding the prime factorization of 377. $\sqrt{377}$ is 19 point something (we certainly don't need that). So let's start checking which primes less than or equal to 19 divide 377. The primes are $2,3,5,7,11,13,17,19$. Now, since 377 is not even, so not divisible by 2. It has sum of digit $3+7+7=17$, not divisible by 3. Last digit is not 5 or 0, so not divisible by 5. $377=7\cdot 53\cdot 7+6$, not divisible by 7. $3+7-7=3$, not divisible by 11 either. Divide it manually by 13, $377=13\cdot 29$. Finally we are done with the factorization. Now, notice that $7n+1$ is a number which leaves remainder 1 when divided by 7. Therefore, look for divisors of 377 greater than 1 which leaves a remainder of 1 when divided by 7. 29 is the only divisor satisfying this condition. Thus $7n+1=29$ and $n=4$.

Problem 1.10. Find all $n\in\mathbb{N}$ for which $n+3$ divides n^2+2.

Solution. This is where we start being tricky. First we show the straightforward solution. $n+3|n^2+3n$ and $n+3|n^2+2$, so $n+3|n^3+3n-(n^2+2)$ or $n+3|3n-2$. Now we need to remove this n, so $n+3|3(n+3)=3n+9$. Finally, $n+3|3n+9-(3n-2)=11$. Since $n+3\geq 1+3=4$, we can't have $n+3=1$. So $n+3=11$ or $n=8$.

Here comes the smarter solution. Notice that,

$$n+3|(n+3)(n-3)\implies n+3|n^2-9.$$

Now, we can do this easily: $n+3|n^2+2-(n^2-9)$ or $n+3|11$.

Problem 1.11. Find the greatest positive integer x for which $x+10$ divides x^3+10.

Solution. Again, $x+10|x^3+10^3$. So $x+10|x^3+1000-(x^3+10)$ or $x+10|990$, which gives $990\geq x+10\implies x\leq 980$.

Problem 1.12. Find all n so that $7n+1|n^6+n^4$.

Solution. How do we approach this problem? One idea is to go ahead like we did in the previous problem, by eliminating n one by one. Here is a better solution.

First write it as, $7n+1|n^4(n^2+1)$. The problematic part is n^4. Now, many beginners make mistakes in such situations claiming that $7n+1$ does not divide n^4, so $7n+1|n^2+1$. This is wrong. For example, 14 divides $28 = 7 \times 4$ but 14 does not divide 7. But in this case, we can still take n^4 off, because n^4 is co-prime to $7n+1$. Just notice that, $7n+1$ leaves a remainder of 1 when divided by n, so $n \perp 7n+1$. Evidently, $n^4 \perp 7n+1$ holds too. Using part 2 of Proposition (1.11), we can cancel out n^4 and get

$$7n+1|n^2+1 \implies 7n+1|49n^2+49.$$

On the other hand, one can write

$$7n+1|(7n)^2-1^2 \implies 7n+1|49n^2-1.$$

Subtracting, we have $7n+1|49n^2+49-(49n^2-1)$ or $7n+1|50$. In such cases, if you have to find divisors by hand, you can boost up the finding. $7n+1$ leaves a remainder of 1 when divided by 7. So look for divisors of 50 which leaves a remainder 1 when divided by 7. The divisors of 50 are $1, 2, 5, 10, 25, 50$. Only 1 and 50 leave a remainder of 1 when divided by 7 but $7n+1 \geq 7 \cdot 1 + 1 = 8$. Therefore, $7n+1 = 50$ or $n = 7$.

Remark. We could handle this another way. $7n+1|n^2+1-(7n+1)$ so

$$7n+1|n^2-7n \implies 7n+1|n(n-7).$$

Again, $n \perp 7n+1$, so $7n+1|n-7$. This forces $|n-7| \geq 7n+1$ unless $n-7=0$. If $n > 7$, then $n-7 < 7n+1$ (check!). If $n < 7$ then $7-n < 7n+1$, so only possible case is $n = 7$.

Problem 1.13. If $ax+by=1$, find (a,b).

Solution. Assume that $(a,b) = g$. Then we can find two integers m, n with $(m,n) = 1$ so that $a = gm, b = gn$. Setting these into the equation: $g(mx+ny) = 1$ which implies g divides 1 i.e. $g = 1$.

Note. We can similarly show that $(x,y) = (x,b) = (a,y) = 1$.

Problem 1.14. Find the number of solutions to the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{2015}$$

in positive integers.

Solution. We can rewrite the equation as:

$$\begin{aligned} \frac{x+y}{xy} &= \frac{1}{2015} \\ xy &= 2015(x+y) \\ xy - 2015x - 2015y &= 0 \\ (x-2015)(y-2015) &= 2015^2 \end{aligned}$$

From Theorem (1.14), we get that the number of solutions is the number of positive divisors of 2015^2, $\tau(2015^2)$.

Problem 1.15. Find all $n \in \mathbb{N}$ such that $2^n + n | 8^n + n$.

Solution. There is 8 on the right side and 2 on the left side. Since $8 = 2^3$, this should certainly provoke us to use the fact that, $a + b | a^3 + b^3$. In this case,

$$\begin{aligned} & 2^n + n | (2^n)^3 + n^3 \\ \implies & 2^n + n | 8^n + n^3 \\ \implies & 2^n + n | (8^n + n^3) - (8^n + n) \\ \implies & 2^n + n | n^3 - n. \end{aligned}$$

Now we need to find all n such that $2^n + n | n^3 - n$. If you play around with the smaller values of n, you will clearly see that 2^n grows a lot faster than n^3. Therefore, we should focus on that because we must have

$$2^n + n \leq n^3 - n$$

whereas you can see that for $n > 9$, $2^n + n > n^3 - n$ which gives us a contradiction, exactly what we need to bound n. But we must prove it first. To prove this at ease, we can use induction (since we don't have any other techniques at our disposal right now). But we leave it to the reader to prove that:

Lemma 1.1. *For $n > 9$, $2^n + n > n^3 - n$.*

Therefore, we now have that $n \leq 9$ in order to satisfy the divisibility relation. We can check them by hand since there aren't many cases. If there were too many cases, we could use the representation of n as $2^k s$.

Problem 1.16 (IMO 1959, Problem 1). Prove that for any integer n, the fraction $\dfrac{14n + 3}{21n + 4}$ is irreducible.

Solution. Let's make sense of the problem first. It asks to prove that a fraction is irreducible. That means it can't be divided by something that's common to both the denominator and numerator anymore. In other words, we must prove that $14n + 3$ and $21n + 4$ don't share any common factor other than 1 i.e. $(14n + 3, 21n + 4) = 1$. How do we prove this? Here we show some ways to do that.

Let $g = (14n + 3, 21n + 4)$. Then,

$$\begin{aligned} g | 14n + 3, \\ g | 21n + 4. \end{aligned}$$

We already know we have to prove $g = 1$. So let's try to remove the n on the right side. Since $[14, 21] = 42$ and $42 = 14 \cdot 3 = 21 \cdot 2$, we should do this:

$$\begin{aligned} g | 3(14n + 3) &\implies g | 42n + 9, \text{ and} \\ g | 2(21n + 4) &\implies g | 42n + 8. \end{aligned}$$

Thus, $g | (42n + 9) - (42n + 8) = 1$ and $g = 1$.

Here is another way. Take $14n+3 = gx$ and $21n+4 = gy$. Note that $3(14n+3) - 2(21n+4) = 1$, and so

$$3gx - 2gy = 1$$
$$g(3x - 2y) = 1.$$

So $g|1$ and this gives us the same result $g = 1$.

Remark. You should understand that both solutions are essentially the same, but with different approaches or thinking styles.

Problem 1.17. Show that if a prime is of the form $2^n + 1$, then $n = 2^m$ for some integer m.

Solution. According to theorem (1.5), write $n = 2^m s$, where s is an odd positive integer. By theorem (1.18), we can write

$$\begin{aligned} p = 2^n + 1 &= 2^{2^m s} + 1 \\ &= \left(2^{2^m}\right)^s + 1 \\ &= \left(2^{2^m} + 1\right)\left(2^{2^m(s-1)} + 2^{2^m(s-2)} + \cdots + 2^{2^m} + 1\right). \end{aligned}$$

Clearly, as p is a prime, this is impossible unless $s = 1$. So $n = 2^m$.

Problem 1.18. Find all integer solutions to the equation

$$a(b+1) + b(c+1) + c(a+1) + abc = 0.$$

Solution. Yes, this looks similar to **SFFT**, but how can we solve it? It has three variables instead of two, so we cannot directly use Simon's trick. However, if you already learned the motivation behind that trick, the form of the problem does not matter. Here, 1 is missing! Add it to both sides to get

$$abc + ab + bc + ca + a + b + c + 1 = 1.$$

The left hand side shows you how SFFT looks like for three variables. Try to compute $(a+j)(b+k)(c+\ell)$ and remember it. You will soon realize that the left hand side of the above equation factors as $(a+1)(b+1)(c+1)$. Therefore

$$(a+1)(b+1)(c+1) = 1.$$

The rest of the solution is just case work. If the product of three integers equals 1, what can they be? The solutions are $(a,b,c) = (0,0,0), (-2,-2,0), (-2,0,-2), (0,-2,-2)$.

Problem 1.19 (Turkey TST 2014, Day 2, Problem 4). Find all odd positive integers m and n such that

$$n|3m+1 \text{ and } m|n^2+3.$$

Solution. Do not panic! Even some TST problems can be solved using simple tricks. The general idea is to first see if there are infinitely many solutions. Check some numbers and some special values for m and n, for instance $(m,n) = (k,k)$, to see if they fit. In this problem, we cannot find a pattern to construct infinitely many solutions, so we guess that there are finite solutions and continue. To be honest, many of such divisibility problems (with finite solutions) rely heavily on case working, and you need to know how to start the case work. One of the best ways to handle this situation is to find a limit for m and n. Remember the properties of divisibility from Proposition (1.1). Limit means boundary, and boundary means inequality (see part 10 of that proposition). So we will use the fact that if $a|b$ for positive integers a and b, then $a \leq b$. After we have found the limit, the case work begins.

Now let's solve the problem. Write $n|3m+1$ as $3m+1 = nk$ or $m = \frac{nk-1}{3}$. Now try to rewrite the second divisibility relation as

$$\frac{nk-1}{3}|n^2+3 \implies nk-1|3n^2+9 \implies nk-1|3n^2k+9k.$$

On the other hand, we know that $nk-1|3n(nk-1) = 3n^2k-3n$. Subtract these two last divisibility relations to find

$$nk-1|3n+9k \overset{n,k>0}{\implies} nk-1 \leq 3n+9k.$$

The final inequality can be simplified using **SFFT** in this way:

$$nk-3n-9k \leq 1 \overset{\text{add } 27}{\implies} (n-9)(k-3) \leq 28.$$

Notice that we have found the limit we wanted! The solution is almost obvious from here on, because one can manually put all possible values for n and k such that $(n-9)(k-3) \leq 28$ and pick those which satisfy the problem conditions ($n|3m+1$ and $m|n^2+3$.) However, it is boring to check that much values. So we have to start a proper case work.

We start case work on the parameter k (you will know why). Notice that $3m+1 = nk$, and so k is even. We check some possible values of k:

(a) If $k = 2$, then from $nk-1|3n+9k$ we have $2n-1|3n+18$, and thus $2n-1|2(3n+18)-3(2n-1) = 39$. This means that $2n-1 = 1, 3, 13$, or 39. None of these values make a solution for the problem.

(b) If $k = 4$, then from $nk-1|3n+9k$ we have $4n-1|3n+36$, and thus $4n-1|4(3n+36)-3(4n-1) = 147$. This means that $4n-1 = 1, 3, 7, 21, 49$, or 147. Checking the values of n, we find that $n = 1$ and $n = 37$ satisfy the conditions of problem and give us the solutions $(m,n) = (1,1)$ and $(m,n) = (49,37)$.

(c) If $k \geq 6$, then

$$(n-9)(k-3) \leq 28 \implies (n-9) \leq \frac{28}{k-3} \leq \frac{28}{3} \implies n \leq 9 + \frac{28}{3}.$$

Since n is a positive integer, the latter inequality simplifies to $n \leq 18$ (why?). Also, n is odd, so we have to check only the numbers $n = 1, 3, 5, 7, 9, 11, 13, 15$, and 17. In this case, only $n = 13$ gives a valid solution (check it) and it is $(m,n) = (43,13)$.

The solutions are $(m,n) = (1,1), (49,37), (43,13)$.