Olympiad Number Theory

Nirjhar Nath
nirjhar@cmi.ac.in

Contents

1 Divisibility

1.1 Multiplication

To understand divisibility, let us look at its source – multiplication tables. As an example, let's look at the multiplication table of 3.

$$\begin{gathered}\vdots\\ 3\times(-3)=-9\\ 3\times(-2)=-6\\ 3\times(-1)=-3\\ 3\times 0=0\\ 3\times 1=3\\ 3\times 2=6\\ 3\times 3=9\\ \vdots\end{gathered}$$

So the set of multiples of 3 is $\mathcal{M}=\{\dots,-9,-6,-3,0,1,3,6,9,\dots\}$ and any number in this list is called a **multiple** of 3, and is said to be **divisible** by 3. Note that the set of multiples of an integer m is of the form $\{mq \mid q\in\mathbb{Z}\}$. So we can formally define the following:

Definition 1.1.1. An integer n is said to be a **multiple** of another integer m if $n=mq$ for some $q\in\mathbb{Z}$ (we can also say that m is a **factor** or **divisor** of n). A number n is said to be **divisible** by n if n is a multiple of m; also, we say that m **divides** n (symbolically $m\mid n$).

We denote 'm does not divide n' by $m\nmid n$.

1.2 Properties of Divisibility

Proposition 1.2.1 (Basic Properties of Divisibility)**.** For any three integers a,b, and c, the following statements are true.

1. $a\mid 0$ and $\pm1\mid a$.
2. $a\mid a$.
3. If $a\neq 0$, then $0\nmid a$. In the case when $a=0$, since $0/0$ is undefined, $0\mid 0$ is also meaningless.
4. If $a\mid b$ and $b\mid c$, then $a\mid c$.
5. If $a\mid b$, then $a\mid -b$, $-a\mid b$ and $-a\mid -b$.
6. If $a\mid b$, then $a\mid bk$ for all $k\in\mathbb{Z}$.
7. If $a\mid b$, then $ak\mid bk$ for all $k\in\mathbb{Z}$.
8. If $ak\mid bk$ for some $k\neq 0$, then $a\mid b$.
9. If $a\mid b$ and $b\neq 0$, then $|b|\geq|a|$. In other words, if $a\mid b$ and $|a|>|b|$, then we have $b=0$.

10. If $a \mid b$, then $a^n \mid b^n$ for all $n \geq 0$.

Proof. These results are very easy to prove. I'll prove a few of them. A general approach to solve this kind of problems is simply transforming them into equations, i.e., when $x \mid y$, write $y = kx$ for some integer k.

3. We want to prove that $a \neq 0 \implies 0 \nmid a$. Note that proving this is equivalent to proving $0 \mid a \implies a = 0$[1]. Now, $0 \mid a$ means $a = 0k$ for some integer k, i.e., $a = 0$.

4. $a \mid b$ means $b = ak_1$ for some $k_1 \in \mathbb{Z}$ and $b \mid c$ means $c = bk_2$ for some $k_2 \in \mathbb{Z}$. Therefore, $c = (ak_1)k_2 = a(k_1k_2)$, where $k_1k_2 \in \mathbb{Z}$, i.e., $a \mid c$.

6,7. $a \mid b$ means $b = aq$ for some $q \in \mathbb{Z}$. So $bk = aqk$, i.e., $a \mid bk$ and $ak \mid bk$.

8. $ak \mid bk$ means $bk = akq$ for some $q \in \mathbb{Z}$. Since $k \neq 0$, so cancelling k from both sides, we get $b = aq$, i.e., $a \mid b$.

9. $a \mid b$ means $b = ak$ for some $k \in \mathbb{Z}$. So, $|b| = |ak| = |a| \cdot |k| \geq |a|$. (Here, $|k| \geq 1$ since $b \neq 0$.)

10. Hint: Use induction on n.

□

Proposition 1.2.2. If $a \mid b$ and $b \mid a$, then $|a| = |b|$. In other words, $a = \pm b$.

Proof. Using part 9 of Proposition 1.2.1 gives $|a| \leq |b|$ and $|b| \leq |a|$, which implies $|a| = |b|$. So $a = \pm b$. (You can also prove this as follows: Write $b = ak_1$ and $a = bk_2$ for integers k_1, k_2. Then $a = (ak_1)k_2 \implies k_1k_2 = 1$. So either $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$, i.e., $a = \pm b$.) □

Proposition 1.2.3. If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for arbitrary integers x, y. More generally, if $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$, then for arbitrary integers $x_1, x_2, \ldots, x_n$,

$$a \mid \sum_{i=1}^{n} a_i x_i.$$

Proof. $b = ak_1$ and $c = ak_2$ for integers k_1, k_2. So $bx+cy = (ak_1)x+(ak_2)y = a(k_1x+k_2y)$, i.e., $a \mid bx + cy$. A similar approach also proves the general result. □

I am proving the following lemma as it will help us to solve the problems in the next section.

Lemma 1.2.1. $a \mid ak + r \iff a \mid r$ for integers a, k, r.

Proof. If $a \mid ak+r$, then $ak+r = aq$ for some $q \in \mathbb{Z}$. So, $a(q-k) = r$, i.e., $a \mid r$. So one direction is proven. To prove the other direction, if $a \mid r$, then $r = aq$ for some $q \in \mathbb{Z}$. Add ak on both sides to get $ak+r = a(q+k)$, i.e., $a \mid ak+r$. (Note that you could also prove this using Proposition 1.2.3 as follows: If $a \mid ak + r$, then since we also have $a \mid a$, so $a \mid (ak+r)(1) + a(-k) = r$. If $a \mid r$, then since $a \mid a$, so $a \mid r(1) + a(k) = ak + r$.) □

Remember this result in the following way: If a divides r plus a multiple of a, then you can just drop the multiple of a to get a divides r. Also, if a divides r, then a also divides r plus any multiple of a (in fact, a also divides any multiple of r plus any multiple of a, due to Proposition 1.2.3, i.e., $a \mid r \implies a \mid ak + r\ell$.)

[1] For statements p and q, the contrapositive of $p \implies q$ is $\sim q \implies \sim p$ and both of them are logically equivalent. Read this.

1.3 Problems

Problem 1.3.1. Show that if $n > 1$ is an integer, we can't have $n \mid 2n^2 + 3n + 1$.

Solution 1.3.1. Observe that $2n^2 + 3n + 1 = n(2n + 3) + 1$, i.e., a multiple of n plus 1. So if $n \mid 2n^2 + 3n + 1$, then by Lemma 1.2.1, we have $n \mid 1$. But since $n > 1$, this is not possible, i.e., we can't have $n \mid 2n^2 + 3n + 1$. □

Problem 1.3.2. Let $a > b$ be natural numbers. Show that $a \nmid 2a + b$.

Solution 1.3.2. If $a \mid 2a + b$, then Lemma 1.2.1 would imply that $a \mid b$. But it is already given that $a > b$, a contradiction. (Why?) □

Problem 1.3.3. For which integers n, $\frac{2n-1}{n+7}$ is an integer.

Solution 1.3.3. $\frac{2n-1}{n+7}$ is an integer if $n + 7 \mid 2n - 1$. Our main idea is to get something of the form: $n + 7$ divides "an integer". So we should try to get rid of the n on the right. Using Lemma 1.2.1, we have,

$$\begin{aligned} & n + 7 \mid 2n - 1 \\ \implies & n + 7 \mid 2(n + 7) - (2n - 1) \\ \implies & n + 7 \mid 15 \end{aligned}$$

i.e., $n + 7$ is a factor of 15. But, all the factors of 15 are $-15, -5, -3, -1, 1, 3, 5, 15$ and $n + 7$ can take only these values, i.e., $\frac{2n-1}{n+7}$ is an integer for the following integer values of n: $-22, -12, -10, -8, -6, -4, -2, 8$. □

1.4 Euclid's Division Lemma

Definition 1.4.1. When an integer b is divided by another integer a, we can write $b = aq + r$ for some integers q and r. In this general case, we call r the **remainder** of the division. However, if we choose q such that $0 \le r < |a|$, then we say r is the **minimum remainder** of the division. A division in which r is the minimum remainder is called a **proper division**. In case of proper division, we call a, b and q the **dividend**, **divisor** and the **quotient** respectively.

Note that proper division is the division you have been doing all along; you always chose r to be the minimum remainder. For example, when I tell you to divide 19 by 3, you directly write $19 = 3 \times 6 + 1$, where $r = 1$ is the minimum remainder, so this is proper division. However, I could have also written $19 = 3 \times 4 + 7$ or $19 = 3 \times 7 + (-2)$ (where the remainders are 7 and (-2) respectively), but these will not be counted as proper division.

Now don't be surprised by the following theorem, as throughout your whole mathematical journey, you always found the remainder to be unique in case of division (we call it proper division now).

Theorem 1.4.1 (Euclid's Division Lemma)**.** *For fixed positive integers a and b, there are unique integers q and r so that $b = aq + r$ with $0 \le r < a$. In other words, the quotient and the minimum remainder of the division are unique.*

Proof. Note that $r = 0 \iff a \mid b$. So we can easily rule out this case.

When $a \nmid b$, b has a non-zero remainder (say r) upon division by a. We can write

$$b = aq + r \iff q = \frac{b - r}{a}.$$

So uniqueness of r implies the uniqueness of q and vice versa. Therefore, we only need to prove that r is unique.

Assume, to the contrary, that r is not unique, i.e., $\exists$ integers q', r' so that

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

But this gives $a(q - q') = r' - r$, i.e., $a \mid r' - r$. Also since both r, r' are less than a, so $|r' - r| < a \leq |a|$. Now recall the alternative statement for part 9 of Proposition 1.2.1: If $a \mid b$ and $|a| > |b|$, then we have $b = 0$. We can use this here (because $a \mid r' - r$ and $|a| > |r' - r|$) to get $r' - r = 0$, i.e., $r' = r$. This means that the minimum remainder is unique and hence the quotient is unique. □

Let me now ask all of you a question. Let a, b, n be positive integers such that $a \mid n$ and $b \mid n$. Do we necessarily have $ab \mid n$? Now note that $ab \mid n^2$ is true, because we can write $n = ak_1$, $n = bk_2$ for some integers k_1, k_2. Multiplying both these equations, we get $n^2 = (ab)(k_1k_2)$. So $ab \mid n^2$. However, $ab \mid n$ is not necessarily true. A possible counterexample[2] could be $2 \mid 12$, $4 \mid 12$ but $2 \times 4 = 8 \nmid 12$. (Note that one counterexample is enough to disprove a statement.) Find other counterexamples.

As we move ahead, you will see that we can add an extra condition, i.e., $\gcd(a, b) = 1$, to make this statement true. We will come to that later.

1.5 Prime numbers

Definition 1.5.1. A number greater than 1 is called a **prime** if it has only two divisors, 1 and the number itself. A number greater than 1 which is not a prime is **composite**.

The list of primes is: $2, 3, 5, 7, 11, 13, 17, \ldots$. Note that 2 is the only even prime. If we agree that atoms are the building blocks of molecules, it follows by analogy that primes are building blocks of natural numbers. You will see how this statement makes sense as you understand the Fundamental Theorem of Arithmetic. However, there is no known pattern in primes. There have been many estimates related to primes, one of the most notable being the Prime Number Theorem, which states that

$$\pi(n) \approx \frac{n}{\log n}$$

where $\pi(n)$ is the number of primes less than n. We shall not go into the details of this. However, let us ask ourselves this very important question: How many primes are there? This was answered by Euclid over 2000 years back!

Theorem 1.5.1 (Euclid)**.** *There are infinitely many primes.*

Proof. Assume, to the contrary, that there are only finitely many primes (say $p_1, p_2, \ldots, p_k$). Suppose $p_1 < p_2 < \cdots < p_k$. Construct a new number $N = p_1p_2 \cdots p_k + 1$. Now N cannot be a prime, because it is clearly larger than p_k and our list of primes (in ascending order) ends at p_k. So N is composite and hence some prime p_i in our finite list of primes should divide N, i.e., $p_i \mid p_1p_2 \cdots p_k + 1$. But since $p_1p_2 \cdots p_k$ is a multiple of p_i, so we can use Lemma 1.2.1 to get $p_i \mid 1$, a contradiction. □

[2] A counterexample is an example that counters or disproves a statement.

1.6 Fundamental Theorem of Arithmetic

Clearly, you can reduce any composite number into a product of primes by a process called the prime factorization. The best part is the following:

Theorem 1.6.1. *Every positive integer n greater than 1 can be written as a product of primes in a unique way. We write this factorization as*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are different primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

Proof. There are two things that we require to prove here– Existence and Uniqueness.
Existence: We require to show that every positive integer greater than 1 is either a prime or a product of primes. Clearly, 2 is a prime. Then by strong induction[3], assume that this is true for all numbers greater than 1 and less than n. If n is prime, there is nothing to prove. If n is composite, then $n = ab$ for some integers a and b such that $1 < a \leq b < n$. By induction hypothesis, $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j}$ and $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}$ are product of primes. But then $n = ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}$ is also a product of primes.
Uniqueness: Assume, to the contrary, that there is an integer n having two distinct prime factorizations, say

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t} \tag{1}$$

for primes p_i, q_j and positive integers α_i, β_j $(1 \leq i \leq s, 1 \leq j \leq t)$. This gives

$$p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

and hence by Euclid's Lemma (Corollary 1.11.1; this will come later), p_1 must divide at least one of $q_1^{\beta_1}, q_2^{\beta_2}, \ldots, q_t^{\beta_t}$. Without loss of generality, suppose that $p_1 \mid q_1^{\beta_1}$. Since q_1 is a prime, the only prime divisor of $q_1^{\beta_1}$ is p_1. This means that $p_1 = q_1$ and $\alpha_1 = \beta_1$. Dividing both sides of equation (1) by $p_1^{\alpha_1}$, we get

$$p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s} = q_2^{\beta_2} q_3^{\beta_3} \cdots q_t^{\beta_t}.$$

With similar reasoning, we can deduce that $p_2^{\alpha_2}$ is equal to some other $q_j^{\beta_j}$, say $q_2^{\beta_2}$. Continuing this process, one soon realizes that $s = t$ and all prime powers in the left side of equation (1) appear in the right side, but maybe in a different order. In other words, the prime factorization is unique. □

1.7 Looking at Numbers as Multisets

It is often useful to look at numbers as their prime factors. So suppose we prime factorize 10 to get $10 = 2 \times 5$, we can just think of 10 as the set $\{2, 5\}$. Similarly, 15 can be thought of as $\{3, 5\}$. But what about 12? We know that $12 = 2^2 \times 3$. So we can think of

[3] In this form of induction, one proves the statement $P(m+1)$ under the assumption that $P(n)$ holds true for all natural numbers $n \leq m$; by contrast, the basic form of induction, also called weak induction, assumes only $P(m)$.

it as the multiset[4] $\{2, 2, 3\}$. So we can write $12 \equiv \{2, 2, 3\}$. Note that we use the symbol $\equiv$, which means that they are equivalent. In general,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \equiv \{\underbrace{p_1, p_1, \ldots, p_1}_{\alpha_1 \text{ times}}, \underbrace{p_2, p_2, \ldots, p_2}_{\alpha_2 \text{ times}}, \ldots, \underbrace{p_k, p_k, \ldots, p_k}_{\alpha_k \text{ times}}\}.$$

We shall use small letters to denote numbers and capital letters (of the respective small letters) to denote their multisets (unless stated otherwise). So if I have a number $n = 30$, then $N = \{2, 3, 5\}$. Also, if a number is negative, I can just include a -1. So if $n = -20$, then $N = \{-1, 2, 2, 5\}$. We clearly have the following theorem:

Theorem 1.7.1 (Divisibility in Sets)**.** *Let a, b be two integers. Then*

$$a \mid b \iff A \subset B.$$

Thinking in terms of sets is useful because we have Venn Diagrams. You will see that a lot of properties of gcd and lcm are trivialized when you think of numbers as multisets. Note that here, $\subset$ is the notation for a subset. I shall use the notation $\subsetneq$ for proper subsets.

1.8 gcd and lcm

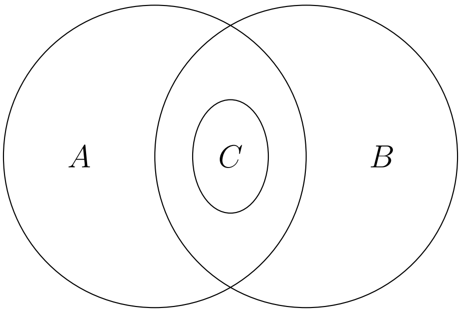
Definition 1.8.1 (gcd and lcm)**.** For two integers a and b which are not zero at the same time, the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the greatest positive integer which divides both a and b. The **least common multiple** of a and b, denoted by $\operatorname{lcm}(a, b)$, is the smallest positive integer that is divisible by both a and b. The concept is the same for the gcd and lcm of more than two integers.

Looking at the prime factorizations of a and b and their respective multisets A and B, it is clear that $\gcd(a, b) = A \cap B$ and $\operatorname{lcm}(a, b) = A \cup B$. The following lemma, therefore, makes sense.

Lemma 1.8.1. Let a, b, c be three integers. Then

$$c \mid a, c \mid b \implies c \mid \gcd(a, b).$$

Note that proving this is equivalent to proving $C \subset A, C \subset B \implies C \subset A \cap B$. We can geometrically interpret this lemma as:



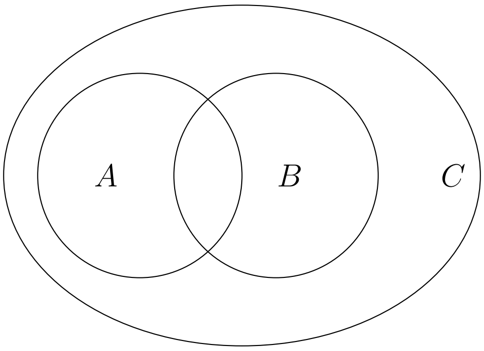
[4] A multiset is an unordered collection of elements that allows duplicates, unlike a set (in which each element occurs exactly once). The number of times an element occurs in the multiset is called the multiplicity of that element.

The following lemma also makes sense.

Lemma 1.8.2. Let a, b, c be three integers. Then

$$a \mid c, b \mid c \implies \operatorname{lcm}(a, b) \mid c.$$

Now, proving this is equivalent to proving $A \subset C, B \subset C \implies A \cup B \subset C$. This lemma can be geometrically interpreted as:



I am not going into the proofs of these set theoretic results. Now, the following obvious lemma gives you a different way to define gcd and lcm.

Lemma 1.8.3 (The prime factorization of gcd and lcm)**.** Let a, b be two integers with prime factorization

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}.$$

where α_i, β_i are non-negative integers (possibly 0). Then

$$\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)},$$
$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}.$$

As a consequence, we have the following result.

Lemma 1.8.4. For positive integers a and b,

$$\gcd(a, b) \leq a, b \leq \operatorname{lcm}(a, b).$$

When does the equality hold? See the first problem of the next problem section. Now, we have the following property that connects gcd and lcm of two numbers.

Lemma 1.8.5 (Product of gcd and lcm)**.** Let a, b be two integers. Then

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$

Proof. By Lemma 1.8.3, we have

$$\begin{aligned}\gcd(a, b) \operatorname{lcm}(a, b) &= \left(p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}\right)\left(p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}\right) \\ &= p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)+\max(\alpha_k,\beta_k)} \\ &= p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k} \\ &= \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right)\left(p_1^{\beta_1} \cdots p_k^{\beta_k}\right) = ab\end{aligned}$$

□

We can also prove this using the notion of multisets. The sum of two multisets A and B, denoted by $A+B$, is a multiset in which we include all the elements of A and B (the multiplicity of each element is also added in $A+B$). Suppose $A=\{2,2,3\}$ and $B=\{2,3,5\}$, then $A+B=\{2,2,2,3,3,5\}$.

Now observe that $(A\cup B)+(A\cap B)=A+B$, and the proof simply follows. (Note that $ab\equiv A+B$.)

1.9 Problems

Problem 1.9.1. Prove that $\gcd(a,b)=a$ if and only if $a\mid b$.

I am not going to prove this formally. But note that this is equivalent to proving

$$A\cap B=A \iff A\subset B.$$

Find a similar condition for $\operatorname{lcm}(a,b)=a$.

Problem 1.9.2. Let a,b be relatively prime. Show that if $a\mid c$, $b\mid c$, then $ab\mid c$.

To prove this, you can basically prove the result: If $A\cap B=\phi$, $A\subset C$ and $B\subset C$, then $A+B\subset C$. I shall leave the formalism in your hands.

1.10 Euclid's Division Algorithm

We always think of the gcd in terms of common prime factors. You know that when we have an expression of the form $m+n$, you can take the $\gcd(m,n)$ as common. For example, suppose $m=p^2q$ and $n=pq^2r$ for primes p,q,r. Then clearly, $\gcd(m,n)=pq$. So $m+n=pq(p+qr)$ where $\gcd(a,b)=pq$ is taken common. After all these discussion, do you see why

$$\gcd(a+b,b)=\gcd(a,b),$$
$$\gcd(a+2b,b)=\gcd(a,b),$$
$$\gcd(a+3b,b)=\gcd(a,b)?$$

Generalizing the above problems, we have the following lemma.

Lemma 1.10.1. Let a and b be two positive integers. Divide b by a and write $b=aq+r$, where q is an integer and $0\le r<a$. Then $\gcd(a,b)=\gcd(a,r)$.

Proof. Let $g=\gcd(a,b)$. So $g\mid a$ and $g\mid b=aq+r$. Now g divides a, so a is a multiple of g, and hence aq is a multiple of g. So in $g\mid aq+r$, we can forget aq to get $g\mid r$. (Note that we have used Lemma 1.2.1.) So we have proved that g divides r, but we are required to prove that g is the gcd of a and r, i.e., g is the greatest of all common divisors of a and r. So we just require to prove: if there exists some c for which $c\mid a$ and $c\mid r$, then $g\ge c$. Note that Proposition 1.2.3 gives $c\mid aq+r=b$. Thus, c is a common divisor of a and b, but g is their gcd (greatest common divisor), so $g\ge c$. □

The more useful fact to remember is that $\gcd(a,b)=\gcd(a\pm kb,b)$. One consequence of the above lemma is the so called **Division Algorithm**. Suppose we want calculate the gcd of 30 and 80. We perform division successively as follows:

$$80=30\times 2+20$$
$$30=20\times 1+10$$
$$20=10\times 2+0.$$

So $\gcd(80,30) = \gcd(30,20) = \gcd(20,10) = 10$. The last part is because 10 divides 20. The general algorithm is defined in a similar way, just keep on reducing $\gcd(a,b)$ to $\gcd(b,r)$ and eventually one number will divide the other (or the remainder becomes zero). We can write this as (I'm not writing the respective inequalities associated with the remainders at every step):

$$\begin{aligned}
a &= bq_1 + r_1\\
b &= r_1q_2 + r_2\\
r_1 &= r_2q_3 + r_3\\
&\vdots\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}\\
r_{n-2} &= r_{n-1}q_n + r_n\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}
\end{aligned}$$

where $r_{n+1} = 0$. By now you should have this question: Why does the algorithm terminate? In other words, why does the remainder eventually become zero? Think about this!

Reversing the process of the Euclid's Division Algorithm, we get the Bezout's Identity.

1.11 Bezout's Identity

Proposition 1.11.1 (Bezout's Identity)**.** For $a, b \in \mathbb{N}$, $\exists\ x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a,b).$$

Proof. We reverse the process of Euclid's Division Algorithm.

$$\begin{aligned}
\gcd(a,b) =& r_n\\
&= r_{n-2} - r_{n-1}q_n\\
&= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})\, q_n\\
&= r_{n-2}(1 + q_nq_{n-1}) - r_{n-3}(q_n)\\
&\ \vdots\\
&= ax + by
\end{aligned}$$

where x and y are some combination of quotients. □

Now if I tell you to write the gcd of 80 and 30 (which is 10, calculated as above) as a combination of 80 and 30. Reverse the process of division algorithm applied to 80 and 30 (refer to that) here.

$$\begin{aligned}
\gcd(80,30) = 10 &= 30 - 20 \times 1\\
&= 30 - (80 - 30 \times 2) \times 1\\
&= 30 \times 3 + 80 \times (-1).
\end{aligned}$$

Lemma 1.11.1. If $c \mid ab$ and $\gcd(c,a) = 1$, then $c \mid b$.

Proof. Use Bezout's identity here. Since $\gcd(c,a) = 1$, so $cx + ay = 1$ for some integers x, y. Multiplying $cbx + aby = b$. Now we can use the fact that $c \mid ab$ to get $ab = ck$ for some integers k. Using this, we get $cbx + cky = b \implies c(bx + ky) = b \implies c \mid b$. □

As a corollary, we have the following result.

Corollary 1.11.1 (Euclid's Lemma)**.** If $p \mid ab$ for a prime p and integers a, b, then $p \mid a$ or $p \mid b$. In fact, the generalization: if $p \mid a_1 a_2 \cdots a_k$, then p divides at least one of $a_1, a_2, \ldots, a_k$, also holds true.

Proof. Given that $p \mid ab$. If $p \mid a$, then we are done. If $p \nmid a$, then $\gcd(a, b) = 1$. Using the previous lemma, we have $p \mid b$. (See for yourself why the generalization is true.) □

Do you remember that the question I asked before after I proved the Euclid's Division Lemma? Adding the extra condition $\gcd(a, b) = 1$, we have the following proposition.

Proposition 1.11.2. Let a, b, n be positive integers such that $\gcd(a, b) = 1$, $a \mid c$ and $b \mid c$. Then $ab \mid c$.

Proof. We shall use Bezout's identity. We know that $\exists\ x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b) = 1. \tag{2}$$

Since $a \mid c$ and $b \mid c$, so $c = ak_1 = bk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Multiplying equation (2) by k_2, we get

$$\begin{aligned} & ak_2x + bk_2y = k_2 \\ \Longrightarrow\ & ak_2x + ak_1y = k_2 \\ \Longrightarrow\ & ab(k_2x + k_1y) = bk_2 = c \\ \Longrightarrow\ & ab \mid c. \end{aligned}$$

□

I shall not discuss any more theory now. We shall solve some problems. But before that, see for yourself why the following equation is true:

$$\gcd\left(a^m - 1, a^n - 1\right) = a^{\gcd(m,n)} - 1. \tag{3}$$

Hint: Apply Euclid's Division Algorithm over the powers m, n.

1.12 Problems

Problem 1.12.1 (PUTNAM 2000)**.** Prove that the expression

$$\frac{\gcd(m, n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

Solution 1.12.1. We apply Bezout's Identity. Write $\gcd(m, n) = mx + ny$. Therefore,

$$\begin{aligned} \frac{\gcd(m, n)}{n}\binom{n}{m} &= \frac{mx + ny}{n}\binom{n}{m} \\ &= x \cdot \frac{m}{n}\binom{n}{m} + y\binom{n}{m} \\ &= x \cdot \frac{m}{n} \cdot \frac{n!}{m!(n-m)!} + y\binom{n}{m} \\ &= x \cdot \frac{(n-1)!}{(m-1)!((n-1)-(m-1))!} + y\binom{n}{m} \\ &= x\binom{n-1}{m-1} + y\binom{n}{m} \in \mathbb{Z}. \end{aligned}$$

as both the addends are integers. □

Problem 1.12.2 (All Russia Mathematics Olympiad 1995)**.** Let m, n be positive integers such that

$$\gcd(m, n) + \operatorname{lcm}(m, n) = m + n.$$

Show that one of the two numbers is divisible by the other.

Solution 1.12.2. Let $\gcd(m, n) = g$. It seems that we really can't do anything here, other writing $\operatorname{lcm}(m, n) = mn/g$. Let's do that.

$$g + \frac{mn}{g} = m + n \implies mn + g^2 = g(m + n) \implies (m - g)(n - g) = 0.$$

Therefore $g = m$ or $g = n$. Remember that we had seen: $\gcd(a, b) = a \iff a \mid b$ (this was Problem 1.9.1). So $g = m \iff m \mid n$ and $g = n \iff n \mid m$,i.e., one of m, n is divisible by the other. □

Problem 1.12.3 (Iran 2005)**.** Let $n, p > 1$ be positive integers and p be a prime. Given that $n \mid p - 1$ and $p \mid n^3 - 1$, prove that $4p - 3$ is a perfect square.

Solution 1.12.3. $n \mid p - 1 \implies p \geq n + 1$ and $p = nk + 1$ for some $k \in \mathbb{Z}$. Now how do you approach this problem? Looking at $n^3 - 1$ hints you to write it as $(n - 1)(n^2 + n + 1)$ and then apply the Euclid's Lemma. Let's do that.

$$p \mid (n - 1)(n^2 + n + 1) \implies p \mid n - 1 \text{ or } p \mid n^2 + n + 1.$$

But note that $p \mid n - 1$ implies $p \leq n - 1$, which contradicts $p \geq n + 1$. Therefore, $p \mid n^2 + n + 1$ only and hence,

$$p \leq n^2 + n + 1 \tag{4}$$

Note that we haven't really used $p = nk + 1$ yet. We use this now:

$$nk + 1 \mid n^2 + n + 1 \mid k(n^2 + n + 1) \implies nk + 1 \mid kn^2 + kn + k - n(nk + 1) = kn + k - n.$$

So $nk + 1 \leq kn + k - n \implies n + 1 \leq k$. Therefore,

$$p = nk + 1 \geq n(n + 1) + 1 = n^2 + n + 1.$$

Combining this with equation (4), we get $p = n^2 + n + 1$. Now you can calculate further to get $4p - 3 = (2n + 1)^2$, which is obviously a perfect square. □

Problem 1.12.4. Define the n^{th} Fermat number $F_n = 2^{2^n} + 1$, $n \geq 0$. Show that for $m \neq n$, $\gcd(F_m, F_n) = 1$.

I shall not prove this. But I'll give you a walkthrough of the solution: First prove the identity $F_n - 2 = F_{n-1}F_{n-2} \cdots F_0$. Suppose $n > m$, then $F_m \mid F_n - 2$. If a prime p divides both F_m and F_n, then $p \mid 2$. (Why?) Do you now see why F_m, F_n should be *relatively prime* (i.e., gcd of them is 1)?

As an ending note, let me cite the book I followed for these notes: Modern Olympiad Number Theory by *Aditya Khurmi*. This book mostly covers all the theory required for number theory in olympiads.