Elementary Number Theory
B. Math. (Hons.) First year
Instructor : B. Sury

September 30, 2021

Introduction.

Among the three texts prescribed in the syllabus, I will primarily follow the one by Niven-Zuckermann-Montgomery. However, I will also discuss examples and applications that may not be found in any of these texts but are relevant to the topics of the syllabus.

Before beginning with purely number theoretic content, we start by discussing certain basic principles that play in many parts of mathematics including number theory. These primarily consist of three topics: (i) Principle of Inclusion-Exclusion, (ii) Pigeon-hole Principle, and (iii) Mathematical Induction. These are introduced and discussed briefly in the beginning and a more detailed study is done at a later stage of the course.
One maxim for this course: Solve as many problems as you can.

Right in the beginning, we recall a basic axiom which we will keep using throughout.

Well-ordering Principle. *Every non-empty set S of integers has a least element; that is, there exists $s \in S$ such that $s \leq t$ for all $t \in S$.*

1 Mathematical Induction

The Principle of Mathematical Induction is an **AXIOM**; it cannot be proved, But, one usually thinks of it as a consequence of the well-ordering principle. The assertion is:
Let S be a set of natural numbers with the two properties :
a natural number $n_0 \in S$, and
whenever $n \geq n_0$ and $n \in S$, we have $n+1 \in S$.
Then S contains all the natural numbers $n \geq n_0$.

One deduces this from the well-ordering principle as follows. If S is not the whole of $\{n|n \geq n_0\}$, consider the set

$$T := \{n \in \mathbb{N} : n \geq n_0, n \notin S\}.$$

This, being a non-empty set of natural numbers, has a least element t. Clearly, $t > n_0$ as $n_0 \in S$; so, $t-1$ is a natural number $\geq n_0$. It is not in T by the choice of t as smallest; hence $t-1 \in S$. By the property of S, this implies $t = (t-1)+1 \in S$, which gives a contradiction. Hence, T must be empty.

Induction is often applied as follows. If a statement S_n is to be proved to be valid for all natural numbers $n \geq n_0$. One first proves S_{n_0} to be valid. Then, one assumes that S_m is valid for all m with $n_0 \leq m \leq n$ and proves S_{n+1} to be valid.

Binomial Theorem for positive integer powers

If u, v are complex numbers, and $n \in \mathbb{N}$, then

$$(u+v)^n = \sum_{r=0}^{n} \binom{n}{r} u^r v^{n-r}$$

where $\binom{n}{r} := \frac{n!}{r!(n-r)!}$.
This follows by induction on n if we use the property

$$\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}$$

for $1 \leq r \leq n$. Note that this identity itself follows on multiplying the evident identity

$$\frac{1}{r} + \frac{1}{n-r+1} = \frac{n+1}{r(n-r+1)}$$

by $\frac{n!}{(r-1)!}(n-r)!$.

Here are more applications of induction. I urge you to try these problems first before looking up the solutions given below. I leave problem 2 as an exercise.

Problem 1.
Prove Fermat's little theorem :
If p is a prime number, then $n^p - n$ is a multiple of n for any natural number n. In particular, if n is a natural number not divisible by p, then p divides $n^{p-1} - 1$.

Problem 2.
Suppose n is a natural number and that two girls Archana and Bharati are assigned one each among the numbers n and $n + 1$. They know their numbers are consecutive but do not know whose number is bigger. After every second a beep goes off and each of them announces independently and simultaneously whether she knows the other's number or not. Prove that after exactly n beeps (and not before), the girl with the smaller number n guesses her friend's number.

Problem 3.
Prove that every rational number $\frac{m}{n}$ with $0 < \frac{m}{n} < 1$ can be expressed as a sum of fractions $\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$ where $n_1 < n_2 < \cdots < n_k$.

Problem 4.
Find the minimum number of steps needed to solve the 'tower of Hanoi' problem :
There are n rings placed around a tower. The rings are numbered 1 to n from top to bottom. The problem is to slide the rings out of the first tower and on to a second tower. The rule is to never have a ring with a larger number over one with a smaller number. To accomplish this, a third tower is also provided.

Problem 5.
Prove that the sequence of numbers defined by $a_1 = 2, a_{n+1} = a_1 a_2 \cdots a_n + 1$ satisfies, for any n, the identity

$$\sum_{i=1}^{n} \frac{1}{a_i} + \prod_{i=1}^{n} \frac{1}{a_i} = 1.$$

Can you deduce from this that there exist infinitely many prime numbers?

Problem 6.
If n points on a circle are joined by all possible secants, find the number of regions produced inside the circle provided no third secant passes through a point of intersection of two secants.

Problem 7.
Consider the Fibonacci sequence defined recursively by $F_1 = 1 = F_2$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 2$. Prove that $F_{n+1} = \sum_{i=0}^{[n/2]} \binom{n-i}{i}$.
Here $[x]$ denotes the largest integer $\leq x$.

Problem 8.
For every natural number n, show that $\sum_{r=0}^{n}(-1)^r \binom{n}{r}(n-r)^d = 0$ if $d < n$ and equals $n!$ if $d = n$.

Problem 9.
Show that the n-th prime number p_n is at the most $2^{2^{n-1}}$.

Problem 10.
Solve the 'marriage problem' by induction :
Suppose each girl among a set of n girls is acquainted with a set of boys in such a way that for each $m \leq n$, the total number of boys that every subset of m girls is aquainted with, is at least m. Then, show that each of the n girls can be paired with a boy who is also an acquaintance.

Solution 1.
Now $1^p - 1 = 0$ which is certainly a multiple of p. Assume that $n^p - n$ is a multiple of p for some $n \geq 1$. Now

$$(n+1)^p-(n+1) = 1+\binom{p}{1}n+\binom{p}{2}n^2+\cdots+n^p-(1+n) = \sum_{r=1}^{p-1}\binom{p}{r}n^r+n^p-n.$$

Now, for each r in between 1 and $p-1$, the number $\binom{p}{r}r(r-1)\cdots 1 = p(p-1)\cdots(p-r+1)$ is a multiple of p whereas p does not divide any of $r, r-1, \cdots, 1$. As p is a prime, we have therefore that p divides $\binom{p}{r}$ for $1 \leq r < p$. Hence $(n+1)^p - (n+1) = n^p - n +$ a multiple of p. As $n^p - n$ is already a multiple of p by assumption, we have that $(n+1)^p - (n+1)$ is also a multiple of p. Therefore, by mathematical induction, it follows that $a^p - a$ is a multiple of p for every natural number a.
To prove the second statement, we have $a^p - a = a(a^{p-1} - 1)$ to be a multiple of p and, for a not divisible by p, this means that $a^{p-1} - 1$ is a multiple of p.

Solution 3.
We apply induction on the numerator m of the fraction. If $m = 1$, clearly $\frac{m}{n}$ is already of the form asserted. Assume now that $m > 1$ and that every fraction $\frac{k}{l}$ with $1 \leq k < m$ is expressible in the asserted form. Write $\frac{1}{r} \leq \frac{m}{n} < \frac{1}{r-1}$

for a unique $r \geq 2$. Then,

$$\frac{m}{n} - \frac{1}{r} = \frac{mr - n}{rn}.$$

As $mr - n < m$ (since $\frac{m}{n} < \frac{1}{r-1}$), we may write $\frac{mr-n}{rn} = \sum_{i=1}^{k} \frac{1}{n_i}$ with $n_1 < n_2 < \cdots < n_k$. But then

$$\frac{m}{n} = \frac{1}{r} + \sum_{i=1}^{k} \frac{1}{n_i}.$$

We note that $r < n_1$; otherwise, we would have $\frac{m}{n} - \frac{1}{r} \geq \frac{1}{n_1} \geq \frac{1}{r}$ which implies $\frac{m}{n} \geq 2r$. This would mean $\frac{1}{r-1} > \frac{2}{r}$; that is, $r < 2$ which is impossible. Therefore, $r < n_1$ and the expression $\frac{m}{n} = \frac{1}{r} + \sum_{i=1}^{k} \frac{1}{n_i}$ is as asserted.

Solution 4.
For $n = 1$, it takes only one step to move the ring from the first tower to the second one (and does not require a third tower). Assume $f(n)$ is the least number of steps required for n rings. Suppose $n > 1$. Move the top $n - 1$ rings to the second tower - this requires $f(n-1)$ steps. Then move the n-th ring to the third tower - this is one step. Move the rings 1 to $n - 1$ from the second to the third to tower - this again requires $f(n-1)$ steps. Thus, $f(n) = 2f(n-1) + 1$. By induction, we get $f(n) = 2^n - 1$.

Solution 5.
Clearly the assertion holds for $n = 1$ since $a_1 = 2$. Assume that it holds for some $n \geq 1$. Now

$$\sum_{i=1}^{n+1} \frac{1}{a_i} + \prod_{i=1}^{n+1} \frac{1}{a_i} = \frac{1}{a_{n+1}} + \sum_{i=1}^{n} \frac{1}{a_i} + \frac{1}{a_{n+1}} \prod_{i=1}^{n} \frac{1}{a_i}$$

$$= \frac{\prod_{i=1}^{n} a_i + 1}{a_{n+1} \prod_{i=1}^{n} a_i} + \sum_{i=1}^{n} \frac{1}{a_i} = \frac{1}{\prod_{i=1}^{n} a_i} + \sum_{i=1}^{n} \frac{1}{a_i} = 1$$

since $a_{n+1} = \prod_{i=1}^{n} a_i + 1$.
Finally, notice that since each a_k is relatively prime to all the a_r with $r < k$ (it leaves a remainder 1), each prime divisor of a_k gives a new prime which does not occur in the prime factorisations of a_r with $r < k$.

Solution 6.
Any two points give rise to a secant and we have $\binom{n}{2}$ secants produced by n

points. Each secant gives rise to an additional region. Further, each set of 4 points produces exactly two secants which have one point of intersection in the interior of the circle - there are $\binom{n}{4}$ such points inside. Each such point of intersection gives rise to an additional region. Therefore, starting with the single region, the total number of regions produced is $\binom{n}{2} + \binom{n}{4} + 1$.

Solution 7.
Clearly, the identity $\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}$ gives us the same recursion for $\sum_{i=0}^{[n/2]} \binom{n-i}{i}$ as the one defining the Fibonacci numbers. Since the values match for $n = 1$ and $n = 2$, we have the assertion.

Solution 8.
Let $f(x)$ be any function and define the 'forward difference operator' Δ on f by $(\Delta f)(x) = f(x+1) - f(x)$. We have $(\Delta^2 f)(x) = \Delta(\Delta f)(x) = f(x+2) - 2f(x+1) + f(x)$. By induction on n, it follows that

$$(\Delta^n f)(x) = \sum_{r=0}^{n} (-1)^r \binom{n}{r} f(x+n-r).$$

This just uses again the identity $\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}$. Now, if $f(x)$ happens to be a polynomial of degree d, we observe that $(\Delta f)(x) = f(x+1) - f(x)$ is again a polynomial whose degree is less than d because the top degree term cancels. Therefore, if $d < n$, then $(\Delta^n f)(x)$ is the zero polynomial. Also, $(\Delta^d f)(x)$ is a constant whose value is $d!$ as proved also by induction on d. The assertion of the problem follows by taking $f(x) = x^d$.

Solution 9.
If $p_1 < p_2 < p_3 < \cdots$ denotes the sequence of all prime numbers, then clearly $p_1 p_2 \cdots p_n + 1$ leaves a remainder of 1 on division by each of the first n primes. So, its smallest prime factor is at least p_{n+1}. In other words

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1.$$

Now $p_1 = 2 \leq 2^{2^0}$ which verifies the assertion of the problem when $n = 1$. Assume now that $n \geq 1$ and that $p_k \leq 2^{2^{k-1}}$ for all $1 \leq k \leq n$. Then,

$$p_{n+1} \leq 2^{1+2+\cdots+2^{2^n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n}$$

as $1 \leq 2^{2^n-1}$.

Solution 10 - Hall's marriage problem:
We apply induction. Clearly, the result holds for $n = 1$. Assume $n > 1$ and that the result holds for all $m < n$.
If, for each k between 1 and $n-1$, every set of k girls are acquainted with at least $k+1$, then get an arbitrary girl married off with an arbitrary acquaintance. Apply induction to the $n-1$ case and we are done. In the other case, suppose there is some $k < n$ such that there is a set of k girls with exactly k acquaintances. The rest of the $n-k$ couples satisfy the hypothesis of the marriage theorem for $n-k$ (otherwise, there is some set of $r \leq n-k$ girls with less than r acquaintances and then there is a set of $r+k$ girls with less than $r+k$ acquaintances in the original set, which is a contradiction of the hypothesis). Thus, one can marry off the rest of the $n-k$ girls with acquaintances by induction. Similarly, applying induction to the set of k girls, we have the theorem for n.

2 The Principle of Inclusion and Exclusion

PIE as the title can be referred to briefly, is an easy combinatorial principle that applies in situations where counting is involved.

If A and B are two finite, overlapping sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

where $|A|, |B|$ etc. denote the sizes of A, B etc. If A, B, C are three finite sets, one can deduce from the above (by replacing B by $B \cup C$) that:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

The PIE allows us to write down an expression for the size of the union of a finite number of finite sets in terms of the sizes of the various partial intersections among them. The general formula (which can be proved by mathematical induction - which will be recalled below) asserts that for finite sets $A_1, \cdots, A_n$, we have:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=0}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |\bigcap_{j=1}^{n} A_i|.$$

This general formula easily lends itself to immediate applications, such as:

If $m_1, m_2, \cdots, m_r$ is a finite sequence of positive integers (that is, some of them may be equal and they may be in any order), then

$$\max(m_1, \cdots, m_r) =$$

$$\sum_i m_i - \sum_{i<j} min(m_i, m_j) + \sum_{i<j<k} min(m_i, n_j, m_k) - \cdots + (-1)^{r-1} min(m_1, \cdots, m_r).$$

In the above expressions, 'max' and 'min' indicate maximum and minimum respectively.

If $n_1, \cdots, n_r$ are arbitrary positive integers, then looking at the exponents $m_1, \cdots, m_r$ to which any prime divides the numbers, and applying the above identity, one obtains:

$$[n_1, \cdots, n_r] = \frac{(\prod_i n_i)(\prod_{i<j<k}(n_i, n_j, n_k)) \cdots}{(\prod_{i<j}(n_i, n_j))(\prod_{i<j<k<l}(n_i, n_j, n_k, n_l)) \cdots}.$$

Here, $[a_1, \cdots, a_k]$ and $(a_1, \cdots, a_k)$ denote the LCM and GCD respectively. This is the generalization of the usual relation $(a, b)[a, b] = ab$.

Another application of PIE is:
If N is a positive integer, and $n_1, n_2, \ldots$ are positive integers, any two of which are relatively prime, then the number of elements of $\{1, 2, 3, \ldots, N\}$ which are not divisible by any of the numbers $n_1, n_2, \ldots$ is

$$N - \left(\left[\frac{N}{n_1}\right] + \left[\frac{N}{n_2}\right] + \cdots\right) + \left(\left[\frac{N}{n_1 n_2}\right] + \left[\frac{N}{n_1 n_3}\right] + \left[\frac{N}{n_2 n_3}\right] + \cdots\right) - \cdots.$$

There is a special case of the above formula which is of great interest in number theory. We consider the following problem.

> *For a given positive integer N, what is the number of positive integers not exceeding N which are relatively prime to N?*

The numbers which are relatively prime to N are exactly those which are not divisible by any of the prime divisors of N. Let us denote the primes dividing N by $p, q, r, \ldots$. Now we apply the idea described in the last section. We conclude that the required number is:

$$N - \left(\frac{N}{p} + \frac{N}{q} + \frac{N}{r} + \cdots\right) + \left(\frac{N}{pq} + \frac{N}{qr} + \frac{N}{pr} + \cdots\right) - \cdots. \tag{1}$$

By factoring out N we find that the resulting expression can be factorized in a convenient manner; we get the following:

$$N\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\cdots. \tag{2}$$

For example, take $N = 30$. Since $30 = 2 \times 3 \times 5$, we see that the number of positive integers not exceeding 30 and relatively prime to 30 is

$$30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$$

This is easily checked. (The positive integers less than 30 and relatively prime to 30 are 1, 7, 11, 13, 17, 19, 23 and 29.)

The second formula defines the famous *totient function* which we associate with the name of Euler. The symbol reserved for this function is $\varphi(N)$. So we may write:

$$\varphi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right), \tag{3}$$

the product being taken over all the primes p that divide N; that is why we have written '$p \mid N$' below the product symbol. (The symbol $\prod$ is used for products in the same way that $\sum$ is used for sums.)
Later, we will be studying 'arithmetic' functions such as $\phi(n)$ in detail.

One further example is the enumeration of 'derangements' - the number of ways that n envelopes bearing addresses of n people are mailed so that nobody gets the right envelope. the number of possibilities when *nobody* receives their correct letter to be

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^n \binom{n}{n} 0! = n! \sum_{r=0}^{n} \frac{(-1)^r}{r!}$$

This is left as an exercise and so is the next problem.

Exercise. Use PIE to show that there are exactly 100 composite numbers not exceeding 1000 which are not multiples of any of the three primes $2, 3$ and 5.

3 Pigeon-hole Principle

This rather simple principle has remarkably strong applications. The pigeon-hole principle was formulated by Dirichlet and is also known as Schubfach-prinzip (schubfach means drawer). Simply stated, it says that if some pigeons are to be placed inside pigeon-holes and there are more pigeons than pigeon-holes, then at least one pigeon-hole must have more than one pigeon. Here are some striking applications of this principle. Try them first before looking at the solutions given below.

Problem 11.
In any party, show that there are (at least) two people who shake hands with the same number of people.

Problem 12.
Given natural numbers $a_1 < a_2 < \cdots < a_{n+1}$ between 1 and $2n$, prove that a_i divides an a_j for some $i \neq j$.

Problem 13.
Show that every natural number n has a multiple of the form $11\cdots10\cdots0$. We can deduce from this that every rational number can be expressed as $\frac{a}{10^b(10^c-1)}$ for some integer a and natural numbers b, c.

Problem 14.
Suppose 25 boys and 25 girls are sitting around a table. Argue that some person must have both neighbors to be girls.

Problem 15.
Inside a forest of dimension 12 miles by 12 miles, if there are 13 lions, argue that there must be two at a distance less than 5 miles.

Problem 16.
If a, b are relatively prime natural numbers, then use the pigeon-hole principle principle to prove that there is a natural number $x < b$ and an integer y such that $ax + by = 1$.

Problem 17.
If every point of the co-ordinate plane is colored either black or white, prove that there must be some rectangle all of whose vertices have the same colors. Generalize to c colors.

Problem 18.
Let $f(X)$ be a polynomial with integer coefficients such that $f(a_1) = f(a_2) = f(a_3) = 2$ for distinct integers a_1, a_2, a_3. Show that there is no integer b such that $f(b) = 3$.

Solution 11.
Suppose there are n people in the party and name them $P_1, \cdots, P_n$. Make an array as follows and fill in the (i, j)-th square with 1 or 0 according as to whether P_i and P_j shake hands or not.

$*$	P_1	P_2	$\cdots$	$\cdots$	P_n
P_1					
P_2					
$\cdot$					
$\cdot$					
P_n					

Thus, the sum s_i of the i-th row is the number of people that the i-th person P_i shakes hands with. The n sums $s_1, s_2, \cdots, s_n$ are all among the n numbers $0, 1, \cdots, n-1$. Now, the numbers 0 and $n-1$ cannot both be values because then there would be a person shaking hands with nobody and one shaking hands with everybody ! Thus, the numbers $s_1, \cdots, s_n$ (the 'pigeons') must be fit inside less than n numbers occurring among $0, 1, \cdots, n-1$ ('pigeon-holes'). So, some $s_i = s_j$ with $i \neq j$.

Solution 12.
Writing $a_i = 2^{b_i} c_i$ with c_i odd and $b_i \geq 0$, we have n pigeon-holes (the odd numbers between 1 and $2n$) and $n + 1$ pigeons $(c_1, \cdots, c_n)$ to fit them in. Thus, $c_i = c_j$ for some $i \neq j$. Now, a_i divides a_j or a_j divides a_i according as to whether $b_i < b_j$ or $b_j < b_i$.

Solutions 13.
To prove 3 first, start with any natural number n. Consider the sequence of numbers $1, 11, 111, 1111, \cdots\cdots$ On dividing them by n, they leave remainders which we denote by r_1, r_2, r_3 etc. But the possible remainders on division by n are the n numbers $0, 1, \cdots, n-1$. Hence there must be two different numbers of the form $11 \cdots 1$ which leave the same remainder on division by n. But then their difference is a multiple of n and is of the asserted form.
Finally, to deduce the second part, start with any rational number $\frac{d}{n}$ where

n is a natural number and d is an integer (possibly zero). If a multiple kn is of the form in problem 3, then the multiple $9kn$ is of the form $99\cdots90\cdots0$ which is a number of the form $10^b(10^c-1)$. Thus

$$\frac{d}{n}=\frac{9kd}{9kn}=\frac{9kd}{10^b(10^c-1)}.$$

Solution 14.
Name the persons in the sitting order (start anywhere) as $P_1, P_2, \cdots, P_{50}$. Bring one more table and make the odd-numbered persons $P_1, P_3, \cdots, P_{49}$ around it in the same order. Now, if originally no person had two girl neighbours, it follows that after the movement of the off-numbered people to the new table, neither table has 2 girl neighbours ! But then in each table there are at the most 12 girls (as each table has 25 persons). Thus it is impossible to account for the 25 girls.

Solution 15.
Dividing the forest into 12 rectangles of dimensions 3 miles by 4 miles, one of the rectangles must have 2 lions. The diagonal of any of these rectangles has length at the most 5 miles.

Solution 16.
The natural numbers $a, 2a, \cdots, (b-1)a$ leave non-zero remainders on dividing by b. Moreover, if two different ones among them leave the same remainder, their difference (which is again of the form ka with $1 \leq k < b-1$) is a multiple of b which is impossible. Thus, they all leave different remainders which must be the numbers $1, 2, \cdots, b-1$ in some order. In particular, there is some ax with $1 \leq x < b$ so that $ax - 1 = bd$ for some natural number d. Take $y = -d$ and we have $ax + by = 1$.

Solution 17.
Consider any three horizontal lines and any vertical line. The three points of intersection can have any one of $2^3 = 8$ color combinations. Thus, if we consider 9 vertical lines, there are at least 2 vertical lines such that the the color combination of points of intersections with the three horizontal lines is identical for both. As at least two of the three points of intersection are identically colored, we have a rectangle with all four vertices with the same color.

Solution 18.
Writing $f(X) = c_0 + c_1X + \cdots + c_nX^n$, notice that for any two integers a, b we have $f(b) - f(a) = (b-a)(c_1 + c_2(b+a) + \cdots + c_n(b^{n-1} + b_{n-2}a + \cdots + a^{n-1})$. In particular, $b - a$ divides $f(b) - f(a)$. Now, if there exists an integer b so that $f(b) = 3$, then we would have each of the three distinct integers $b - a_1, b - a_2, b - a_3$ to be factors of $f(b) - f(a_i) = 3 - 2 = 1$. As 1 has only 1 and -1 as factors, this is an impossibility.

4 Euclidean Division Algorithm

We will assume the fundamental theorem of arithmetic which asserts that every positive integer > 1 is uniquely (up to order) expressible as a product of prime numbers.

Theorem. If a, b are integers with $b \neq 0$, then the division algorithm assures us that there exist integers q, r with $0 \leq r < |b|$ and $a = qb + r$.
The proof is as follows.
By the well-ordering principle, the (non-empty) set of non-negative numbers among the set $\{a - qb : q \in \mathbb{Z}\}$ has a least element; call it r. Then, $0 \leq r < |b|$. Indeed, if $r \geq |b|$, we derive a contradiction as follows.
When $b > 0$, then if $r = a - qb \geq |b| = b$, we have

$$0 \leq r' := a - b(q+1) < a - bq = r;$$

a contradiction.
When $b < 0$, then if $r = a - qb \geq |b| = -b$, then

$$0 \leq r' := a - b(q-1) < a - qb = r;$$

a contradiction.

Recall that the Euclidean division algorithm implies that the GCD of any two positive integers m, n can be found by successive usage as the remainder keeps decreasing until it reaches 0. Indeed, write

$$m = q_1 n + r_1;$$

$$n = r_1 q_2 + r_2;$$

$$r_1 = r_2 q_3 + r_3;$$

$$\cdots\cdots\cdots$$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1};$$

$$r_{n-2} = r_{n-1} q_n$$

where $r_n = 0$. Note that $n > r_1 > r_2 > \cdots > r_{n-1} > r_n = 0$ as the remainders are non-negative and decreasing until they reach 0. Notice that inductively each r_i is of the form $mu + nv$ for some integers u, v. So, if d divides m and n, then it divides each r_i; in particular, d divides r_{n-1}. Now, r_{n-1} divides r_{n-2} by the last equality, which implies it divides r_{n-3} by the penultimate one. Proceeding in this manner, r_{n-1} divides both m and n. Hence, $r_{n-1} = GCD(m, n)$.

Henceforth, we will write (m, n) for $GCD(m, n)$.
The fact that the GCD of m, n is of the form $mu + nv$ can also be proved non-constructively as follows.
Among the positive integers of the form $mu+nv$, choose the smallest one. If $d = mu+nv$, then each divisor of m, n divides d. Further, d itself must divide m as well as n for, dividing m by d, we have $m = qd+r$ with $0 \leq r < d$ which gives $r = m - qd = m(1 - qu) + n(-qv) < d$, which would be a contradiction of the choice of d as the smallest of that form unless $r = 0$. Hence, $d|m$; similarly, $d|n$. hence $d = (m, n)$.

The above proof yields also:
Corollary. For integers m, n - not both zero - the set $\{mu + nv : u, v \in \mathbb{Z}\} = \{dr : r \in \mathbb{Z}\}$ where $d = (m, n)$.

Now, we recall:

The Fundamental Theorem of Arithmetic. Every positive integer $n > 1$ can be expressed as a product of prime numbers, uniquely up to ordering.
The proof of existence of a product expression follows by induction applied suitably. Start with 2 which is a prime and there is nothing to prove. Assume $n > 2$ and that for every $1 < m < n$, the positive integer m is expressible as a product of prime numbers. Now, if n is prime, then there is nothing to prove. If not, then it is composite and, by the well-ordering principle, we have a smallest positive number d_1 with $1 < d < n$ which divides n. Writing $n = d_1 n_1$, we have that both d_1 and n_1 are larger than 1 and less than n. By

the induction hypothesis, both of them are products of primes which means that n itself is such a product.
To prove uniqueness, let $p_1p_2\cdots p_r = q_1q_2\cdots q_s$ for primes p_i, q_j, with $r+s$ smallest possible. If $r+s=2$, we clearly have $r=s=1$ and $p_1=q_1$. Assume $r+s>2$. Then, since p_1 is a prime dividing $q_1q_2\cdots q_s$, it divides one of the q_j's, say q_k. As q_j's are primes, we have $p_1=q_k$. Canceling off this from both sides, we have an equality of products whose sum of lengths is $r+s-2<r+s$. We derive a contradiction to the choice of $r+s$, This proves the theorem.

by the fundamental theorem of arithmetic, we have the property of primes that, then $u=1$ or $v=1$. Other basic properties of divisibility also follow such as:
$(ra, rb) = r(a, b)$ for any positive integer r;
$(a+bc, b) = (a, b)$ for a, b, c integers; and
$a|bc$ and $GCD(a, c) = 1$ implies $a|b$.
$(m, n) = \prod_{p\ prime} p^{min(v_p(m), v_p(n)}$ where $v_p(n)$ is the power of p dividing n (allowing 0).
Similarly, $[m, n] := LCM(m, n) = \prod_{p\ prime} p^{max(v_p(m), v_p(n)}$.