

Lecture 1: Elementary Number Theory

The integers are the simplest and most fundamental objects in discrete mathematics. All calculations by computers are based on the arithmetical operations with integers (or more precisely, with finite decimals). The central ideas of the mathematical logic, theory of algorithms, and set theory also originate in elementary number theory.

The set of integers is denoted by Z . That is $Z = \{0, \pm 1, \pm 2, \dots\}$. The non-negative integers (natural numbers) are denoted by N $N = \{0, 1, 2, \dots\}$. The positive integers are denoted by Z^+ .

To represent integers, we use a *position-value* system with the base 10. For example, $573 = 5 \cdot 10^2 + 7 \cdot 10 + 3 \cdot 1$, i.e., it is a sum of digital multiples of powers of 10. Another way to say this is that each integer is represented as a linear combination of powers of ten: $1 = 10^0, 10 = 10^1, 100 = 10^2, 1000 = 10^3, \dots$ with coefficients from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The fact that we are using the base 10 is only an anatomical accident. In computer science, the systems with bases: $b = 2, 4$, or 16 are more popular.

The following example in *binary* notation will further illustrate the idea of positional notation:

$$(1011)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = 8 + 2 + 1 = (11)_{10}$$

For the binary system (base 2), the digits are only 0 and 1, while in decimal notation:

$$(\overline{a_k a_{k-1} \dots a_0})_{10} = a_k \cdot 10^k + a_{k-1} 10^{k-1} + \dots + a_1 \cdot 10 + a_0,$$

where each of the digits a_i is one of the decimal digits 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9 and $a_k \neq 0$. The overbar notation is used to emphasize the fact that we are using position notation. We use the overbar notation when the expression would otherwise be ambiguous. For example xyz might be misunderstood. Thus xyz means the product $x \cdot y \cdot z$ whereas \overline{xyz} means $100x + 10y + z$.

For arbitrary base b , $(a_k \dots a_1 a_0)_b = a_k \cdot b^k + \dots + a_1 \cdot b + a_0$, where $0 < a_k < b$ and all the other a_j 's satisfy $0 \leq a_j < b$.

The invention of position-value system is due to several cultures, Babylonian, Hindu, and Arab. It represents one of the greatest inventions of the human mind. Ancient European systems, for example the Roman system, where

$$7 = VII, \quad 13 = XIII, \quad 24 = XXIV \text{ etc.}$$

were inappropriate for most calculations.

Let's discuss arithmetic operations for the classical system. These operations have an *algorithmic nature*, that is, they can be represented as a sequence of elementary steps (commands). We must not use our intuition. Arithmetic operations can be simply realized on the computer, especially for the binary system (base $b = 2$). It will be the subject of Lecture 2. In the next few examples, we illustrate the algorithmic nature of arithmetic operations.

Examples of operations

1. *Addition.* The addition problem $23+379$ is written in vertical format with a zero inserted before the 2 of 23 to produce two three digit numbers.

$$\begin{array}{r} 023 \\ +379 \\ \hline 402 \end{array}$$

Each of the two digit sums $3+9$, $2+7$, and $0+3$ can be read from the table of digit sums. All that is needed besides the table is the idea of "carry".

2. *Multiplication.* Multiplication is based on the table of multiplication for digits.

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	21	24	27
4	4	8	12	16	20	24	28	32	36
5	5	10	15	20	25	30	35	40	45
6	6	12	18	24	30	36	42	48	54
7	7	14	21	28	35	42	49	56	63
8	8	16	24	32	40	48	56	64	72
9	9	18	27	36	45	54	63	72	81

With this table, multiplication can be reduced to a series of additions. The only problem is to carry over suitable numbers to the higher digits (if necessary).

$$\begin{array}{r} 137 \\ \times 43 \\ \hline 411 \\ 5480 \\ \hline 5891 \end{array}$$

3. *Division.* Division is not always possible in the set of integers. The ratio $\frac{m}{n}$ is usually not an integer. The collection of fractions obtainable in this way is

called the rational numbers. A calculator gives in these cases a finite number of digits after the point, i.e., only an approximation. Say,

$$\frac{1}{3} = .333\dots \quad \frac{2}{7} = .285714285\dots$$

Both these calculator representations are approximations. When an exact representation is required, we use the overbar notation. Every rational number either terminates with a string of 0's, like $5/2 = 2.50\dots$ or, as in the two examples above, begin at some position to repeat in blocks of digits. The overbar notation $0.\overline{3}$ is used to indicate that the single digit block 3 repeats forever. Thus $ab.c\overline{defg}$ is interpreted to mean $ab.cdefgfefgfefg\dots$, where the block efg repeats forever. The exact representation of $2/7$ using this notation is $0.28571\overline{4}$.

Next we develop the concept and the notation related to *divisibility*. If d and n are integers, the notation $d|n$ means that the ratio n/d is an integer. When this is the case, we say ' d divides n ' and ' n is a multiple of d '. Notice that $d|n$ is not a number, but a statement that is either true or false. We also say that ' d is a divisor of n ' and that ' n is divisible by d '. More formally, $d|n$ if there is an integer q such that $n = d \cdot q$. The number q is called the quotient of n and d .

The notation $d \nmid n$ means that d does not divide n . In this case we can use the *division algorithm*. The division algorithm states that given any pair of integers n and d with $d \neq 0$, there exists a unique pair of integers q and r , called the *quotient* and *remainder* respectively, such that

$$n = dq + r \text{ and } 0 \leq r < |d|.$$

To carry out this algorithm means to find q and r , which we can do by long division.

$$\begin{array}{r} 28 \\ 37 \overline{) 1045} \\ \underline{-740} \\ 305 \\ \underline{-296} \\ 9 \end{array} \quad \begin{array}{l} q = 28 \\ r = 9 \\ 1045 = 37q + r \\ 1045 = 37 \cdot 28 + 9 \end{array}$$

Thus when $n = 1045$ and $d = 37$, it follows that $q = 28$ and $r = 9$.

Can we use the calculator to find q and r ? The answer is 'yes', but we must first discuss another pair of ideas, the *fractional part* and the *integer part* of a number. The integer part of a number x , denoted $\lfloor x \rfloor$, is called the *floor* of x , and is defined to be the largest integer that is less than or equal to x . The fractional part, denoted $\{x\}$, is defined by $\{x\} = x - \lfloor x \rfloor$. Thus, each real number x can be represented in the form $x = \lfloor x \rfloor + \{x\}$. For example $4.5 = \lfloor 4.5 \rfloor + \{4.5\} = 4 + .5$

and $-2.5 = \lfloor -2.5 \rfloor + \{-2.5\} = -3 + .5$ If the fraction $x = \frac{n}{d}$ is not an integer, the calculator may give $x = ab.feg\dots$ where $\lfloor x \rfloor = ab$ and $\{x\} = 0.fegfeg\dots$. The function $\lfloor \cdot \rfloor$ is called the *floor* function.

Let us continue solving the problem with a calculator. Note that if n and d are given then n/d can be written in the form above; that is, as the sum of its integer part and its fractional part.

$$\frac{n}{d} = \left\lfloor \frac{n}{d} \right\rfloor + \left\{ \frac{n}{d} \right\}.$$

Multiply through by d to get

$$n = \frac{n}{d} \cdot d = \left\lfloor \frac{n}{d} \right\rfloor \cdot d + \left\{ \frac{n}{d} \right\} \cdot d.$$

Now $\left\{ \frac{n}{d} \right\} \cdot d = n - \left\lfloor \frac{n}{d} \right\rfloor \cdot d$, so $\left\{ \frac{n}{d} \right\} \cdot d$ is a nonnegative integer. Also, $\left\{ \frac{n}{d} \right\} \cdot d < d$ because $\left\{ \frac{n}{d} \right\} < 1$. Therefore, $q = \left\lfloor \frac{n}{d} \right\rfloor$ and $r = \left\{ \frac{n}{d} \right\} \cdot d$ are the unique integers guaranteed by the division algorithm.

For instance, if $n = 2173$ and $d = 43$, then $\frac{2173}{43} = 50.53488\dots$. Hence $q = \left\lfloor \frac{n}{d} \right\rfloor = 50$ and $r = 2173 - q \cdot d = 2173 - 43 \cdot 50 = 23$ or $r = 43 \cdot \left\{ \frac{2173}{43} \right\} = 43 \cdot (0.53488\dots) = 23$. Thus $2173 = 43 \cdot 50 + 23$. In this section, we explore divisibility of n by each of the

numbers 2, 3, 4, 5, 6, 8, 9, and 11. The goal is to find a test for divisibility that can be carried out using the digits of n but without long division. Throughout the discussion, $n = (\overline{a_k a_{k-1} \dots a_0})_{10}$.

- a. The number $n = (\overline{a_k a_{k-1} \dots a_0})_{10}$ is divisible by 2 if and only if the last digit a_0 is divisible by 2.

The proof is simple. Recall that if $d|n$ and $d|m$, then $d|n \pm m$ because the sum and the difference of two integers is an integer. Because all the positive integer powers of 10 are divisible by 2, it follows that for suitable m ,

$$n = 2m + a_0.$$

Thus the divisibility of n by 2 depends simply on a_0 being divisible by 2.

- b. The same analysis, this time with the **two** rightmost digits gives divisibility by 4. Thus $4|n$ if and only if $4|10a_1 + a_0$; that is, $4|(\overline{a_1 a_0})_{10}$, again because $10^2, 10^3, \dots$, are divisible by 4.
- c. The divisibility of n by $d = 3$. Let's remark that each power of 10 is one larger than a multiple of 3. For example, $10 = 9 + 1$, $100 = 99 + 1$, and $1000 = 999 + 1$.

More generally,

$$\begin{aligned}
 n &= (a_k \dots a_0)_{10} \\
 &= a_k \left(\underbrace{99 \dots 9}_{k \text{ 9's}} + 1 \right) + a_{k-1} \left(\underbrace{9 \dots 9}_{(k-1) \text{ 9's}} + 1 \right) + \dots + a_1 (9 + 1) + a_0 \\
 &= a_k \left(\underbrace{99 \dots 9}_{k \text{ 9's}} \right) + a_{k-1} \left(\underbrace{9 \dots 9}_{(k-1) \text{ 9's}} \right) + \dots + a_1 (9) + (a_k + a_{k-1} + \dots + a_0) \\
 &= 9M + \left(\underbrace{a_k + a_{k-1} + \dots + a_0}_{\text{sum of digits}} \right).
 \end{aligned}$$

For example $437 = 4(99 + 1) + 3(9 + 1) + 7(1) = 4 \cdot 99 + 3 \cdot 9 + 4 + 3 + 7$, so 437 is a multiple of 3 if and only if $4 + 3 + 7$ is a multiple of 3. This means that a number n is divisible by 3 if and only if the sum of the digits of n is divisible by 3. Divisibility tests for 6, 8, and 11 are left as exercises.

- d. A divisibility test for 9. This works similarly to 3. Note that all the positive integer powers of 10 are one bigger than a multiple of 9. This means that a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Now let's discuss the *prime numbers*. Just as the number 1 is a basic building block for Z^+ under addition, the prime numbers are the building blocks for Z^+ under multiplication.

A *prime* number is an integer greater than 1 that has no positive divisors other than 1 and itself. Thus 2, 3, 5, 7, and 11 are prime numbers. The non-prime numbers bigger than 1 are called *composite* numbers. The first few are 4, 6, 8, 9 and 10. In fact, $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 2 \cdot 2 = 2 \cdot 4$, $9 = 3 \cdot 3$, and $10 = 2 \cdot 5$.

Lemma 1. Every integer $n > 1$ is divisible by a prime.

Proof. Either n is prime and we are done or n has non-trivial divisors d ($1 < d < n$). The set of all possible divisors is finite and therefore contains a smallest element, say $d_0 > 1$, which we claim is prime. If d_0 has a divisor d' between 1 and d_0 , then $d' | n$. But this is impossible, so d_0 is prime.

Lemma 2. Every integer n , $n > 1$, can be written as a product of primes.

Proof. It follows from Lemma 1 that there is a prime p_1 such that $p_1 | n$; i.e. $n = p_1 \cdot q_2$. If $q_2 > 1$, we can use Lemma 1 again to find a prime p_2 such that $q_2 = p_2 \cdot q_3$, or $n = p_1 \cdot p_2 \cdot q_3$. We can continue this process and after a finite number of steps (the total number of divisors for n is finite!), we obtain $n = p_1 p_2 \dots p_k$.

Theorem 1. Factorization theorem (without proof). Any positive number $n > 1$ can be written as a product of primes in one and only one way (factorizations that differ only in the order of the factors are considered identical, i.e., $24 = 2^3 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 2$ are identical representations.). This theorem is also called the Fundamental Theorem of Arithmetic.

How can we find the primes for the given interval $1 < n < N$? The following method was proposed by the Greek mathematician Erathosthenes from Alexandria in 3rd century BC and is known as Sieve of Erathosthenes (or Erathosthenes' Algorithm). (Remark: Erathosthenes was the first scientist to estimate the radius of the Earth. His estimation, based on geometrical and astronomical ideas, is in modern units near to $R_E \simeq 6,000$ km, which is very accurate.)

Lemma 3. If n is composite, then it has divisor d such that $1 < d \leq \sqrt{n}$.

Proof. If $n = d_1 \cdot d_2$ and $d_1 \leq d_2$, then $n \geq d_1^2$, i.e. $d_1 \leq \sqrt{n}$.

The idea of the algorithm is very simple: to eliminate all composite numbers from the set $1, 2, \dots, N$. Let's fix the first prime number 2 and eliminate all numbers (greater than 2) that are multiples of 2 (even numbers). The first of the remaining numbers is prime; it is 3. Let's remove all numbers (greater than 3) which are multiples of 3. The first of the remaining numbers is prime; it is 5, etc. According to Lemma 3 we can continue this process until we have crossed out the multiples of all primes less than \sqrt{N} . The remaining numbers will be prime.

Example. $N = 100$, $\sqrt{N} = 10$

2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100

The table below shows the first stage of the algorithm, after all the multiples of 2 have been eliminated. The final result is shown in the last table after all the multiples of 3, 5, and 7 have been eliminated.

2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100

2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100

The primes ≤ 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Lemma 3 shows that each composite number $n \leq 10,000 = 10^4$ has a prime factor ≤ 100 , i.e. the list of primes above is sufficient to solve the problem of factorization for all $n \leq 10^4$.

Theorem 2 (Euclid). There are infinitely many primes. This is one of the oldest and most beautiful results of number theory. The proof was published in Euclid's *Elements* in the 3rd century BC.

Proof by contradiction. Suppose the opposite, that there is a finite number of primes $p_1 = 2, p_2 = 3, \dots, p_k$. Construct the new integer:

$$N = p_1 \cdot p_2 \cdots p_k + 1.$$

Either N is prime or N has a prime factor $0 < d < N$ (see Lemma 1). In both cases we find a prime q which is a factor of N . According to our assumption, q must be among $p_1 \dots p_k$. Thus

$$q|N \quad \text{and} \quad q|p_1 \cdots p_k.$$

But $p_1 \dots p_k$ and N are two consecutive integers, so q is a divisor of their difference, which is 1. But $q|1$ is a contradiction.

Now we'll discuss some applications of the factorization theorem (Theorem 1). According to this theorem each positive integer n can be represented as a product of primes.

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad a_1, \dots, a_k \geq 1 \text{ and } p_1 < p_2 < \dots < p_k \text{ are prime.}$$

Let's consider two integers m and n , both greater than 1.

Definition of LCM Number d is the greatest common divisor of m and n if both

1. $d|n$ and $d|m$, and
2. if $d'|n$ and $d'|m$, then $d'|d$.

Condition 1. says that d is a common divisor of m and n , and condition 2. says that d is the largest (in a sense) of the common divisors.

The greatest common divisor of m and n is denoted $d = GCD(m, n)$.

Definition of GCD The number k is the least common multiple of m and n if both

1. $n|k$ and $m|k$, and
2. if $n|k'$ and $m|k'$ then $k|k'$.

The first condition says that k is a common divisor of m and n , and the second says that k is a divisor of any other common divisor, hence k is the least such divisor. The least common multiple of m and n is denoted $k = LCM(m, n)$.

Theorem 3. Let p_1, \dots, p_k be all the prime factors for n or m . One can represent

$$\begin{aligned} n &= p_1^{a_1} \cdots p_k^{a_k} \\ m &= p_1^{b_1} \cdots p_k^{b_k}. \end{aligned}$$

Now $0 \leq a_i, b_i$. Then

$$GCD(m, n) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}.$$

$$LCM(m, n) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}.$$

Theorem 3 is a consequence of the Factorization Theorem.

Example. $n = 75, m = 90$.

$$\begin{aligned} n &= 3^1 \cdot 5^2 = 2^0 \cdot 3^1 \cdot 5^2. \\ m &= 2 \cdot 3^2 \cdot 5 = 2^1 \cdot 3^2 \cdot 5^1. \end{aligned}$$

$$GCD(75, 90) = 2^0 \cdot 3^1 \cdot 5^1 = 15.$$

$$LCM(75, 90) = 2^1 \cdot 3^2 \cdot 5^2 = 450.$$

Theorem 4. For any two positive integers, m and n , $n \cdot m = GCD(m, n) \cdot LCM(m, n)$. In other words, the product of the gcd and lcm of two integers is the same as the product of the integers themselves.

Proof.

$$\begin{aligned} n &= p_1^{a_1}, \dots, p_k^{a_k} \\ m &= p_1^{b_1}, \dots, p_k^{b_k} \\ n \cdot m &= p_1^{a_1+b_1}, \dots, p_k^{a_k+b_k} \end{aligned}$$

But for the arbitrary integers a, b

$$a + b = \max(a, b) + \min(a, b).$$

Apply this repeatedly to the pairs (a_i, b_i) to finish the proof. There are different applications of the prime numbers or factorization theorem: security and cryptography. Let's briefly discuss one of them.

Security of passwords. The section is covered only in Molchanov's class. Let's consider the following important problem. A computer system (or Bank) has many users. Each user (to get the access to the system) must identify himself by entering a secret password. It is extremely insecure to store direct information about users (their names and passwords) in the memory of the system, since it is almost impossible to keep this file secret.

A modern approach to the problem is based on the general idea of *one way functions*. Each user v_i , $i = 1, 2, \dots$ has a password P_i (usually it is one or several numbers, written in the decimal or binary forms). This is a *private password* of the user V_i . The system is not storing private passwords, but their functions $f(P_i) = f_i$, so-called *public passwords*.

To get the access to the system, the user simply type in his name V_i and his private password P_i , (to identify himself as a user). The computer has to calculate $f(P_i)$ and compare with a number f_i in the central file. If $f_i = f(P_i)$, the access is open, otherwise it is not. Let's stress that the function $f(\cdot)$ and public passwords are available for everybody! Function $f(\cdot)$ must be a one-way function. This means that *it is easy to find the value $f(P)$ if the argument P is known* and practically impossible to find the solution of the equation $A = f(P)$ i.e. find an inverse function $f^{-1}(A)$. A classical example of a one-way function that is popular in cryptography and security applications is based on prime number factorization. It gives the following solution to the password problem. Password P_i consists of two very large prime numbers (p_i, q_i) , and the function $f(P_i)$ is simply $f(P_i) = p_i q_i = f_i$.

To recount p_i, q_i for given f_i , we have to solve a factorization problem. If, for instance, p_i, q_i are 50-digit primes then f_i about 100 digits. Factorization requires roughly speaking the $\sqrt{f_i} \simeq 10^{50}$ divisions of the very long numbers (see above).

If our computer can make even 10^{12} such divisions per second, then the total time will be of the order 10^{38} sec. But one year contains only about $3 \cdot 10^7$ sec, i.e. the factorization of f_i will require billions and billions years!

It is also interesting to remark that the complexity of the factorization of very large numbers is the basis for completely different applications: many modern algorithms for the generation of *random numbers* depend on the arithmetical operations with very large primes.