Number Theory Part-1

P. Sam Johnson

NITK, Surathkal

Overview

We discuss the following in two lectures :

- greatest common divisor of two integers m and n, denoted by $gcd(m, n)$
- a famous Euclid's algorithm to calculate $gcd(m, n)$
- primes numbers – the fundamental building blocks of all the positive integers
- fundamental theorem of arithmetic (unique factorization theorem).

"Mod" : The binary operation

If m and n are positive integers, then the **quotient** of

$$\text{“}n \text{ divided by } m\text{”}$$

is

$$\lfloor n/m \rfloor.$$

We use a simple notation for the remainder of this division, and we call "r **is congruent to** n **modulo an integer** $m > 0$" and write it

$$r \equiv n \mod m.$$

That is, $r \equiv n \mod m \iff m \text{ divides } (r - n)$.

Since

$$n = \underbrace{m\lfloor n/m \rfloor}_{\text{quotient}} + \underbrace{n \mod m}_{\text{remainder}}$$

the basic formula for $n \mod m$ is $n - m\lfloor n/m \rfloor$.

Hence we can generalize to negative integers, and in fact to arbitrary real numbers:

$$x \mod y = x - y\lfloor x/y \rfloor, \text{ for } y \neq 0.$$

This defines "mod" as a binary operation, just an addition and subtraction are binary operations. What is the meaning of x mod y when x and y are positive real numbers?

Imagine a circle of circumference y whose points have been assigned real numbers in the interval $[0, y)$. Starting at 0, if we travel a distance x around the circle we end up at x *mod* y.

Here are some integer-valued examples for x and y, when x or y is negative.

$$\begin{array}{rrrrr} 5 & mod & 3 & = & 2 \\ 5 & mod & -3 & = & -1 \\ -5 & mod & 3 & = & 1 \\ -5 & mod & -3 & = & -2. \end{array}$$

The number after '*mod*' is called the **modulus**. There is no name to call the number before '*mod*'.

- Modulus may be negative. But in applications, the modulus is usually positive.
- In both cases the value of x *mody* is between 0 and the modulus: $0 \leq x \ mod \ y < y$, for $y > 0$; $0 \geq x \ mod \ y > y$, for $y < 0$.

What about $y = 0$?

When $y = 0$, $x \ mod \ y = x - y\lfloor x/y \rfloor$ is undefined. In order to avoid division by zero, we can define

$$x \ mod \ 0 = x.$$

This convention preserves the property that $x \ mod \ y$ always differs from x by a multiple of y.

Divisibility

We say that "m **divides** n" or n is **divisible** by m (denoted by $m \backslash n$) if $m > 0$ and n/m is an integer ($n = mk$ for some integer k).

The definition of "$m \backslash n$" requires that "n is a multiple of m" and m has to be positive.

In some text books, the definition for "m **divides** n" is defined as "n is a multiple of m". It means almost the same thing except that m does not have to be positive.

Both notions are different. They can be understood from the following:

- 0 is the only one multiple of 0, but nothing is divisible by 0.
- Every integer is a multiple of -1, but no integer is divisible by -1.

Greatest common divisor

These two definitions ("divisible" and "multiple of") are same if we consider only positive integers.

These two definitions ("divisible" and "multiple of") can be applied when m and n are real numbers. But we discuss for integers.

The **greatest common divisor** of two integers m and n is the largest integer that divides them both :

$$\gcd(m, n) = \max\{k : k \backslash m \text{ and } k \backslash n\}.$$

- If $n > 0$, then $gcd(0, n) = n$, because any positive number divides 0, and because n is the largest divisor of itself.
- The value of $gcd(0, 0)$ is undefined.

Euclid's algorithm, by great mathematician, who lived around 2300 years ago

We can compute $gcd(m, n)$ for $0 \leq m < n$, a 2300-year-old method called **Euclid's algorithm**, which uses the recurrence

$$\begin{aligned} gcd(0, n) &= n; \\ gcd(m, n) &= gcd(n \ mod \ m, m), \quad \text{for} \quad n \geq 0. \end{aligned}$$

The stated recurrence is valid, because any common divisor of m and n must also be a common divisor of both m and the number "$n \ mod \ m$", which is $n - \lfloor n/m \rfloor m$.

Example

$gcd(12, 18) = gcd(6, 12) = gcd(0, 6) = 6.$

m	n	$r = n \ mod \ m$	m	$gcd(m, n)$
12	18	6	12	–
6	12	0	6	6

Euclid's algorithm

Exercise

Use Euclid's algorithm to compute integers m' and n' (m' or n' can be negative) satisfying

$$mm' + n'n = gcd(m, n).$$

Euclid's algorithm is most well-known and effective method of finding integers m' and n' satisfying

$$mm' + n'n = gcd(m, n).$$

Proof. If $m = 0$, we can take $m' = 0$ and $n' = 1$.

Otherwise we let $r = n \ mod \ m$ and apply the method recursively with r and m in place of m and n, computing $\overline{r}$ and $\overline{m}$ such that

$$\overline{r}r + \overline{m}m = gcd(r, m).$$

Since $r = n - \lfloor n \backslash m \rfloor m$ and $gcd(r, m) = gcd(m, n)$, there equation tells us that

$$\overline{r} = \left(n - \lfloor n \backslash m \rfloor m\right) + \overline{m} m = gdc(m, n).$$

The left side can be rewritten to show its dependency on m and n:

$$\left(\overline{m} - \lfloor n \backslash m \rfloor \overline{r}\right) m + \overline{r} n = gdc(m, n)$$

hence $m' = \overline{m} - \lfloor n \backslash m \rfloor \overline{r}$ and $n' = \overline{r}$ are the required integers.

Corollary

$k \backslash m$ *and* $k \backslash n \iff k \gcd(m, n)$.

The example shown below illustrates a procedure to calculate $gcd(12, 6)$.

Example

m	n	$\lfloor n/m \rfloor$	r	m	$\bar{r}$	$\overline{m}$	m'	n'	$m'm + n'n = gcd(m, n)$
6	12	2	0	6	0	1	1	0	$\underline{1}.6 + \underline{0}.12 = 6$
12	18	1	6	12	1	0	-1	1	$\underline{-1}.12 + \underline{1}.18 = 6$

Exercises

- *Write the identity with (a single sum) "$\sum$-notation" to do sum over all divisors on n.*
- *Do above exercise with a double sum, "double $\sum$-notation" to do sum over all divisors on n.*

Least common multiple

The **least common multiple** of two integers m and n is the smallest integer that is divisible by both m and n:

$$lcm(m, n) = \min\{k : k > 0, m \backslash k \text{ and } n \backslash k\}.$$

lcm is undefined if $m \leq 0$ or $n \leq 0$.

Primes

A positive integer p is called **prime** if it has just two divisors, namely 1 and p.

By convention, 1 is not a prime, so the sequence of primes starts out like this: $2, 3, 5, 7, 11, 13, \ldots$.

- The numbers have 3 or more divisors are called **composite**.
- Every integer greater than 1 is either prime or composite, but not both.
- Primes are of great importance, because they are the **fundamental building blocks** of all the positive integers.

Theorem

Any positive integer n can be written as a product as primes,

$$n = p_1, p_2 \dots p_n = \prod_{k=1}^{n} p_k, \quad p_1 \leq p_2 \leq \cdots \leq p_n. \tag{1}$$

Moreover, the expansion in (1) is unique: There is **only one way** to write n as a product of primes in nondecreasing order.

This statement is called the **fundamental theorem of arithmetic (unique factorization theorem)**.

Proof.

We prove by induction.

If $m = 0$, we consider this to be an empty product, whose value is 1 by definition.

If $n > 1$ is not prime, it has a divisor n_1 such that $1 < n_1 < n$; thus we can write $n = n_1 n_2$ and (by induction) we know that n_1 and n_2 can be written as a product of primes.

There is certain only one possibility when $n = 1$, since the product must be empty in that case.

Let us suppose that $n > 1$ and that all smaller numbers factor **uniquely**.

Suppose we have 2 factorization $n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_k$ where $p_1 \leq \cdots p_m$ and $q_1 \leq \cdots \leq q_k$, where the p's and q's are all primes.

Claim : Each p_i is some q_j and $m = k$.

Suppose $p_1 < q_1$. Since p_1 and q_1 are prime, $gcd(p_1, q_1) = 1$.

Hence by Euclid'd algorithm, there are integers a and b such that $ap_1 + bq_1 = 1$.

Therefore $(ap_1)q_2 \cdots q_k + (bq_1)q_2 \cdots q_k - q_2 \cdots q_k$.

Since p_1 divides $(ap_1)(p_2 \cdots p_k)$ and $n = q_1 q_2 \cdots q_k$, p_1 divides $q_2 \cdots q_k$.

Thus p_1 divides $q_2 \cdots q_k$ so $q_2 \cdots q_k / p_1$ is an integer, and $q_2 \ldots q_k$ has a prime factorization in which p_1 appears.

But $q_2 \cdots q_k < n$, so it has a unique factorization (by induction). This contradiction proves that $p_1 = q_1$.

Hence $\frac{n}{p_1} = p_2 \cdots p_m$.

Reasoning the same way, p_2 must equal one of the remaining q_j.

Relabeling again if necessary, say $p_2 = q_2$.

Then $\frac{n}{p_1 p_2} = p_3 \ldots p_m = q_3 \ldots q_k$.

This can be done for each of the m b_i's showing that $m \leq n$ and every p_i is a q_j.

Applying the same argument with the p's and q's reversed shows $n \leq m$ (hence $m = n$) and every q_j is a p_i.

This completes the proof.

Uniqueness in the theorem

The requirement that the factors be prime is necessary : factorizations containing composite numbers may not be unique. For example, $12 = 2 \times 6 = 3 \times 4$.

This theorem is one of the main reasons for which 1 is not considered as a prime number: if 1 were prime, the factorization would not be unique, as, for example, 3, 1.3, 1.1.3, etc. are all valid factorization of 3.

An important fact : If a prime p divides a product mn then it divides either m or n, perhaps both, gives the unique factorization theorem and vice-versa.

Do composite numbers have this property?

If p is not prime, it may happen that p divides mn, but p does not divide both m and n.

$4 \backslash 60$ but $4 \backslash 6$ and $4 \backslash 10$. The reason is simple: In the factorization $60 = 6.10 = (2.3)(2.5)$, the two prime factors of 4.2.2 have been split into two parts, hence 4 divides neither part.

But a **prime is unsplittable**, so it must divide one of the original factors.

Fundamental theorem in another way

Theorem

Every positive integer can be written uniquely in the form

$$n = \prod_p p^{n_p}, \tag{2}$$

where each $n_p \geq 0$.

The right-hand-side is a product over infinitely many primes ; but for any particular n, "all" but a few exponents are zero, so the corresponding factors are 1.

Therefore it is really a finite product.

For example,

$$\begin{aligned} 1200 &= 24 \times 31 \times 52 = 3 \times 2 \times 2 \times 2 \times 2 \times 5 \times 5 \\ &= 5 \times 2 \times 3 \times 2 \times 5 \times 2 \times 2 = 5^2.3^1.2^4. \end{aligned}$$

The theorem is stating two things: first, that 1200 can be represented as a product of primes, and second, no matter how this is done, there will always be four 2s, one 3, two 5s, and no other primes in the product.

Canonical representation of a positive integer

Theorem

Every positive integer $n > 1$ can be represented in exactly one way as a product of prime powers:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the α_i are positive integers.

This representation is called the **canonical representation** of n, or the **standard form** of n.

For example

$999 = 33 \times 37, 1000 = 23 \times 53, 1001 = 7 \times 11 \times 13.$

Note that factors $p^0 = 1$ may be inserted without changing the value of n (e.g. $1000 = 2^3 \times 3^0 \times 5^3$).

In fact, any positive integer can be uniquely represented as an infinite product taken over all the positive prime numbers,

$$n = 2^{n_1} 3^{n_2} 5^{n_3} 7^{n_4} \cdots = \prod p_i^{n_i},$$

where a finite number of the ni are positive integers, and the rest are zero.

Allowing negative exponents provide a canonical form for positive rational numbers.

Formula $n = \prod_p p^{n_p}$ gives unique respresentation of n, where each $n_p \geq 0$.

For a positive integer n, we have the sequence $\langle n_2, n_3, \ldots \rangle$ as a **number system**.

For example, the prime-exponent representation of 12 is $\langle 2, 1, 0, 0, \ldots \rangle$ and the prime-exponent representation of 18 is $\langle 1, 2, 0, 0, \ldots \rangle$.

- $k = mn \iff k_p = m_p + n_p$ for all p.
- $m \backslash n \iff m_p \leq n_p$ for all p.
- $k = gcd(m, n) \iff k_p = \min\{m_p, n_p\}$ for all p.
- $k = lcm(m, n) \iff k_p = \max\{m_p, n_p\}$ for all p.

Arithmetic operations

The canonical representation, when it is known, is convenient for easily computing products, gcd, and lcm:

$$\begin{aligned}
a \cdot b &= 2^{a_2+b_2}\, 3^{a_3+b_3}\, 5^{a_5+b_5}\, 7^{a_7+b_7} \ldots \\
&= \prod p_i^{a_{p_i}+b_{p_i}} \\
\gcd(a,b) &= 2^{\min(a_2,b_2)}\, 3^{\min(a_3,b_3)}\, 5^{\min(a_5,b_5)}\, 7^{\min(a_7,b_7)} \ldots \\
&= \prod p_i^{\min(a_{p_i},b_{p_i})} \\
\operatorname{lcm}(a,b) &= 2^{\max(a_2,b_2)}\, 3^{\max(a_3,b_3)}\, 5^{\max(a_5,b_5)}\, 7^{\max(a_7,b_7)} \ldots \\
&= \prod p_i^{\max(a_{p_i},b_{p_i})}.
\end{aligned}$$

Exercise

Find gcd$(12, 18)$ and lcm$(12, 18)$, using prime-exponent representations.

However, as Integer factorization of large integers is much harder than computing their product, gcd or lcm, these formulas have, in practice, a limited usage.

We have seen that any integer $n > 1$ has a unique prime factorization. How many primes are there ?

Theorem (Euclid)

There are infinitely many primes.

Proof.

Suppose there are finitely many, say, $p_1, p_2, \ldots, p_k$.

Let $M = p_1 p_2 \cdots p_k + 1$.

Each prime p_i $(1 \leq i \leq k)$ divides $M - 1$, none of the k primes can divide M.

So M itself is prime (no prime divides consective integers), or, M has a prime factor $q \neq p_i$ for any $1 \leq i \leq k$, a contradiction to our assumption that $p_1, p_2, \ldots, p_k$ are the only primes.

Trial division

The property of being prime (or not) is called **primality**. A simple but slow method of verifying the primality of a given number n is known as **trial division**.

It consists of testing whether n is a multiple of any integer between 2 and $\sqrt{n}$.

Algorithms much more efficient than trial division have been devised to test the primality of large numbers. Particularly fast methods are available for numbers of special forms, such as **Mersenne numbers**.

As of September 2015, the largest known prime number has $17,425,170$ decimal digits (17 billion 425 thoudsand and 170).

Distribution of primes : How are the primes scattered or distributed in $\mathbb{N}$?

There are infinitely many primes, as demonstrated by Euclid around 300 BC.

There is no known useful formula that sets apart all of the prime numbers from composites.

However, the distribution of primes, that is to say, the statistical behaviour of primes in the large, can be modelled.

Guess by Gauss : Let $\pi(x)$ be the number of primes $\leq x$.

Gauss attempted to show (but failed) that

$$\lim_{n \to \infty} \frac{\pi(x)}{x \log x} = 1.$$

Prime Number Theorem

The first result in that direction is the prime number theorem which describes the asymptotic distribution of the prime numbers among the positive integers.

It formalizes the intuitive idea that primes become less common as they become larger by precisely quantifying the rate at which this occurs.

The theorem was proved independently by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896 using ideas introduced by Bernhard Riemann (in particular, the Riemann zeta function).

The theorem says that the probability that a given, randomly chosen number n is prime is inversely proportional to its number of digits, or to the logarithm of n.

The first such distribution found is $\pi(N) \sim N/\log(N)$, where $\pi(N)$ is the **prime-counting function** and $\log(N)$ is the natural logarithm of N. This means that for large enough N, the probability that a random integer not greater than N is prime is very close to $1/\log(N)$.

Consequently, a random integer with at most $2n$ digits (for large enough n) is about half as likely to be prime as a random integer with at most n digits.

For example, among the positive integers of at most 1000 digits, about one in 2300 is prime ($\log(10^{1000}) \approx 2302.6$), whereas among positive integers of at most 2000 digits, about one in 4600 is prime ($\log(10^{2000}) \approx 4605.2$). In other words, the average gap between consecutive prime numbers among the first N integers is roughly $\log(N)$.

Open Problems

Many questions regarding prime numbers remain open, such as **Goldbach's conjecture** (that every even integer greater than 2 can be expressed as the sum of two primes), and the **twin prime conjecture** (that there are infinitely many pairs of primes whose difference is 2).

- Are there infinitely primes of type $2n+1$?
- Are there infinitely primes of type $4n+1$?
- Are there infinitely primes of type $4n+3$?
- Are there infinitely primes of type $6n+1$?
- Are there infinitely primes of type $6n+5$?

Various braches of number theory due to prime numbers

Such questions spurred the development of various branches of number theory, focusing on analytic or algebraic aspects of numbers.

Primes are used in several routines in information technology, such as public-key cryptography, which makes use of properties such as the difficulty of factoring large numbers into their prime factors.

Prime numbers give rise to various generalizations in other mathematical domains, mainly algebra, such as prime elements and prime ideals.

References

1. **Graham, Knuth and Patashnik**, *"Concrete Mathematics – A Foundation for Computer Science"*, Pearson Education.
2. **Marko Petkovsek, Herbert S. Wilf and Doron Zeilberger**, "$A = B$", AK Peters Ltd., Wellesley, Massachusetts.
3. **Herbert S. Wilf**, *"Generatingfunctionology"*, Third Edition, AK Peters Ltd., Wellesley, Massachusetts.