Mathematics for Computer Science
CSE 401
Number Theory

Dr. Shah Murtaza Rashid Al Masud
Department of CSE
University of Asia Pacific

Number Theory

- Factor, Multiple, Division
- 'MOD': the Congruence Relation
- Prime
- GCD and LCM

Number Theory and Integer

Of course, you already know what the integers are..

An integer is a whole number with no decimal or fractional part, from the set of negative and positive numbers, including zero. **Examples of integers** are: -5, 0, 1, 5, ...

However: There are some specific notations, terminology, and theorems associated with these concepts which you may not know.

These form the basics of *number theory*.

- Vital in many important **algorithms** today (hash functions, cryptography, digital signatures; in general, on-line security).

Division and The divides operator

New notation: 3 | 12

- To specify when an integer evenly divides another integer
- Read as "3 divides 12"

The not-divides operator: $5 \nmid 12$

- To specify when an integer does *not* evenly divide another integer
- Read as "5 does not divide 12"

Divides, Factor, Multiple

Let $a,b \in \mathbf{Z}$ with $a \neq 0$.

Def.: $a|b \equiv$ "*a divides b*" $:\equiv$ $(\exists\, c \in \mathbf{Z}: \mathbf{b=ac})$

b = 12; a = 3 ; 12 = 3 c ; 12/3=c=4*

"There is an integer *c* such that *c* times *a* equals *b*."

– Example: $3|-12 \Leftrightarrow$ **True**, but $3|7 \Leftrightarrow$ **False**.

Iff *a* divides *b*, then we say *a* is a *factor* or a *divisor* of *b*, and *b* is a *multiple* of *a*. 20 = 5 * c

Ex.: "*b* is even" $:\equiv 2|b$. Is 0 even or odd? Is −4 (hw)?

R = real numbers, **Z = integers (a whole number)**, N=natural numbers, Q = rational numbers, P = irrational numbers.

Divides, Factor, Multiple

As a whole number/integer that can be written without a remainder, 0 classifies as an integer. So to determine whether it is even or odd, we must ask the question: Is 0 divisible by 2?

A number is divisible by 2 if the result of its division by 2 has no remainder or fractional component—in other terms, if the result is an integer.

So, let's tackle 0 the same way as any other integer. **When 0 is divided by 2, the resulting quotient turns out to also be 0—an integer, thereby classifying it as an even number.**

Results on the divides operator

If a | b and a | c, then a | (b + c)

– Example: if 5 | 25 and 5 | 30, then 5 | (25+30) (25*m+30*n)

If a | b, then a | bc for all integers c

– Example: if 5 | 25, then 5 | 25*c for all integers c

If a | b and b | c, then a | c

– Example: if 5 | 25 and 25 | 100, then 5 | 100

("common facts" but good to repeat for background)

Divides Relation

Theorem: $\forall a,b,c \in \mathbf{Z}$:

1. $a|0$
2. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
3. $a|b \rightarrow a|bc$
4. $(a|b \wedge b|c) \rightarrow a|c$

Proof of (2): $a|b$ means there is an s such that $b=as$, and $a|c$ means that there is a t such that $c=at$, so $b+c = as+at = a(s+t)$, so $a|(b+c)$ also.■

Corollary: If a, b, c are integers, such that a | b and a | c, then **a | mb + nc** whenever m and n are integers.

a=5, b=5, c=5, a/(b+c), 5/5m+5n=5/5*2+5*3=5/10+15=5/25

Corollary is a theorem that follows on from another existing theorem.

More Detailed Version of Proof

Show $\forall a,b,c \in \mathbf{Z}: (a|b \wedge a|c) \rightarrow a \mid (b + c)$.

Let a, b, c be any integers such that $a|b$ and $a|c$, and show that $a \mid (b + c)$.

By defn. of $|$, we know $\exists s: b=as$, and
$\exists t: c=at$. Let s, t, be such integers.

Then $b+c = as + at = a(s+t)$, so
$\exists u: b+c=au$, namely $u=s+t$. Thus $a|(b+c)$.

More Detailed Version of Proof

List of Mathematical Symbols

- $\mathbb{R}$ = real numbers, $\mathbb{Z}$ = integers, $\mathbb{N}$=natural numbers, $\mathbb{Q}$ = rational numbers, $\mathbb{P}$ = irrational numbers.
- $\subset$= proper subset (not the whole thing) $\subseteq$=subset
- $\exists$ = there exists
- $\forall$ = for every
- $\in$= element of
- $\bigcup$ = union (or)
- $\bigcap$ = intersection (and)
- s.t.= such that
- $\implies$ implies
- $\iff$ if and only if
- $\sum$ = sum
- $\setminus$ = set minus
- $\therefore$= therefore

The Division "theorem"

Theorem:

Division Algorithm --- Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = d*q+r$.

It's really just a theorem

a=17, d=5, q=? And r=?

- *q* is called the **quotient/result**
- *r* is called the **remainder**
- *d* is called the **divisor**
- *a* is called the **dividend**

The number will be **unique if it is positive integer and there are no repeated digits in the number**. In other words, a number is said to be unique if and only if the digits are not duplicate. For example, 20, 56, 9863, 145, etc. are the unique numbers while 33, 121, 900, 1010, etc. are not unique numbers.

The Division “theorem”

- *q* is called the **quotient**
- *r* is called the **remainder**
- *d* is called the **divisor**
- *a* is called the **dividend**

What are the quotient and remainder when 101 is divided by 11?

a d q r

$101 = 11 \times 9 + 2$

We write:

$q = 9 = 101$ **div** 11

$r = 2 = 101$ **mod** 11

$a = dq+r.$

The Division “theorem”

If $a = 7$ and $d = 3$, then $q = 2$ and $r = 1$, since $7 = (2)(3) + 1$.

If $a = -7$ and $d = 3$, then $q = -3$ and $r = 2$, since $-7 = (-3)(3) + 2$.

$$a = dq+r.$$

So: given positive **a** and (positive) **d**, in order to get **r** we repeatedly subtract **d** from **a**, as many times as needed so that what remains, **r**, is less than **d**.

$$-a = d(-q)+r.$$

Given negative **a** and (positive) **d**, in order to get **r** we repeatedly add **d** to **a**, as many times as needed so that what remains, **r**, is positive (or zero) and less than **d**.

Modular arithmetic

Modular arithmetic is a system of **arithmetic** for integers, which considers the remainder.

If *a* and *b* are integers and *m* is a positive integer, then

"*a* is *congruent to b modulo m*" if *m* divides *a-b* *(//similar)*

- Notation: $a \equiv b \pmod{m}$
- Rephrased: $m \mid a-b$
- **Rephrased: *a* mod *m* = *b mod m***
- If they are not congruent: $a \not\equiv b \pmod{m}$

In **modular arithmetic**, numbers "wrap around" upon reaching a given fixed quantity (this given quantity is known as the modulus) to leave a remainder.

Example: Is 17 (a) congruent to 5 (b) modulo 6 (m)?

- Rephrased: $17 \equiv 5 \pmod{6}$
- As 6 divides 17-5, they are congruent (17 mod 6 = 5 mod 6)

Congruent means exactly equal

Example: Is 24 congruent to 14 modulo 6?

- Rephrased: $24 \equiv 14 \pmod{6}$
- As 6 does not divide 24-14 = 10, they are not congruent

Note: this is a different use of "≡" than the meaning "is defined as" used before.

Modular arithmetic

Modular arithmetic is a system of **arithmetic** for integers, which considers the remainder.

Example: Is 17 (a) congruent to 5 (b) modulo 6 (m)?

- Rephrased: $17 \equiv 5 \pmod 6$
- As 6 divides 17-5, they are congruent (17 mod 6 = 5 mod 6)

Example: Is 24 congruent to 14 modulo 6?

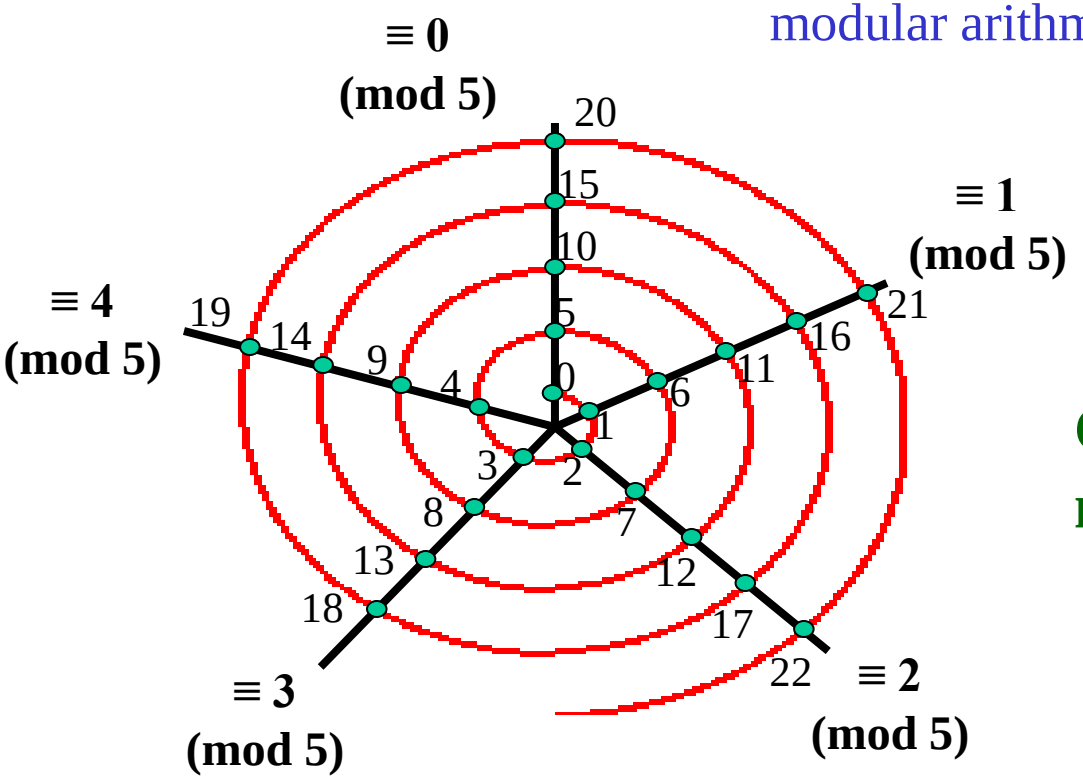
- Rephrased: $24 \not\equiv 14 \pmod 6$
- As 6 does not divide 24-14 = 10, they are not congruent

Note: this is a different use of "≡" than the meaning "is defined as" used before.

Spiral Visualization of mod

Example shown:
modulo 5
arithmetic

The spiral/circular view is useful to keep in mind when doing modular arithmetic!



Congruence classes modulo 5.

So, e.g., 19 is congruent to 9 modulo 5.

More on congruence

Theorem: Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Even more Properties on congruence
Congruence of sums, differences, and products

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv (b+d) \pmod{m}$ and $ac \equiv bd \pmod{m}$

Example

- We know that $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
- We know that $8 \equiv 2 \pmod{3}$ and $11 \equiv 2 \pmod{3}$
- $ac \equiv bd \pmod{m}$
- Thus, $7+11 \equiv (2+1) \pmod{5}$, or $18 \equiv 3 \pmod{5}$
- Thus, $7*11 \equiv 2*1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$

$$11 \equiv 1 \pmod{10} \implies 11^{999} \equiv 1^{999} \equiv 1 \pmod{10}$$

$$9 \equiv -1 \pmod{10} \implies 9^{999} \equiv (-1)^{999} \pmod{10}$$

Even more Properties on congruence
Congruence of sums, differences, and products

Symmetry: if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Transitivity: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

15 ≡5 (mod 5) and 5 ≡0 (mod 5)

15 ≡0 (mod 5)

Application of congruence relation

Find the remainder of the division of $a = \mathbf{1395}^4 \cdot \mathbf{675}^3 + 12 \cdot 17 \cdot 22$ by 7 .

As $1395 \equiv 2 \pmod 7$, $675 \equiv 3 \pmod 7$, $12 \equiv 5 \pmod 7$, $17 \equiv 3 \pmod 7$ and $22 \equiv 1 \pmod 7$, we have:

$$a \equiv 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod 7$$

As $2^4 = 16 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, and $5 \cdot 3 \cdot 1 = 15 \equiv 1 \pmod 7$, it follows

$$a \equiv 2 \cdot 6 + 1 = 13 \equiv \mathbf{6} \pmod 7$$

Application of congruence relation

Example 2: Find the remainder of the division of $a = 53 \cdot 47 \cdot 51 \cdot 43$ by 56.

A. As $53 \cdot 47 = 2491 \equiv 27 \pmod{56}$ and $51 \cdot 43 = 2193 \equiv 9 \pmod{56}$,

$$a \equiv 27 \cdot 9 = 243 \equiv 19 \pmod{56}$$

B. As $53 \equiv -3 \pmod{56}$, $47 \equiv -9 \pmod{56}$, $51 \equiv -5 \pmod{56}$ and $43 \equiv -13 \pmod{56}$,

$$a \equiv (-3)\cdot(-9)\cdot(-5)\cdot(-13) = 1755 \equiv \mathbf{19} \pmod{56}$$

Application of congruence relation

There is a close connection between congruences and remainders:

Lemma 9.6.1 (Remainder)**.**

$$a \equiv b \pmod{n} \quad \textit{iff} \quad \text{rem}(a,\ n) = \text{rem}(b,\ n).$$

So we can also see that

$$29 \equiv 15 \pmod{7} \quad \text{because } \text{rem}(29,\ 7) = 1 = \text{rem}(15,\ 7).$$

Application of congruence relation

Remainder Arithmetic

The Congruence Lemma 9.6.1 says that two numbers are congruent iff their remainders are equal, so we can understand congruences by working out arithmetic with remainders. And if all we want is the remainder modulo n of a series of additions, multiplications, subtractions applied to some numbers, we can take remainders at every step so that the entire computation only involves number in the range $[0..n)$.

General Principle of Remainder Arithmetic

To find the remainder on division by n of the result of a series of additions and multiplications, applied to some integers

- replace each integer operand by its remainder on division by n,
- keep each result of an addition or multiplication in the range $[0..n)$ by immediately replacing any result outside that range by its remainder on division by n.

Application of congruence relation

For example, suppose we want to find

$$\text{rem}((44427^{3456789} + 15555858^{5555})403^{6666666},\ 36). \tag{9.9}$$

This looks really daunting if you think about computing these large powers and then taking remainders. For example, the decimal representation of $44427^{3456789}$ has about 20 million digits, so we certainly don't want to go that route. But remembering that integer exponents specify a series of multiplications, we follow the General Principle and replace the numbers being multiplied by their remainders. Since $\text{rem}(44427,\ 36) = 3, \text{rem}(15555858,\ 36) = 6$, and $\text{rem}(403,\ 36) = 7$, we find that (9.9) equals the remainder on division by 36 of

$$(3^{3456789} + 6^{5555})7^{6666666}. \tag{9.10}$$

Application of congruence relation

That's a little better, but $3^{3456789}$ has about a million digits in its decimal representation, so we still don't want to compute that. But let's look at the remainders of the first few powers of 3:

$$\begin{aligned} \text{rem}(3,\ 36) &= 3 \\ \text{rem}(3^2,\ 36) &= 9 \\ \text{rem}(3^3,\ 36) &= 27 \\ \text{rem}(3^4,\ 36) &= 9. \end{aligned}$$

We got a repeat of the second step, $\text{rem}(3^2,\ 36)$ after just two more steps. This means means that starting at 3^2, the sequence of remainders of successive powers of 3 will keep repeating every 2 steps. So a product of an odd number of at least three 3's will have the same remainder on division by 36 as a product of just three 3's. Therefore,

$$\text{rem}(3^{3456789},\ 36) = \text{rem}(3^3,\ 36) = 27.$$

Application of congruence relation

Powers of 6 are even easier because $\text{rem}(6^2,\ 36) = 0$, so 0's keep repeating after the second step. Powers of 7 repeat after six steps, but on the fifth step you get a 1, that is $\text{rem}(7^6,\ 36) = 1$, so (9.10) successively simplifies to be the remainders of the following terms:

$$
\begin{aligned}
&(3^{3456789} + 6^{5555})7^{6666666} \\
&(3^3 + 6^2 \cdot 6^{5553})(7^6)^{1111111} \\
&(3^3 + 0 \cdot 6^{5553})1^{1111111} \\
&= 27.
\end{aligned}
$$

Application of congruence relation

Euler's Theorem

The RSA cryptosystem examined in this section, and other current schemes for encoding secret messages, involve computing remainders of numbers raised to large powers. A basic fact about remainders of powers follows from a theorem due to Leonhard Euler about congruences.

RSA means Rivest, Shamir, Adleman. They are the inventors of the popular RSA Algorithm. The RSA algorithm is based on public-key encryption technology which is a public-key cryptosystem for reliable data transmission.

Application of congruence relation

Euler's Theorem

Definition 9.10.1. For $n > 0$, define

$$\phi(n) ::= \text{the number of integers in } [0..n), \text{ that are relatively prime to } n.$$

This function ϕ is known as Euler's ϕ function.[15]

For example, $\phi(7) = 6$ because all 6 positive numbers in $[0..7)$ are relatively prime to the prime number 7. Only 0 is not relatively prime to 7. Also, $\phi(12) = 4$ since 1, 5, 7, and 11 are the only numbers in $[0..12)$ that are relatively prime to 12.[16]

1 is relatively prime with every number even itself. 0 and 1 are relatively prime numbers, as the common factor is 1. 0 is not relatively prime with any other integer except 1. It is divisible by any integer.

Application of congruence relation

Euler's Theorem

Euler's Theorem is traditionally stated in terms of congruence:

Theorem (*Euler's Theorem*)**.** *If n and k are relatively prime, then*

$$k^{\phi(n)} \equiv 1 \pmod{n}. \tag{9.15}$$

Relatively prime number: when two numbers have no common factors other than 1. In other words there is no value that you could divide them both by exactly (without any remainder).

Application of congruence relation

Euler's Theorem

Fermat's Little Theorem

For the record, we mention a famous special case of Euler's Theorem that was known to Fermat a century earlier.

Corollary 9.10.8 (*Fermat's Little Theorem*)**.** *Suppose p is a prime and k is not a multiple of p. Then*

$$k^{p-1} \equiv 1 \pmod{p}.$$

Application of congruence relation

Computing Euler's ϕ Function

RSA works using arithmetic modulo the product of two large primes, so we begin with an elementary explanation of how to compute $\phi(pq)$ for primes p and q:

Lemma 9.10.9.

$$\phi(pq) = (p-1)(q-1)$$

for primes $p \neq q$.

Lemma: a subsidiary or intermediate theorem in an argument or proof.

Application of congruence relation

Computing Euler's ϕ Function

The following theorem provides a way to calculate $\phi(n)$ for arbitrary n.

Theorem 9.10.10.

(a) If p is a prime, then

$$\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^k - p^{k-1}$$

for $k \geq 1$.

(b) If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.

Here's an example of using Theorem 9.10.10 to compute $\phi(300)$:

$$\begin{aligned}
\phi(300) &= \phi(2^2 \cdot 3 \cdot 5^2) \\
&= \phi(2^2) \cdot \phi(3) \cdot \phi(5^2) && \text{(by Theorem 9.10.10.(b))} \\
&= (2^2 - 2^1)(3^1 - 3^0)(5^2 - 5^1) && \text{(by Theorem 9.10.10.(a))} \\
&= 80.
\end{aligned}$$

Basic Applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher

Primes and Composite Numbers

Prime and composite numbers

Every integer greater than 1 is either prime or composite, but not both:

A positive integer p is prime if it has only two positive divisors: namely, 1 and p. By convention, 1 is not prime

Prime numbers: $2,3,5,7,11,13,17,19,23,29,31,37,41,...$

An integer $n \geq 2$ that has three or more positive divisors is called composite.

Composite numbers: $4,6,8,9,10,12,14,15,16,18,20,21,22,...$

Prime numbers

A positive integer p is prime if the only positive factors of p are 1 and p

- If there are other factors, it is composite
- Note that 1 is not prime!
  - It's not composite either – it's in its own class

An integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$

Fundamental theorem of arithmetic

Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size

Examples

100 = 2 * 2 * 5 * 5

182 = 2 * 7 * 13

29820 = 2 * 2 * 3 * 5 * 7 * 71

In a fundamental sense, primes are the *building blocks* of the natural numbers.

Showing a number is prime

E.g., show that 113 is prime. How?

Solution

- The only prime factors less than $\sqrt{113} = 10.63$ are 2, 3, 5, and 7
- None of these divide 113 evenly
- Thus, by the fundamental theorem of arithmetic, 113 must be prime

Showing a number is composite

Show that 899 is composite.

Solution

- Divide 899 by successively larger primes, starting with 2
- We find that 29 and 31 divide 899

Prime and Composite Numbers

Definition

An integer n > 1 is called a prime number if its positive divisors are 1 and n.

Definition

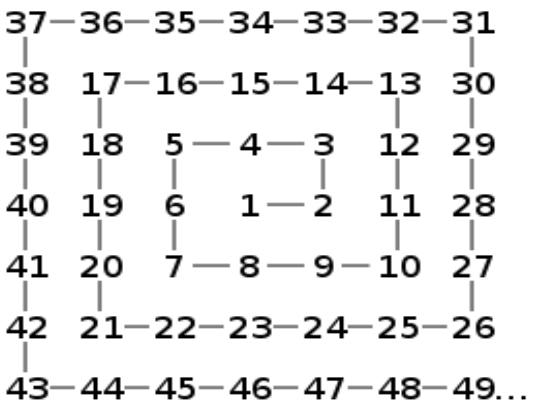
Any integer number n > 1 that is not prime, is called a composite number.

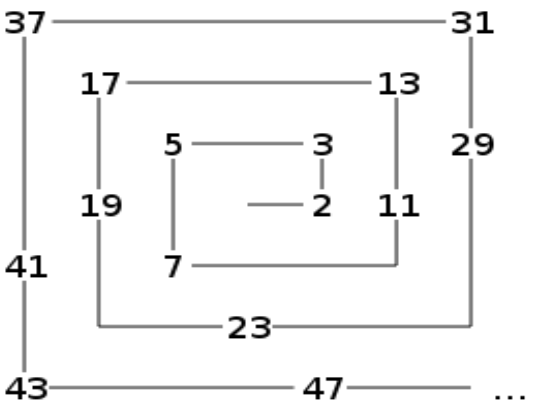
Example

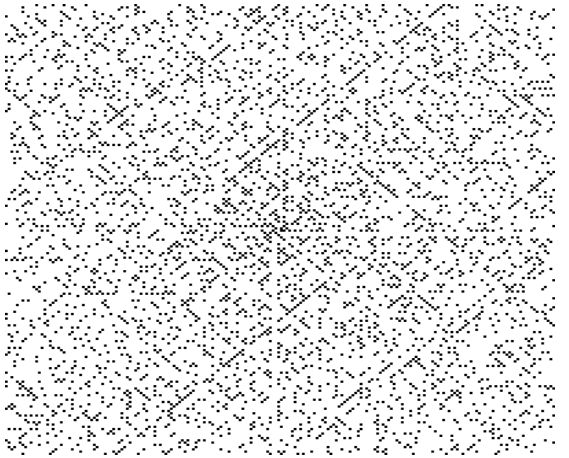
Prime numbers: 2, 3, 5, 7, 11, 13, 17 …

Composite numbers: 4, 6, 25, 900, 17778, …

Distribution diagrams for primes







Greatest Common Divisor (GCD)

De nition

The greatest common divisor (gcd) of two or more nonzero integers is the largest positive integer that divides the numbers without a remainder.

Example

The common divisors of 36 and 60 are 1, 2, 3, 4, 6, 12. The greatest common divisor is gcd(36, 60) = 12.

The greatest common divisor always exists, because the set of common divisors of any two given integers is non-empty

Greatest Common Divisor (GCD)

How to Find the Greatest Common Divisor?

For a set of two positive integers (a, b) we use the below-given steps to find the greatest common divisor:

Step 1: Write the divisors of positive integer "a".

Step 2: Write the divisors of positive integer "b".

Step 3: Enlist the common divisors of "a" and "b".

Step 4: Now find the divisor which is the highest of both "a" and "b".

Example: Find the greatest common divisor of 13 and 48.

Solution: We will use the below steps to determine the greatest common divisor of (13, 48).

Divisors of 13 are 1, and 13.

Divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24 and 48.

The common divisor of 13 and 48 is 1.

The greatest common divisor of 13 and 48 is 1.

Thus, GCD(13, 48) = 1.

Greatest common divisor

The greatest common divisor of two integers *a* and *b* is the largest integer *d* such that *d* | a and *d* | b

– Denoted by gcd(a,b)

Examples

gcd (24, 36) = 12

gcd (17, 22) = 1

gcd (100, 17) = 1

Relative primes

Two numbers are *relatively prime* if they don't have any common factors (other than 1)

- Rephrased: *a* and *b* are relatively prime if gcd (a,b) = 1

gcd (25, 16) = 1, so 25 and 16 are relatively prime

Pairwise relative prime

A set of integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime

- Formally: The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if gcd(a_i, a_j) = 1 whenever $1 \leq i < j \leq n$.

Example: are 10, 17, and 21 pairwise relatively prime?

- gcd(10,17) = 1, gcd (17, 21) = 1, and gcd (21, 10) = 1
- Thus, they are pairwise relatively prime

Example: are 10, 19, and 24 pairwise relatively prime?

- Since gcd(10,24) ≠ 1, they are not

More on gcd's

Given two numbers *a* and *b*, rewrite them as:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

- Example: gcd (120, 500)
  - $120 = 2^3*3*5 = 2^3*3^1*5^1$
  - $500 = 2^2*5^3 = 2^2*3^0*5^3$

Then compute the gcd by the following formula:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}$$

- Example: $\gcd(120,500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$

More on gcd's

Euclid's Algorithm

The first thing to figure out is how to find gcd's. A good way called *Euclid's algorithm* has been known for several thousand years. It is based on the following elementary observation.

Lemma 9.2.1. *For $b \neq 0$,*

Lemma 9.2.1 is useful for quickly computing the greatest common divisor of two numbers. For example, we could compute the greatest common divisor of 1147 and 899 by repeatedly applying it:

$$\begin{aligned}
\gcd(1147, 899) &= \gcd(899, \underbrace{\text{rem}(1147,\ 899)}_{=248}) \\
&= \gcd\,(248, \text{rem}(899,\ 248) = 155) \\
&= \gcd\,(155, \text{rem}(248,\ 155) = 93) \\
&= \gcd\,(93, \text{rem}(155,\ 93) = 62) \\
&= \gcd\,(62, \text{rem}(93,\ 62) = 31) \\
&= \gcd\,(31, \text{rem}(62,\ 31) = 0) \\
&= 31
\end{aligned}$$

Greatest Common Divisor (GCD)

Definition

Given integers a > 0 and b > 0, we define gcd(a, b) = c, the greatest common divisor (GCD), as the greatest number that divides both a and b.

Example

gcd(256, 100)=4

Definition

Two integers a > 0 and b > 0 are relatively prime if gcd(a, b) = 1.

Example

25 and 128 are relatively prime.

Least common multiple (LCM)

FIND THE LEAST COMMON MULTIPLE (LCM) OF TWO NUMBERS BY LISTING MULTIPLES

- List the first several multiples of each number.
- Look for multiples common to both lists. If there are no common multiples in the lists, write out additional multiples for each number.
- Look for the smallest number that is common to both lists.
- This number is the LCM.

Least common multiple (LCM)

FIND THE LEAST COMMON MULTIPLE (LCM) OF TWO NUMBERS BY LISTING MULTIPLES

Find the LCM of 1515 and 2020 by listing multiples.
Solution:
List the first several multiples of 1515 and of 2020. Identify the first common multiple.
15: 15,30,45,60,75,90,105,12020: 20,40,60,80,100,120,140,16015: 15,30,45,60,75,90,105,12020: 20,40,60,80,100,120,140,160
The smallest number to appear on both lists is 6060, so 6060 is the least common multiple of 1515 and 2020.
Notice that 120120 is on both lists, too. It is a common multiple, but it is not the least common multiple.

Least common multiple (LCM)

The LCM of 3500 and 625 is 17500.

Steps to find LCM

Find the prime factorization of 3500

$3500 = 2 \times 2 \times 5 \times 5 \times 5 \times 7$

Find the prime factorization of 625

$625 = 5 \times 5 \times 5 \times 5$

Multiply each factor the greater number of times it occurs in steps i) or ii) above to find the LCM:

$LCM = 2 \times 2 \times 5 \times 5 \times 5 \times 5 \times 7$

LCM = **17500**

Least common multiple (LCM)

The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*.

- Denoted by lcm (*a*, *b*)

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$$

Example: lcm(10, 25) = 50

What is lcm (95256, 432)?

What is lcm ($2^3 3^5 7^2$, $2^4 3^3$)?

- $95256 = 2^3 3^5 7^2$, $432 = 2^4 3^3$
- lcm ($2^3 3^5 7^2$, $2^4 3^3$) = $2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$

  $= 2^4 3^5 7^2 = 190512$

lcm and gcd theorem

Theorem: Let a and b be positive integers.

Then $a*b = \gcd(a,b) * \text{lcm}(a, b)$

Example: gcd (10,25) = 5, lcm (10,25) = 50

So, 10*25 = 5*50

Example: gcd (95256, 432) = 216, lcm (95256, 432) = 190512

So, 95256*432 = 216*190512

Some other operations

The greatest common divisor and the least common multiple (lcm)

$$\gcd(m,n) = \langle \min(m_1, n_1), \min(m_2, n_2), \min(m_3, n_3), \ldots \rangle$$

Dually,

$$\operatorname{lcm}(m,n) = \langle \max(m_1, n_1), \max(m_2, n_2), \max(m_3, n_3), \ldots \rangle$$

Example

$$120 = 2^3 \cdot 3^1 \cdot 5^1 = \langle 3,1,1,0,0,\ldots \rangle$$

$$36 = 2^2 \cdot 3^2 = \langle 2,2,0,0,\ldots \rangle$$

$$\gcd(120,36) = \langle \min(3,2), \min(1,2), \min(1,0), \ldots \rangle = \langle 2,1,0,0,\ldots \rangle = 12$$

$$\operatorname{lcm}(120,36) = \langle \max(3,2), \max(1,2), \max(1,0), \ldots \rangle = \langle 3,2,1,0,0,\ldots \rangle = 360$$

Mathematics for Computer Science

revised Wednesday 6th June, 2018, 13:43

Eric Lehman
Google Inc.

F Thomson Leighton
Department of Mathematics
and the Computer Science and AI Laboratory,
Massachussetts Institute of Technology;
Akamai Technologies

Albert R Meyer
Department of Electrical Engineering and Computer Science
and the Computer Science and AI Laboratory,
Massachussetts Institute of Technology

Reference: Concrete mathematics by Ronald, Knuth