Number Theory

ITT9132 Concrete Mathematics
Lecture 7 – 13 March 2019

Chapter Four

- Divisibility
- Primes
- Prime examples
- Relative primality

Contents

Next section

Next subsection

Division (with remainder)

Definition

Let a and b be integers and $a > 0$. Then division of b by a is finding an integer quotient q and a remainder r satisfying the condition

$$b = aq + r \quad \text{with} \quad 0 \leqslant r < a \,.$$

Here:

b – dividend

a – divider (=divisor) (=factor)

$q = \lfloor a/b \rfloor$ – quotient

$r = a \bmod b$ – remainder (=residue)

Example

If $a = 3$ and $b = 17$, then the division of b by a yields:

$$17 = 3 \cdot 5 + 2.$$

Division (with remainder)

Definition

Let a and b be integers and $a > 0$. Then division of b by a is finding an integer quotient q and a remainder r satisfying the condition

$$b = aq + r \quad \text{with } 0 \leqslant r < a\,.$$

Here:

b	– dividend
a	– divider (=divisor) (=factor)
$q = \lfloor a/b \rfloor$	– quotient
$r = a \bmod b$	– remainder (=residue)

Example

If $a = 3$ and $b = 17$, then the division of b by a yields:

$$17 = 3 \cdot 5 + 2.$$

Negative dividends

- If the divisor is positive, then the remainder is always **non-negative**.

For example

If $a = 3$ and $b = -17$, then the division of b by a yields:

$$-17 = 3 \cdot (-6) + 1.$$

- The integer b can be always represented as $b = aq + r$ with $0 \leqslant r < a$ due to the fact that b either coincides with a term of the sequence

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots$$

or lies between two consecutive elements.

Negative dividends

- If the divisor is positive, then the remainder is always **non-negative**.

For example

If $a = 3$ and $b = -17$, then the division of b by a yields:

$$-17 = 3 \cdot (-6) + 1.$$

- The integer b can be always represented as $b = aq + r$ with $0 \leqslant r < a$ due to the fact that b either coincides with a term of the sequence

$$\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots$$

or lies between two consecutive elements.

NB! Division by a negative integer yields a negative remainder

$$5 \bmod 3 = 5 - 3\lfloor 5/3 \rfloor = 2$$

$$5 \bmod -3 = 5 - (-3)\lfloor 5/(-3) \rfloor = -1$$

$$-5 \bmod 3 = -5 - 3\lfloor -5/3 \rfloor = 1$$

$$-5 \bmod -3 = -5 - (-3)\lfloor -5/(-3) \rfloor = -2$$

Be careful!

Some computer languages use another definition.

From now on, we assume $a > 0$.

Divisibility

Definition

Let a and b be integers. We say that a divides b , or a is a divisor of b, or b is a multiple of a, if there exists an integer m such that $b = a \cdot m$.

Notations:

- $a|b$: a divides b
- $a \mid b$: a divides b
- $b \,\vdots\, a$: b is a multiple of a

For example

$$3 \mid 111 \qquad 7 \mid -91 \qquad -7 \mid -91$$

Divisors

Definition

If $a \mid b$, then:

- a is called a divisor, or factor, or multiplier of b.

Properties

- Every integer $b \neq 0, 1, -1$ has at least four divisors: $1, -1, b, -b$.
- $a \mid 0$ for any integer a; reverse relation $0 \mid a$ is valid only for $a = 0$. So: $0 \mid 0$.
- $1 \mid b$ for any integer b, whereas $b \mid 1$ iff $b = 1$ or $b = -1$.

More properties

1. If $a \mid b$, then $\pm a \mid \pm b$.
2. If $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for every $m, n \in \mathbb{Z}$.
3. $a \mid b$ iff $ac \mid bc$ for every integer c.

Notes:

- Property 1 allows to only study divisibility between positive integers.
- By property 2, if a is a divisor of both b and c, then it is a divisor of both $b+c$ and $b-c$.
  We then say that a is a common divisor of b and c (as well as of $b+c$, $b-c$, $b+2c$ etc.)

Next section

Next subsection

Greatest Common Divisor

Definition

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 and finite.

Next subsection

TAL TECH

The Euclidean algorithm

The algorithm to compute $\gcd(a, b)$ for positive integers a and b

Input: Positive integers a and b, assume that $a > b$
Output: $\gcd(a, b)$

- **while** $b > 0$ **do**
  1. $r := a \textbf{ mod } b$
  2. $a := b$
  3. $b := r$

  done
- **return**(a)

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

TAL TECH

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Example: compute $\gcd(2322, 654)$

a	b
2322	654
654	360
360	294
294	66
66	30
30	6
6	0

Important questions to answer:

- Does the algorithm terminate for every input?
- Is the result the *greatest* common divisor?
- How long does it take?

Termination of the Euclidean algorithm

- In any cycle, the pair of integers (a, b) is replaced by (b, r), where r is the remainder of division of a by b.
- Hence, $r < b$.
- The second number of the pair decreases, but remains non-negative, so the process cannot last infinitely long.

Correctness of the Euclidean algorithm

Theorem

If r is a remainder of division of a by b, then

$$\gcd(a,b) = \gcd(b,r)$$

Proof. It follows from the equality $a = bq + r$ that:

1. if $d|a$ and $d|b$, then $d|r$;
2. if $d|b$ and $d|r$, then $d|a$.

That is: the common divisors of a and b are precisely the common divisors of b and r.

Then the greatest common divisors must also coincide. Q.E.D.

Complexity of the Euclidean algorithm

Theorem

The number of steps of the Euclidean algorithm applied to two positive integers a and b is at most $1 + \lg a + \lg b$.

Proof:

- Let us consider the step where the pair (a, b) is replaced by (b, r).
- Then $r < b$ and $b + r \leqslant a$
- Hence, $2r < r + b \leqslant a$, that is, $br < ab/2$. So the product of the two parameters halves at each step.
- If after k cycles the product is still positive, then $ab/2^k > 1$, so:

$$k \leqslant \lg(ab) = \lg a + \lg b\,.$$

Q.E.D.

The numbers produced by the Euclidean algorithm

$$
\begin{aligned}
a &= bq_1 + r_1 && r_1 \text{ can be expressed in terms of } b \text{ and } a \\
b &= r_1 q_2 + r_2 && r_2 \text{ can be expressed in terms of } r_1 \text{ and } b \\
r_1 &= r_2 q_3 + r_3 && r_3 \text{ can be expressed in terms of } r_2 \text{ and } r_1 \\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && r_{k-1} \text{ can be expressed in terms of } r_{k-2} \text{ and } r_{k-3} \\
r_{k-2} &= r_{k-1} q_k + r_k && r_k \text{ can be expressed in terms of } r_{k-1} \text{ and } r_{k-2} \\
r_{k-1} &= r_k q_{k+1}
\end{aligned}
$$

Now, one can extract $r_k = \gcd(a, b)$ from the second last equality and substitute there step-by-step $r_{k-1}, r_{k-2}, \ldots$ using previous equations.
We obtain finally that r_k equals to a linear combination of a and b with (not necessarily positive) integer coefficients.

GCD as a linear combination

Theorem (Bézout's identity)

Let $d = \gcd(a, b)$. Then:

$$\gcd(a,b) = \min\{n \geqslant 1 \mid \exists s, t \in \mathbb{Z} : n = sa + tb\}.$$

For example: $a = 360$ and $b = 294$

$$\gcd(a,b) = 294 \cdot (-11) + 360 \cdot 9 = -11a + 9b$$

Proof of Bézout's identity

We may suppose $a \geqslant b \geqslant 1$. Call:

$$L ::= \{m \in \mathbb{Z} \mid \exists s, t \in \mathbb{Z} \,.\, m = sa + tb\}$$

- As $a = 1a + 0b$ and $b = 0a + 1b$, $L \cap \mathbb{Z}^+$ is nonempty:
  Let $\ell = sa + tb$ be its minimum.
- Then every common divisor of a and b is a divisor of ℓ.
  The proof is complete if we show that $\ell \mid a$ and $\ell \mid b$.
- Now, for $q = \lfloor a/\ell \rfloor$ it is:

  $$0 \leqslant r = a - \ell \cdot \lfloor a/\ell \rfloor = a - q\ell = (1 - qs)a + (-qt)b \in L\,.$$

  As ℓ is the minimum positive integer in L, it must be $r = 0$: that is, $\ell \mid a$.
- The proof that $\ell \mid b$ is similar.

Application of EA: solving of linear Diophantine Equations

Corollary

Let a, b and c be positive integers. The equation $ax + by = c$ has integer solutions if and only if c is a multiple of $\gcd(a, b)$.

The method: Making use of Euclidean algorithm, compute $s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$. Then:

$$x = \frac{cs}{\gcd(a, b)}$$
$$y = \frac{ct}{\gcd(a, b)}$$

Linear Diophantine Equations (2)

Example: $92x + 17y = 3$

From EA:

a	b	Relation
92	17	
17	7	$92 = 5 \cdot 17 + 7$
7	3	$17 = 2 \cdot 7 + 3$
3	1	$7 = 2 \cdot 3 + 1$
1	0	

Transformations:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (17 - 7 \cdot 2) = (-2) \cdot 17 + 5 \cdot 7 = \\ &= (-2) \cdot 17 + 5 \cdot (92 - 5 \cdot 17) = 5 \cdot 92 + (-27) \cdot 17 \end{aligned}$$

$\gcd(92, 7) | 3$ yields a solution

$$x = \frac{3 \cdot 5}{\gcd(92, 17)} = 3 \cdot 5 = 15$$

$$y = \frac{3 \cdot (-27)}{\gcd(92, 17)} = -3 \cdot 27 = -81$$

Linear Diophantine Equations (3)

Example: $5x + 3y = 2$ has multiple solutions

$$\gcd(5, 3) = 1$$

As $1 = 2 \cdot 5 + 3 \cdot 3$, then one solution is:

$$x = 2 \cdot 2 = 4$$
$$y = -3 \cdot 2 = -6$$

As $1 = (-10) \cdot 5 + 17 \cdot 3$, then another solution is:

$$x = -10 \cdot 2 = -20$$
$$y = 17 \cdot 2 = 34$$

Example: $15x + 9y = 8$ has no solutions

As $\gcd(15, 9) = 3$, the equation can be rewritten:

$$3 \cdot (5x + 3y) = 8.$$

The left-hand side of the equation is divisible by 3, but the right-hand side is not, therefore the equality cannot be valid for any integer x and y.

Linear Diophantine Equations (3)

Example: $5x+3y=2$ has multiple solutions

$$\gcd(5,3)=1$$

As $1=2\cdot 5+3\cdot 3$, then one solution is:

$$x=2\cdot 2=4$$
$$y=-3\cdot 2=-6$$

As $1=(-10)\cdot 5+17\cdot 3$, then another solution is:

$$x=-10\cdot 2=-20$$
$$y=17\cdot 2=34$$

Example: $15x+9y=8$ has no solutions

As $\gcd(15,9)=3$, the equation can be rewritten:

$$3\cdot(5x+3y)=8.$$

The left-hand side of the equation is divisible by 3, but the right-hand side is not, therefore the equality cannot be valid for any integer x and y.

More about Linear Diophantine Equations (1)

- The general solution of a Diophantine equation $ax + by = c$ is

$$\begin{cases} x &= x_0 + \frac{kb}{\gcd(a,b)} \\ y &= y_0 - \frac{ka}{\gcd(a,b)} \end{cases}$$

  where x_0 and y_0 are particular solutions and k is an integer.

- Particular solutions can be found with the Euclidean algorithm:

$$\begin{cases} x_0 &= \frac{cs}{\gcd(a,b)} \\ y_0 &= \frac{ct}{\gcd(a,b)} \end{cases}$$

- This equation has a solution with x and y integer if and only if $\gcd(a,b) \mid c$.
- The general solution above provides all integer solutions of the equation.
  (see proof in http://en.wikipedia.org/wiki/Diophantine_equation)

TAL TECH

More about Linear Diophantine Equations (2)

Example: $5x+3y=2$

We have found that $\gcd(5,3)=1$ and its particular solutions are $x_0=4$ and $y_0=-6$.

Thus, for any $k\in\mathbb{Z}$:

$$\begin{cases} x = 4+3k \\ y = -6-5k \end{cases}$$

Solutions of the equation for $k=\ldots,-3,-2,-1,0,1,2,3,\ldots$ are infinite sequences of numbers:

$$\begin{array}{ccccccccccc} x & = & \ldots, & -5, & -2, & 1, & 4, & 7, & 10, & 13, & \ldots \\ y & = & \ldots, & 9, & 4, & -1, & -6, & -11, & -16, & -21, & \ldots \end{array}$$

Among others, if $k=-8$, then we get the solution $x=-20, y=34$.

Next section

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: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$

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

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

Next subsection

Another application of the Euclidean algorithm

The Fundamental Theorem of Arithmetic

Every positive integer n can be written uniquely as a (possibly empty for $n = 1$) product of primes:

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k \,, \;\; p_1 \leqslant \ldots \leqslant p_m$$

Proof:

- Let $n \geqslant 2$ be the smallest integer with two different prime factorizations:

$$n = p_1 \ldots p_m = q_1 \cdots q_k \,, \;\; p_1 \leqslant \ldots \leqslant p_m \,, \; q_1 \leqslant \ldots \leqslant q_k$$

- If $p_1 < q_1$, let $s, t \in \mathbb{Z}$ such that $sp_1 + tp_2 = 1$. Then:

$$sp_1 q_2 \cdots q_k + tq_1 q_2 \ldots q_k = q_2 \cdots q_k$$

- Now, as $\gcd(p_1, q_1) = 1$ and $p_1 \mid q_1 q_2 \cdots q_k$, it is $p_1 \mid q_2 \cdots q_k$. But then, $n/p_1 = q_1 q_2 \cdots q_k / p_1 < n$ is an integer, despite p_1 being smaller than any prime factor of n: contradiction.
- Similarly, it cannot be $p_1 > q_1$. Hence, $p_1 = q_1$. But then, $x = p_2 \cdots p_m = q_2 \cdots q_k < n$ has two different prime factorizations, against n being the smaller such positive integer: contradiction. Q.E.D.

Canonical form of integers

- Every positive integer n can be represented uniquely as a product

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_p p^{n_p}, \text{ where } n_p \geqslant 0 \forall p$$

For example:

$$600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdots$$

$$35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdots$$

$$5\ 251\ 400 = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^1 \cdot 11^2 \cdot 13^0 \cdots \cdot 29^0 \cdot 31^1 \cdot 37^0 \cdots$$

Prime-exponent representation of integers

- The canonical form of an integer $n = \prod_p p^{n_p}$ provides a sequence of powers $\langle n_1, n_2, \ldots \rangle$ as another representation.

For example:

$$600 = \langle 3,1,2,0,0,0,\ldots \rangle$$
$$35 = \langle 0,0,1,1,0,0,0,\ldots \rangle$$
$$5\ 251\ 400 = \langle 3,0,2,1,2,0,0,0,0,0,1,0,0,\ldots \rangle$$

Prime-exponent representation and arithmetic operations

Multiplication

Let

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} = \prod_p p^{m_p}$$

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_p p^{n_p}$$

Then

$$mn = p_1^{m_1+n_1} p_2^{m_2+n_2} \cdots p_k^{m_k+n_k} = \prod_p p^{m_p+n_p}$$

Using prime-exponent representation:

$$mn = \langle m_1 + n_1, m_2 + n_2, m_3 + n_3, \ldots \rangle$$

For example

$$600 \cdot 35 = \langle 3,1,2,0,0,0,\ldots \rangle \cdot \langle 0,0,1,1,0,0,0,\ldots \rangle$$
$$= \langle 3+0, 1+0, 2+1, 0+1, 0+0, 0+0, \ldots \rangle$$
$$= \langle 3,1,3,1,0,0,\ldots \rangle = 21\ 000$$

Prime-exponent representation and arithmetic operations

Multiplication

Let

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} = \prod_p p^{m_p}$$

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_p p^{n_p}$$

Then

$$mn = p_1^{m_1+n_1} p_2^{m_2+n_2} \cdots p_k^{m_k+n_k} = \prod_p p^{m_p+n_p}$$

Using prime-exponent representation:

$$mn = \langle m_1 + n_1, m_2 + n_2, m_3 + n_3, \ldots \rangle$$

For example

$$\begin{aligned} 600 \cdot 35 &= \langle 3,1,2,0,0,0,\ldots\rangle \cdot \langle 0,0,1,1,0,0,0,\ldots\rangle \\ &= \langle 3+0, 1+0, 2+1, 0+1, 0+0, 0+0, \ldots\rangle \\ &= \langle 3,1,3,1,0,0,\ldots\rangle = 21\ 000 \end{aligned}$$

Prime-exponent representation and arithmetic operations

Multiplication

Let

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} = \prod_p p^{m_p}$$

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_p p^{n_p}$$

Then

$$mn = p_1^{m_1+n_1} p_2^{m_2+n_2} \cdots p_k^{m_k+n_k} = \prod_p p^{m_p+n_p}$$

Using prime-exponent representation:

$$mn = \langle m_1 + n_1, m_2 + n_2, m_3 + n_3, \ldots \rangle$$

For example

$$\begin{aligned} 600 \cdot 35 &= \langle 3,1,2,0,0,0,\ldots \rangle \cdot \langle 0,0,1,1,0,0,0,\ldots \rangle \\ &= \langle 3+0, 1+0, 2+1, 0+1, 0+0, 0+0, \ldots \rangle \\ &= \langle 3,1,3,1,0,0,\ldots \rangle = 21\ 000 \end{aligned}$$

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,

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

Example

$$\begin{aligned}
120 &= 2^3 \cdot 3^1 \cdot 5^1 = \langle 3,1,1,0,0,\ldots \rangle \\
36 &= 2^2 \cdot 3^2 = \langle 2,2,0,0,\ldots \rangle \\
\gcd(120,36) &= \langle \min(3,2), \min(1,2), \min(1,0), \ldots \rangle = \langle 2,1,0,0,\ldots \rangle = 12 \\
\mathrm{lcm}(120,36) &= \langle \max(3,2), \max(1,2), \max(1,0), \ldots \rangle = \langle 3,2,1,0,0,\ldots \rangle = 360
\end{aligned}$$

TAL TECH

Properties of the GCD

Homogeneity

$\gcd(na, nb) = n \cdot \gcd(a, b)$ for every positive integer n.

Proof.

Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, and $\gcd(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, where $\gamma_i = \min(\alpha_i, \beta_i)$. If $n = p_1^{n_1} \cdots p_k^{n_k}$, then

$$\begin{aligned}
\gcd(na, nb) &= p_1^{\min(\alpha_1+n_1, \beta_1+n_1)} \cdots p_k^{\min(\alpha_k+n_k, \beta_k+n_k)} = \\
&= p_1^{\min(\alpha_1, \beta_1)} p_1^{n_1} \cdots p_k^{\min(\alpha_k, \beta_k)} p_k^{n_k} = \\
&= p_1^{n_1} \cdots p_k^{n_k} p_1^{\gamma_1} \cdots p_k^{\gamma_k} = n \cdot \gcd(a, b)
\end{aligned}$$

Q.E.D.

TAL TECH

Properties of the GCD

GCD and LCM

$\gcd(a,b) \cdot \mathrm{lcm}(a,b) = ab$ for every two positive integers a and b

Proof.

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

Q.E.D.

Relatively prime numbers

Definition

Two integers a and b are *coprime*, or relatively prime, if $\gcd(a,b) = 1$.

Notations used:

- $\gcd(a,b) = 1$
- $a \perp b$

For example

$16 \perp 25$ and $99 \perp 100$

Some simple properties:

- Dividing a and b by their GCD yields relatively prime numbers:

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

- Any two positive integers a and b can be represented as $a = a'd$ and $b = b'd$, where $d = \gcd(a,b)$ and $a' \perp b'$

Relatively prime numbers

Definition

Two integers a and b are *coprime*, or relatively prime, if $\gcd(a,b) = 1$.

Notations used:

- $\gcd(a,b) = 1$
- $a \perp b$

For example

$16 \perp 25$ and $99 \perp 100$

Some simple properties:

- Dividing a and b by their GCD yields relatively prime numbers:

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

- Any two positive integers a and b can be represented as $a = a'd$ and $b = b'd$, where $d = \gcd(a,b)$ and $a' \perp b'$

Properties of relatively prime numbers

Theorem

If $a \perp b$, then $\gcd(ac, b) = \gcd(c, b)$ for every positive integer c.

Proof:

- Write $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}$, and $c = \prod_p p^{\gamma_p}$.
- Then for every prime p, either $\alpha_p = 0$ or $\beta_p = 0$ (or both).
- If $\alpha_p = 0$, then $p^{\min(\alpha_p + \gamma_p, \beta_p)} = p^{\min(\gamma_p, \beta_p)}$.
- If $\beta_p = 0$, then $p^{\min(\alpha_p + \gamma_p, \beta_p)} = p^{\min(\alpha_p + \gamma_p, 0)} = 1 = p^{\min(\gamma_p, 0)} = p^{\min(\gamma_p, \beta_p)}$.
- Hence, the common divisors of ac and b are the same as the common divisors of c and b. Q.E.D.

Divisibility

Observation

Let $a = \prod_p p^{\alpha_p}$ and $b = \prod_p p^{\beta_p}$. Then:

$$a | b \text{ iff } \alpha_p \leqslant \beta_p \text{ for every prime } p.$$

Consequently:

1. If $a \perp c$ and $b \perp c$, then $ab \perp c$
2. If $a | bc$ and $a \perp b$, then $a | c$
3. If $a | c$, $b | c$ and $a \perp b$, then $ab | c$

Divisibility

Observation

Let $a = \prod_p p^{\alpha_p}$ and $b = \prod_p p^{\beta_p}$. Then:

$$a | b \text{ iff } \alpha_p \leqslant \beta_p \text{ for every prime } p.$$

Consequently:

1. If $a \perp c$ and $b \perp c$, then $ab \perp c$
2. If $a | bc$ and $a \perp b$, then $a | c$
3. If $a | c$, $b | c$ and $a \perp b$, then $ab | c$

Example: compute $\gcd(560, 315)$

$$\begin{aligned} \gcd(560, 315) &= \gcd(5 \cdot 112, 5 \cdot 63) \\ &= 5 \cdot \gcd(112, 63) \text{ by the observation} \\ &= 5 \cdot \gcd(2^4 \cdot 7, 63) \\ &= 5 \cdot \gcd(7, 63) \text{ by the theorem} \\ &= 5 \cdot 7 = 35 \end{aligned}$$

The number of divisors

The canonic form of a positive integer allows to compute the number of its factors without factorization:

- Let $n = p_1^{n_1} \cdots p_k^{n_k}$.
- Then any positive divisor of n has the form:

$$m = \prod_{j=1}^{k} p_j^{m_j} \text{ with } 0 \leqslant m_j \leqslant n_j \text{ for every } 1 \leqslant j \leqslant k\,.$$

- Then the number of divisors of n is: $(n_1 + 1) \cdot (n_2 + 1) \cdots (n_k + 1)$.

Example

$694575 = 3^4 \cdot 5^2 \cdot 7^3$ has $(4+1) \cdot (2+1) \cdot (3+1) = 5 \cdot 3 \cdot 4 = 60$ positive factors.

Next subsection

The number of prime numbers

Euclid's theorem

There are infinitely many prime numbers.

Proof. Suppose there are only finitely many primes:

$$p_1, p_2, p_3, \ldots, p_k .$$

Consider then the number:

$$n = p_1 p_2 p_3 \cdots p_k + 1$$

By the Fundamental Theorem of Arithmetics, n is a product of powers of primes. But:

$$n \bmod p_i = 1 \ \text{for every}\ i = 1, 2, 3, \ldots, k .$$

So there must exist some other prime number (possibly n itself) which is not in the list $p_1, \ldots, p_k$. Q.E.D.

The number of prime numbers (another proof)

Theorem

For every positive integer n there exists a prime $p > n$.

Proof:

- Let p be the smallest nontrivial divisor of $m = n! + 1$.
- Then p must be prime, because any divisor q of p is also a divisor of n.
- But every integer $1 \leqslant k \leqslant n$ is a factor of $n!$, so the division of m by k gives remainder 1. Q.E.D.

The number of prime numbers: A proof by Paul Erdős

Theorem

$$\sum_{p\,\mathrm{prime}} \frac{1}{p} = +\infty .$$

Primes are distributed "very irregularly"

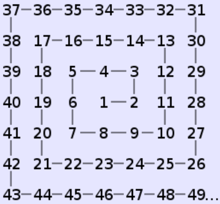
- Since all primes except 2 are odd, the difference between two primes must be at least two, except 2 and 3.
- Two primes whose difference is two are called twin primes. For example, $(17, 19)$ or $(3557, 3559)$.
- There is *no proof* of the conjecture that there are infinitely many twin primes.

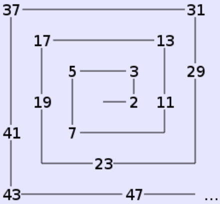
Theorem

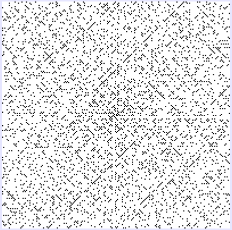
For every positive integer k, there exist k consecutive composite integers.

Proof. Let $n = k + 1$ and consider the numbers $n! + 2, n! + 3, \ldots, n! + n$. All these numbers are composite because of $i \mid n! + i$ for every $i = 2, 3, \ldots, n$. Q.E.D.

Distribution diagrams for primes







The prime counting function $\pi(n)$

- Definition:

$$\pi(n) = \text{number of primes in the set } \{1, 2, \ldots, n\}$$

- The first values:

$$\pi(1) = 0\,; \pi(2) = 1\,; \qquad \pi(3) = 2\,; \pi(4) = 2\,;$$
$$\pi(5) = 3\,; \pi(6) = 3\,; \qquad \pi(7) = 4\,; \pi(8) = 4$$

The Prime Number Theorem

Theorem

$$\pi(n) \sim \frac{n}{\ln n}\,, \text{ that is, } \lim_{n\to\infty} \frac{\pi(n)\cdot \ln n}{n} = 1\,.$$

- Studying prime tables, Carl-Friedrich Gauss came up with the formula in 1791.
- Jacques Hadamard and Charles de la Vallée Poussin proved the theorem independently from each other in 1896.

The Prime Number Theorem (2)

Example: How many primes are with 200 digits?

- The total number of positive integers with 200 digits is:

$$10^{200} - 10^{199} = 9 \cdot 10^{199}$$

- The approximate number of primes with 200 digits is then:

$$\pi(10^{200}) - \pi(10^{199}) \approx \frac{10^{200}}{200 \ln 10} - \frac{10^{199}}{199 \ln 10} \approx 1.95 \cdot 10^{197}$$

- The proportion of 200-digit numbers which are prime is thus:

$$\frac{1,95 \cdot 10^{197}}{9 \cdot 10^{199}} \approx \frac{1}{460} = 0.22\%$$

Warmup: Extending $\pi(x)$ to positive reals

Problem

Let $\pi(x)$ be the number of primes which are not larger than $x \in \mathbb{R}$.
Prove or disprove: $\pi(x) - \pi(x-1) = [x \text{ is prime}]$.

Warmup: Extending $\pi(x)$ to positive reals

Problem

Let $\pi(x)$ be the number of primes which are not larger than $x \in \mathbb{R}$.
Prove or disprove: $\pi(x) - \pi(x-1) = [x \text{ is prime}]$.

Solution

The formula is true if x is integer: but x is real ...

Warmup: Extending $\pi(x)$ to positive reals

Problem

Let $\pi(x)$ be the number of primes which are not larger than $x \in \mathbb{R}$.
Prove or disprove: $\pi(x) - \pi(x-1) = [x \text{ is prime}]$.

Solution

The formula is true if x is integer: but x is real ...

But clearly $\pi(x) = \pi(\lfloor x \rfloor)$: then

$$\begin{aligned} \pi(x) - \pi(x-1) &= \pi(\lfloor x \rfloor) - \pi(\lfloor x-1 \rfloor) \\ &= \pi(\lfloor x \rfloor) - \pi(\lfloor x \rfloor - 1) \\ &= [\lfloor x \rfloor \text{ is prime}] , \end{aligned}$$

which is the correct form of the thesis.