Greatest Common Divisor

Definition

The greatest common divisor (gcd) of two or more non-zero 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 $gcd(36, 60) = 12$

- The greatest common divisor exists always because of the set of common divisors of the given integers is non-empty and finite

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. $r := a$ **mod** b
  2. $a := b$
  3. $b := r$

  od
- **return**(a)

Example: compute $gcd(2322, 654)$

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

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 $d|a$

In other words, the set of common divisors of a and b equals to the set of common divisors of b and r, recomputing of (b,r) does not change the greatest common divisor of the pair

The number returned $r = gcd(r,0)$ 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

$$1 + \log_2 a + \log_2 b.$$

Proof. Let consider the step where the pair (a, b) is replaced by (b, r) Then we have $r < b$ and $b + r \leqslant a$ Hence $2r < r + b \leqslant a$ or $br < ab/2$ This is that the product of the elements of the pair decreases at least 2 times

If after k cycles the product is still positive, then $ab/2^k > 1$, that gives

$$k \leqslant \log_2(ab) = \log_2 a + \log_2 b$$

Q E D

GCD as a linear combination

Theorem (Bézout's identity)

Let $d = gcd(a, b)$ Then d can be written in the form

$$d = as + bt$$

where s and t are integers In addition,

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

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

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

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 such coefficients s and t 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	Seos
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: $5x+3y=2 \quad \rightarrow$ many 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: $15x+9y=8 \quad \rightarrow$ no solutions

Whereas, $gcd(15,9)=3$, then the equation can be expressed as

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

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)

- 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 by means of 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 (where x and y are integers) if and only if $gcd(a, b)|c$
- The general solution above provides all integer solutions of the equation (see proof in http://en.wikipedia.org/wiki/Diophantine_equation)

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 $x = -20$ ja $y = 34$.

Prime and composite numbers

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

- A positive integer p is called prime if it has just two 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 that has three or more divisors is called composite

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

Another application of EA

The Fundamental Theorem of Arithmetic

Every positive integer n can be written uniquely as a product of primes:

$$n = p_1 \dots p_m = \prod_{k=1}^{m} p_k, \qquad p_1 \leqslant \dots \leqslant p_m$$

Proof. Suppose we have two factorizations into primes

$$n = p_1 \dots p_m = q_1 \dots q_k, \qquad p_1 \leqslant \dots \leqslant p_m \text{ and } q_1 \leqslant \dots \leqslant q_k$$

Assume that $p_1 < q_1$. Since p_1 and q_1 are primes, $gcd(p_1, q_1) = 1$. That means that EA defines integers s and t that $sp_1 + tq_1 = 1$. Therefore

$$sp_1 q_2 \dots q_k + tq_1 q_2 \dots q_k = q_2 \dots q_k$$

Now p_1 divides both terms on the left, thus $q_2 \dots q_k / p_1$ is integer that contradicts with $p_1 < q_1$. This means that $p_1 = q_1$.

Similarly, using induction we can prove that $p_2 = q_2$, $p_3 = q_3$, etc

Q.E.D.

Canonical form of integers

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

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

For example:

$$\begin{aligned}
600 &= 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdots \\
35 &= 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdots \\
5\ 251\ 400 &= 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^1 \cdot 11^2 \cdot 13^0 \cdot \cdots \cdot 29^0 \cdot 31^1 \cdot 37^0 \cdots
\end{aligned}$$

Prime-exponent representation of integers

- 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

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

Some other operations

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

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

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

Example

$$120 = 2^3 \cdot 3^1 \cdot 5^1 = \langle 3,1,1,0,0,\cdots \rangle$$
$$36 = 2^2 \cdot 3^2 = \langle 2,2,0,0,\cdots \rangle$$

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

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.

Properties of the GCD

GCD and LCM

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

Proof.

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

Q.E.D.

Relatively prime numbers

Definition

Two integers a and b are said to be relatively prime (or co-prime) if the only positive integer that evenly divides both of them is 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 greatest common divisor yields relatively primes:

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

- 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.

Assuming canonic representation of $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}$ and $c = \prod_p p^{\gamma_p}$, one can conclude that for any prime p:

- The premise $a \perp b$ implies that $p^{\min(\alpha_p, \beta_p)} = 1$, it is that either $\alpha_p = 0$ or $\beta_p = 0$.
- 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 set of common divisors of ac and b is equal to the set of common divisors of c and b.

Q.E.D.

Consequences from the theorems above

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 $gcd(560, 315)$

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

The number of divisors

- Canonic form of a positive integer permits to compute the number of its factors without factorization:
- If
$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$
then any divisor of n can be constructed by multiplying $0, 1, \cdots, n_1$ times the prime divisor p_1, then $0, 1, \cdots, n_2$ times the prime divisor p_2 etc
- Then the number of divisors of n should be
$$(n_1 + 1)(n_2 + 1) \cdots (n_k + 1).$$

Example

Integer 694 575 has $694\,575 = 3^4 \cdot 5^2 \cdot 7^3$ on $(4 + 1)(2 + 1)(3 + 1) = 60$ factors

Number of primes

Euclid's theorem

There are infinitely many prime numbers.

Proof. Let's assume that there is finite number of primes:

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

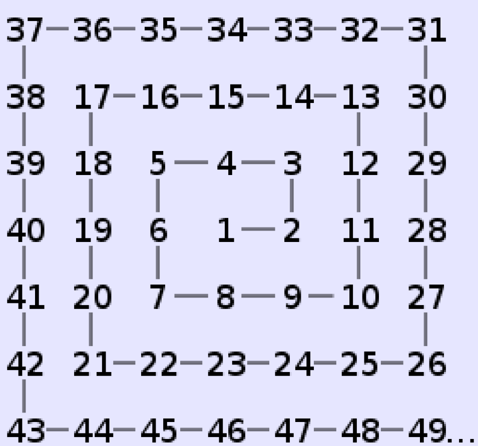
Consider

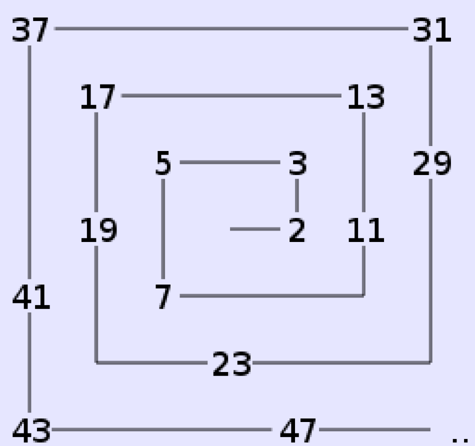
$$n = p_1 p_2 p_3 \cdots p_k + 1.$$

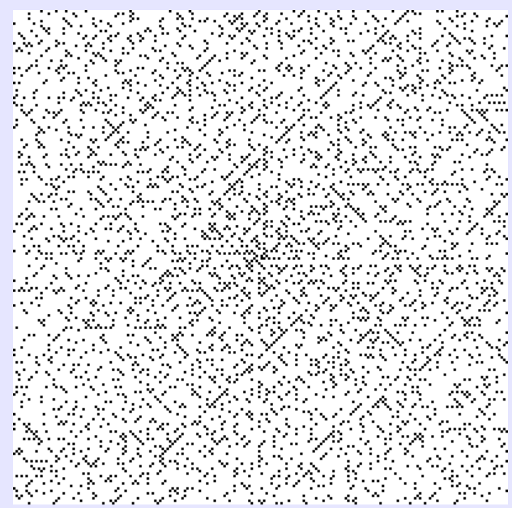
Like any other natural number, n is divisible at least by 1 and itself, i.e. it can be prime. Dividing n by $p_1, p_2, p_3, \ldots$ or p_k yields the remainder 1. So, n should be prime that differs from any of numbers $p_1, p_2, p_3, \ldots, p_k$, that leads to a contradiction with the assumption that the set of primes is finite.

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:

$$\begin{array}{llll} \pi(1) = 0 & \pi(2) = 1 & \pi(3) = 2 & \pi(4) = 2 \\ \pi(5) = 3 & \pi(6) = 3 & \pi(7) = 4 & \pi(8) = 4 \end{array}$$

The Prime Number Theorem

Theorem

The quotient of division of $\pi(n)$ by $n/\ln n$ will be arbitrarily close to 1 as n gets large. It is also denoted as

$$\pi(n) \sim \frac{n}{\ln n}$$

- Studying prime tables C. F. Gauss come up with the formula in ~ 1791.
- J. Hadamard and C. 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:

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

- Approximate number of primes with 200 digits

$$\pi(10^{200}) - \pi(10^{199}) \approx \frac{10^{200}}{200 \ln 10} - \frac{10^{199}}{199 \ln 10} \approx 1,95 \cdot 10^{197}$$

- Percentage of primes

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

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: $\pi(x) - \pi(x-1) = [x \,\text{is}\, \text{prime}]$.

Solution

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

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

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

which is true.