Extended Euclidean algorithm

E-OLYMP 1155. Euclid Problem From Euclid it is known that for any positive integers a and b there exist such integers x and y that $ax + by = d$, where d is the greatest common divisor of a and b. The problem is to find for given a and b corresponding x, y and d.

► Consider the equation: $7x + 9y = 1$, where GCD(7, 9) = 1. You must find such pair (x, y) for which $|x| + |y|$ is minimal. The answer will be $(x, y) = (4, -3)$, because $7 * 4 + 9 * (-3) = 1$.

Let for positive integers a and b ($a > b$) we know the value of

$$d = \text{GCD}(b, a \bmod b),$$

and also the numbers x' and y', for which

$$d = x' * b + y' * (a \bmod b)$$

d = GCD(a,b)	d = a * x + b * y
d = GCD(b,a%b)	d = b * x' + (a % b) * y'

Since $a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor * b$, then

$$d = x' * b + y' * (a - \left\lfloor \frac{a}{b} \right\rfloor * b) = y' * a + (x' - y' * \left\lfloor \frac{a}{b} \right\rfloor) * b = x * a + y * b,$$

where we denote

$$\begin{cases} x = y' \\ y = x' - \left\lfloor \frac{a}{b} \right\rfloor \cdot y' \end{cases}$$

a	b	x	y
a	b	y'	$x' - \lfloor a/b \rfloor * y'$
b	a % b	x'	y'

Let ***gcdext***(int a, int b, int &d, int &x, int &y) be a function that by input numbers a and b finds d = GCD(a, b) and such x, y that $d = a * x + b * y$. To find the unknowns x and y its necessary to run recursively the function *gcdext*(b, a mod b, d, x, y) and recalculate the values x and y according to the formula above. The recursion terminates when $b = 0$. If $b = 0$, then GCD(a, 0) = a and $a = a * 1 + 0 * 0$, therefore we set $x = 1$, $y = 0$.

Consider the third test case. The GCD(5, 3) calculation and finding the corresponding values of x and y are given in the table:

a	b	x	y	
5	3	-1	2	← 1 – 5/3 * -1
3	2	1	-1	← 0 – 3/2 * 1
2	1	0	1	
1	0	1	0	

From the table we find that GCD(5, 3) = 5 * (-1) + 3 * 2 = 1.

Find the solution to equation 5x + 7y = 1.

a	b	x	y	
5	7	3	-2	← -2 – 5/7 * 3
7	5	-2	3	← 1 – 7/5 * -2
5	2	1	-2	← 0 – 5/2 * 1
2	1	0	1	
1	0	1	0	

The answer is: GCD(5, 7) = 5 * 3 + 7 * (-2) = 1.

Function ***gcdext*** by the given *a* and *b* finds such values *x*, *y*, *d*, that *ax* + *by* = *d* using the *extended Euclidean algorithm*.

```
void gcdext(int a, int b, int &d, int &x, int &y)
{
  if (b == 0)
  {
    d = a; x = 1; y = 0;
    return;
  }
  gcdext(b, a % b, d, x, y);
  int s = y;
  y = x - (a / b) * y;
  x = s;
}
```

The main part of the program. Process multiple test cases. Read the input data.

```
while(scanf("%d %d",&a,&b) == 2)
{
```

Call the function ***gcdext*** and print the answer.

```
  gcdext(a,b,d,x,y);
  printf("%d %d %d\n",x,y,d);
}
```

E-OLYMP **563. Simple equation** Peter found in a book a simple mathematical equation: *a***x* + *b***y* = 1. His interest is only integral solutions of this equation, and only those for which *x* ≥ 0 and *x* is the smallest possible.

► Given the values of a and b, using the extended Euclidean algorithm, we find d = GCD(a, b), x_0 and y_0 such that $a*x_0 + b*y_0 = d$. Since the equation $a*x + b*y = 1$ is being solved, there is no solution for $d > 1$.

Theorem. All solutions of the Diophantine equation $a*x + b*y = 1$ are given with the formula

$$\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases},$$

where (x_0, y_0) is a partial solution of the original equation, $k \in Z$.

Substitute the pair ($x_0 + kb$, $y_0 – ka$) into the equation $a*x + b*y = 1$:

$$a*(x_0 + kb) + b*(y_0 – ka) = 1,$$
$$ax_0 + akb + by_0 – bka = 1,$$
$$ax_0 + by_0 = 1, \text{ which is true}$$

In order for x to be the smallest possible non-negative value, it is necessary that k be the smallest for which $x_0 + kb \geq 0$. Or $k \geq -x_0 / b$. The smallest integer k that satisfies the last inequality is $k = \lceil -x_0 / b \rceil$. For this value of k the solution should be found and printed.

Since the extended Euclidean algorithm finds a solution (x_0, y_0) for which the sum $|x_0| + |y_0|$ is minimal, then for $x_0 < 0$ the desired solution (with the smallest non-negative value of x) equals to

$$\begin{cases} x = x_0 + b \\ y = y_0 - a \end{cases}$$

If the inequality $x_0 \geq 0$ is satisfied in a partial solution (x_0, y_0), then it will itself be a solution to the problem.

Find the partial solution of equation $7x + 11y = 1$ with the smallest possible non-negative value of x. After running the extended Euclidean algorithm, we get a partial solution $x_0 = -3$, $y_0 = 2$. Really,

$$7x_0 + 11y_0 = 7 * (-3) + 11 * 2 = 1$$

Then $k = \lceil -x_0 / b \rceil = \lceil -(-3)/11 \rceil = 1$. The desired solution to the equation will be

$$\begin{cases} x = x_0 + kb = -3 + 1 \cdot 11 = 8 \\ y = y_0 - ka = 2 - 1 \cdot 7 = -5 \end{cases}$$

Test: 7 * 8 + 11 * (-5) = 56 – 55 = 1.

E-OLYMP **1565. Play with floor and ceil** **Theorem.** For any two integers x and k there exists two more integers p and q such that

$$x = p \left\lfloor \frac{x}{k} \right\rfloor + q \left\lceil \frac{x}{k} \right\rceil$$

It's a fairly easy task to prove this theorem, so we'd not ask you to do that. We'd ask for something even easier! Given the values of x and \, you'd only need to find integers p and q that satisfies the given equation.

► If x is divisible by k, then $\lfloor x/k \rfloor = \lceil x/k \rceil = x / k$. Choosing $p = 0$, $q = k$, we get: $0 * (x / k) + k * (x / k) = x$.

Let x is not divisible by k. If $n = \lfloor x/k \rfloor$, then $m = \lceil x/k \rceil = n + 1$. Since GCD($n$, m) = GCD(n , n + 1) = 1, then based on the extended Euclidean algorithm, there exist integers t and u such that $1 = tn + um$. Multiplying the equality by x, we get $x = xtn + xum$, wherefrom $p = xt$, $q = xu$.

In the first test case $x = 5$, $k = 2$. The value of x is not divisible by k. Compute $n = \lfloor 5/2 \rfloor = 2$, $m = \lceil 5/2 \rceil = 3$. The solution to the equation $2t + 3u = 1$ is the pair $(t, u) = (-1, 1)$. Multiply the equation by $x = 5$. The solution to the equation $2p + 3q = 5$ is the pair $(p, q) = (5t, 5u) = (-5, 5)$. The next relation holds:

$$5 = (-5) * \lfloor 5/2 \rfloor + 5 * \lceil 5/2 \rceil = (-5) * 2 + 5 * 3 = -10 + 15$$

E-OLYMP 5213. Inverse Prime number n is given. The **inverse** number to i ($1 \le i < n$) is such number j that $i * j = 1 \pmod{n}$. Its possible to prove that for each i exists only one inverse.

For all possible values of i find the inverse numbers.

► The *inverse* can be found using the ***extended Euclidean algorithm***. Let the the modulo equation should be solved: $ax = 1 \pmod{n}$. Consider the equation

$$ax + ny = 1$$

and find its partial solution (x_0, y_0) using the extended Euclidean algorithm. Taking the equation $ax_0 + ny_0 = 1$ modulo n, we get $ax_0 = 1 \pmod{n}$. If x_0 is negative, add n to it. So $x_0 = a^{-1} \pmod{n}$ is the inverse for a.