How to find $a^{-1}\ (mod\ b)$
(by Alexander Zhak, ver. 0.1 – May 05, 2006)

The method described below is only tested and correct for integers $a > 1$ and $b > 1$ so that $GCD(a,b) = 1$. In other words the greatest common divisor of these numbers are equal to 1. (I don't know if the problem can be solved for $GCD(a,b) \neq 1$. I didn't check it, but I'll do it for sure when I'll have some spare time.)

Example: a = 7, b = 31; $p = 7^{-1} \pmod{31} = ?$

First of all we should find GCD(a,b) and check if it is equal to 1.
So we should do the following:
In general:

$$b = a \cdot q_1 + r_1; \qquad (1)$$
$$a = r_1 \cdot q_2 + r_2;$$
$$r_1 = r_2 \cdot q_3 + r_3;$$
$$r_2 = r_3 \cdot q_4 + r_4;$$
$$\ldots$$
$$r_{n-2} = r_{n-1} \cdot q_n + r_n;$$
$$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}, \text{ where } r_n = 1,\ r_{n+1} = 0.$$

NOTE: Iterations (1) are known as Euclidian algorithm. Refer to http://mathworld.wolfram.com for detailed description of this algo.

Example:

$31 = 7 \cdot 4 + 3;$ $\quad (q_1 = 4)$
$7 = 3 \cdot 2 + 1;$ $\quad (q_2 = 2)$
$3 = 1 \cdot 2 + 1;$ $\quad (q_3 = 2,\ n = 3)$
$1 = 1 \cdot 1 + 0;$

Ok, now we can easily find $a^{-1} = p$ using equation (2)
In general:

$$p = (-1)^n \cdot p_n, \qquad (2)$$
where $p_n = p_{n-1} \cdot q_n + p_{n-2},$
$$p_0 = 1,$$
$$p_{-1} = 0;$$

Example: $n = 3$, then $p = p_2 \cdot q_3 + p_1$

$p_1 = 1 \cdot 4 + 0 = 4;$
$p_2 = 4 \cdot 2 + 1 = 9;$
$p_3 = 9 \cdot 2 + 4 = 22;$
$p = (-1)^3 \cdot 22 = -22\ (mod\ 31) = 9\ (mod\ 31);$

Verification: $a \cdot p\ (mod\ b) = 1$ For our example: $7 \cdot 9\ (mod\ 31) = 63\ (mod\ 31) = 1$

One more example:

Given:
a = 937;
b = 1089;
$p = a^{-1} \pmod{b} = ?$

Solution:
1. Using Euclidean algorithm we find *GCD(937, 1089)*:

*1089 = 937*1 + 152;*
*937 = 152*6 + 25;*
*152 = 25*6 + 2;*
*25 = 2*12 + 1;*
*2 = 1*2 + 0;*

GCD(937, 1089) = 1. That's good. We've got $n = 4;\ q_1 = 1;\ q_2 = 6;\ q_3 = 6;\ q_4 = 12;$

2. Now we can find $p = 1/937 \pmod{1089}$:

$p_1 = 1 \cdot 1 + 0 = 1;$ *(remember that* $p_0 = 1$ *and* $p_{-1} = 0$*)*
$p_2 = 1 \cdot 6 + 1 = 7;$
$p_3 = 7 \cdot 6 + 1 = 43;$
$p_4 = 43 \cdot 12 + 7 = 523;$

$p = (-1)^4 \cdot 523 = 523 \pmod{31};$

3. Verification: 937*523 (mod 1089) = 1;

Here are some problems for you to solve:

1) a = 139; b = 900; (Result: p = 259)
2) a = 17; b = 20; (Result: p = 13)