Finding Inverses Mod $p$

**by William Gasarch**

# 1 Introduction

Recall that if $p$ is a prime then all $a \in \{1, \ldots, p-1\}$ have a MULT INVERSE MOD $p$. That is, there is a number $b$ such that $ab \equiv 1 \pmod{p}$. How do we find it quickly?

# 2 An EXAMPLE

We first go to the (seemingly) unrelated problem of finding the GCD of two numbers.

We give an EXAMPLE of the algorithm.

Find the GCD of 101 and 32. (We know its 1 since 101 is prime, but bear with me).

Divide 101 by 32 and note the quotient and remainder:
$101 = 32 \times 3 + 5$.

Now divide 32 by 5 and note that quotient and remainder:
$32 = 5 \times 6 + 2$.

Now divide 5 by 2.
$5 = 2 \times 2 + 1$.

Now divide 2 by 1. OH-don't bother since that goes in evenly.

The last remainder encountered is 1. THATS THE GCD. But that's not that interesting. Here is what's interesting: We can use these equations to write 1 as a weighted sum of 101 and 32.

First express ALL of the questions in terms of REMAINDER equals something

$1 = 5 - 2 \times 2 = 2 \times 2$.

$2 = 32 - 5 \times 6 = 32 - 6 \times 5$.

$5 = 101 - 32 \times 3 = 101 - 3 \times 32$.

We start with the first equation and keep working up to the 101 and 32.

$1 = 5 - 2 \times 2 = (101 - 3 \times 32) - 2 \times (32 - 6 \times 5) = 101 - 5 \times 32 + 12 \times 5$

Leave the 101 and 32 alone but we can rewrite the 5.

$1 = 101 - 5 \times 32 + 12 \times (101 - 3 \times 32) = 13 \times 101 - 41 * 32$

Okay. So what? Take this equation MOD 101.

$$1 = 13 \times 101 - 41 * 32$$

$$\equiv -41 * 32 \pmod{101}.$$

AH HA- -41 is the INVERSE of 32 mod 101. Wow? -41= 101-41= 60.

# 3 General Method

Say $a, b$ are rel prime and you want to find the INVERSE of $a$ mod $b$.

$b = aq_1 + r_1$

$a = r_1q_2 + r_2$

$r_1 = r_2q_3 + r_3$

$r_2 = r_3q_4 + r_4$

KEEP doing this until you don't get a remainder. Say the last one is

$r_L = r_{L+1}q_{L+2} + 1$

Rewrite all of these in terms of $r_i = \ldots$

use these and work backwards to get 1 as a linear combo of $a, b$. Take that equation mod $b$ to find inverse.