1 Introduction

Recall that if \( m \in \mathbb{N} \) and \( a \) is rel prime to \( m \) then there exists a MULT INVERSE MOD \( m \). That is, there is a number \( b \) such that \( ab \equiv 1 \pmod{m} \). How do we find it quickly?

2 First GCDs

If \( a, b \in \mathbb{N} \) then the greatest common divisor of \( a, b \) is the greatest number that divides both \( a \) and \( b \). We abbreviat this as \( GCD \).

Thought experiment: we want to find the largest number that divides \( a \) and \( b \). Assume \( a < b \).

If \( d \) divides both \( a \) and \( b \) then \( d \) divides both \( a \) and \( b - a \). SO we seem to have reduced to a smaller problem!

But what if \( 2a < b \). Then we can do even better: if \( d \) divides \( a \) and \( b \) then \( d \) divides \( a \) and \( b - 2a \). An even smaller problem!

Why stop there? Find the largest \( q \) such that \( qa < b \) and look at \( a \) and \( a - qb \).

There is another very common name for this:

Given \( a, b \) DIVIDE \( b \) by \( a \) to get a remainder and a quotient. So you get

\[
b = qa + r \quad \text{with} \quad 0 \leq r \leq a - 1.
\]

KEY: \( GCD(a, b) = GCD(a, b - qa) = GCD(a, r) \).

We can keep doing this. Note that since \( r < a \) we will now divide \( a \) by \( r \). When does it end?

Lets do an example (NOTE- this is just for teaching. When we get to the real algorithm you would never do it this way.)

EXAMPLE ONE

What is \( GCD(37, 102) \).

\[
102 = 2 \times 37 + 28.
\]

SO \( GCD(37, 102) = GCD(37, 28) = GCD(28, 37) \)

\[
37 = 1 \times 28 + 9
\]

So \( GCD(28, 37) = GCD(28, 9) = GCD(9, 28) \).

\[
28 = 3 \times 9 + 1
\]

SO \( GCD(9, 28) = GCD(9, 1) \).

The ONLY number that divides both 9 and 1 is 1. So GCD is 1.

END OF EXAMPLE ONE

Lets do an example where the answer is NOT 1.

\( GCD(4, 10) \)

\[
10 = 2 \times 4 + 2
\]
\[ \text{GCD}(4, 10) = \text{GCD}(4, 2) = \text{GCD}(2, 4) \]
\[ 4 = 2 \times 2 + 0 \]
\[ \text{GCD}(2, 4) = \text{GCD}(2, 0). \]

The only number that divides both 2 and 0 is 2. So GCD is 2.

Here is the formal algorithm:

1. Input \((a, b)\)

2. If \(a = b\) then output \(a\). If \(a = 0\) then output \(b\). If \(a = 1\) then output 1. If none of these occur then goto the next step.

3. Divide \(b\) by \(a\) to find \(b = qa + r\) with \(0 \leq r \leq a - 1\). Call this algorithm recursively on \((r, a)\).

3 More Information

We do the GCD of 101 and 32 and find some more information in the process.

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.
\[ 5 = 2 \times 2 + 1. \]

SO the GCD is 1. 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 \text{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.
\[ 1 = 101 - 5 \times 32 + 12 \times (101 - 3 \times 32) = 13 \times 101 - 41 \times 32 \]

Okay. So what? Take this equation \text{MOD} 101.
\[ 1 = 13 \times 101 - 41 \times 32 \equiv -41 \times 32 \pmod{101}. \]

AH HA- -41 is the \text{INVERSE} of 32 \text{mod} 101. Wow? -41= 101-41= 60.
4 General Method

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

\begin{align*}
    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
\end{align*}

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

\begin{align*}
    r_L &= r_{L+1}q_{L+2} + 1
\end{align*}

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.