Applications of Number Theory

Greatest common divisor as a linear combination

Theorem

If \(a\) and \(b\) are positive integers and \(\gcd(a, b) = d\) then there are integers \(s\) and \(t\) such that \(d = s \times a + t \times b\).

We illustrate first a method of finding these multipliers \(s\) and \(t\) by reversing the calculations of the Euclidean Algorithm. Later we show a direct way of finding \(s\) and \(t\) using the Extended Euclidean Algorithm.

Example

We see by Euclidean Algorithm that \(\gcd(84, 60) = 12\):

\[
\begin{align*}
84 &- 60 \times (1) = 24 \\
60 &- 24 \times (2) = 12 \\
24 &- 12 \times (2) = 0,
\end{align*}
\]

so \(\gcd(84, 60) = \gcd(60, 24) = \gcd(24, 12) = 12\).

Rewriting these equations in reverse:

\[
\begin{align*}
12 &= 60 + 24 \times (-2) \\
24 &= 84 + 60 \times (-1)
\end{align*}
\]

Replacing 24 in the first equation yields

\[
12 = 60 + [84 + 60 \times (-1)] \times (-2) = 84 \times (-2) + 60 \times (3).
\]

Example

We see by Euclidean Algorithm that \(\gcd(216, 126) = 18\):

\[
\begin{align*}
216 &- 126 \times (1) = 90 \\
126 &- 90 \times (1) = 36 \\
90 &- 36 \times (2) = 18 \\
36 &- 18 \times (2) = 0,
\end{align*}
\]

so \(\gcd(216, 126) = \gcd(126, 90) = \gcd(90, 36) = \gcd(36, 18) = 18\).

Rewriting these equations in reverse:

\[
\begin{align*}
18 &= 90 + 36 \times (-2) \\
36 &= [126 + 90 \times (-1)] \times (-2) = 126 \times (-2) + 90 \times (3) \\
&= 126 \times (-2) + [216 + 126 \times (-1)] \times (3) = 216 \times (3) + 126 \times (-5).
\end{align*}
\]

The Extended Euclidean Algorithm can be used to find the gcd of two numbers and express it as a linear combination of those numbers. It uses auxiliary numbers 1 and 0 and two starting conditions to produce an invariant expression \(G = S \times A + T \times B\) that yields the desired result.

Example

We can show that \(\gcd(356, 252) = 4\) and that \(4 = (17)356 + (-24)252\).

In the following tableau, the first two lines express \(A\) and \(B\) as linear combinations of themselves. The calculation begins in the third line where \(Q_n = \text{floor} ( R_{(n-2)} / R_{(n-1)} ) \) and \(A = R_{(n-1)}\) and \(B = R_{(n)}\). Each of the other columns uses \(Q_n\) to find the subsequent entry, and the process is repeated for each line. Specifically, \(R_n = R_{(n-2)} - R_{(n-1)} \times Q_n\), and \(S_n = S_{(n-2)} - S_{(n-1)} \times Q_n\), and \(T_n = T_{(n-2)} - T_{(n-1)} \times Q_n\).

<table>
<thead>
<tr>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>G = S \times A + T \times B</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>356</td>
<td>1</td>
<td>0</td>
<td>356 = 1 \times A + 0 \times B</td>
</tr>
<tr>
<td>B</td>
<td>252</td>
<td>0</td>
<td>1</td>
<td>252 = 0 \times A + 1 \times B</td>
</tr>
<tr>
<td>1</td>
<td>104</td>
<td>1</td>
<td>-1</td>
<td>104 = 1 \times A + (-1) \times B</td>
</tr>
<tr>
<td>2</td>
<td>44</td>
<td>-2</td>
<td>3</td>
<td>44 = (-2) \times A + 3 \times B</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>5</td>
<td>-7</td>
<td>16 = 5 \times A + (-7) \times B</td>
</tr>
<tr>
<td>12</td>
<td>17</td>
<td>-12</td>
<td>17</td>
<td>12 = (-12) \times A + 17 \times B</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>-24</td>
<td>4</td>
<td>17 = 17 \times A + (-24) \times B</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>-63</td>
<td>89</td>
<td></td>
</tr>
</tbody>
</table>
Lemma If $a$, $b$, $c$ are positive integers such that $\gcd(a, b) = 1$ and if $a \mid bc$, then $a \mid c$.
Proof: Set $1 = sa + tb$ and multiply by $c$, getting $c = sac + tbc$.
Since $a$ divides any multiple of itself and any multiple of $bc$, $a \mid sac$ and $a \mid tbc$, so it must divide $c$.

Lemma A prime that divides a product of integers must divide at least one of the factors.

From this lemma follows the unique factorization of positive integers.

Another consequence of the lemma is the

Theorem If $m$ is a positive integer and $a$, $b$, $c$ are integers such that $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Linear Congruences $ax \equiv b \pmod{m}$
Note that we may not divide in a modular system, but we can multiply to produce one if we know the modular inverse. It is possible to find the modular inverse by repeated trials, but the Extended Euclidean Algorithm may be more efficient when the modulus is large.

To find the modular inverse of 2 (mod 7), consider that $\gcd(7, 2) = 1 = (1)7 + (-3)2$. Reducing this equation (mod 7), where 0 replaces 7, and 4 replaces (-3) produces $1 .\equiv. 0 + (4)2 \pmod{7}$. Now to solve the linear congruence $2x .\equiv. 5 \pmod{7}$ we multiply by 4, which is the modular inverse of 2: $8x .\equiv. 20 \pmod{7}$ which reduces to $x .\equiv. 6 \pmod{7}$.

To find the modular inverse of 3 (mod 13), consider that $\gcd(13, 3) = 1 = (1)13 + (-4)3$. Reducing this equation (mod 13), where 0 replaces 13, and 9 replaces (-4) produces $1 .\equiv. 0 + (9)3 \pmod{13}$. Now to solve the linear congruence $3x .\equiv. 7 \pmod{13}$ we multiply by 9, which is the modular inverse of 3: $27x .\equiv. 63 \pmod{13}$ which reduces to $x .\equiv. 11 \pmod{13}$.

To find the modular inverse of 21 (mod 26), consider that $\gcd(26, 21) = 1 = (-4)26 + (5)21$. Reducing the equation (mod 26), where 0 replaces 26, and 5 stands for itself produces $1 .\equiv. 0 + (5)21 \pmod{26}$. Now to solve the linear congruence $21x .\equiv. 3 \pmod{26}$ we multiply by 5, which is the modular inverse of 21: $105x .\equiv. 15 \pmod{26}$ which reduces to $x .\equiv. 15 \pmod{26}$.

Chinese Remainder Theorem
The earliest recorded Chinese Remainder Problem is as stated below:
"We have a number of things, but we do not know exactly how many. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?" (Quoted from Sun Tze Suan Ching).

The solution represents the smallest simultaneous solution to three linear congruences:
x .\equiv. 2 \pmod{3} and x .\equiv. 3 \pmod{5} and x .\equiv. 2 \pmod{7}.
The solution may be expressed as $x = 2 \cdot (3 \cdot 5 \cdot 2 + 3 \cdot (21 \cdot 1) + 2 \cdot (15 \cdot 1)) = 233 = 23 \pmod{105}$.

To understand the method of solution, we consider that all solutions to the congruence
x .\equiv. 2 \pmod{3} belong to the set { 2, 5, 8, 11, 14, . . . } and that all solutions to the congruence
x .\equiv. 3 \pmod{5} belong to the set { 3, 8, 13, 18, . . . } and that all solutions to the congruence
x .\equiv. 2 \pmod{7} belong to the set { 2, 9, 16, . . . }.
Inspection of these sets shows that 23 is the smallest simultaneous solution, and we see that the set of all simultaneous solutions consists of numbers that are equivalent modulo 105, the product of the respective moduli. A representative solution will be a linear combination of the respective residues, such that the factors in parentheses above are congruent to 1 or 0 depending on the modulus used to reduce the terms.

We determine each of the parenthesized factors by multiplying the product of the two other moduli by the respective modular inverse of that product. The details of the calculations are shown below:

**modulo 3**: the inverse of 5*7 = 35 is 2 because 35y = 2y .=. 1 has a solution y = 2
We see that 35•2 = 1 (mod 3) = 0 (mod 5) = 0 (mod 7)

**modulo 5**: the inverse of 3*7 = 21 is 1 because 21y = 1y .=. 1 has a solution y = 1
We see that 21•1 = 1 (mod 5) = 0 (mod 3) = 0 (mod 7)

**modulo 7**: the inverse of 3*5 = 15 is 1 because 15y = 1y .=. 1 has a solution y = 1
We see that 15•1 = 1 (mod 7) = 0 (mod 3) = 0 (mod 5)
Hence the solution may be expressed as x = 2•(35•2) + 3•(21•1) + 2•(15•1) = 233 ≡ 23 (mod 105).

**Another example**
Find the simultaneous solution to x .=. 2 (mod 4) and x .=. 3 (mod 5) and x .=. 5 (mod 7).

**modulo 4**: the inverse of 5*7 = 35 is 3 because 35y = 3y .=. 1 has a solution y = 3
We see that 35•3 = 1 (mod 4) = 0 (mod 5) = 0 (mod 7)

**modulo 5**: the inverse of 4*7 = 28 is 2 because 28y = 3y .=. 1 has a solution y = 2
We see that 28•2 = 1 (mod 5) = 0 (mod 4) = 0 (mod 7)

**modulo 7**: the inverse of 4*5 = 20 is 6 because 20y = 6y .=. 1 has a solution y = 6
We see that 20•6 = 1 (mod 7) = 0 (mod 4) = 0 (mod 5)
Hence the solution may be expressed as x = 2•(35•3) + 3•(28•2) + 2•(20•6) = 978 ≡ 138 (mod 140).

**Another example**
Find the simultaneous solution to x .=. 2 (mod 3) and x .=. 1 (mod 4) and x .=. 4 (mod 5).

**modulo 3**: the inverse of 4*5 = 20 is 2 because 20y = 2y .=. 1 has a solution y = 2
We see that 20•2 = 1 (mod 3) = 0 (mod 4) = 0 (mod 5)

**modulo 4**: the inverse of 3*5 = 15 is 3 because 15y = 3y .=. 1 has a solution y = 3
We see that 15•3 = 1 (mod 4) = 0 (mod 3) = 0 (mod 5)

**modulo 5**: the inverse of 3*4 = 12 is 3 because 12y = 2y .=. 1 has a solution y = 3
We see that 12•3 = 1 (mod 5) = 0 (mod 3) = 0 (mod 4)
Hence the solution may be expressed as x = 2•(20•2) + 1•(15•3) + 4•(12•3) = 269 ≡ 29 (mod 60).