Linear congruences

$ax \equiv b \bmod m$ the solution is all integers x satisfy the congruence

$\bar{a}a \equiv 1 \bmod m$: the inverse of a modulo m.

Computing inverse

e.g. Find an inverse of 3 modulo 7

1. $7 = 2 \times 3 + 1$
2. $-2 \times 3 + 1 \times 7 = 1$ $\bar{a}a \equiv 1$
3. -2 and 1 are Bézout coefficient of 3 and 7.
4. Hence, $-2 \cdot 3 \equiv 1 \bmod 7$ and -2 is an inverse of 3 modulo 7.
5. Also, every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7.

Using Euclidean algorithm to get the inverse.

Computing inverses

Find an inverse of 101 modulo 4620.

1. First use the Euclidean algorithm to show $\gcd(101, 4620) = 1$.
2. Second, working backwards to find Bézout coefficients.

1. $4620 = 45 \cdot 101 + 75$
2. $101 = 1 \cdot 75 + 26$
3. $75 = 2 \cdot 26 + 23$
4. $26 = 1 \cdot 23 + 3$
5. $23 = 7 \cdot 3 + 2$
6. $3 = 1 \cdot 2 + 1$
7. $2 = 2 \cdot 1$

Since the last nonzero remainder is 1, $\gcd(101, 4260) = 1$

8. $1 = 3 - 1 \cdot 2$
9. $1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
10. $1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
11. $1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
12. $1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$ to prove 75 is an inverse of 101.
    $= 26 \cdot 101 - 35 \cdot 75$
13. $1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$ express 25 in terms of 4620 and 101, prove that 1601 is an inverse of 101 modulo 4620.
    $= -35 \cdot 4620 + 1601 \cdot 101$

a. Bézout coefficients for 4620 and 101 are: -35 and 1601
b. 1601 is an inverse of 101 modulo 4620
c. Also, -35 is an inverse of 4620 modulo 101

Using inverse to solve congruence.

$ax \equiv b \mod m \iff x \equiv \bar{a}b \mod m$.

e.g. solving $3x \equiv 4 \mod 7$.

1. $\gcd(3,7)=1$ and -2 is an inverse of 3 modulo 7.
2. $-2 \cdot 3x \equiv -2 \cdot 4 \mod 7$.
   $-6x \equiv -8 \mod 7$. → $x \equiv -8 \mod 7$.
   → $x \equiv 6 \mod 7$ since $6 \equiv -8 \mod 7$.
3. varify the solution, $x \equiv 6 \mod 7$.
   $3x \equiv 3 \cdot 6 \equiv 18 \equiv 4 \mod 7$,
   all such x satisfy the congruence
4. The solution are the integers x such that $x \equiv 6 \mod 7$
   namely 6, 13, 20 ---- and $-1, -8, -15$ ----

The Chinese Remainder Theorem

Find all integers x such that $0 \le x < 15$, $x \equiv 1 \mod 3$ and $x \equiv 2 \mod 5$.

1. We apply the Chinese Remainder Theorem (as stated above).
2. Using the notations of the theorem, we have $m = 3$, $n = 5$, $a = 1$, $b = 2$. $c \equiv a \mod m$ and $c \equiv b \mod n$.
3. We need s and t such that $sm + tn = 1$, hence
4. we can choose $s = 2$ and $t = -1$. $3s + 5t = 1$
5. Then, we have

$$c \equiv a + (b - a)\, s\, m \equiv 1 + (2 - 1) \times 2 \times 3 \equiv 7 \mod 15.$$

$c \equiv 1 + (2-1) \cdot 2 \cdot 3 \equiv 2 + (1-2) \times (-1) \times 3 \equiv 7 \mod 15$

Hash function : $h(k) = k \mod m$.