WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 15(Revision)

May 23, 2024

Finding Multiplicative Inverses Using Extended Euclid's Algorithm

Definition 1

If b is a solution to the congruence $ax \equiv 1 (\bmod m)$ then b is the multiplicative inverse of a modulo m and so we say that a is invertible.

Note that a in $ax \equiv 1 (\bmod m)$ is invertible only if a and m are coprime. That is, if $\gcd(m, a) = 1$.

We can use the extended Euclid's algorithm to find inverses in modular arithmetic.

$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2[7 - 1 \cdot 5]$$
$$= \underline{5} - 2 \cdot 7 + \underline{2 \cdot 5}$$

$$= -2 \cdot 7 + 3 \cdot 5$$
$$= -2 \cdot 7 + 3[19 - 2 \cdot 7$$
$$= -2 \cdot 7 + 3 \cdot 19 - 6 \cdot 7$$

Example 1

$= -2\cdot 7 + 3\cdot 19 - 6\cdot 7$

Find $7^{-1} \bmod 19$ $\quad 1 = 3\cdot 19 - 8\cdot 7$

$-8 \bmod 19 = 11$

Solution

By Euclid's algorithm algorithm we have

$19 = 7(2) + 5$ $\qquad 19 = 2\cdot 7 + 5$

$7 = 5(1) + 2$ $\qquad 7 = 1\cdot 5 + 2$

$5 = 2(2) + 1$ $\qquad 5 = 2\cdot 2 + 1$

$2 = 1(2) + 0$

We solve for $\gcd$

$1 = 5 - 2(2) = 5 - [7 - 5(1)](2) = 5 - 7(2) + 5(2) = -7(2) + 5(3)$

$= -7(2) + [19 - 7(2)](3) = -7(2) + 19(3) - 7(6)$

$= 19(3) + 7(-8)$

That is, $1 = 19(3) + 7(-8)$.

Thus, $7^{-1} = -8 \equiv 11 \bmod 19$

Example 2

Find $11^{-1} \bmod 19$

Solution

By Euclid's algorithm we have;

$$19 = 1 \cdot 11 + 8$$

$$11 = 1 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

By the extended Euclid's algorithm we have

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (8 - 2 \cdot 3) = -1 \cdot 8 + 3 \cdot 3$$

$$= -1 \cdot 8 + 3(11 - 1 \cdot 8) = 3 \cdot 11 - 4 \cdot 8$$

$$= 3 \cdot 11 - 4(19 - 1 \cdot 11) = -4 \cdot 19 + 7 \cdot 11$$

Thus, $1 = -4 \cdot 19 + 7 \cdot 11$ and so $11^{-1} \bmod 19 = 7$

Example 3

Find $364^{-1} \bmod 765$

Solution

$$765 = 364(2) + 37$$

$$364 = 37(9) + 31$$

$$37 = 31(1) + 6$$

$$31 = 6(5) + 1$$

$$6 = 1(6) + 0$$

Now solve for $\gcd$

$$1 = 31 - 6(5) = 31 - [37 - 31(1)](5)$$

$$= -37(5) + 31(6) = -37(5) + [364 - 37(9)](6)$$

$$= 364(6) - 37(59) = 364(6) - [765 - 364(2)](59)$$

$$= 765(-59) + 364(124)$$

Hence $1 = 765(-59) + 364(124)$. Thus $364^{-1} \bmod 765 = 124$

Revision Questions 1

1. Find the following multiplicative inverses

   a) $7^{-1} \bmod 20$ ✓ b) $23^{-1} \bmod 715$

   c) $13^{-1} \bmod 715$ d) $313^{-1} \bmod 715670$

2. Use your answers in question 1 above to solve;

   a) $7x \equiv 3 \bmod 20$ b) $23a \equiv 14 \bmod 715$

   c) $10n - 9 \equiv 2 - 3n \bmod 715$

   d) $313b \equiv 1 \bmod 715670$

Solution

Solution (conti...)

Find $9^{-1} \bmod 23$

(i) Euclids

$9^{-1} \bmod 23$

$23 = 2 \cdot 9 + 5$

$9 = 1 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

gcd

$5 = 23 - 2 \cdot 9$

$4 = 9 - 1 \cdot 5$

Solution (conti...)

$$1 = 5 - 1\cdot 4 \quad [9 - 1\cdot 5]$$

$$= 5 - 1\cdot[9 - 1\cdot 5]$$

$$= 5 - 1\cdot 9 + 1\cdot 5$$

$$= 1\cdot 5 - 1\cdot 9 + 1\cdot 5$$

$$= 2\cdot 5 - 1\cdot 9$$

$$= -1\cdot 9 + 2\cdot[23 - 2\cdot 9]$$

$$= -1\cdot 9 + 2\cdot 23 - 4\cdot 9$$

Solution (conti...)

$$= -1\cdot 9 - 4\cdot 9 + 2\cdot 23$$

$$1 = -5\cdot 9 + 2\cdot 23$$

$$\equiv 5 \bmod 23$$

$$= 18 \bmod 23$$

Solution (conti...)

$$9 \times 18 \bmod 23 \equiv 1$$

$$-5$$

Solution (conti...)

(2) $7^{-1} \bmod 20$

$20 = 2\cdot 7 + 6$

$7 = 1\cdot 6 + 1$

$6 =$

$1 = 7 - 1\cdot 6$

$= 7 - 1\{20 - 2\cdot 7\}$

$= 7 - 1\cdot 20 + 2\cdot 7$

Solution (conti...)

$$\equiv 7 - 3$$

$$3 \cdot 7 - 1 \cdot 20$$

$$= 3 \bmod 20$$

Solution (conti...)

Find $384^{-1} \bmod \cancel{745}$

$384^{-1} \bmod 743$

$743 = 384 \cdot 1 + 359$

$384 = 1 \cdot 359 + 25$

$359 = 25 \cdot 14 + 9$

$25 = 9(2) + 7$

Solution (conti...)

$$9 = 7(1) + 2$$
$$7 = 2(3) + 1$$

$$1 = 7 - 2(3)$$
$$1 = 7 - [9 - 7(1)](3)$$
$$1 = 7 - 9(3) + 7(3)$$
$$1 = 7(4) - 9(3)$$
$$1 = [25 - 9(2)](4) - 9(3)$$
$$1 = 25(4) - 9(8) - 9(3)$$

Solution (conti...)

$$1 = 25(4) - 9(11)$$

$$1 = 25(4) - [359 - 25 \cdot 14](11)$$

$$1 = 25(4) - 359(11) + 25(154)$$

$$1 = 25(158) - 359(11)$$

$$1 = [384 - 359(1)](158) - 359(11)$$

$$1 = 384(158) - 359(158) - 359(11)$$

$$1 = 384(158) - 359(169)$$

Solution (conti...)

$$1 = 384(158) - [743 - 384(1)](169)$$

$$1 = 384(158) - 743(169) + 384(169)$$

$$1 = 384(327) - 743(169)$$

$$1 = 384(327) + 743(-169)$$

$$\equiv 327 \mod 743$$

Solution (conti...)

Find $13^{-1} \bmod 730$

Euclid's

$730 = 13(56) + 2.$

$13 = 2(6) + 1$

Extended

$1 = 13 - \underline{2}(6)$

$13 - [\underline{730} - 13(56)]$
$6.$

$1 = 13 - 7$

Solution (conti...)

$$1 = 13(1) - 730(6) + 13(336)$$

$$1 = 13(337) - 730(6)$$

$$x = 337$$

$$\frac{4381}{730}$$

Solution (conti...)

~~Next~~: Find $20^{-1} \bmod 87$

EA

$87 = 20(4) + 7$

$20 = 7(2) + 6$

$7 = 6(1) + 1$ gcd

Solution (conti...)

Ext. Euc

$$1 = 7 - 2(1)$$

$$= 7 - \left[20 - 7(2)\right]$$

$$= 7(1) - 20 + 7(2)$$

$$= 7(3) - 20$$

$$= \left[87 - 20(4)\right]3 - 20$$

$$= 87(3) - 20(12) - 20$$

$$= 87(3) - 20(13)$$

$$\Rightarrow 7^4$$

Solution (conti...)

Find $7^{-1} \bmod 41$

G.C.D $=1$

$41 = 5(7) + 6$

$7 = 1\cdot 6 + 1$

$6 = 41 - 5(7)$

$= 6 \cdot 7$

$1 \cdot 41$

$1 = 7 - 1\cdot 6$

$1 = 7 - 1\cdot[41 - 5(7)]$ $= 6$

$1 = 7 - 1\cdot 41 + 5\cdot 7$

Solution (conti...)

$7^{-1} \bmod 41$

$7x \equiv 3 \bmod 41$ Find $\underline{x}$

$\underline{6 \cdot 7}x \equiv 6 \cdot 3 \bmod 41$

$x \equiv \underline{\underline{18}} \bmod 41$

Solution (conti...)

Find $13^{-1} \bmod 50$ and use it to solve

$$13x \equiv 4 \bmod 50$$

$$50 = 13(3) + 11$$

$$13 = 11(1) + 2$$

$$11 = 2(5) + 1$$

Solution (conti...)

$$1 = 11 - 2(5)$$

$$1 = 11 - [13 - 11(1)]\,5$$

$$1 = 11 - 13(5) + 11(5)$$

$$1 = 11(6) - 13(5)$$

$$1 = [50 - 13(3)](6) - 13(5)$$

$$1 = 50(6) - 13(18) - 13(5)$$

$$1 = 50(6) - 13(23)$$

Solution (conti...)

$$1 = 50(6) + 13(-23)$$

$$= -23 \mod 50$$

$$= 27 \mod 50$$

$$13x \equiv 4 \mod 50$$

$$27 \cdot 13x \equiv 4 \cdot 27 \mod 50$$

$$= 108 \mod 50$$

$$= 8 \mod 50$$

Solution (conti...)

Find $7^{-1} \bmod 19$ and ~~then~~ use it to solve

$4x+2 \equiv (9-3x) \bmod 19$

Euclids

$19 = 7(2)+5$

$7 = 5(1)+2$

$5 = 2(2)+1$

Solution (conti...)

Extended

$1 = 5 - 2(2)$

$5 - [7 - 5(1)]2$

$5 - 7(2) + 5(2)$

$5(3) - 7(2)$

$[19 - 7(2)]3$

$-7(2)$

$19(3)$.

$7($

Solution (conti...)

$$19(3) - 7(6) - 7(2)$$

$$19(3) + 7(-8)$$

$$-8 \bmod 19$$

$$\underline{11}$$

Solution (conti...)

$$4x + 2 \equiv (9 - 3x) \bmod 19$$

$$4x + 3x \equiv (9 - 2) \bmod 19$$

$$7x \equiv 7 \bmod 19$$

$$7 \cdot 11\, x \equiv 11 \cdot 7 \bmod 19$$

Solution (conti...)

$$x = 77 \bmod 19$$

$$4$$

$$= 1 \bmod 19$$

Solution (conti...)

Find $11^{-1} \bmod 75$ and use it to solve for x in

$11x \equiv 13 \bmod 75$

$75 = 11(6) + 9$

$11 = 9(1) + 2$

$9 = 2(4) + 1$

$1 = 9 - 2(4)$

$1 = 9 - [11 - 9$

Solution (conti...)

$$1 = 9 - [11 - 9(1)]4$$

$$= 9 - 11(4) + 9(4)$$

$$= 9 - 11(4) + 9(4)$$

$$= 9 \times 1 + 9 \times 4 - 11 \times 4$$

$$= 9(1+4) - 11(4)$$

$$= 9(5) - 11(4)$$

$$= 5[75 - 11(6)] - 11(4).$$

Solution (conti...)

$$5(75) - 11(30) - 11(4)$$

$$5(75) - 11(34)$$

$$5(75) + 11(-34)$$

$$11^{-1} \equiv -34 \mod 75$$

$$\equiv 41 \mod 75$$

Solution (conti...)

$11x \equiv 13 \mod 75$

$11 \times 41 \equiv (13 \mod 75) \, 41.$

$\Rightarrow x \equiv 533 \mod 75$

$\frac{533}{75}$

58

Solution (conti...)

Find $11^{-1} \bmod 94$ and use it to solve

$11a \equiv 13 \bmod 94$

$11^{-1} \bmod 94$

Euclids

$94 = 11(8) + 6$ (i)

$11 = 1(6) + 5$ (ii)

$6 = 1(5) + 1$ (iii)

G.C.D = 1

$1 = 6 - 1 \cdot 5$

$5 = 11 - 1 \cdot 6$

$1 = 6 - [11 - 1 \cdot 6]$

$1 = 6 - 1 \cdot 11 + 1 \cdot 6$

$1 = 1 \cdot 6 - 1 \cdot 11 + 1 \cdot 6$

$1 = 2 \cdot 6 - 1 \cdot 11$

Solution (conti...)

$94 = 11(8) + 6$

$6 = 94 - 11 \cdot 8$

$1 = 2[94 - 11 \cdot 8] - 1 \cdot 11$

$1 = 2 \cdot 94 - 2 \cdot 11 \cdot 8 - 1 \cdot 11$

$1 = 2 \cdot 94 - 16 \cdot \underline{11} - 1 \cdot \underline{11}$

$1 = 2 \cdot 94 - 17 \cdot \underline{11}$

$= -17 \bmod 94$

$= 77$

$11a = 13 \bmod 94$

$77 \times \underline{11a} = (\underline{13} \bmod 94)\, 77$

$a = 1001 \bmod 94$

$= 61 \checkmark$