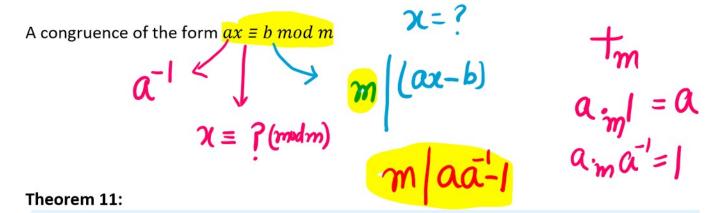
Lemma 2:

If a, b, and c are positive integers such that gcd(a, b) = 1 and $a \mid bc$, then $a \mid c$.

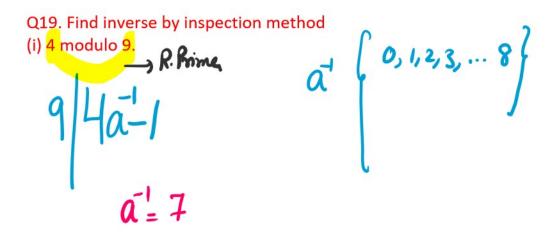
Lemma 3:

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Linear Congruences



If a and m are relatively prime integers and m > 1, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer \overline{a} less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to \overline{a} modulo m.)



Inverse of 4 modulo
$$9 = 7$$
(ii) 2 modulo 17
 $|7|(2a^{-1})$, $a = 9$

Q20. Find inverse by using Bezout coefficients

(i) 4 modulo 9

$$9=4(2)+1$$
, $1=9-4(2)$
 $4=1(4)+0$
 $1=9(1)+4(-2)$
Inverse of 4 modulo $9=-2$, $-2+9=7$

$$26 = 7(3) + 5$$

$$1 = (26 - 7(3))(3) - 7(2)$$

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

$$1 = 5 - (7 - 5(1)) (2), \quad | = 5(3) - 7(2)$$

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

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

$$1 = 26(3) - 7(11), \quad | = 26(3) + 7(-11)$$

Inverse of 7 modulo 26 = -11+26=15

(iii) 200 modulo 1001

$$|00| = 200(5) + 1$$

$$200 = 1(200) + 0$$

$$| = |001(1) + 200(-5)$$

$$| = |001(1) + 200(-5)$$

$$| = |001(1) + 200(-5)$$

$$| = |001(1) + 200(-5)$$

$$-5+100=996$$

Q21. Solve the linear congruence equation

(i)
$$3x \equiv 4 \pmod{7}$$

$$a=3, m=7, b=4$$

Inverse of 3 modulo
$$7 = 5$$

$$\frac{7}{3}a^{-1}$$

$$\frac{15}{15} \approx \frac{20}{15} \pmod{\frac{7}{15}}$$

$$|-\chi = 6 \mod 7$$
 $\chi = 6 \mod 7$

(ii)
$$19x \equiv 4 \pmod{141}$$

```
/= /7(3)~(パカピカイン
 |4|= 19 (7 ) + 8
 19 = 8(2) + 3 1 = (19 - 8(2))(3) - 8(1), 1 = 19(3) - 8(7)
8 = 3(2) + 2 1 = 3 - (8 - 3(2))(1), 1 = 3(3) - 8(1)
3 = 2(1) + 1 1 = 3 - 2(1)
                |= |9(52) - |41(7)
                1= 19(52) + 141 (-7)
Inverse of 19 modulo 141=52
Multiply 52
        988 X = 208 (mod 141)
988 = 1 mod (141) 208 = 67 (mod 141)
        X = 67 mod (141)
(iii) 55x = 34 \pmod{89}
  gcd(55,89)=1, 1/34 solm exist
      a exist
  1= 55(34)+89(-21)
  Inverse of Samodulo 89 = 34
                                  1870x = 1156 (mud 89)
  (55.34) x = (34.34) mod 89,
                                  1 x = 88 (mud 89)
```

(iv) Solve $6x \equiv 33 \mod 81$

alos com evist

(iv) Solve $6x \equiv 33 \mod 81$ $9cd (6,81) = 3, \quad 3|33 \quad \text{soln. exist}$ $22 \equiv |1 \pmod{27}$ 1 1 2 = 14 2 = 14 2 = 14 2 = 14 3 = 14

28x = 154 (mod 27)

1.2 = 19 (mod 27) Three solves

19,19†27,19+27+27 19,46,73