4.4. **15:** Show that if m is an integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m / \gcd(c, m)}$.

Proof:

$ac \equiv bc \pmod{m} \iff c(a-b) \equiv 0 \pmod{m}$ (1)

Let $d = \gcd(c, m)$; (2)

$c = d \cdot c_1$ (3) and $m = d \cdot m_1$, (4)

where $\gcd(c_1, m_1) = 1$

From (1), (3) and (4):

$d \cdot c_1 (a-b) \equiv 0 \pmod{(d \cdot m_1)} \quad | : d$

$c_1 (a-b) \equiv 0 \pmod{m_1}$

Since $\gcd(c_1, m_1) = 1$; the only way $c_1 (a-b)$ can be divisible by m_1 is if $(a-b)$ divisible by m_1 $\Rightarrow$

$a \equiv b \pmod{m_1} \overset{\text{using (4)}}{\iff}$

$a \equiv b \left(\bmod \dfrac{m}{\gcd(c,m)}\right)$ ▨

17. Show that if p is prime, the only solution of $x^2 \equiv 1 \pmod{p}$ are integers x such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Proof: $x^2 \equiv 1 \pmod{p}$

$$x^2 - 1 \equiv 0 \pmod{p}$$

$$(x-1)(x+1) \equiv 0 \pmod{p}$$

$x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

$\blacksquare$

19. This exercise outlines a proof of Fermat's little theorem.

a) Suppose that a is not divisible by the prime p. Show that no two of the integers $1 \cdot a, 2 \cdot a, \ldots, (p-1)a$ are congruent modulo p.

$[\, a^{p-1} \equiv 1 \pmod{p} \; ; \; a^p \equiv a \pmod{p} \,]$

$\forall$ int i and j, where $i < j < (p-1)$, $ia \not\equiv ja \pmod{p}$

Proof by contradiction:

Let's assume the opposite: that there exist i, j such that:

$$ia \equiv ja \pmod{p}$$

$$ia - ja \equiv 0 \pmod{p}$$

$$a(i-j) \equiv 0 \pmod{p}$$

$a \not\equiv 0 \pmod{p}$ by problem statement

or

$(i-j) \not\equiv 0 \pmod{p}$ since $i-j$ non-zero integers less than p, it cannot be divisible by p.

$\blacksquare$

b) Conclude from part (a) that the product of $1, 2, \ldots, p-1$ is congruent modulo p to the product of $a, 2a, \ldots, (p-1)a$. Use this to show that

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$$

From (a):

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (1 \cdot a)(2 \cdot a) \cdot \ldots \cdot ((p-1) \cdot a) \pmod p$$

$$(p-1)! \equiv a^{p-1} \cdot (1 \cdot 2 \cdot \ldots \cdot (p-1)) \pmod p$$

$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod p$$

c) Use Theorem 7 to show from part (b) that $a^{p-1} \equiv 1 \pmod p$ if $p \nmid a$.

By Wilson's theorem:

$$(p-1)! \equiv 1 \pmod p$$

From (b): $(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod p$

$$-1 \equiv a^{p-1}(-1) \pmod p$$

$$-(a^{p-1}) \equiv -1 \pmod p \quad | \cdot (-1)$$

$$a^{p-1} \equiv 1 \pmod p$$

d) Use part (c) to show that $a^p \equiv a \pmod p$ for all integers a.

1) If $p \nmid a$, from (c):

$$a^{p-1} \equiv 1 \pmod p \quad | \cdot a$$

$$a^p \equiv a \pmod p$$

2) If $p \mid a$, then both sides of $a^p \equiv a \pmod p$ are 0 modulo p.

25. Write out in pseudocode an algorithm for solving a simultaneous system of linear congruences based on the construction in the proof of the Chinese remainder theorem.

```
procedure chinese (m_1, m_2, ..., m_n : relatively prime positive int,
                   a_1, a_2, ..., a_n : int)
  m = 1
  for i = 1 to n:
        m = m · m_i
  x = 0
  for i = 1 to n:
      M_i = m / m_i
      y_i = M_i^(-1) mod m_i
  for i = 1 to n:
      x = x + a_i M_i y_i
  while x ≥ m :
      x = x - m
  return x  { the smallest solution to the system
            { x ≡ a_k (mod m_k) , k = 1, 2, ... n } }
```

39a) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, $5^{2003} \bmod 13$.

$5^{2003} \bmod 7$; $5^6 \equiv 1 \pmod 7$; $2003 = 333 \cdot 6 + 5$

$5^{(333 \cdot 6+5)} = (5^6)^{333} \cdot 5^5 = 1^{333} \cdot 3125 \equiv 3 \pmod 7$

$5^{2003} \bmod 11$; $5^{10} \equiv (1 \pmod{11})$; $2003 = 200 \cdot 10 + 3$

$5^{2003} = 5^{(200 \cdot 10 + 3)} = (5^{10})^{200} \cdot 5^3 = 1^{200} \cdot 125 \equiv 4 \pmod{11}$

$5^{2003} \bmod 13$; $5^{12} = 1 \pmod{13}$; $2003 = 166 \cdot 12 + 11$

$5^{2003} = 5^{166 \cdot 12 + 11} = (5^{12})^{166} \cdot 5^{11} = 1^{166} \cdot 48{,}828{,}125 \equiv$

$\equiv 8 \pmod{13}$

b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$.

$m = 1001 = 7 \cdot 11 \cdot 13$

$M_1 = m/7 = 143$; $M_2 = m/11 = 91$, $M_3 = m/13 = 77$

$\bar{a}_1 = 5$ for 143 modulo 7

$\bar{a}_2 = 4$ for 91 modulo 11

$\bar{a}_3 = 12$ for 77 modulo 13

$(3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12) \bmod 1001 = 10993 \bmod 1001 =$

$= 983$