1. $19 \equiv 1 \cdot 19 \pmod{503}$ $\qquad 19^{53} = 19^{110101_2} = 19^{32} \cdot 19^{16} \cdot 19^{4} \cdot 19$

$361 \equiv 19^2 \pmod{503}$

$44 \equiv 19^4 \pmod{503}$

$333 \equiv 19 \cdot 44 \pmod{503}$

$427 \equiv 19^8 \pmod{503}$

$243 \equiv 19^{16} \pmod{503}$

$439 \equiv 333 \cdot 243 \pmod{503}$

$198 \equiv 19^{32} \pmod{503}$

$406 \equiv 439 \cdot 198 \pmod{503}$

2. $9^2 \equiv 81 \pmod{100}$

$9^4 \equiv 81^2 = 6561 \equiv 61 \pmod{100}$

$9^8 \equiv 61^2 \equiv 3721 \equiv 21 \pmod{100}$

$9^{9^1} = 9^8 \cdot 9 \equiv 21 \cdot 9 \equiv 189 \equiv 89 \pmod{100}$

$9^{9^2} \equiv 89^2 \equiv 7921 \equiv 21 \pmod{100}$

$9^{9^4} \equiv 21^2 \equiv 441 \equiv 41 \pmod{100}$

$9^{9^8} \equiv 41^2 \equiv 1681 \equiv 81 \pmod{100}$

$9^{9^9} = 9^{9^1} \cdot 9^{9^8} \equiv 89 \cdot 81 \equiv 7209 \equiv 09 \pmod{100}$

Because 9^{9^9} is congruent to 09 mod 100 this means that its last two digits must be 0 and 9

3. a. working modulo 11 the digits form an alternating sum.

$51840 \equiv 5-1+8-4+0 \equiv 8 \pmod{11}$

$273581 \equiv 2-7+3-5+8-1 \equiv 0 \pmod{11}$

$51840 \cdot 273581 \equiv 8 \cdot 0 \equiv 0 \pmod{11}$

$\therefore 1418243x040 \equiv 0 \pmod{11}$

$1-4+1-8+2-4+3-x+0-4+0 \equiv$

$-13-x \equiv 0 \pmod{11}$

$-13-9 \equiv -22 \equiv 0 \pmod{11}$ $\qquad \therefore x = 9$

b. $[3(523+x)]^2 = 9(523+x)^2 \Leftarrow 9k$

$\therefore 9 \mid [3(523+x)]^2$

$(3(523+x))^2 \equiv 0 \pmod{9}$

$2x99561 \equiv 0 \pmod{9}$

$2+9+9+5+6+1+x \equiv 0 \pmod{9}$

$32+x \equiv 0$

$x \equiv -5 \pmod{9}$

$x \equiv 4 \pmod{9}$ $\qquad \therefore x = 4$

c. $2784x \equiv x \cdot 5569 \pmod{9}$

$2+7+8+4+x \equiv x(5+5+6+9) \pmod{9}$

$21 + x \equiv x \cdot 25 \pmod{9}$

$3+x \equiv x \cdot 7 \pmod{9}$

$3+5 \equiv 5 \cdot 7 \pmod{9}$ $\qquad \therefore x = 5$

$8 \equiv 35 \equiv 8 \pmod{9}$

4. $495 \mid 273x49y5$

$495 = 3 \cdot 3 \cdot 5 \cdot 11 = 9 \cdot 5 \cdot 11$ ← no common factors so relatively prime

Because 9, 5, and 11 are all relatively prime we can use Euclids lemma (theorem 2-5) ~~to~~ show that the number must be divided by 5, 9 and 11.

✓ – $\underline{5 \mid 273x49y5}$: we know this is true as ~~the~~ all multiples of 5 must end w/ 5 or 0 in base 10

+ $\underline{\text{lemma}}$: ending with a 0 or 5 guarantees that a number is divisible by 5.

+ any number in base 10 can be represented as a polynomial of such

$a_n \cdot 10^n + \ldots + a_0$ where a_n is a base 10 digit at index n from the right

putting this into a congruence equation showing that it's divisible by 5

$5 \mid a_n \cdot 10^n + \ldots + a_0$

$a_n \cdot 10^n + \ldots + a_0 \equiv 0 \pmod 5$

$a_n \cdot 10^n \equiv a_n \cdot 0 \pmod 5$
$\equiv 0 \pmod 5$

∴ each term where $n > 0$ must be congruent with zero mod 5 because its divisible by 10

$a_0 \equiv 0 \pmod 5$ therefore the last digit must be divisible by 5 and between 0 and 9 leaving only $\underline{0 \text{ and } 5}$ $\boxed{\times}$

– $9 \mid 273x49y5$ via theorem 4-5

$273x49y5 \equiv 2+7+3+4+9+5+x+y \equiv 30+x+y \equiv 3+x+y \equiv 0 \pmod 9$

$x+y \equiv 6 \pmod 9$

– $11 \mid 273x49y5$ via theorem 4-6

$273x49y5 \equiv 2-7+3-x+4-9+y-5 \equiv -12-x+y \equiv -1-x+y \equiv 0 \pmod{11}$

$y - x \equiv 1 \pmod{11}$

via inference

let $k=0$ $x=7$, $y=8$

$3+7+8 \equiv 18 \equiv 0 \pmod 9$ ✓

$-1-7+8 \equiv 0 \pmod{11}$ ✓

$= 3 \cdot 3 \cdot 5 \cdot 11 = 9 \cdot 5 \cdot 11$ ← no common factors so relatively prime

$ax \equiv b \pmod{n}$

7. a. $34x \equiv 8 \pmod{102}$

4.7: $\gcd(a,n) \mid b$ - must be true for slns

$\gcd(34, 102) \overset{?}{\mid} 8$

$6 \nmid 8$

There is no solution according to theorem 4-7

b. $25x \equiv 15 \pmod{29}$

$5x \equiv 3 \pmod{29}$

$\gcd(25, 29) = 1$

$1 \mid 15$ ✓ ∴ has slns.

$5x - 29y = 3$

$5(18) - 29(3) = 3$

∴ $x = 18$

$29 = 5 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$4 = 4 \cdot 1 + 0$

c. $6x \equiv 15 \pmod{21}$

$2x \equiv 5 \pmod{7}$ via theorem 4-3.

$\gcd(6, 21) = 3$

$3 \mid 15$ ✓ ∴ has slns.

$2x - 7y = 5$

$2(-1) - 7(-1) = 5$

$x = -1 \equiv 6$

8. see attached sagemath program.

9. $x \equiv a \pmod{n}$ + $x \equiv b \pmod{m}$

$x - a \equiv 0 \pmod{n}$ $x - b \equiv 0 \pmod{m}$ ∴ $d = \gcd(n, m)$ $d \mid x-a$ $d \mid x-b$