Solutions exercise set 5 MA1301

Section 9.3

1. We use the same method as in example 4.5 Page 71.

$19^{53} \pmod{503}$

$53 = 32+16+4+1$ and

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

$19^4 \equiv 44 \pmod{503}$, $19^8 \equiv 427 \pmod{503}$

$19^{16} \equiv 293 \pmod{503}$, $19^{32} \equiv 198 \pmod{503}$

So $19^{53} = 19^{32} \cdot 19^{16} \cdot 19^4 \cdot 19 \equiv 198 \cdot 293 \cdot 44 \cdot 19 \equiv 406 \pmod{503}$

$141^{47} \pmod{1537}$

$47 = 32+8+4+2+1$ and

$141 \equiv 141 \pmod{1537}$, $141^2 \equiv 1437 \equiv -100 \pmod{1537}$

$141^4 \equiv 778 \pmod{1537}$, $141^8 \equiv 1293 \equiv -294 \pmod{1537}$

$141^{16} \equiv 364 \pmod{1537}$, $141^{32} \equiv 314 \pmod{1537}$

So $141^{47} = 141^{32} \cdot 141^8 \cdot 141^4 \cdot 141^2 \cdot 141 \equiv$

$\equiv 314 \cdot (-294) \cdot (778) \cdot (-100) \cdot 141 \equiv 658 \pmod{1537}$

2 a)

$$a = \sum_{n=0}^{n} a_n 10^n \text{, where } a_0 \text{ is the units digit,}$$

and $a_0 = 0, 1, 2, \ldots, 9$

We can write this as $a^2 \equiv a_0 \pmod{10}$

We want to show that a^2 is equal to $0, 1, 4, 5, 6$ or 9 mod 10. We do this by considering the different cases, depending on the value of a_0.

case 1: $a_0 = 0$

Then $a^2 \equiv 0^2 \equiv 0 \pmod{10}$

case 2: $a_0 = 1$

Then $a^2 \equiv 1^2 \equiv 1 \pmod{10}$

case 3: $a_0 = 2$

Then $a^2 \equiv 2^2 \equiv 4 \pmod{10}$

case 4: $a_0 = 3$

Then $a^2 \equiv 3^2 \equiv 9 \pmod{10}$

case 5: $a_0 = 4$

Then $a^2 \equiv 4^2 \equiv 6 \pmod{10}$

case 6: $a_0 = 5$

Then $a^2 \equiv 5^2 \equiv 5 \pmod{10}$

The remaining cases now follows as well since $6 \equiv -4 \pmod{10}$, $7 \equiv -3 \pmod{10}$, $8 \equiv -2 \pmod{10}$

$9 \equiv -1 \pmod{10}$, and since we are squaring

so the signs does not matter.

Hence, we have shown that the units digit of a^2 must be $0, 1, 4, 5, 6$ or 9.

4. We will here use Theorems 4.5 and 4.6.

$$1765212221 = 1\cdot10^8 + 7\cdot10^7 + 6\cdot10^6 + 5\cdot10^5 + 2\cdot10^4 + 1\cdot10^3 + 2\cdot10^2 + 2\cdot10^1 + 1\cdot10^0$$

We know from Theorem 4.5 that

$9 \mid 1765212221$ IFF $9 \mid S$ where

$S = 1+2+2+1+2+5+6+7+1 = 27$, and

$9 \mid 27$ so $9 \mid 1765212221$

From Theorem 4.6 we know that

$11 \mid 1765212221$ IFF $11 \mid T$ where

$T = 1-2+2-1+2-5+6-7+1 = -3$ and

$11 \nmid -3$ so $11 \nmid 1765212221$.

We deal with 149235678 in the same way. In this case

$$S = 8+7+6+5+3+2+9+4+1 = 45$$ and

$9 \mid 45$ so $9 \mid 149235678$

and

$$T = 8-7+6-5+3-2+9-4+1 = 9$$ and

$11 \nmid 9$ so $11 \nmid 149235678$

Section 4.4

1 a) $25x \equiv 15 \pmod{29}$

We note that $\gcd(25, 29) = 1$ and $1 \mid 15$, so according Theorem 4.7 there exist 1 solution of this equation modulo 29

We find this solution by solving a Diophantine equation

Indeed, $25x \equiv 15 \pmod{29}$ $\Longleftrightarrow$

$25x - 29 \cdot y = 15$ for some $y \in \mathbb{Z}$.

$25x - 29 \cdot y = 15$ is a Diophantine equation which we can solve using the Euclidean algorithm.

$29 = 25 + 4$

$25 = 6 \cdot 4 + 1$ so $1 = 25 - 6 \cdot 4 = 25 - 6 \cdot (29 - 25) =$
$= 7 \cdot 25 - 6 \cdot 29$

So $1 = 25 \cdot 7 - 29 \cdot 6$ $\Longleftrightarrow$

$15 = 25 \cdot 105 - 29 \cdot 90$

So $x = 105$ is a solution of the original equation

and $105 \equiv 18 \pmod{29}$

Answer: $x \equiv 18 \pmod{29}$

↑ b) $5x \equiv 2 \pmod{26}$

$\gcd(5, 26) = 1$ and $1 \mid 2$

So by Theorem 4.7 we know that there exists a unique solution X modulo 26.

We could solve this as in the previous exercise, but we instead do the following:

$5X \equiv 2 \pmod{26}$ $\Longleftarrow$ ← multiply by 5.

$25X \equiv 10 \pmod{26}$ $\Longleftrightarrow$

$-X \equiv 10 \pmod{26}$ $\Longleftrightarrow$

$X \equiv -10 \pmod{26}$ $\Longleftrightarrow$

$X \equiv 16 \pmod{26}$

Answer: $X \equiv 16 \pmod{26}$.

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

$\gcd(6, 21) = 3$ and $3 \mid 15$, so according to Theorem 4.7 there exist three incongruent solutions modulo 21

Moreover if x_0 is a solution, then we get the two other solutions via the formula

$$x_0 + 7, \quad x_0 + 2 \cdot 7.$$

We solve

$$6x - 21y = 15.$$

$$21 = 3 \cdot 6 + 3$$
$$6 = 2 \cdot 3 \quad \text{and so} \quad 3 = 6 \cdot (-3) - 21 \quad \Leftrightarrow$$

$$15 = 6 \cdot (-15) - 21 \cdot 5$$

so $x_0 = -15 \equiv 6 \pmod{21}$ is a solution of the original equation. The two other solutions are

$$6 + 7 = 13, \quad 6 + 14 = 20$$

Answer: $x \equiv 6, 13, 20 \pmod{21}$

3.

$3x - 7y \equiv 11 \pmod{13}$ $\Leftrightarrow$

$3x \equiv 11 + 7y \pmod{13}$ $\Leftrightarrow$

$12x \equiv 44 + 28y \pmod{13}$ $\Leftrightarrow$

$-x \equiv 5 + 2y \pmod{13}$ $\Leftrightarrow$

$x \equiv -5 - 2y \pmod{13}$ $\Leftrightarrow$

$x \equiv 8 + 11y \pmod{13}$

So the solution set can be parametrized by $x \equiv 8 + 11t \pmod{13}$, $y \equiv t \pmod{13}$

4 a) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

We solve these by following the proof of Theorem 4.8

Let $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, $N = n_1 \cdot n_2 \cdot n_3 = 105$ and

$N_1 = n_2 \cdot n_3 = 35$

$N_2 = n_1 \cdot n_3 = 21$

$N_3 = n_1 \cdot n_2 = 15$

We then solve the linear congruences

$N_k x \equiv 1 \pmod{n_k}$, $k = 1, 2, 3$.

So we want to solve

$35x \equiv 1 \pmod 3$

$21x \equiv 1 \pmod 5$

$15x \equiv 1 \pmod 7$

since $\gcd(N_k, n_k) = 1$ all of these are solvable with a unique solution mod n_k.

$35x \equiv 1 \pmod 3 \iff$

$\leftarrow 70 = 69 + 1$

$70x \equiv 2 \pmod 3 \iff$

$x \equiv 2 \pmod 3$

$\leftarrow 21 = 20 + 1$

$21x \equiv 1 \pmod 5 \iff$

$x \equiv 1 \pmod 5$

$\leftarrow 15 = 14 + 1$

$15x \equiv 1 \pmod 7 \iff$

$x \equiv 1 \pmod 7$

The solution of the original system is then given by

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv$$

$$\equiv 52 \pmod{105}$$

4. b) $X \equiv 5 \pmod{11}$, $X \equiv 19 \pmod{29}$, $X \equiv 15 \pmod{31}$.

Let $n_1 = 11$, $n_2 = 29$, $n_3 = 31$, $N = n_1 \cdot n_2 \cdot n_3 = 9889$

and $N_1 = n_2 \cdot n_3 = 899$

$N_2 = n_1 \cdot n_3 = 341$

$N_3 = n_1 \cdot n_2 = 319$

We solve $N_k X \equiv 1 \pmod{n_k}$, $k = 1, 2, 3$.

$899X \equiv 1 \pmod{11} \iff$

$8X \equiv 1 \pmod{11} \iff$

$32X \equiv 4 \pmod{11} \iff$ ← $32 = 33 - 1$

$-X \equiv 4 \pmod{11} \iff$

$X \equiv -4 \pmod{11} \iff$

$X \equiv 7 \pmod{11}$

$$391x \equiv 1 \pmod{29}$$

$$22x \equiv 1 \pmod{29} \iff$$

$$-7x \equiv 1 \pmod{29} \iff$$

$$7x \equiv -1 \pmod{29} \iff$$

$$28x \equiv -4 \pmod{29} \iff$$

$$-x \equiv -4 \pmod{29} \iff$$

$$x \equiv 4 \pmod{29}$$

$$319x \equiv 1 \pmod{31} \iff$$

$$9x \equiv 1 \pmod{31} \iff$$

$$27x \equiv 3 \pmod{31} \iff$$

$$-4x \equiv 3 \pmod{31} \iff$$

$$4x \equiv -3 \pmod{31} \iff$$

$$32x \equiv -24 \pmod{31} \iff$$

$$x \equiv -24 \pmod{31} \iff$$

$$x \equiv 7 \pmod{31}$$

The solution of the original equation is given by

$$X \equiv 5 \cdot 899 \cdot 7 + 19 \cdot 391 \cdot 9 + 15 \cdot 319 \cdot 7 \equiv$$

$$\equiv 49499 \pmod{9889}$$

5. The system can be written as

$$x \equiv 1 \pmod 2$$
$$x \equiv 0 \pmod 3$$
$$2x \equiv 3 \pmod 5$$
$$3x \equiv 3 \pmod 7$$

From the second equation we get

$x = 3k$, for some $k \in \mathbb{Z}$.

We insert this in the first equation.

$$3k \equiv 1 \pmod 2 \iff$$

$k \equiv 1 \pmod 2$, so $k = 1 + 2j$, for some $j \in \mathbb{Z}$.

Then $x = 3(1+2j) = 3 + 6j$

we insert this in the third equation

$$2(3+6j) \equiv 3 \pmod 5 \iff$$

$$12j \equiv -3 \pmod 5 \iff$$

$$2j \equiv 2 \pmod 5 \iff$$

$j \equiv 6 \pmod 5 \iff$

$j \equiv 1 \pmod 5$, so $j = 1 + 5i$, for some $i \in \mathbb{Z}$.

Then $x = 3 + 6j = 3 + 6(1+5i) =$

$= 9 + 30i$.

Finally, we insert this in the third equation.

$3(9+30i) \equiv 3 \pmod 7 \iff$

$90i \equiv -24 \pmod 7 \iff$

$6i \equiv -3 \pmod 7 \iff$

$i \equiv 3 \pmod 7$ so $i = 3 + 7t$ for some $t \in \mathbb{Z}$.

Then $x = 9 + 30(3+7t) = 99 + 210t$.

So $x \equiv 99 \pmod{210}$ solves the system and so also the original equation.