Number theory Mixed exercise

1 $444 = 7 \times 60 + 24$

$60 = 2 \times 24 + 12$

$24 = 2 \times 12$

So $\gcd(444, 60) = 12$

2 a $721 = 4 \times 150 + 121$

$150 = 1 \times 121 + 29$

$121 = 4 \times 29 + 5$

$29 = 5 \times 5 + 4$

$5 = 1 \times 4 + 1$

So $\gcd(721, 150) = 1$, hence 150 and 721 are relatively prime

b Working backwards through the steps of the Euclidean algorithm gives:

$1 = 5 - 1(4)$

$= 5 - (29 - 5(5)) = 6(5) - 1(29)$

$= 6(121 - 4(29)) - 1(29) = 6(121) - 25(29)$

$= 6(121) - 25(150 - 121) = 31(121) - 25(150)$

$= 31(721 - 4(150)) - 25(150)$

$= 31(721) - 149(150)$

Hence $a = -149$, $b = 31$

c $150a + 721b = 1 \Rightarrow 150 \times 5a + 721 \times 5b = 5$

Hence $p = 5a = -5 \times 149 = -745$, $q = 5b = 5 \times 31 = 155$

3 a $362 = 17 \times 21 + 5$

$21 = 4 \times 5 + 1$

$5 = 5 \times 1 + 0$

So $\gcd(362, 21) = 1$, hence 362 and 21 are relatively prime

b Working backwards through the steps of the Euclidean algorithm gives:

$1 = 21 - 4(5)$

$= 21 - 4(362 - 17(21))$

$= 69(21) - 4(362)$

Hence $69 \times 21 - 4 \times 362 = 1 \Rightarrow 10 \times 69 \times 21 - 10 \times 4 \times 362 = 10$

So $x = 690$, $y = -40$

4 a $507 = 5 \times 99 + 12$

$99 = 8 \times 12 + 3$

$12 = 4 \times 3$

So $\gcd(507, 99) = 3$

4 b Working backwards through the steps of the Euclidean algorithm gives:

$3 = 99 - 8(12)$

$= 99 - 8(507 - 5(99))$

$= 41(99) - 8(507)$

Hence $41 \times 99 - 8 \times 507 = 3 \Rightarrow 8 \times 41 \times 99 - 8 \times 8 \times 507 = 24$

So $a = 8 \times 41 = 328,\ b = -8 \times 8 = -64$

5 a $0 \times 10 + 5 \times 9 + 2 \times 8 + 1 \times 7 + 7 \times 6 + 3 \times 5 + 5 \times 4 + 2 \times 3 + 5 \times 2 + 4 \times 1 = 165 \equiv 0 \pmod{11}$

b i $0 \times 10 + 1 \times 9 + 4 \times 8 + 1 \times 7 + 4 \times 6 + 3 \times 5 + 9 \times 4 + 7 \times 3 + 6 \times 2 + x \times 1 = 156 + x \equiv 2 + x \pmod{11}$,
hence $x = 9$

ii $0 \times 10 + 4 \times 9 + 6 \times 8 + 5 \times 7 + 0 \times 6 + 2 \times 5 + 6 \times 4 + 5 \times 3 + 6 \times 2 + x \times 1 = 180 + x \equiv 4 + x \pmod{11}$,
hence $x = 7$

6 By Fermat's little theorem, $23^6 \equiv 1 \pmod 7$

As $999 = 6 \times 166 + 3$

$\Rightarrow 23^{999} = 23^{6 \times 166 + 3} = (23^6)^{166} \times 23^3 \equiv 23^3 \times (1)^{166} \equiv 23^3 \pmod 7$

As $23^3 = (21+2)^3 = 21^3 + 3 \times 2 \times 21^2 + 3 \times 2^2 \times 21 + 2^3 = 7(3 \times 21^2 + 18 \times 21 + 36) + 2^3$

$\Rightarrow 23^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7$

So the remainder is 1.

7 $99 \equiv -1 \pmod{100} \Rightarrow 99^{51} \equiv (-1)^{51} \equiv -1 \pmod{100}$

$51^2 = 2601 \equiv 1 \pmod{100} \Rightarrow 51^{99} = (51^2)^{49} \times 51 \equiv 1^{49} \times 51 = 51 \pmod{100}$

Hence $99^{51} + 51^{99} \equiv -1 + 51 \equiv 50 \pmod{100}$

8 $50 \equiv 1 \pmod 7 \Rightarrow 50^{50} \equiv 1^{50} \equiv 1 \pmod 7$

9 $3^{100} = (3^2)^{50} = 9^{50}$

$9 = -1 \pmod{10} \Rightarrow 3^{100} \equiv 9^{50} \equiv (-1)^{50} \equiv 1 \pmod{10}$

So the unit digit in 3^{100} is 1.

10 $13^2 = 169 \equiv -1 \pmod{170}$

$\Rightarrow 13^{99} = 13 \times 13^{98} = 13 \times (13^2)^{49} \equiv 13 \times (-1)^{49} \equiv -13 \equiv 157 \pmod{170}$

So the remainder is 157.

11 $3 + 3 + 5 + 0 + 4 + 9 = 24$ and $3 \mid 24$, thus 335 049 is divisible by 3.

$3 - 3 + 5 - 0 + 4 - 9 = 0$, thus 335 049 is divisible by 11.

12 $N = 100a + 10b + c = (99+1)a + (9+1)b + c \equiv 3(33a + 3b) + a + b + c \equiv a + b + c \pmod 3$

So $3 \mid (a + b + c) \Leftrightarrow 3 \mid N$

13 The number is divisible by 9, so $9\,|\,6+1+a+1+1+6+b \Rightarrow 9\,|\,15+a+b$
The number is divisible by 11, so $11\,|\,6-1+a-1+1-6+b \Rightarrow 11\,|\,-1+a+b$
As $-1 \leqslant -1+a+b \leqslant 17$, the only solutions divisible by 11 are $-1+a+b=0$ and $-1+a+b=11$
If $-1+a+b=0$, then $15+a+b=16$ which is not divisible by 9.
If $-1+a+b=11$, then $15+a+b=15+12=27$ which is divisible by 9.
Hence $a+b=12$

14 As N is divisible by 4, then $8b$ is divisible by 4. This happens only if $b=0,4,8$.
As $11\,|\,N$, then $7-a+2-8+b=1-a+b$ is divisible by 11.
If $b=0, 11\,|\,1-a \Rightarrow a=1$, which gives $N=71\,280$
If $b=4, 11\,|\,5-a \Rightarrow a=5$, which gives $N=75\,284$
If $b=8, 11\,|\,9-a \Rightarrow a=9$, which gives $N=79\,288$

15 N divisible by 9 $\Rightarrow 9\,|\,a+b+c$
So as $a+b+c$ is odd, $a+b+c=9$ or $a+b+c=27$

As $100 \equiv 1 \pmod{11}$ and $10 \equiv -1 \pmod{11}$, $N=100a+10b+c \equiv a-b+c \equiv 10 \pmod{11}$
If $a+b+c=27$ then $a=b=c=9$ and so $a-b+c=9 \not\equiv 10 \pmod{11}$

So, to satisfy all conditions, $a+b+c=9$ and $a-b+c=-1 \equiv 10 \pmod{11}$
Adding $a+b+c=9$ and $a-b+c=-1$ gives $2(a+c)=8 \Rightarrow a+c=4$
Because $a+c=4$ and $a>0$, this gives $\{a,c\}=\{1,3\},\{2,2\},\{3,1\},\{4,0\}$.
Subtracting the two equations gives $2b=10 \Rightarrow b=5$
Therefore, the solutions are 153, 252, 351, 450

16 a $299 = 3\times 75+74$
$75 = 1\times 74+1$
So gcd $(299,75)=1$
Working backwards through the steps of the Euclidean algorithm gives:
$$\begin{aligned}1 &= 75-1(74)\\ &= 75-(299-3(75))\\ &= 4(75)-1(299)\end{aligned}$$
Hence $a=4,\ b=-1$

b $4\times 75 \equiv 1 \pmod{299}$ from part **a**
$75x \equiv 5 \pmod{299} \Rightarrow 4\times 75x \equiv 4\times 5 \pmod{299} \Rightarrow x \equiv 20 \pmod{299}$

17 a $741 = 12\times 60+21$
$60 = 2\times 21+18$
$21 = 1\times 18+3$
$18 = 6\times 3$
So gcd $(60,741)=3$

b gcd $(60,741)=3$ implies there are three solutions.

17 c $60x \equiv 30 \pmod{741} \Rightarrow 20x \equiv 10 \pmod{247}$

Using the Euclidean algorithm:

$247 = 12 \times 20 + 7$

$20 = 2 \times 7 + 6$

$7 = 1 \times 6 + 1$

So $\gcd(20, 247) = 1$

Working backwards:

$1 = 7 - 6 = 7 - (20 - 2(7))$

$= 3(7) - 20 = 3(247 - 12(20)) - 20$

$= 3(247) - 37(20)$

So $-37 \times 20 \equiv 1 \pmod{247}$

$20x \equiv 10 \pmod{247} \Rightarrow -37 \times 20x \equiv -37 \times 10 \pmod{247}$

$\Rightarrow x \equiv -370 \pmod{247} \Rightarrow x \equiv -370 + 2 \times 247 \equiv 124 \pmod{247}$

So solutions are 124, $124 + 247$, $124 + 2 \times 247$, i.e. $x \equiv 124, 371, 618 \pmod{741}$

18 As $\gcd(20, 14) = 2$, dividing the equation by 2 gives $7n \equiv 3 \pmod{10}$

Using the Euclidean algorithm:

$10 = 1 \times 7 + 3$

$7 = 2 \times 3 + 1$

So $\gcd(7, 10) = 1$

Working backwards:

$1 = 7 - 2(3) = 7 - 2(10 - (7))$

$= 3(7) - 2(10)$

So $3 \times 7 \equiv 1 \pmod{10}$

$7n \equiv 3 \pmod{10} \Rightarrow 3 \times 7n \equiv 3 \times 3 \pmod{10}$

$\Rightarrow n \equiv 9 \pmod{10} \Rightarrow n \equiv 9, 19 \pmod{20}$

So solutions are 9 and 19

19 Using the Euclidean algorithm:

$500 = 16 \times 31 + 4$

$31 = 7 \times 4 + 3$

$4 = 1 \times 3 + 1$

So $\gcd(31, 500) = 1$

Working backwards:

$1 = 4 - 1(3) = 4 - (31 - 7(4))$

$= 8(4) - 1(31) = 8(500 - 16(31)) - 1(31)$

$= 8(500) - 129(31)$

So $-129 \times 31 \equiv 1 \pmod{500}$

$31x \equiv 2 \pmod{500} \Rightarrow -129 \times 31x \equiv -129 \times 2 \pmod{500}$

$\Rightarrow x \equiv -258 \equiv 242 \pmod{500}$

20 a $\gcd(39, 600) = 3$, and 3 does not divide 5, hence the equation has no solutions.

20 b As $\gcd(39{,}600) = 3$, dividing the equation by 3 gives $13x \equiv 2 \pmod{200}$

Using the Euclidean algorithm:

$200 = 15 \times 13 + 5$

$13 = 2 \times 5 + 3$

$5 = 1 \times 3 + 2$

$3 = 1 \times 2 + 1$

So $\gcd(13{,}200) = 1$

Working backwards:

$1 = 3 - 2 = 2(3) - 5$

$= 2(13 - 2(5)) - 5 = 2(13) - 5(5)$

$= 2(13) - 5(200 - 15(13))$

$= 77(13) - 5(200)$

So $77 \times 13 \equiv 1 \pmod{200}$

$13x \equiv 2 \pmod{200} \Rightarrow 77 \times 13x \equiv 77 \times 2 \pmod{200}$

$\Rightarrow x \equiv 154 \pmod{200} \Rightarrow n \equiv 154, 354 \text{ or } 554 \pmod{600}$

21 a If p is prime and a is any integer then $a^p \equiv a \pmod{p}$

In the case where a is not divisible by p, then this result can be written as $a^{p-1} \equiv 1 \pmod{p}$

b By Fermat's little theorem, $7^{12} \equiv 1 \pmod{13}$

$\Rightarrow 7^{25} = 7^{24} \times 7 = (7^{12})^2 \times 7 \equiv 7 \pmod{13}$

So the least residue of 7^{25} modulo 13 is 7.

22 By Fermat's little theorem, $x^{11} \equiv x \pmod{11}$, for any integer x.

Hence $10x^{11} \equiv 3 \pmod{11} \Rightarrow x \times 10x^{11} \equiv x \times 3 \pmod{11} \Rightarrow 10x \equiv 3 \pmod{11}$

As $10 \times 10 \equiv 1 \pmod{11}$, so

$10x \equiv 3 \pmod{11} \Rightarrow 10 \times 10x \equiv 10 \times 3 \pmod{11}$

$\Rightarrow x \equiv 30 \pmod{11} \Rightarrow x \equiv 8 \pmod{11}$

23 a In total, there are $5 \times 10 \times 10 \times 10 - 1 = 4999$ positive integers less than 5000 as 0 is excluded.
There are $5 \times 9 \times 9 \times 9 - 1 = 3644$ numbers that do not include 9.
Hence there are $4999 - 3644 = 1355$ numbers that include 9 at least once.

b There are $5 \times 9 \times 9 \times 3 = 1215$ numbers that include 9 exactly once.
Hence there are $4999 - 3644 - 1215 = 140$ numbers that include 9 at least twice.

24 a All the letters are different, so there are $5! = 120$ number of ways to arrange the letters.

b i Treat the word HAT as a single letter, so there are $3! = 6$ ways to arrange the letters.

ii The number of ways will be 6 times the number of ways that the letters in HAT can be arranged, which is 3!.
Hence the answer is $6 \times 3! = 6 \times 6 = 36$.

25 There are three identical letters (E).

Thus there are $\frac{9!}{3!} = 60\,480$ number of ways of arranging the letters.

26 a There are $10! = 3\,628\,800$ possible orders.

b There are $5! \times 5! = 14\,400$ possible orders.

27 The number of ways of selecting the numbers is ${}^{50}C_5 \times {}^{12}C_2 = 2\,118\,760 \times 66 = 139\,838\,160$.

28 Let S be the set of the n different colours. Then the number of unique colour combinations available is equal to the number of subsets of S less 1 (as the empty set must be excluded).
So the artist has $2^n - 1$ unique colour combinations available.
As $2^8 = 256$ and $2^9 = 512$, the least possible number of different colours available is 9.

29 a The number of subsets of S containing 3 elements is ${}^nC_3 = \frac{n!}{(n-3)!3!}$

b If a set contains n elements, each element can be either selected for the subset or not selected.
Hence the total number of possible subsets is 2^n.

c Total number of subsets of S is a number of ways that different combinations of 0, 1, 2, 3,…n elements from the set can be made.
It is given by $\sum_{r=0}^{n} {}^nC_r = {}^nC_0 + {}^nC_1 + {}^nC_2 + \ldots + {}^nC_n = 2^n$, by part **b**.

Challenge

a By Bezout's identity, if m and n are coprime integers, there are integers x and y such that $mx + ny = 1$
Suppose p is prime, and $p \mid ab$. If a and p are not relatively prime, then $p \mid a$.
Similarly, if b and p are not relatively prime, then $p \mid b$.
Suppose a and p are relatively prime. Then $ax + py = 1$, and multiply both sides by b, which gives $bax + bpy = b$. Because $p \mid ab$, b must be divisible by p. This argument can be repeated for b.
Hence $p \mid ab \Rightarrow p \mid a$, $p \mid b$ or both.

b Assume there exist coefficients of a, n and m such that $na \equiv ma \pmod p$
Then $(n-m)a \equiv 0 \pmod p$, which means that either $a \equiv 0 \pmod p$ or $n - m \equiv 0 \pmod p$
Because p does not divide a, $n - m \equiv 0 \pmod p \Rightarrow n \equiv m \pmod p$
But since $1, 2, \ldots, p-1 < p$, none of the coefficients of a can be congruent to each other.
So all $p-1$ elements of the set are unique modulo p and they must make up the set $\{1, 2, \ldots, p-1\}$.

c Taking the product of all elements in the set in part **b**,

$$a \times 2a \times 3a \times \ldots \times (p-1)a \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) \pmod p$$

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

$\gcd(p, p-1) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p \Rightarrow a^p \equiv a \pmod p$