

- 1) The numbers in the list that are not crossed out are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47. These are the prime numbers lying between 1 and 50. The label for the crossed out numbers (which are composite) denotes the smallest prime factor. This is because, a number is crossed out for the first time only when we are in the process of taking multiples of the smallest non-trivial ($\neq 1$) factor. This factor has to be prime.

$$15 = 3^2 + 2^2 + 1^2 + 1^2, \quad 23 = 3^2 + 3^2 + 1^2 + 1^2$$

$$2) \quad 54 = 7^2 + 2^2 + 1^2 + 0^2, \quad 78 = 8^2 + 3^2 + 2^2 + 1^2$$

$$93 = 8^2 + 4^2 + 3^2 + 2^2$$

Trial and error.

(Lagrange's four squares theorem states that any natural number can be written as the sum of four squares of elements in $\mathbb{N} \cup \{0\}$.)

- 3) Let $x + y = a, xy = b$. Without loss of generality, we may assume $x \geq y$. Then as $(x - y)^2 = x^2 + y^2 - 2xy = x^2 + y^2 + 2xy - 4xy = (x + y)^2 - 4xy = a^2 - 4b$, we see that $x - y = \sqrt{a^2 - 4b}$. (We needed the assumption $x \geq y$ to conclude that $x - y = \sqrt{a^2 - 4b}$. The other option is $x - y = -\sqrt{a^2 - 4b}$.)

We also proved in class that $xy = \text{GCD}(x, y) \times \text{LCM}(x, y)$.

$$(i) \quad x + y = 60, xy = 12 \times 72 = 864. \quad \text{Thus } x - y = \sqrt{60^2 - 4 \times 864} = \sqrt{3600 - 3456} = \sqrt{144} = 12.$$

$$x + y = 60, x - y = 12$$

Thus $2x = (x + y) + (x - y) = 60 + 12 = 72 \Rightarrow x = 36 \Rightarrow y = 60 - 36 = 24$.
In conclusion, $(x, y) = (36, 24)$ or $(24, 36)$.

$$(ii) \quad x + y = 60, xy = 5 \times 175 = 875. \quad \text{Thus } x - y = \sqrt{60^2 - 4 \times 875} = \sqrt{3600 - 3500} = \sqrt{100} = 10.$$

$$x + y = 60, x - y = 10$$

Thus $2x = (x + y) + (x - y) = 60 + 10 = 70 \Rightarrow x = 35 \Rightarrow y = 60 - 35 = 25$.
In conclusion, $(x, y) = (35, 25)$ or $(25, 35)$.

$$(iii) \quad x + y = 16, xy = 1 \times 15 = 15. \quad \text{Thus } x - y = \sqrt{16^2 - 4 \times 15} = \sqrt{256 - 60} = \sqrt{196} = 14.$$

$$x + y = 16, x - y = 14$$

Thus $2x = (x + y) + (x - y) = 16 + 14 = 30 \Rightarrow x = 15 \Rightarrow y = 16 - 15 = 1$.
In conclusion, $(x, y) = (15, 1)$ or $(1, 15)$.

$$(iv) \quad x + y = 45, xy = 3 \times 168 = 504. \quad \text{Thus } x - y = \sqrt{45^2 - 4 \times 504} = \sqrt{2025 - 2016} = \sqrt{9} = 3.$$

$$x + y = 45, x - y = 3$$

Thus $2x = (x + y) + (x - y) = 45 + 3 = 48 \Rightarrow x = 24 \Rightarrow y = 45 - 24 = 21$.
In conclusion, $(x, y) = (24, 21)$ or $(21, 24)$.

- 4) The inverse of a number a modulo 13, is the number b such that ab leaves remainder 1 when divided by 13 (More accurately, the remainder classes of the numbers rather than the number themselves). One could do this by trial and error as 13 is a small number, but a more algorithmic way is by using Euclid's division algorithm.

- (i) $13 = 2 \times 6 + 1$. Thus $13 \times 1 + 2 \times (-6) = 1$. Thus the inverse of 2 is -6 which may also be written as $7 (= 13 + (-6))$.
- (ii) $13 = 3 \times 4 + 1$. Thus $13 \times 1 + 3 \times (-4) = 1$. Thus the inverse of 3 is -4 which may also be written as $9 (= 13 + (-4))$.
- (iii) $13 = 5 \times 2 + 3$,
 $5 = 3 \times 1 + 2$,
 $3 = 2 \times 1 + 1$.

Tracing our steps backwards to write 1 as a combination of 13 and 5, we get the following :

$$\begin{aligned} 1 &= 3 \times 1 + 2 \times (-1) = 3 \times 1 + (5 \times 1 + 3 \times (-1)) \times (-1) = 3 \times 2 + 5 \times (-1) \\ &= (13 + 5 \times (-2)) \times 2 + 5 \times (-1) = 13 \times 2 + 5 \times (-5) \end{aligned}$$

Thus the inverse of 5 is -5 which may also be written as $8 (= 13 + (-5))$

- (iv) $13 = 6 \times 2 + 1$. Thus $13 \times 1 + 6 \times (-2) = 1$. Thus the inverse of 6 is -2 which may also be written as $11 (= 13 + (-2))$.
- (v) $13 = 7 \times 1 + 6$,
 $7 = 6 \times 1 + 1$.

Tracing our steps backwards to write 1 as a combination of 13 and 7, we get the following :

$$1 = 7 \times 1 + 6 \times (-1) = 7 \times 1 + (13 + 7 \times (-1)) \times (-1) = 7 \times 2 + 13 \times (-1)$$

Thus the inverse of 7 is 2.

- 5) For this problem we use the following facts about modular arithmetic. All the variables take values in the set of integers.

$a \equiv b \pmod{m} \Rightarrow c \cdot a \equiv c \cdot b \pmod{m}$
$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, n \in \mathbb{N}$

- (i) The last digit of 7^{25} is equal to the remainder when it is divided by 10.
 $7^2 \equiv -1 \pmod{10} \Rightarrow (7^2)^{12} \equiv (-1)^{12} \equiv 1 \pmod{10} \Rightarrow 7^{24} \equiv 1 \pmod{10} \Rightarrow 7^{25} \equiv 7 \pmod{10}$.
Thus the last digit is 7.
- (ii) The last two digits of 2^{100} is equal to the remainder r when it is divided by 100. As $100 = 25 \times 4$, 2^{100} and r leave the same remainders when divided by 25 and 4. So we try to compute $2^{100} \pmod{25}$ and $2^{100} \pmod{4}$ instead.

Clearly 2^{100} is divisible by 4 ($2^{100} = 4 \times 2^{98}$). Thus $2^{100} \equiv 0 \pmod{4}$.

$$\begin{aligned} 2^5 (= 32) &\equiv 7 \pmod{25} \Rightarrow (2^5)^2 \equiv 7^2 (= 49) \equiv -1 \pmod{25} \\ \Rightarrow 2^{10} &\equiv -1 \pmod{25} \Rightarrow 2^{20} \equiv 1 \pmod{25} \Rightarrow (2^{20})^5 \equiv 1^5 \pmod{25} \\ \Rightarrow 2^{100} &\equiv 1 \pmod{25}. \end{aligned}$$

Thus we also have that $r \equiv 0 \pmod{4}$ and $r \equiv 1 \pmod{25}$. As $0 \leq r < 100$, from the second part, we have that r must be one of the following: 1, 26, 51, 76. Only one of the above numbers, 76, is divisible by 4 i.e. leaves remainder 0 when divided by 4. Thus $r = 76$.

- (iii) In base 9, the last two digits will be the remainder when the number is divided by $9^2 = 81$. Of course, we also have to express the remainder in base 9.

$$2^8 (= 256) \equiv 13 \pmod{81} \Rightarrow 2^{16} \equiv 169 \equiv 7 \pmod{81} \Rightarrow 2^{32} \equiv 7^2 (= 49) \equiv -2^5 (= 32) \pmod{81}$$

$$\begin{aligned} \text{Thus } 2^{64} &\equiv (-2^5)^2 \equiv 2^{10} \pmod{81} \\ \Rightarrow 2^{64} \times 2^{32} (= 2^{96}) &\equiv 2^{10} \times (-2^5) \equiv -2^{15} \pmod{81} \end{aligned}$$

Below we use our knowledge of the remainders of $2^8, 2^{16}, 2^{32}, 2^{64}$ modulo 81.

$$2^{97} (= 2 \times 2^{96}) \equiv -2^{16} \equiv -7 \pmod{81} \Rightarrow 2^{100} \equiv -7 \times 8 \equiv -56 \equiv 25 \pmod{81}.$$

Thus when 2^{100} is divided by 81, the remainder is 25. As $25 = 2 \times 9 + 7 \times 1$, we see that $(25)_{10} = (27)_9$. Thus the last two digits of 2^{100} in base 9 are 2, 7.