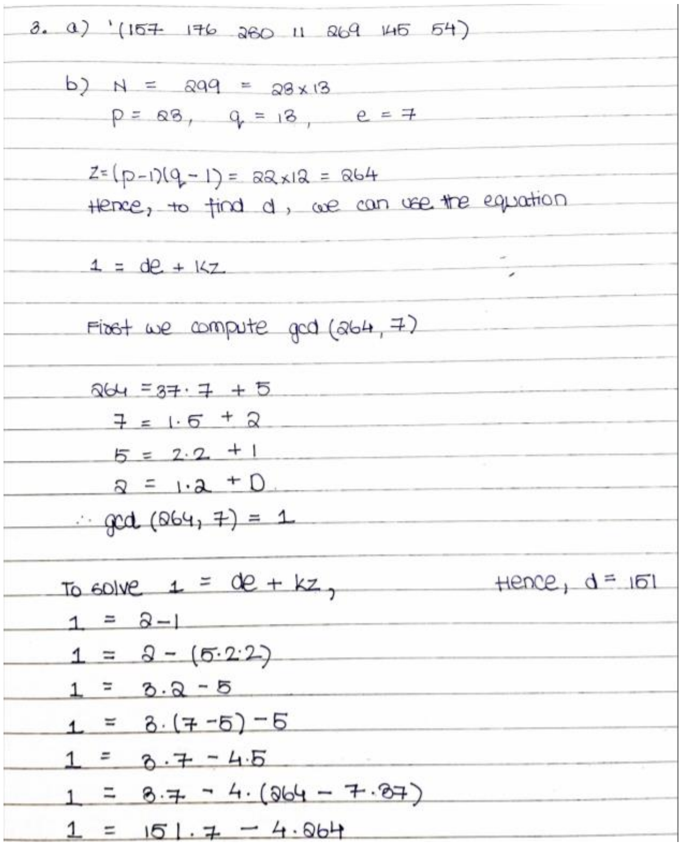
Answers

2. $b^{2n} = b^n * b^n$

   $b^{2n+1} = b^{2n} * b = b^n * b^n * b$

3. a) NetID: diveya2 is encrypted to '(157 176 280 11 269 145 54)

   b) 

   3. a) '(157 176 280 11 269 145 54)

   b) $N = 299 = 23 \times 13$

   $p = 23, \quad q = 13, \quad e = 7$

   $z = (p-1)(q-1) = 22 \times 12 = 264$

   Hence, to find d, we can use the equation

   $1 = de + kz$

   First we compute gcd (264, 7)

   $264 = 37 \cdot 7 + 5$

   $7 = 1 \cdot 5 + 2$

   $5 = 2 \cdot 2 + 1$

   $2 = 1 \cdot 2 + 0$

   $\therefore \gcd(264, 7) = 1$

   To solve $1 = de + kz$, Hence, $d = 151$

   $1 = 2 - 1$

   $1 = 2 - (5 \cdot 2 \cdot 2)$

   $1 = 3 \cdot 2 - 5$

   $1 = 3 \cdot (7 - 5) - 5$

   $1 = 3 \cdot 7 - 4 \cdot 5$

   $1 = 3 \cdot 7 - 4 \cdot (264 - 7 \cdot 37)$

   $1 = 151 \cdot 7 - 4 \cdot 264$

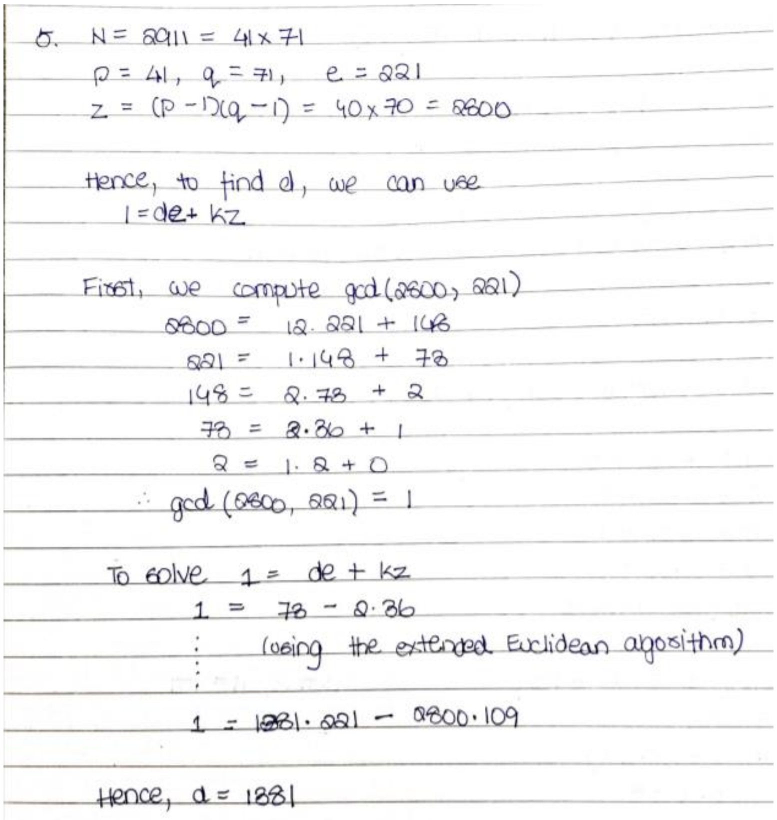
   d is found to be 151

   Decrypting '(280 220 63 220 93 220 176 244 157 176 145 43 63 145 23) gives the phrase **VORONI DIAGRAM**

4. 0 is marked as a space and not # (mistake) because when converting from groups of 2 to 3 or from groups of 3 to 2, 0 is non-trivial. If 0 is marked as a mistake, it may result in a change in the outcome when performing the reverse operation on a string/list. Marking it as a mistake helps us retrieve the original message back without any distortion.

An input list containing only zeroes in any order or grouping will always produce an output of 0, whether converting from 2 to 3 groups, or 3 to 2 groups.

5.



5. $N = 2911 = 41 \times 71$

$p = 41, \quad q = 71, \quad e = 221$

$z = (p-1)(q-1) = 40 \times 70 = 2800$

Hence, to find d, we can use

$1 = de + kz$

First, we compute gcd(2800, 221)

$2800 = 12 \cdot 221 + 148$

$221 = 1 \cdot 148 + 73$

$148 = 2 \cdot 73 + 2$

$73 = 2 \cdot 36 + 1$

$2 = 1 \cdot 2 + 0$

$\therefore \gcd(2800, 221) = 1$

To solve $1 = de + kz$

$1 = 73 - 2 \cdot 36$

$\vdots$ (using the extended Euclidean algorithm)

$1 = 1381 \cdot 221 - 2800 \cdot 109$

Hence, $d = 1381$

d is found to be 1381

Decrypting ‘(2377 1020 1652 1476 1500 2000 141 1208 2331) gives the phrase **BREAD PUDDING**