Q1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | L | M | N | P | Q | R | S | T | U | V | W | X | Z |
| Y | S | U | P | O | W | C | E | G | K | V | B | L | M | T | R | I | N | A | X | F | D | H |

CipherText:

BEETWSTSBZHXSQEWWFZUQUGCRSECBWHHNSTIBUSXUNSGHSPCBQMHBZCQQSTICDNSJHUQHNHBGEDHUTXBESQFUBSTXHHXBZHFUBTEFETNAQHTSTGZHBZSIZUTXZHRWUGHMRSIZQHTHXCDUQQZHQZECIZQQZUQBZHFUBTEFQZHRSIZQBSVHWERIESTIQZRECIZQZHNSQQNHXEERSTQEQZUQNELHNAIURXHTWSRBQZEFHLHRBZHFUSQHXWERUWHFPSTCQHBQEBHHSWBZHFUBIESTIQEBZRSTJUTAWCRQZHRBZHWHNQUNSQQNHTHRLECBUMECQQZSBWERSQPSIZQHTXAECJTEFBUSXUNSGHQEZHRBHNWSTPAIESTIECQUNQEIHQZHRNSJHUGUTXNHSFETXHRFZUQSBZECNXMHNSJHQZHTUTXBZHQRSHXQEWUTGAFZUQQZHWNUPHEWUGUTXNHSBNSJHUWQHRQZHGUTXNHSBMNEFTECQWERBZHGECNXTEQRHPHPMHRHLHRZULSTIBHHTBCGZUQZSTIUWQHRUFZSNHWSTXSTIQZUQTEQZSTIPERHZUDDHTHXBZHXHGSXHXETIESTISTQEQZHIURXHTUQETGHMCQUNUBWERDEERUNSGHFZHTBZHIEQQ

SOON FINISH EDIT OFF WHAT ACURIOUS FEELING SAID ALICE I MUST BE SHUTTING UP LIKE A TELESCOPE AND SO IT WAS IN DEED SHE WAS NOW ONLY TEN INCHES HIGH AND HER FACE BRIGHT ENEDUPAT THE THOUGHT THAT SHE WAS NOW THE RIGHT SIXE FOR GOING THROUGH THE LITTLE DOOR INTO THAT LOVELY GARDEN FIRST HOWEVER SHE WAITED FOR A FEW MINUTES TO SEE IF SHE WAS GOING TO SHRINK ANY FURT HER SHE FELT A LITTLE NERVOUS ABOUT THIS FOR IT MIGHT END YOU KNOW SAID ALICE TO HERSELF IN MY GOING OUT AL TOGETHER LIKE A CANDLE I WONDER WHAT IS HOULD BE LIKE THEN AND SHE TRIED TO FANCY WHAT THE FLAME OF A CANDLE IS LIKE AFTER THE CANDLE IS BLOWN OUT FOR SHE COULD NOT REMEMBER EVER HAVING SEEN SUCH A THING AFTER A WHILE FINDING THAT NOTHING MORE HAPPENED SHE DECIDED ONGOING INTO THE GARDEN AT ONCE BUT ALAS FOR POOR ALICE WHEN SHE GOTT

metin, beyaz, döşenmiş içeren bir resim

Açıklama otomatik olarak oluşturuldutablo içeren bir resim

Açıklama otomatik olarak oluşturuldu

First of all, I drew the letter density chart. I assigned the letter E to H and the letter T to Q, which is the first thing that comes to mind. Then I thought I should match the letters S, E, Z, T, U, B with the letters A, O, I, N, S, H.

tablo içeren bir resim

Açıklama otomatik olarak oluşturuldutablo içeren bir resim

Açıklama otomatik olarak oluşturuldu

Then I looked at the two-letter density of the text and started to match according to the intensities. Based on the two letters I matched, I thought that QZ could be TH, in this case I could match the letter Z with the letter H. After this match, it was logical that ZH was HE. Looking at the first end of the two graphs, I tried to find meaningful words by matching ST with IN. And then I tried to capture words from the text and things went like this:



 U=A B=S E=O I=G R=R

 C=U X=D G=C W=F

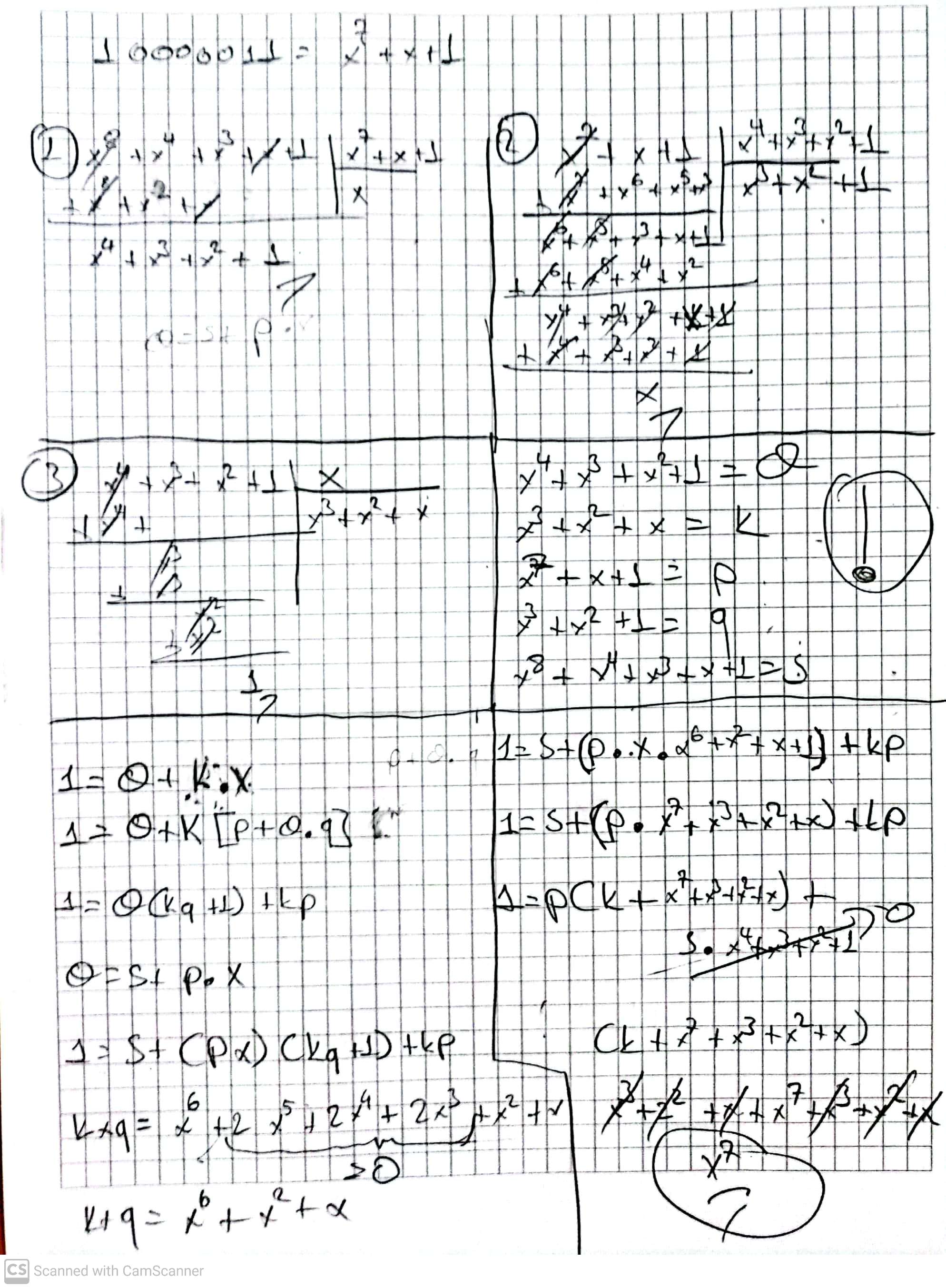
N=L D=P F=W L=V



P=M, M=B J=K A=Y

Q2

1. 70209008 (mod 2) = 10001000
2. Row number:11 = 00001011
3. XOR 10001000 (XOR) 00001011 = 10000011

d,e)

Q3)

a)

P=127 2\*\*7 = 126 (because 127 is prime)

A = 126/2=63

B = 126/3=42

C = 126/7=18

metin içeren bir resim

Açıklama otomatik olarak oluşturulduOutput is =

3, 6, 7, 12, 14, 23, 29, 39, 43, 45, 46, 48, 53, 55, 56, 57, 58, 65, 67, 78, 83, 85, 86, 91, 92, 93, 96, 97, 101, 106, 109, 110, 112, 114, 116, 118

127 has 36 primitive roots.

b)

127=5\*25+2 1=5-2\*2

5=2\*2+1 1=5-2(127-5\*25)

2=1\*2+0 1=(5\*51)-(2\*127) 5\*51=0

Q4)

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

1049~1048=

A = 1048/2 = 524

B = 1048/131 = 8

1049 has 520 primitive roots

3, 6, 7, 12, 14, 15, 17, 23, 24, 27, 28, 30, 31, 33, 34, 35, 37, 39, 41, 46, 47, 48, 54, 56, 57, 60, 62, 63, 66, 67, 68, 70, 71, 74, 75, 77, 78, 82, 83, 85, 87, 89, 91, 92, 94, 96, 101, 108, 109, 112, 114, 115, 120, 124, 126, 127, 129, 132, 133, 134, 135, 136, 137, 139, 140, 142, 147, 148, 150, 151, 153, 154, 155, 156, 157, 159, 164, 165, 166, 170, 173, 174, 175, 177, 178, 179, 182, 183, 184, 185, 187, 188, 191, 192, 195, 199, 202, 203, 205, 207, 211, 216, 218, 219, 221, 224, 228, 229, 230, 235, 237, 240, 241, 243, 248, 252, 253, 254, 258, 263, 264, 266, 268, 269, 270, 271, 272, 274, 278, 279, 280, 281, 283, 284, 285, 291, 294, 296, 297, 299, 300, 301, 302, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 317, 318, 321, 323, 328, 330, 332, 333, 335, 337, 339, 340, 341, 343, 346, 347, 348, 349, 350, 351, 353, 354, 355, 356, 357, 358, 363, 364, 366, 367, 368, 369, 370, 371, 374, 375, 376, 379, 382, 383, 384, 385, 389, 390, 393, 398, 403, 404, 406, 407, 410, 413, 414, 415, 419, 421, 422, 423, 425, 427, 429, 431, 432, 433, 435, 436, 437, 438, 442, 445, 446, 447, 448, 449, 451, 455, 456, 457, 458, 460, 467, 470, 474, 479, 480, 481, 482, 483, 486, 487, 489, 491, 493, 496, 501, 504, 505, 506, 507, 508, 509, 511, 513, 516, 517, 521, 523, 526, 528, 532, 533, 536, 538, 540, 541, 542, 543, 544, 545, 548, 553, 556, 558, 560, 562, 563, 566, 567, 568, 569, 570, 575, 579, 582, 589, 591, 592, 593, 594, 598, 600, 601, 602, 603, 604, 607, 611, 612, 613, 614, 616, 617, 618, 620, 622, 624, 626, 627, 628, 630, 634, 635, 636, 639, 642, 643, 645, 646, 651, 656, 659, 660, 664, 665, 666, 667, 670, 673, 674, 675, 678, 679, 680, 681, 682, 683, 685, 686, 691, 692, 693, 694, 695, 696, 698, 699, 700, 701, 702, 703, 706, 708, 709, 710, 712, 714, 716, 717, 719, 721, 726, 728, 731, 732, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 747, 748, 749, 750, 752, 753, 755, 758, 764, 765, 766, 768, 769, 770, 771, 775, 777, 778, 779, 780, 781, 783, 785, 786, 791, 795, 796, 797, 801, 806, 808, 809, 812, 814, 819, 820, 821, 825, 828, 830, 831, 833, 838, 842, 844, 846, 847, 850, 854, 857, 858, 861, 862, 864, 865, 866, 867, 870, 871, 872, 874, 875, 876, 879, 883, 884, 885, 890, 892, 893, 894, 895, 896, 898, 899, 901, 902, 907, 909, 910, 912, 913, 914, 915, 916, 917, 920, 922, 923, 925, 929, 934, 935, 937, 940, 941, 948, 953, 955, 957, 958, 960, 962, 964, 966, 967, 971, 972, 974, 975, 978, 979, 981, 982, 983, 986, 987, 989, 992, 993, 995, 1001, 1002, 1003, 1008, 1010, 1012, 1014, 1015, 1016, 1018, 1019, 1021, 1022, 1025, 1026, 1032, 1034, 1035, 1037, 1042, 1043,1046.

Assume g=5 A = (mod 1049) = 994

p=1049 B = (mod 1049) = 927

a=32 keyA =  (mod 1049) = 402

b=64 keyB =  (mod 1049) = 402

key=402

a=7 p=1049

The sequence of numbers are,

7, 14, 21, 28, 35, 42, 49, 56, …, a\*1048

Reduce mod 1049, then the sequence of numbers are,

7, 14, 21, 28, 35, 42, 49, 56, …, 1042, 7, 14, 21, 18, 35, 42, 49, 56, ….

From the theorem,

7\*14\*21\*28\*35\*42\*…\*a\*1048 ≡ 7\*14\*21\*28\*35\*42\*49\*56\*…\*1042 (mod 1049)

(mod 1049) ≡ 1

Hence the Fermat's Little Theorem is proved.