**2020380029**

HOME WORK

4.3,4.4,4.5,4.6

**RAIHAN MD RAKIBUL ISLAM**

* **4.3**

16. Determine whether the integers in each of these sets are pair wise relatively prime.

a) 21, 34, 55

21,34, 55

Let us determine the prime factorization of each integer:

21 = 3 \*7

34 = 2\*17

55 = 5\*11

Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.

ged(21, 34) = 1

god(21, 55) = 1

ged(34, 55) =1

The integers are then pair wise relatively prime, because all greatest common divisors are equal to 1

b) 14, 17, 85

14, 17, 85

Let us determine the prime factorization of each integer:

14 = 2\*7

17 = 17

85 = 5\*17

Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.

gcd(14, 17) = 1

gcd(14, 85) = 1

ged(17,85) = 17

The integers are then not pair wise relatively prime, because there exists a pair of integers that has a greatest common divisor different from 1.

c) 25, 41, 49, 64

25, 41, 49, 64

Let us determine the prime factorization of each integer:

25 =

41 = 41

49 =

64 =

Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.

ged(25, 41) = 1

ged(25, 49) = 1

ged(25, 64) = 1

gcd(41, 49) = 1

gcd(41, 64) = 1

ged(49, 64) = 1

The integers are then pair wise relatively prime, because all greatest common divisors are equal to 1.

d) 17, 18, 19, 23

17, 18, 19, 23

Let us determine the prime factorization of each integer:

17 = 17

18 = 2\*

19 = 19

23 = 23

Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.

ged(17, 18) = 1

ged(17, 19) = 1

ged(17, 23) = 1

ged(18, 19) = 1

ged(18, 23) = 1

ged(19, 23) = 1

The integers are then pair wise relatively prime, because all greatest common divisors are equal to 1.

24. What are the greatest common divisors of these pairs of integers?

a) · ·, · ·

a = · ·,

b = · ·

The prime factorizations of the numbers have been given. The prime factorization of the greatest common divisor then contains all common primes in the prime factorizations of a and b, where its power is the minimum of the powers of the prime in the prime factorization of a and b.

ged(a, b) = \* \*

= \* \*

= 2700

c) 17,

a = 17

b =

The prime factorizations of the numbers have been given. The prime factorization of the greatest common divisor then contains all common primes in the prime factorizations of a and b, where its power is the minimum of the powers of the prime in the prime factorization of a and b.

ged(a, b) =

= 17

f) 2 · 3 · 5 · 7, 2 · 3 · 5 · 7

a = 2 · 3 · 5 · 7

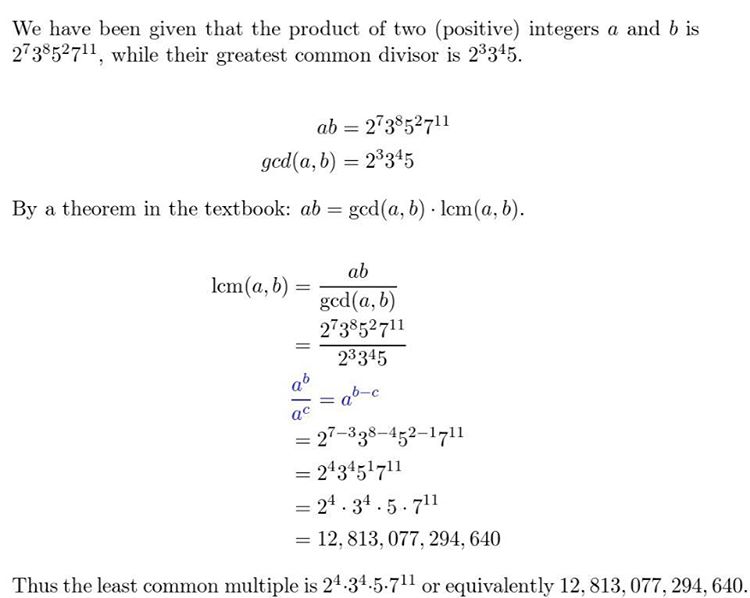
b = 2 · 3 · 5 · 7

The prime factorizations of the numbers have been given. The prime factorization of the greatest common divisor then contains all common primes in the prime factorizations of a and b, where its power is the minimum of the powers of the prime in the prime factorization of a and b.

ged(a, b)= 2 · 3 · 5 · 7

=210

30. If the product of two integers is and their greatest common divisor is 5, what is their least common multiple?



* **4.4**

12. Solve each of these congruencies using the modular inverses found in parts (b), (c), and (d) of Exercise 6.

a) 34x ≡ 77 (mod 89)

**52**

b) 144x ≡ 4 (mod 233)

**123**

c) 200x ≡ 13 (mod 1001)

**936**

19. This exercise outlines a proof of Fermat’s little theorem.

a) Suppose that a is not divisible by the prime p. Show that no two of the integers 1 · a, 2 · a, . . . , (p − 1) a are congruent modulo p.

Suppose that ia ≡ ja (mod p), where 1 ≤ i<j<p. Then p divides j a − ia = a(j − i).

By Theorem 1, because a is not divisible by p, p divides j − i, which is impossible because j − i is a positive integer less than p.

b) Conclude from part (a) that the product of 1, 2,..., p − 1 is congruent modulo p to the product of a, 2a, . . . , (p − 1)a. Use this to show that (p − 1)! ≡ (p − 1)! (mod p).

By part (a), because no two of a, 2a, . . . , (p − 1)a are congruent modulo p, each must be congruent to a different number from 1 to p−1. It follows that a · 2a · 3a ·····(p −1)· a ≡ 1 · 2 · 3 ·····(p −1) (mod p). It follows that(p−1)!·ap−1 ≡ p−1 (mod p).

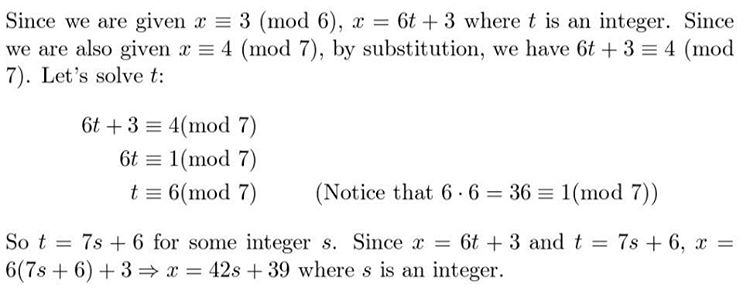
c) Use Theorem 7 of Section 4.3 to show from part (b) that ≡ 1 (mod p) if p | a. [Hint: Use Lemma 3 of Section 4.3 to show that p does not divide (p − 1)! and then use Theorem 7 of Section 4.3. Alternatively, use Wilson’s theorem from Exercise 18(b).]

By Wilson’s theorem and part (b), if p does not divide a, it follows that (−1)· ap−1 ≡ −1 (mod p). Hence, ≡ 1 (mod p).

d) Use part (c) to show that ap ≡ a (mod p) for all integers a.

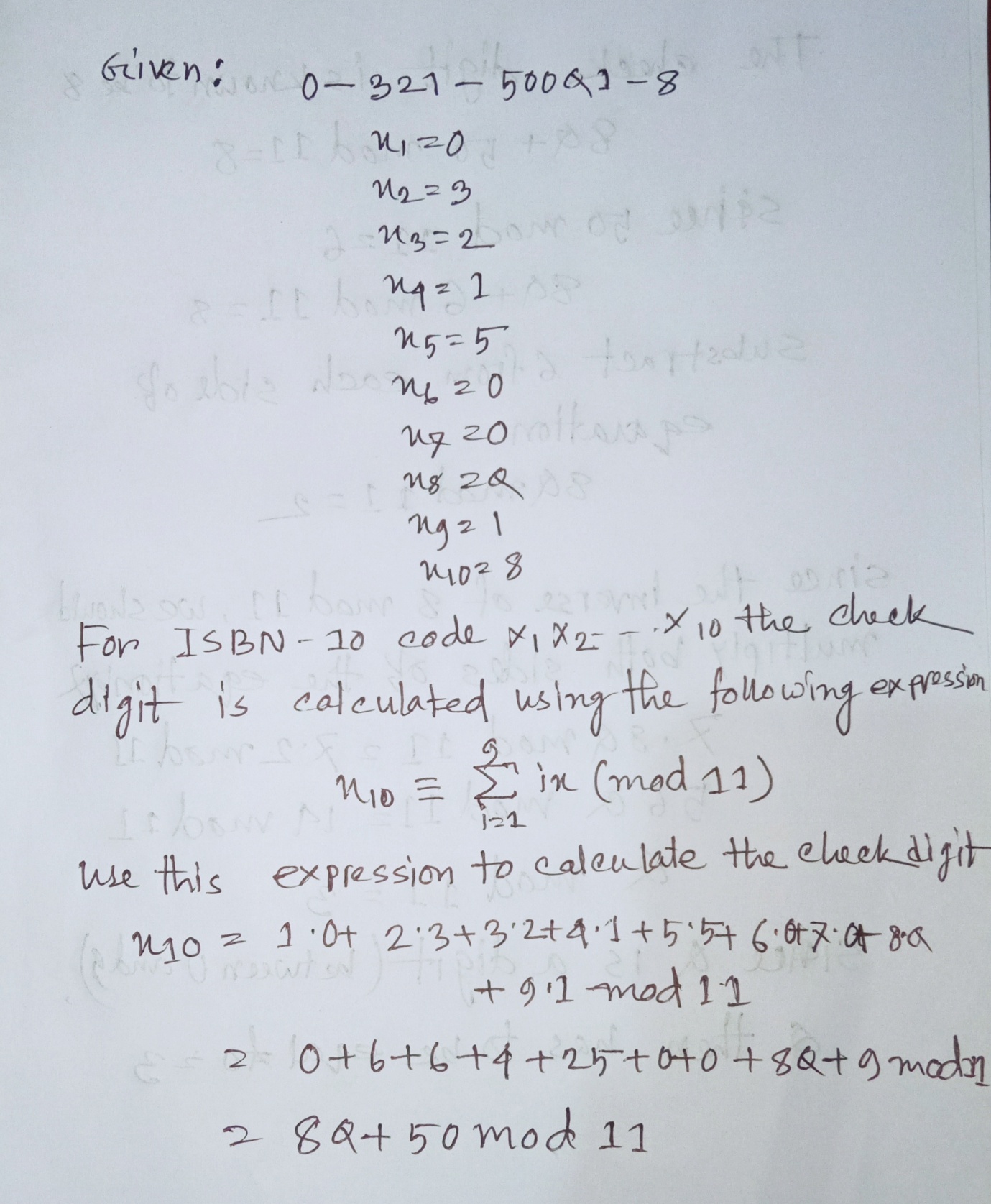
If p | a, then p | ap. Hence, ap ≡ a ≡ 0 (mod p). If p does not divide a, then≡ a (mod p), by part (c). Multiplying both sides of this congruence by a gives ap ≡ a (mod p).

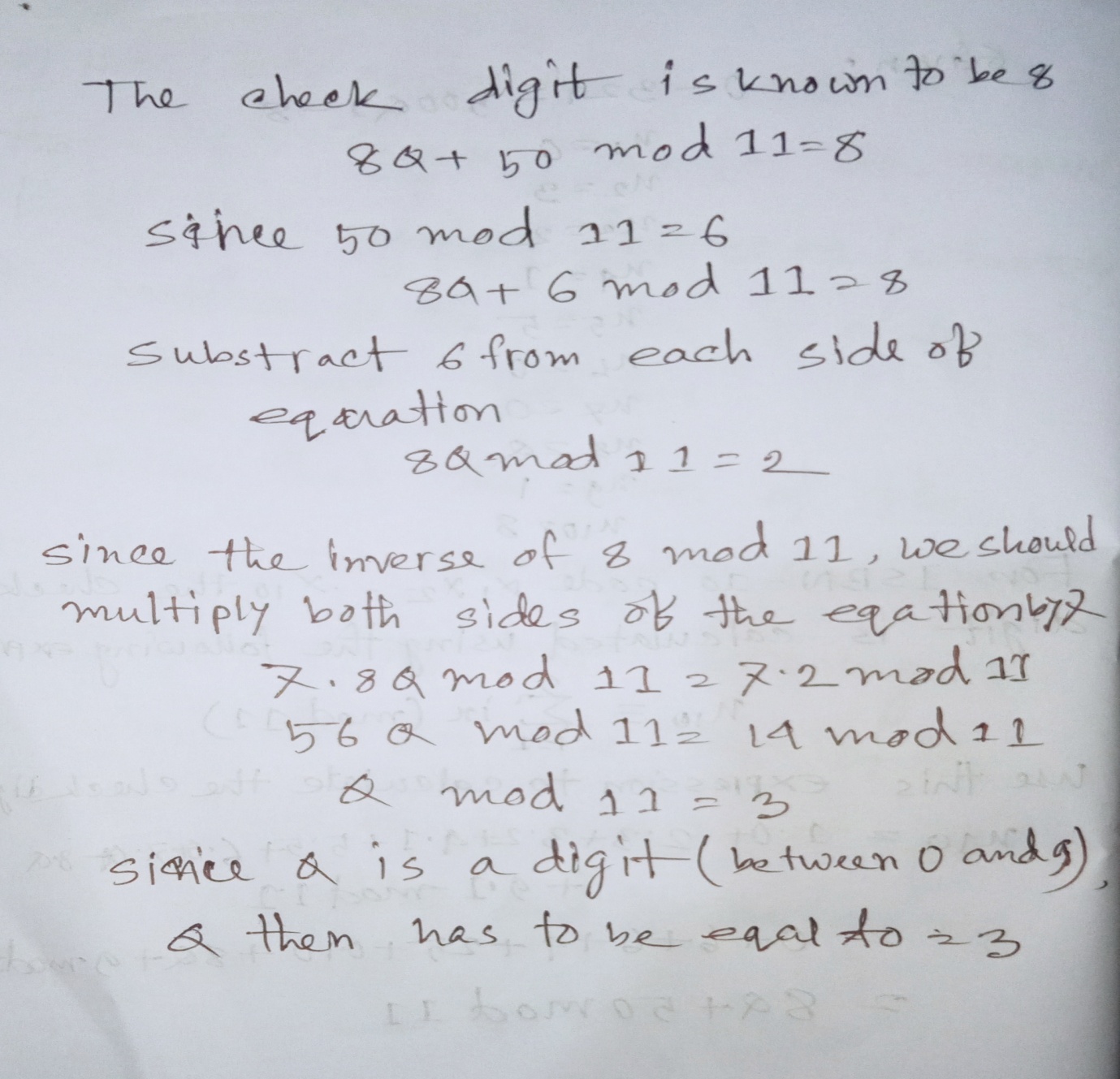
22. Solve the system of congruence x ≡ 3 (mod 6) and x ≡ 4 (mod 7) using the method of back substitution.



* **4.5**

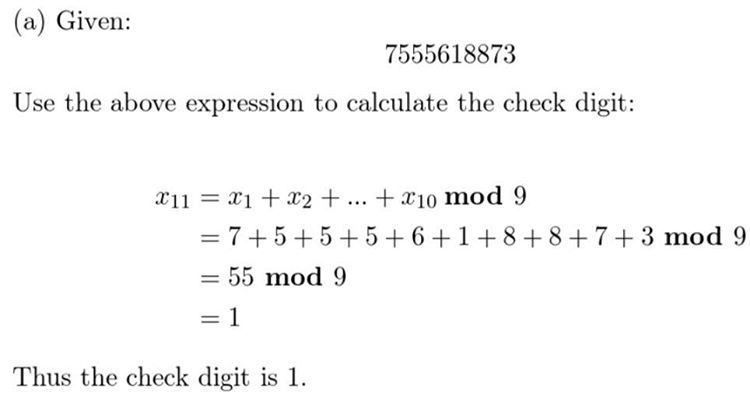
16. The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.



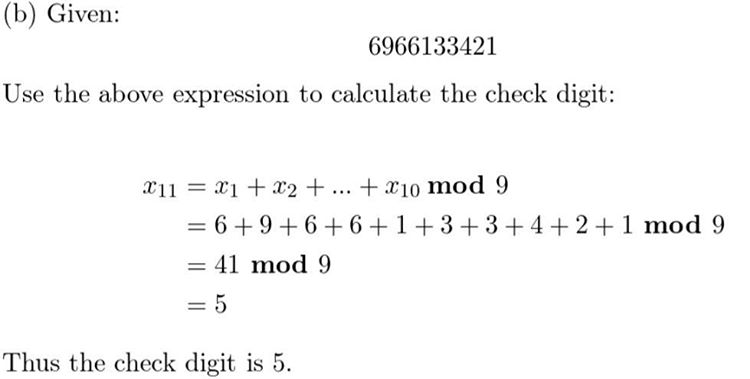


18. Find the check digit for the USPS money orders that have identification number that start with these ten digits.

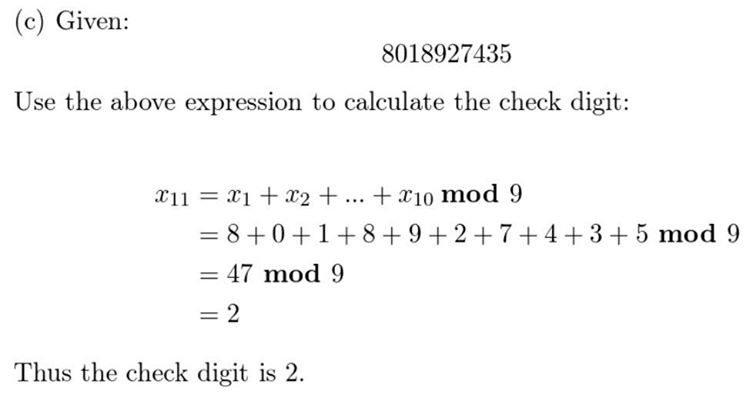
a) 7555618873



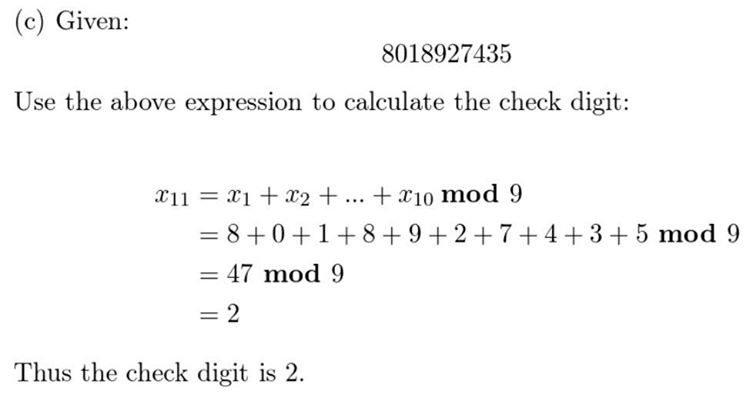
b) 6966133421



c) 8018927435



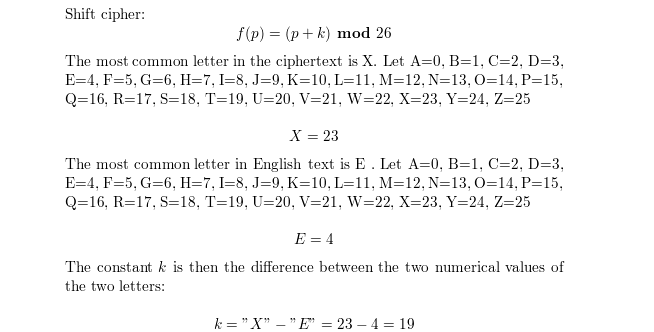
d) 3289744134



* **4.6**

6. Suppose that when a long string of text is encrypted using a shift cipher f (p) = (p + k) mod 26, the most common letter in the cipher text is X. What is the most likely value for k assuming that the distribution of letters in the text is typical of English text?

K= 19



8. Suppose that the cipher text DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

MEN LOVE TO WONDER AND THAT IS THE SEED OF SCIENCE

In Exercises 24first express your answers without computing modular exponentiations. Then use a computational aid to complete these computations.

24. Encrypt the message ATTACK using the RSA system with n = 43 · 59 and e = 13, translating each letter into integers and grouping together pairs of integers, as done in Example 8.

Given text: ATTACK

n= 43 \* 59 = 2537

e = 13 Let A=00, B-01, C=02, D=03, E=04, F=05. G=06, H=07, I-08, J=09, K=10, L=11, M=12, N=13, O=14, P-15, Q=16, R=17, S=18, T=19, U=20. V=21, W=22, X-23, Y=24, Z=25

00 19 19 00 02 10

We then group the numbers in blocks of four digits (since 2525 i 2537 i 252525).

0019 1900 0210

Encrypt each block using the mapping C = mod 2537

= mod 2537 = 2299

= mod 2537 = 1317

= mod 2537 = 2117

The encryption is then: 2299 1317 2117

* **5.1**

6. Prove that 1 · 1! + 2 · 2!+···+ n · n! = (n + 1)! − 1 whenever n is a positive integer.

To proof: 1.1!+2.2! + .. +n- n! = (n+1)!- 1 for every positive integer n.

PROOF BY INDUCTION

Let P(n) be 1 - 1!+2. 2! + . +n. n! = (n + 1)! - 1

Basis step n = 1

1\*1!+2\* 2!+... +n \* n! = 1 \* 1! = 1\*1= 1

(n + 1)! - 1 = (1+1)! - 1 = 2! -1 = 2-1 = 1

We then note P(1) is true. Induction step Let P(k) be true.

1\* 1! +2\* 2! +... +k\* k! = (k + 1)! – 1

We need to prove that P(k + 1) is also true.

1\*1!+2\*2!+.. + k\* k! + (k + 1) \*(k+1)!

= (k +1)! \* 1+ (k + 1) \*(k +1)!

=1\* (k + 1)! + (k +1) \* (k+1)! - 1

= (1+k + 1)(k+ 1)! – 1

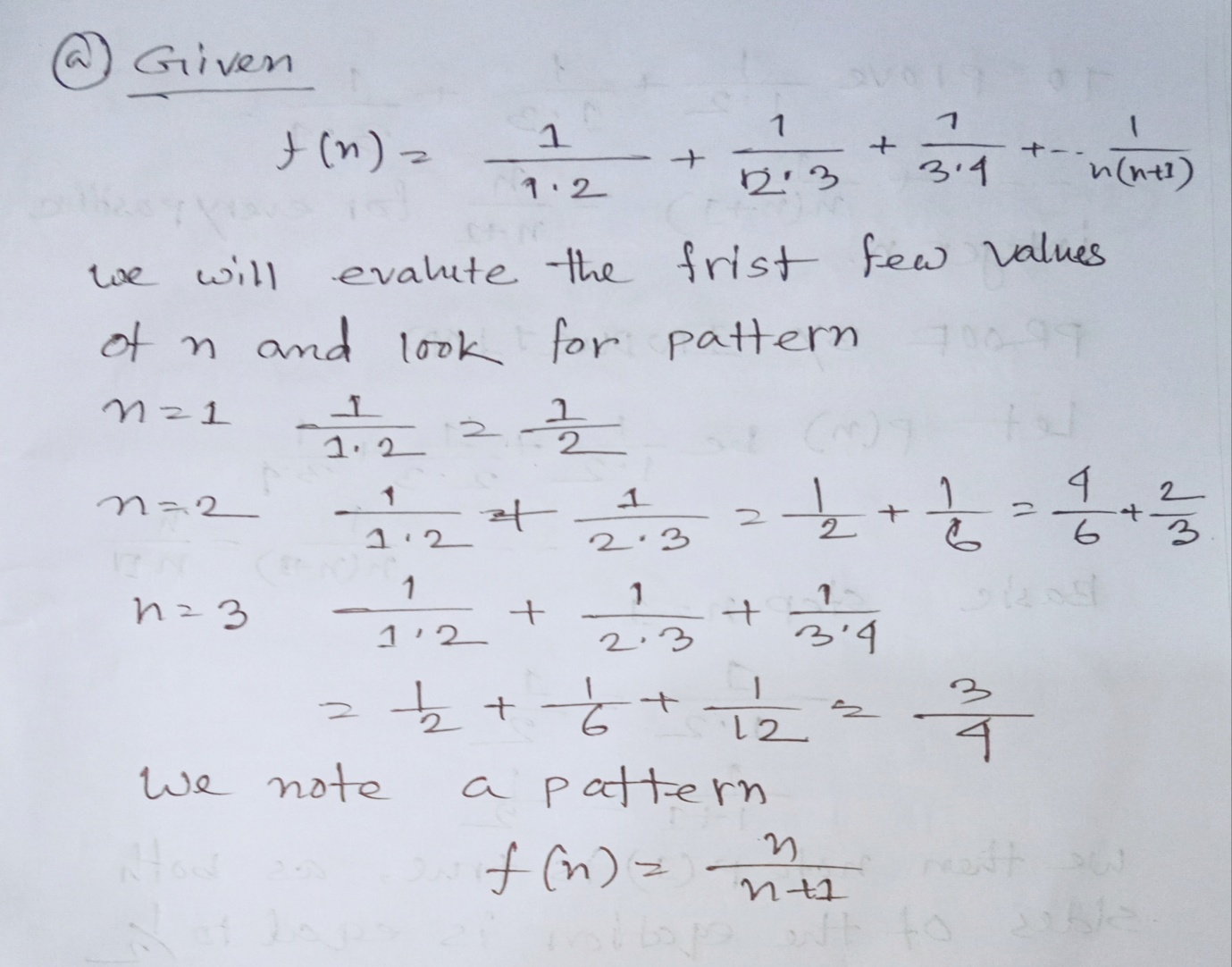
= (k +2)(k + 1)! -1 = (k +2)! – 1

= ((k + 1) + 1)! - 1

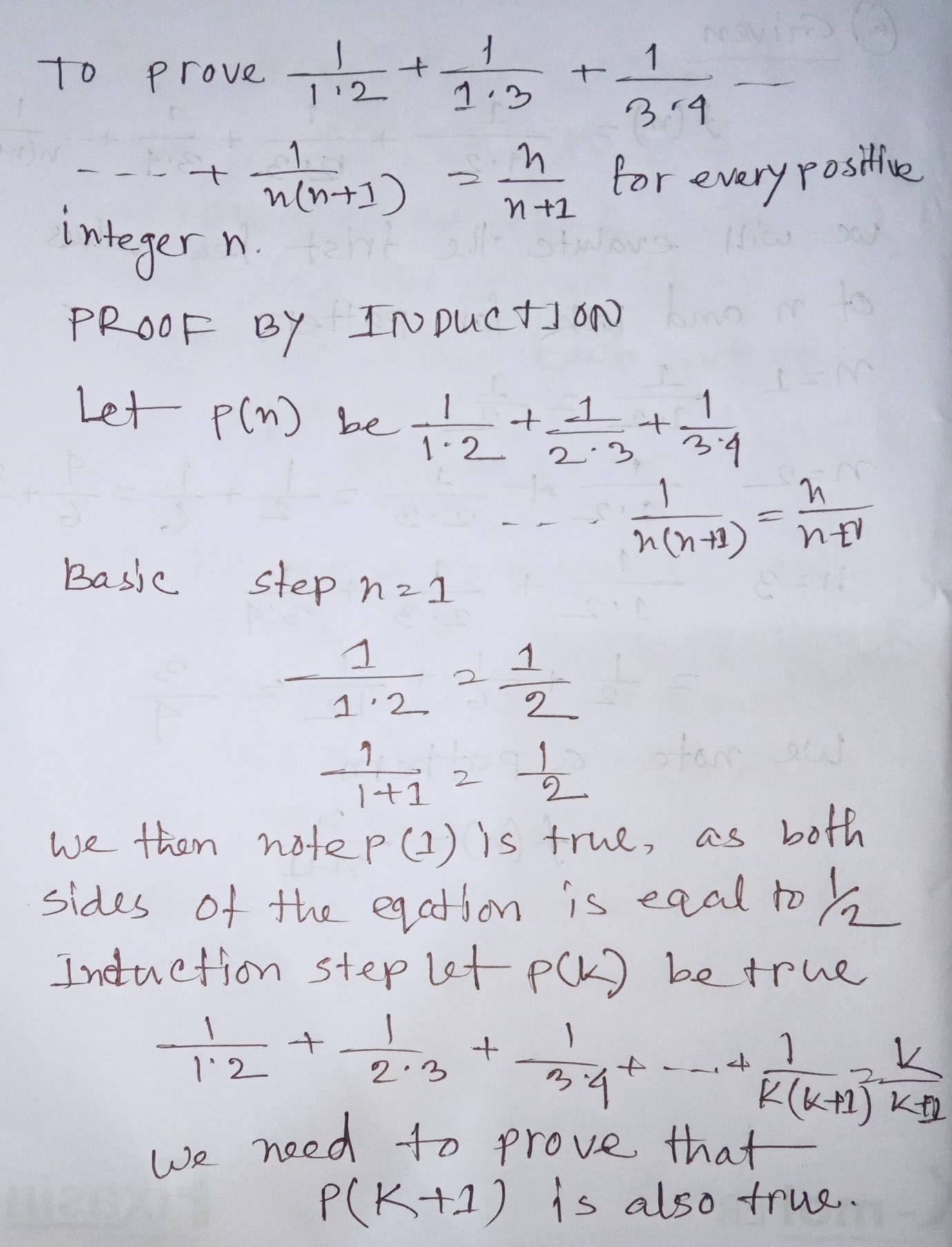
We then note that P(k + 1) is also true. Conclusion By the principle of mathematical induction, P(n) is true for all positive integers n.

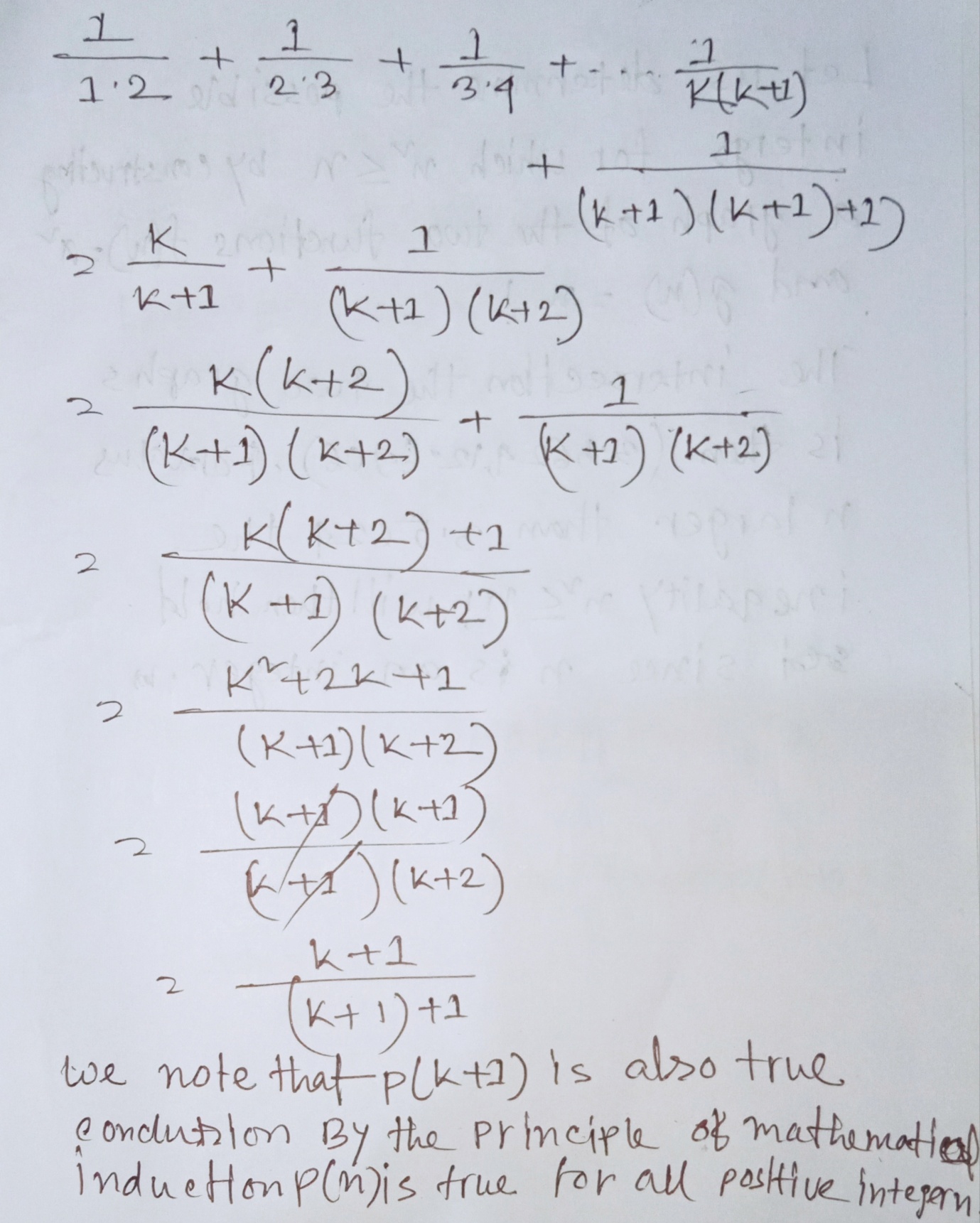
10. a) Find a formula for

+ +··· + by examining the values of this expression for small values of n.



b) Prove the formula you conjectured in part (a).





22. For which nonnegative integer’s n is ≤ n!? Prove your answer.

