1. Use modular exponentiation to find:

i)$7^{644}\ mod\ 645$.

ii)$3^{2003}\ mod\ 99$.

iii)$242^{329}\ mod\ 243$.

Solution:

i) Algorithm 5 initially sets x = 1 and power = 7 mod 645 = 7.

In the computation of 7^644 mod 645, this algorithm determines 7^(2^j) mod 645 for j = 1, 2, . . . , 9 by successively squaring and reducing modulo 645. If a j = 1 (where a j is the bit in the j th position in the binary expansion of 644, which is (1010000100)2), it multiplies the current value of x by 7^(2^j) mod 645 and reduces the result modulo 645. Here are the steps used:

i =0 Because a0 = 0, we have x = 1 and power = 7^2 mod 645 =49 mod 645=49;

i =1 Because a1 = 0, we have x = 1 and power = 49^2 mod 645 = 2401 mod 645 =466;

i =2 Because a2 = 1, we have x = 1·466 mod 645 =466 and power = 466^2 mod 645 =217156 mod 645 = 436;

i =3 Because a3 = 0, we have x = 466 and power = 436^2 mod 645 = 190096 mod 645 = 466;

i =4 Because a4 = 0, we have x = 466 and power = 466^2 mod 645 = 217156 mod 645 = 436;

i =5 Because a5 = 0, we have x = 466 and power = 436^2 mod 645 = 190096 mod 645 = 466;

i =6 Because a6 = 0, we have x = 466 and power = 466^2 mod 645 = 217156 mod 645 = 436;

i =7 Because a7 = 1, we have x = 466·436 mod 645 = 1 and power = 436^2 mod 645 =190096 mod 645 = 466;

i =8 Because a8 = 0, we have x = 1 and power = 466^2 mod 645 = 217156 mod 645 = 436;

i =9 Because a9 = 1, we have x = 1·436 mod 645 = 436.

ii) Let us first determine the binary expansion of 2003:

2003=$(111\ 1101\ 001)_2$

a_i then represents the ith digit in the binary expansion of 2003.

$a_0=a_1=a_4=a_6=a_7=a_8=a_9=a_{10}=1$
$a_2=a_3=a_5=0$
Initially x is set to 1 and power is set to 3 mod 99.
$x=1$

power=3 mod 99 =3
When $a_i=1$ then x is first multiplied by the power and reduced modulo 99.
Then on each iteration the power is multiplied by itself and reduced modulo 99.

i=0 Since $a_0=1$:
x=1.3 mod 99=3 mod 99=3
power=3^2 mod 99=9 mod 99=9

i=1 Since $a_1=1$:
x=3.9 mod 99=27 mod 99=27
power=9^2 mod 99=81mod 99=81

i=2 Since $a_2=0$:
x=27
power=81^2 mod 99=6561 mod 99=27

i=3 Since $a_3=0$:
x=27
power=27^2 mod 99=729 mod 99=36

i=4 since $a_4=1$:
x=27 · 36 mod 99=972 mod 99=81
power=36^2 mod 99=1296 mod 99=9

i=5 since $a_5=0$:
x=81
power=9^2 mod 99=81 mod 99=81

i=6 since $a_6=1$:
x=81 · 81 mod 99=6561 mod 99=27
power=81^2 mod 99=6561 mod 99=27

i=7 since a_7=1:
x=27.27 mod 99 = 729 mod 99 = 36
power=27^2 mod 99=729 mod 99=36

i=8 since a_8=1:
x=36.36 mod 99 = 1296 mod 99 = 9
power=36^2 mod 99=1296 mod 99=9

i=9 since a_9=1:
x=9.9 mod 99 = 81 mod 99 = 81
power=9^2 mod 99=81 mod 99=81

i=10 since a_10=1:
x=81.81 mod 99 = 6561 mod 99 = 27
power=81^2 mod 99=6561 mod 99=27

iii)242^329 mod 243 = 242.
2. Not covered in syllabus.

3. Let a, b,c, and d be integers, where a ≠ 0 such that a | c and b | d, then prove that ab | cd.
Solution:
DEFINITIONS

a divides b if there exists an integer c such that b=ac
Notation: a|b
Given: a,b,c, and d are integers with a|c and b|d and a≠0
To proof: ab|cd
PROOF
Since a|c, there exists an integer f such that:
c=af
Since b|d, there exists an integer g such that:
d=bg
Multiply these two equations:
cd=(af)(bg)=afbg=abfg=(ab)(fg)
Since f and g are integers, their product fg is an also integer.
By the definition of divides, we have then shown that ab divides cd.

ab|cd

4. Prove that if n is an odd positive integer, then $n^2 \equiv 1 \pmod 8$.

Solution:

If n is odd, we can write n =2k +1 for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$

To show that $n^2 \equiv 1 \pmod 8$, it is sufficient to show that $8|n^2 - 1$. We have that $n^2 - 1 = 4k^2 + 4k$ =4k(k +1). Now, we have two cases to consider: if k is even, there is some integer d such that k =2d. Then n^2−1=4(2d)(2d+1)=8d(d+1), and clearly this is divisible by 8 since it is a multiple of 8. If k is odd, then there is some integer d such that k =2d+1. Then n^2 =4(2d+1)(2d+2)=8(2d+1)(d+1), and again, this is divisible by 8. Thus, in both cases, n^2−1is divisible by 8, so $n^2 \equiv 1 \pmod 8$.

5. Find the integer a such that:

i) a ≡ −11 (mod 21) and 90 ≤ a ≤ 110.

ii) a ≡ 99 (mod 41) and 100 ≤ a ≤ 140.

iii) a ≡ 17 (mod 29) and −14 ≤ a ≤ 14.

Solution:

i)Answer: a = 94 (we can check by seeing that 21|(94−(−11)))

ii)Answer:a=140 (we can check by seeing that 41|(140-(99)))

iii)Answer: a = −12 (we can check by seeing that 29|(17−(−12)))

6. Find the quotient and remainder when:

i) 1,234,567 is divided by 1001?

ii) −123 is divided by 19?

iii) 0 is divided by 17?

iv) −2002 is divided by 87?

v) 1001 is divided by 13?

Solution:

i)Quotient: 1233,Remainder:334

ii)Quotient: -7,Remainder:10

iii)Quotient:0 ,Remainder:0

iv)Quotient:-24 ,Remainder:86

v)Quotient: 77,Remainder:0

7. Find the prime factorization of the following numbers:
i)909,090.
ii)10!
iii)7007.
Solution:
i)2, 3, 3, 3, 5, 7, 13, 37.
ii)2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 5, 5, 7.
iii)7, 7, 11, 13.
8. Show that if a and b are positive integers, then ab = gcd(a, b) · lcm(a, b).
Solution:
Given: a and b are positive integers

To proof: ab = gcd(a, b) · lcm(a, b)

PROOF

Let $p_1,p_2,...,p_k$ be the primes in the prime factorization in either aa or bb. Then the prime factorization of aa and bb is of the form:

$a=p_1^{a_1}. p_2^{a_2}. p_k^{a_k}$
$b=p_1^{b_1}. p_2^{b_2}. p_k^{b_k}$

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.

$gcd(a,b)=p_1^{min(a_1,b_1)}.p_2^{min(a_2,b_2)}. p_k^{min(a_k,b_k)}$
The prime factorizations of the numbers have been given. The prime factorization of the least common multiple then contains all primes in the prime factorizations of a and b, where its power is the maximum of the powers of the prime in the prime factorization of a and b.

$lcm(a,b)=p_1^{max(a_1,b_1)}. p_2^{max(a_2,b_2)}. p_k^{max(a_k,b_k)}$
Let us determine the product of the greatest common divisor and least common multiple (use the fact that if $min(a_i,b_i)=a_i$ then $max(a_i,b_i)=b_i$
and if $min(a_i,b_i)=b_i$ then $max(a_i,b_i)=a_i$

gcd(ab). lcm(a,b)&=(p_1^(a_1,b_1)}. p_2^(a_2,b_2)}. p_k^(a_k,b_k)) .
(p_1^max(a_1,b_1). p_2^max(a_2,b_2. p_k^max(a_k,b_k))
=p_1^min(a_1,b_1)+max(a_1,b_1)}. p_2^min(a_2,b_2)+max(a_2,b_2).
p_k^min(a_k,b_k)+max(a_k,b_k) \
=p_1^{a_1+b_1}.p_2^{a_2+b_2}. p_k^{a_k+b_k}
=(p_1^{a_1}.p_2^{a_2}.p_k^{a_k}). (p_1^{b_1}. p_2^{b_2}.p_k^{b_k})
=a. b
$ab=\gcd(ab)\cdot \mathrm{lcm}(a,b)$

9. Determine whether the integers in each of these sets are pairwise relatively prime:
i)14,17,85.
ii)21,34,55.
iii) 25, 41, 49, 64.
iv) 17, 18, 19, 23.

Solution:

i)Let us determine the prime factorization of each integer:

$14=2\cdot 7$
$17=17$
$85=5\cdot 17$

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

$\gcd(14,17)=1$
$\gcd(14,85)=1$
$\gcd(17,85)=17$

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

ii)Let us determine the prime factorization of each integer:

$21=3\cdot 7$
$34=2\cdot 17$
$55=5\cdot 11$

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

$\gcd(21,34)=1$
$\gcd(21,55)=1$
$\gcd(34,55)=1$

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

iii)Let us determine the prime factorization of each integer:

$25=5^2$
$41=41$
$49=7^2$
$64=2^6$

Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.
gcd(25,41)=1
gcd(25,49)=1
gcd(25,64)=1
gcd(41,49)=1
gcd(41,64)=1
gcd(49,64)=1
The integers are then pairwise relatively prime, because all greatest common divisors are equal to 1.
iv)Let us determine the prime factorization of each integer:
$17=17$
$18=2 \cdot 3^2$
$19=19$
$23=23$
Let us use the prime factorizations to determine the greatest common divisor of each pair of the given integers.

gcd(17,18)=1
gcd(17,19)=1
gcd(17,23)=1
gcd(18,19)=1
gcd(18,23)=1
gcd(19,23)=1
The integers are then pairwise relatively prime because all greatest common divisors are equal to 1

10. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.
i) 252,198.

ii) 35,78.

iii) 33,44.

Solution:

i) The Euclidean algorithm uses these divisions:

$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + 18$

$36 = 2 \cdot 18.$

Using the next-to-last division (the third division), we can express gcd(252, 198) = 18 as a linear combination of 54 and 36. We find that

$18 = 54 - 1 \cdot 36.$

The second division tells us that

$36 = 198 - 3 \cdot 54.$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198.We have

$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$

The first division tells us that

$54 = 252 - 1 \cdot 198.$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

ii) The Euclidean algorithm starts by dividing the largest integer by the smallest. The divisor is then divided by the remainder in the following steps until we obtain a remainder of 0.

$78=2 \cdot 35+8$

$35=4 \cdot 8+3$

$8=2 \cdot 3+2$

$3=1 \cdot 2+1$

$2=2 \cdot 1$

The greatest common divisor is then the last nonzero remainder: gcd(35, 78)=1.

By solving the 4th equation of the Euclidean algorithm to the greatest common divisor, we then obtain:

gcd(35,78)=1
$=3-1\cdot 2$
$=1\cdot 3+(-1)\cdot 2$
$=1\cdot 3+(-1)\cdot(8-2\cdot 3)$
$=3\cdot 3+(-1)\cdot 8$
$=3\cdot(35-4\cdot 8)+(-1)\cdot 8$
$=3\cdot 35+(-13)\cdot 8$
$=3\cdot 35+(-13)\cdot(78-2\cdot 35)$
$=29\cdot 35+(-13)\cdot 78$

iii)The Euclidean algorithm starts by dividing the largest integer by the smallest. The divisor is then divided by the remainder in the following steps until we obtain a remainder of 0.

44=1.33+11
$33=3\cdot 11$

The greatest common divisor is then the last nonzero remainder: gcd(33, 44)=11

By solving the first equation of the Euclidean algorithm to the greatest common divisor, we then obtain:
gcd(33, 44)=1=44-1.33=1.44+(-1).33

11. Find the greatest common divisors and the least common multiples of the following Pairs:
i)$3^{13}.5^{17}, \ 2^{12}.7^{21}$
ii)$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13, 2^{11}.3^{9}.11.17^{14}$
iii)$41\cdot 43\cdot 53$, $41\cdot 43\cdot 53$
Solution:
i)We note that the two prime factorizations have no factors in common, then the greatest common divisor is 1.
gcd(a,b)=1.
lcm(a,b)=$2^{12}.3^{13}.5^{17}.7^{21}$

ii) gcd(a,b)

$2^{min(1,11)}.3^{min(1,9)}.11$
=66.
lcm(a,b)=2.3.11

iii) gcd(a,b) = 41.43.53=93439.
lcm(a,b)=41.43.53=93439.

12. Show that if a, b, and m are integers such that m ≥ 2 and a ≡ b (mod m), then gcd(a,m) = gcd(b,m).

Solution:
DEFINITIONS
a divides b if there exists an integer c such that b=ac
Notation: a|b
a is congruent to b modulo m if m divides a-b
Notation: a≡b(mod m)
Given: a, b and m are integers with m≥2
a≡b(mod m)
To proof: gcd(a,m)=gcd(b,m)
PROOF
Since a≡b(mod m), m divides a-b and thus there exists an integer c such that: a-b=mc or equivalently a=mc+b.
Let us define the constants A and B as:
A=gcd(a,m)
B=gcd(b,m)
The greatest common divisor of two integers divides both integers:
A|a A|m B|b B|m
Since a=mc+b, A|a and A|m implies A|b
A|b
Since a=mc+b, B|b and B|m implies B|a
B|a
If an integer divides two integers, then the integer also divides their greatest common divisor:
A|gcd(b,m)
B|gcd(a,m)
Since A=gcd(a,m) and B=gcd(b,m)

A|B
B|A
A | B and B|A then imply A=B
gcd(a,m)=gcd(b,m).

13. If the product of two integers is $2^7 3^8 5^2 7^{11}$ and their greatest common divisor is $2^3 3^4 5$, what is their least common multiple?

Solution:-

we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is

$2^7 3^8 5^2 7^{11} / 2^3 3^4 5 = 2^4 . 3^4 . 5 . 7^{11}$

14. Find the greatest common divisor of the following pair of numbers using the Euclidean
Algorithm:
i) 11111, 111111.
ii) 1529, 14038.
iii) 750,900.
iv) 414,662.

Solution:-

To apply the Euclidean algorithm, we divide the larger number by the smaller, replace the larger by the smaller and the smaller by the remainder of this division, and repeat this process until the remainder is 0. At that point, the smaller number is the greatest common divisor.

i) gcd(11111,111111)= gcd(11111,1) = gcd(1,0) = 1
ii)gcd(1529,14038)=gcd(1529,277)=gcd(277,144)=gcd(144,133)=gcd(133,11)=gcd(11,1)=gcd(1,0)= 1
iii) gcd(750,900)=gcd(750,150)=gcd(150,0)=150
iv)gcd(414,662)=gcd(414,248)=gcd(248,166)=gcd(166,82)=gcd(82,2)=gcd(41,0)=41.

15.How many divisions are required to find gcd(21, 34) using the Euclidean algorithm?

Solution:-

By using the Euclidean algorithm

$34 = 21 \times 1 + 13$

$21 = 13 \times 1 + 8$

$13 = 8 \times 1 + 5$

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

As 1 is the last nonzero remainder.

So, gcd(21, 34) is 1.

Therefore, 7 divisions are required to find gcd(21, 34) using the Euclidean algorithm.