1. Use the method of successive squaring to compute each of the following powers.

(a) 5^{13} (mod 23) (b) 28^{749} (mod 1147)

k/2	Q	R
13/2	6	1
6/2	3	0
3/2	1	1
1/2	0	1

CH-16

(a)Answer- a = 5, k = 13, m = 23.

step1- *W*rite k as sum of powers of 2.

$k = (1101)_2$

$= 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0$

$(u_0 = 1, u_1 = 0, u_2 = 1, u_3 = 1)$

$= 8 + 4 + 1.$

step2- Make a table of powers of 5 modulo 23 using successive squaring.

$5^1 \equiv 5 \equiv 5 \pmod{23}$

$5^2 \equiv 25 \equiv 2 \pmod{23}$

$5^4 \equiv (5^2)^2 \equiv (2)^2 \equiv 4 \equiv 4 \pmod{23}$

$5^8 \equiv (5^4)^2 \equiv (4)^2 \equiv 16 \equiv 16 \pmod{23}$

step3- $5^{13} = 5^{8+4+1}$

$= 5^8 . 5^4 . 5^1$

$\equiv (16.4).5 \pmod{23}$ (using step 2)

$\equiv 18.5 \pmod{23}$ $(64 \equiv 18 \pmod{23})$

$5^{13} \equiv 21 \pmod{23}$ $(90 \equiv 21 \pmod{23})$

(b) **answer- a = 28, k = 749, m = 1147.**

***step1*- Write k as sum of powers of 2.**

$k = (1011101101)_2$

$= 2^9 + 2^7 + 2^6 + 2^5 + 2^3 + 2^2 + 1$

$= 512 + 128 + 64 + 32 + 8 + 4 + 1$

K/2	Q	R
749/2	374	1
374/2	187	0
187/2	93	1
93/2	46	1
46/2	23	0
23/2	11	1
11/2	5	1
5/2	2	1
2/2	1	0
1/2	0	1

***step2*- Make a table of powers of 28 modulo 1147 using successive squaring.**

$28^1 \equiv 28 \equiv 28 \pmod{1147}$

$28^2 \equiv 784 \equiv 784 \pmod{1147}$

$28^4 \equiv (28^2)^2 \equiv (784)^2$

$\equiv 614656 \equiv 1011 \pmod{1147}$

$28^8 \equiv (28^4)^2 \equiv (1011)^2 \equiv 1022121 \equiv 144 \pmod{1147}$

$28^{16} \equiv (28^8)^2 \equiv (144)^2 \equiv 20736 \equiv 90 \pmod{1147}$

$28^{32} \equiv (28^{16})^2 \equiv (90)^2 \equiv 8100 \equiv 71 \pmod{1147}$

$28^{64} \equiv (28^{32})^2 \equiv (71)^2 \equiv 5041 \equiv 453 \pmod{1147}$

$28^{128} \equiv (28^{64})^2 \equiv (453)^2 \equiv 205209 \equiv 1043 \pmod{1147}$

$28^{256} \equiv (28^{128})^2 \equiv (1043)^2 \equiv 1087849 \equiv 493 \pmod{1147}$

$28^{512} \equiv (28^{256})^2 \equiv (493)^2 \equiv 243049 \equiv 1032 \pmod{1147}$

step3- $28^{749} = 28^{512 + 128 + 64 + 32 + 8 + 4 + 1}$

$= 28^{512} . 28^{128} . 28^{64} . 28^{32} . 28^{8} . 28^{4} . 28^{1}$

$\equiv (1032. 1043). (453. 71). (144. 1011). 28 \pmod{1147}$

$\equiv (490. 47). (1062.28) \ (\bmod 1147)$

$\equiv 90. 1061 \ (\bmod 1147)$

$28^{749} \equiv 289 \ (\bmod 1147)$

≥

≥

2. The method of successive squaring described in the text allows you to compute $a^k \pmod{m}$ quite efficiently, but it does involve creating a table of powers of a modulo m.

(a) Show that the following algorithm will also compute the value of $a^k \pmod{m}$. It is a more efficient way to do successive squaring, well-suited for implementation on a computer.

(1) Set b= 1

(2) Loop while $k \geq 1$

(3) If k is odd, set $b = a.b \pmod{m}$

(4) Set $a = a^2 \pmod{m}$

(5) Set $k = k/2$ (round down if k is odd)

(6) End of Loop

(7) Return the value of b (which equals $a^k \pmod{m}$)

(b) Implement the above algorithm on a computer using the computer language of your choice.

(c) Use your program to compute the following quantities: (i) $2^{1000} \pmod{2379}$

(ii) $567^{1234} \pmod{4321}$ (iii) $47^{258008} \pmod{1315171}$.

1. Solve the congruence $x^{329} \equiv 452 \pmod{1147}$.

Answer- $k = 329$, $b = 452$, $m = 1147$;

$m = 31.37$

(1) $\boldsymbol{\varnothing(m) = \varnothing(1147) = \varnothing(31)\,\varnothing(37)}$

$\boldsymbol{= 30.36 = 1080.}$

(2) Find positive integers u and v that satisfy $329u - 1080v = 1$

$(u,v) = (929,283)$

(3) Compute $\boldsymbol{452^{929} \pmod{1147}}$ by successive squaring.

$\boldsymbol{X \equiv 763 \pmod{1147}}$ ***Ans.***

CFC-17

(2) $329u - 1080v = 1$

$A = 329,\ B = 1080$

$1080 = 3*329 + 93$	$93 = -3A + B$
$329 = 3*93 + 50$	$50 = A - 3*(-3A + B) = 10A - 3B$
$93 = 1*50 + 43$	$43 = (-3A + B) - (10A - 3B) = -13A + 4B$
$50 = 1*43 + 7$	$7 = \mathbf{(}10A - 3B\mathbf{)} \mathbf{-} \mathbf{(}-13A + 4B\mathbf{)} = \mathbf{23A - 7B}$
$43 = 6*7 + 1$	$1 = (-13A + 4B) - 6*(\mathbf{23A - 7B})$
$7 = 7*1 + 0$	$= A(-151) - B(-46)$

$u_0 = -151 + 1080 = 929$

$v_0 = -46 + 329 = 283$

$452^{1} \equiv 452 \pmod{1147}$ **(3)**

$452^{2} \equiv 204304 \equiv 138 \pmod{1147}$

$452^{4} \equiv (452^{2})^{2} \equiv 19044 \equiv 692 \pmod{1147}$

$452^{8} \equiv (452^{4})^{2} \equiv 478864 \equiv 565 \pmod{1147}$

$452^{16} \equiv (452^{8})^{2} \equiv 319225 \equiv 359 \pmod{1147}$

$452^{32} \equiv (452^{16})^{2} \equiv 128881 \equiv 417 \pmod{1147}$

$452^{64} \equiv (452^{32})^{2} \equiv 173889 \equiv 692 \pmod{1147}$

$452^{128} \equiv (452^{64})^{2} \equiv 478864 \equiv 565 \pmod{1147}$

$452^{256} \equiv (452^{128})^{2} \equiv 319225 \equiv 359 \pmod{1147}$

$452^{512} \equiv (452^{256})^{2} \equiv 128881 \equiv 417 \pmod{1147}$

$k = 929 = (\mathbf{1110100001})_2$

$= \; 2^9 + 2^8 + 2^7 + 2^5 + 1$

$452^{929} = 452^{\,2^9 + 2^8 + 2^7 + 2^5 + 1}$

$= 452^{2^9} \cdot 452^{2^8} \cdot 452^{2^7} \cdot 452^{2^5} . 452^1$

$\equiv 452^{512} . 452^{256} . 452^{128} . 452^{32} . 452^1$

$\equiv 417.359.565.417.452 \pmod{1147}$

$\equiv 593.470.452 \; (\bmod\; 1147)$

$\equiv 763 \; (\bmod\; 1147)$ *Ans.*

2. (a) Solve the congruence $x^{113} \equiv 139 \pmod{588}$.

Answer- (a)

K = 113, b = 139, m = 588.

(1) $\emptyset(m) = \emptyset(588) = 462$.

(2) Find positive integers u and v that satisfy 113u -462v = 1

A = 113, B = 462.

462 = 4*113 + 10	10 = B – 4A
113 = 11*10 + 3	3 = A – 11*(B-4A) = 45A - 11B
10 = 3*3 + 1	1 = (B-4A) – 3*(45A – 11B)
3 = 3*1 + 0	= A(-139) - B(-34)

(u,v) = (-139, -37)

positive solution: (u_0,v_0) = (-139 + 462, -34 + 113) = (323,79)

(3) Compute **139^{323}(mod 588)** by successive squaring.

$323 = (101000011)_2$

$= 1 + 2 + 2^6 + 2^8 = 1 + 2 + 64 + 256$

$$
\begin{aligned}
139^1 &\equiv 139 && && \equiv 139 \pmod{588}\\
139^2 &\equiv (139^1)^2 \equiv 120409 && && \equiv 29 \pmod{588}\\
139^4 &\equiv (139^2)^2 \equiv (29)^2 && \equiv 841 && \equiv 378 \pmod{588}\\
139^8 &\equiv (139^4)^2 \equiv (378)^2 && \equiv 142884 && \equiv 280 \pmod{588}\\
139^{16} &\equiv (139^8)^2 \equiv (280)^2 && \equiv 78400 && \equiv 153 \pmod{588}\\
139^{32} &\equiv (139^{16})^2 \equiv (153)^2 && \equiv 23409 && \equiv 259 \pmod{588}\\
139^{64} &\equiv (139^{32})^2 \equiv (259)^2 && \equiv 67081 && \equiv 409 \pmod{588}\\
139^{128} &\equiv (139^{64})^2 \equiv (409)^2 && \equiv 167281 && \equiv 138 \pmod{588}\\
139^{256} &\equiv (139^{128})^2 \equiv (138)^2 && \equiv 19044 && \equiv 61 \pmod{588}
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{139^{323}} = \mathbf{139}^{1+2+64+256} &= 139^1 \,.\, 139^2 \,.\, 139^{64} \,.\, 139^{256}\\
&\equiv 139.\ 29\ .\ 409\ .\ 61 \pmod{588}\\
&\equiv 139.\ 29\ .\ 409\ .\ 61 \pmod{588}\\
&\equiv 340.\ 410 \pmod{588}\\
&\equiv 37 \pmod{588}
\end{aligned}
$$

$x \equiv 37 \pmod{588}$ *Ans.*

(b) Solve the congruence $x^{275} \equiv 139 \pmod{588}$.

Answer- $k = 275$, $b = 139$, $m = 588$.

$m = 2^2 * 3 * 7^2$.

(1) $\varnothing(m) = \varnothing(2^2 * 3 * 7^2) = \varnothing(2^2)\,\varnothing(3)\,\varnothing(7^2)$

$=(2^2 - 2^1)(3 - 1)(7^2 - 7^1)$

$= 2*2*42$

$= 168.$

(2) Find positive integers u and v that satisfy $275u - 168v = 1$.

$A = 275$, $B = 168$.

$275 = 1*168 + 107$	$107 = A - B$
$168 = 1*107 + 61$	$61 = B - (A-B) = 2B - A$
$107 = 1*61 + 46$	$46 = (A-B) - (2B - A) = 2A - 3B$
$61 = 1*46 + 15$	$15 = (2B - A) - (2A - 3B) = 5B - 3A$
$46 = 3*15 + 1$	$1 = (2A - 3B) - 3*(5B - 3A) = 11A - 18B$
$15 = 15*1 + 0$	

$(u,v) = (11, 18)$

(3) Compute $\mathbf{139^{11} \pmod{588}}$ by successive squaring.

$11 = 1 + 2 + 8$

$$139^1 \equiv 139 \equiv 139 \pmod{588}$$

$$139^2 \equiv (139^1)^2 \equiv 19321 \equiv 505 \pmod{588}$$

$$139^4 \equiv (139^2)^2 \equiv (505)^2 \equiv 255025 \equiv 421 \pmod{588}$$

$$139^8 \equiv (139^4)^2 \equiv (421)^2 \equiv 177241 \equiv 253 \pmod{588}$$

$$139^{11} = 139^{1+2+8} = 139^1 . 139^2 . 139^8$$

$$\equiv 139.505.253 \pmod{588}$$

$$\equiv 559 \pmod{588}$$

$x \equiv 559 \pmod{588}$ Ans.

Q.3 Use Korselt's Criterion to determine which of the following numbers are Carmichael numbers.

CH-19

(a) 1105 (e) 8911 (i) 126217

(b) 1235 (f) 10659 (j) 162401

(c) 2821 (g) 19747 (k) 172081

(d) 6601 (h) 105545 (1) 188461

Answer- **(a)** n= 1105 = 5*13*17 , p_1 = 5, p_2 = 13, p_3 = 17.

(1) All p_i's are distinct ⇨ $p_i^{\,2}$ does not divide n.

(2) $p_i - 1$ / (n-1) for all i.

Therefore 1105 is a Carmichael number.

(b) n= 1235 = 5*13*19 , p_1 = 5, p_2 = 13, p_3 = 19.

(1) All p_i's are distinct ⇨ $p_i^{\,2}$ does not divide n.

(2) p_1 - 1 = 4 does not divide n – 1 = 1234.

Therefore 1235 is not a Carmichael number.

(c) 2821 Y

(d) 6601 Y

(e) 8911 Y check for the rest.

Q.4 Suppose that k is chosen so that the three numbers 6k + 1, 12k + 1, 18k + 1 are all prime numbers.

(a) Prove that their product n = (6k + 1)(12k + 1)(18k + 1) is a Carmichael number.

(b) Find the first five values of k for which this method works and give the Carmichael numbers produced by the method.

Answer- **(a)** $p_1 = 6k + 1$, $p_2 = 12k + 1$, $p_3 = 18k + 1$.

$$n = p_1 p_2 p_3 = (6k + 1)(12k + 1)(18k + 1)$$

$$= 6k.12k.18k + 6k.12k + 12k.18k + 18k.6k + 6k + 12k + 18k + 1$$

$$n - 1 = 36k(36k^2) + 36k(2k) + 36k(6k) + 36k(3k) + 36k$$

$$= 36k\,(24\,k^2 + 2k + 6k + 3k + 1)$$

- n is composite number.

(1) p_i^2 does not divide n, for i = 1,2,3.

(2) $p_1 - 1 = 6k$ divides $n - 1$, $p_2 - 1 = 12k$ divides $n - 1$ and $p_3 - 1 = 18k$ divides $n - 1$.

Therefore n is Carmichael number.

(b)

k = 1

$p_1 = 6*1 + 1 =$ **7**, $p_2 = 12*1 + 1 =$ **13**, $p_3 = 18*1 + 1 =$ **19**.

~~k = 2~~

$p_1 = 6*2 + 1 =$ **13**, $p_2 = 12*2 + 1 =$ **25(not a prime)...**

~~k = 3~~

$p_1 = 6*3 + 1 =$ **19**, $p_2 = 12*3 + 1 =$ **37**, $p_3 = 18*3 + 1 =$ **55(not a prime).**

~~k = 4~~

$p_1 = 6*4 + 1 =$ **25(not a prime) ....**

~~k = 5~~

$p_1 = 6*5 + 1 =$ **31**, $p_2 = 12*5 + 1 =$ **61**, $p_3 = 18*5 + 1 =$ **91(not a prime).**

k = 6

$p_1 = 6*6 + 1 =$ **37**, $p_2 = 12*6 + 1 =$ **73**, $p_3 = 18*6 + 1 =$ **109**.

.

.

.

20- Squares Modulo p

Q1. Make a list of all the quadratic residues and all the nonresidues modulo 19.

Answer-

A number a is called a quadratic residue (QR) mod p if there exists an integer x such that :

$$x^2 \equiv a \pmod{p}$$

Otherwise, a is called a quadratic nonresidue (NR) mod p.

b	b^2
1	$1^2 \equiv 1$
2	$2^2 \equiv 4$
3	$3^2 \equiv 9$
4	$4^2 \equiv 16$
5	$5^2 = 25 \equiv 6$
6	$6^2 = 36 \equiv 17$
7	$7^2 = 49 \equiv 11$
8	$8^2 = 64 \equiv 7$
9 = (19-1)/2	$9^2 = 81 \equiv 5$

mod (19)

List of all the QRs modulo 19:

1,4,5,6,7,9,11,16,17

List of all the NRs modulo 19:

2,3,8,10,12,13,14,15,18

Q2. For each odd prime p, we consider the two numbers

$$A = \text{sum of all } 1 \le a < p \text{ such that } a \text{ is a quadratic residue modulo } p,$$

$$B = \text{sum of all } 1 \le a < p \text{ such that } a \text{ is a nonresidue modulo } p.$$

(a) Make a list of A and B for all odd primes p < 20.

(b) What is the value of A+ B? Prove that your guess is correct.

(c) Compute A mod p and B mod p. Find a pattern and prove that it is correct.

(d) Compile some more data and give a criterion on p which ensures that A= B.

Answer-

Odd primes p < 20 : 3,5,7,11,13,17,19

p	A	B	A + B	A (mod p)	B (mod p)
3	1	2	3	1	2
5	5	5	10	0	0
7	7	14	21	0	0
11	22	33	55	0	0
13	39	39	78	0	0
17	68	68	136	0	0
19	76	95	171	0	0

(a)

For p = 3, QR : {1} , NR : {2}

A = 1 , B = 2;

For p = 5, QRs : {1,4}, NRs : {2,3}

A = 1 + 4 = 5, B = 2 + 3 = 5;

For p = 7, QRs : {1,4,2}, NRs : {3,5,6}

A = 1 + 4 + 2 = 7, B = 3 + 5 + 6 = 14;

For p = 11, QRs : {1,4,9, 5, 3}, NRs : {2,6,7,8,10}

A = 1+4+9+5+3 = 22, B = 2+6+7+8+10= 33;

For p = 13, QRs : {1,4,9,3,12,10}, NRs : {2,5,6,7,8,11}

A = 1+4+9+3+12+10 = 39, B = 2+5+6+7+8+11= 39;

For p = 17, QRs : {1,4,9,16,8,2,15,13}, NRs : {3,5,6,7,10,11,12,14}

A = 1+4+9+16+8+2+15+13 = 68, B = 3+5+6+7+10+11+12+14= 68;

For p = 19, QRs : {1,4,9,16,6,17,11,7,5}, NRs : {2,3,8,10,12,13,14,15,18}

A = 1+4+9+16+6+17+11+7+5 = 76, B = 2+3+8+10+12+13+14+15+18= 95;

(b) A + B = $\dfrac{p(p-1)}{2}$

Proof - **A + B =** QRs mod p + NRs mod p

= 1 + 2 + ... + (p-1)

= $\dfrac{p(p-1)}{2}$

(c) If p =3 , A (mod p) = 1 and B (mod p) =2.

If p > 3 , then A ≡ 0(mod p) and B ≡ 0(mod p).

We know that there are exactly (p-1)/2 QRs mod p and they are

$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ (mod p)

$A \equiv 1^2 + 2^2 + \ldots + \left(\frac{p-1}{2}\right)^2$ (mod p)

$$\equiv \frac{\left(\frac{(p-1)}{2}\right)\left(\frac{(p-1)}{2}+1\right)\left(2\frac{(p-1)}{2}+1\right)}{6} \pmod{p}$$

$\equiv \dfrac{p\left(p^2-1\right)}{24} \pmod{p}$ ≡ pk (mod p) where k = $(p^2 -1)/24$ is an integer. (*)

$\equiv 0$ (since p divides $p(p^2 -1)/24$)

(*) there are two reasons for k to be an integer.

(i) As p is an odd prime and 24 can't divide it. Therefore $(p^2 - 1)$ must be divisible by 24 .

(OR)

(ii) p is odd prime.

p is congruent to 1 (mod 4) or 3 (mod 4)

i.e. $p = 4k + 1$ or $4k + 3$, where k belongs to integer.

if we change mod to 3, then p is congruent to 1 (mod 3) or 2 (mod 3)

i.e $p = 3m + 1$ or $3m + 2$, where m belongs to integer.

p	p-1	p+ 1	p^2 -1
4k+1	4k	2(2k+1)	8k(2k+1)
4k+3	2(2k+1)	4(k+1)	8(2k+1)(k+1)
3m + 1	3m	(3m+2)	3m(3m+2)
3m + 2	3m+1	3(m+1)	3(3m+1)(m+1)

From the above table -

p^2 -1 is divisible by 8 and 3 both. Therefore

p^2 -1 is divisible by 8*3 =24.//

B = (A + B) – A

$$\equiv \left(\frac{p(p-1)}{2} - 0 \right) (\mathrm{mod}\ p)$$

$$\equiv p\left(\frac{p-1}{2} \right) (\mathrm{mod}\ p)$$

$$\equiv 0$$

(since 2 divides (p-1))

(d) A = B for p = 5, 13, 17.

Conjecture: If p ≡ 1 (mod 4) , then A =B.