Remainders
by Software Engineer - Monday, 31 August 2009, 09:25 PM

It is uncanny how children pick up a lot of small habits and beliefs of their parents. Even the ones that rebel against their parents bear subconscious resemblance to their father or mother. There is a lesson for instructors in this. It is important for them to realize that students mirror their feelings about CAT. If the instructor expresses or feels that CAT is tough, or is fearful about CAT, his students will mirror the same feeling and will be less confident. If the instructor is brazen and casual about the paper and scoffs the competition, his students would reflect the same feelings. Also, it is so necessary to have unflinching faith in one's students. I still remember that during my school days my mother used to proudly proclaim that I was an intelligent kid. I was barely scrapping passing marks in the school exams. If truth be told I was at the bottom of the class, but my mother had her blinkers on. And because of my mother I also believed that I was second to none. It was only years later, during my boards exams, that I took to studying seriously, and managed to outperform everyone else. I don't know if it was my mother's blind love for me or that she could see some bright spark in me that made her claim my intelligence but it really had great effect on my attitude. And attitude, in an exam like CAT, is everything.

While I am trying to write a DI lesson for the CAT CBT Club, here is another sparkling gem produced by a TGite already famous amongst you all- Software Engineer. When I saw the sheer size of the article I was awed. And so will you all be. The hard work demands applause from all of you. So read the article guys and do not forget to thank Software Engineer for this one. - Total Gadha

Modulo Order

The **smallest exponent** e for which $b^e = 1 \pmod n$, where n is relatively prime to b, is called the modulo order of b (mod n). For example, the modulo order of 13 (mod 24) is 2, since $13^2 = 1 \bmod 24$.

The term 'modulo order' is defined for the numbers that are relatively prime to each other. If e is the modulo order of b (mod n), by definition, n is relatively prime to b.

If e is the modulo order of b (mod n), then $b^0, b^{1e}, b^{2e}, b^{3e}, \dots, b^{N*e}$ leave the same remainder 1 when divided by n, where N is a whole number.
For example, the modulo order of 13 (mod 24) is 2, therefore,

$13^0 = 1 \bmod 24$
$13^2 = 1 \bmod 24$
$13^4 = (13^2)^2 \bmod 24 = (1)^2 \bmod 24 = 1 \bmod 24$
and so on.

If e is the modulo order of b (mod n), then $b^K, b^{K-e}, b^{K-2e}, \dots, b^{K-N*e}$ leave the same remainder R when divided by n, where N, K are whole numbers and $K \ge N*e$.

For example, $13^{15} = 13 \bmod 24$.
$13^{15-2*1} = 13^{13} \bmod 24 = 13 \bmod 24$.
$13^{15-2*2} = 13^{11} \bmod 24 = 13 \bmod 24$.
and so on .... upto
$13^{15-2*7} = 13^1 \bmod 24 = 13 \bmod 24$.

Therefore, to find the remainder when b^K is divided by n, subtract the highest multiple of the modulo order e of b (mod n) less than or equal to K, from K. Let K' = K – N*e. The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

For example, $13^{15} \bmod 24 = 13^{15-7*2} \bmod 24 = 13^1 \bmod 24 = 13 \bmod 24$.

In other words, to find the remainder when b^K is divided by n, first find the remainder K' when K is divided by the modulo order e of b (mod n). K = K' mod e. The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

For example, $13^{15} \bmod 24$.
The modulo order of 13 (mod 24) is 2. Therefore, find the remainder when 15 is divided by 2.
$15 = 1 \bmod 2$.
Therefore, $13^{15} \bmod 24 = 13^1 \bmod 24 = 13 \bmod 24$.

But the killer question is how to find the modulo order of b (mod n)? Is there any ready-made formula that calculates the smallest exponent e such that $b^e = 1 \pmod n$? Unfortunately, no such formula exists.

However, there are some formulas that calculate the exponent E such that the modulo order e of b (mod n) is always a factor of E. Let E=m*e. $b^E \bmod n = b^{me} \bmod n = (b^e)^m \bmod n = (1)^m \bmod n = 1 \bmod n$. Therefore, if E is a multiple of the modulo order e of b (mod n), then $b^0, b^{1E}, b^{2E}, b^{3E}, \dots, b^{N*E}$ leave the same remainder 1 when divided by n. If E is a multiple of the modulo order e of b (mod n), then $b^K, b^{K-e}, b^{K-2e}, \dots, b^{K-N*e}$ leave the same remainder R when divided by n. Therefore, to find the remainder when b^K is divided by n, first find the remainder K' when K is divided by E. K = K' mod E. The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

The first such formula that calculates the multiple E of modulo order e of b (mod n) was invented by Euler – Euler's Totient Function.

Euler's Totient Function

The Euler's totient function Ø(n) is defined as the number of positive integers less than or equal to n that are relatively prime to n, where 1 is counted as being relatively prime to all numbers.

If n is a natural number such that $n = a^p * b^q * c^r * \dots$ where a, b, c, ... are different prime factors and p, q, r

... are positive integers then the number of positive integers less than or equal to and prime to n is
Ø(n) = $n*\left(1-\frac{1}{a}\right)*\left(1-\frac{1}{b}\right)*\left(1-\frac{1}{c}\right)...$

Euler's Theorem

If n is relatively prime to b then $b^{Ø(n)} = 1$ mod n.

The modulo order e of b (mod n) is always a factor of Ø(n). Therefore, to find the remainder when b^K is divided by n, first find the remainder K' when K is divided by Ø(n). K = K' mod Ø(n). The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

The second such formula that calculates the multiple E of modulo order e of b (mod n) was invented by Carmichael – Carmichael's Reduced Totient Function.

Carmichael's Reduced Totient Function

Carmichael's Reduced Totient function is defined as
$\lambda(1) = 1$

$\lambda(2) = 1$
$\lambda(2^2) = 2$
$\lambda(2^n) = 2^{n-2}$ if n>2

$\lambda(p^n) = Ø(p^n)$ if p is an odd prime

$\lambda(a*b) = LCM[\lambda(a), \lambda(b)]$ if a and b are relatively prime to each other

Carmichael's Theorem

If n is relatively prime to b then $b^{\lambda(n)} = 1$ mod n.

The modulo order e of b (mod n) is always a factor of λ(n). Therefore, to find the remainder when b^K is divided by n, first find the remainder K' when K is divided by λ(n). K = K' mod λ(n). The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

Furthermore, λ(n) is always a factor of Ø(n).

$Ø(2^n) = 2 * \lambda(2^n)$ where n>2
Find Ø(128).
$Ø(128) = Ø(2^7) = 2^7*\left(1-\frac{1}{2}\right) = 64.$

Find λ(128).
$\lambda(128) = \lambda(2^7) = 2^{7-2} = 32.$

$Ø(p^n) = \lambda(p^n)$ where p is an Odd Prime
Find Ø(81).
$Ø(81) = Ø(3^4) = 3^4*\left(1-\frac{1}{3}\right) = 54.$

Find λ(81).
$\lambda(81) = \lambda(3^4) = Ø(3^4) = 3^4*\left(1-\frac{1}{3}\right) = 54.$

$\lambda(C) < Ø(C)$ where C is a composite number
Find Ø(20).
$Ø(20) = Ø(2^2 * 5^1) = 2^2*5^1*\left(1-\frac{1}{2}\right)*\left(1-\frac{1}{5}\right) = 8.$

Find λ(20).
$\lambda(20) = \lambda(2^2 * 5^1) = LCM[\lambda(2^2), \lambda(5^1)) = LCM[2, 4] = 4.$

Find Ø(180).
$Ø(20) = Ø(2^2 * 3^2 * 5^1) = 2^2*3^2*5^1*\left(1-\frac{1}{2}\right)*\left(1-\frac{1}{3}\right)*\left(1-\frac{1}{5}\right) = 48.$

Find λ(180).
$\lambda(20) = \lambda(2^2 * 3^2 * 5^1) = LCM[\lambda(2^2), \lambda(3^2), \lambda(5^1)) = LCM[2, 6, 4] = 12.$

As λ(n) is always a factor of Ø(n), there are two possible possibilities:- Either λ(n) = Ø(n), Or λ(n) < Ø(n).
λ(n) = Ø(n) if and only if $n=p^e$ where p is an odd prime; otherwise λ(n) < Ø(n).

- If $n=p^e$ where p is an odd prime then λ(n) = Ø(n). It does not matter whether we subtract the highest multiple of Ø(n) or highest multiple of λ(n), less than or equal to K, from K, because both are the same. So here, regardless whether we use Euler's Theorem or Carmichael's Theorem, we'll have to do the same calculations to get the remainder when b^K is divided by n.

- In any other case, λ(n) < Ø(n), therefore, rather than subtracting the highest multiple of Ø(n) less than or equal to K, from K, if we subtract the highest multiple of λ(n) less than or equal to K, from K; we'll end up with comparatively smaller power, so it would be comparatively easier for us to calculate the remainder when b^K is divided by n.

Let's compare, 'Euler's Totient Function' vs. 'Carmichael's Reduced Totient Function'.

Comparison#1 – Divisor is of the form 2^n

Find the remainder when 13^{239} is divided by 16.

16 is relatively prime to 13, therefore, we can apply Euler's theorem.
Ø(16) = 8. 239 = 7 mod 8.
13^{239} mod 16
= 13^7 mod 16
= $13^2 * 13^2 * 13^2 * 13$ mod 16
= 9 * 9 * 9 * 13 mod 16
= 81 * 117 mod 16
= 1 * 5 mod 16
= 5 mod 16

Find the remainder when 13^{239} is divided by 16.

16 is relatively prime to 13, therefore, we can apply Carmichael's theorem.
λ (16) = 4. 239 = 3 mod 4.
13^{239} mod 16
= 13^3 mod 16
= $13^2 * 13$ mod 16
= 9 * 13 mod 16
= 117 mod 16
= 5 mod 16

Comparison#2 – Divisor is of the from (Odd Prime)^n

What is remainder when 2^{1003} is divided by 25?

25 is relatively prime to 2, therefore, we can apply Euler's theorem.
Ø(25) = 20. 1003 = 3 mod 20.
2^{1000} mod 25
= 2^3 mod 25
= 8 mod 25

What is remainder when 2^{1003} is divided by 25?

25 is relatively prime to 2, therefore, we can apply Carmichael's theorem.
λ (25) = 20. 1003 = 3 mod 20.
2^{1000} mod 25
= 2^3 mod 25
= 8 mod 25

Comparison#3 – Divisor is Composite Number

Find the remainder when 5^{116} is divided by 63.

63 is relatively prime to 5, therefore, we can apply Euler's theorem.
Ø(63) = 36. 116 = 8 mod 36.
5^{116} mod 63
= 5^8 mod 63
= $5^3 * 5^3 * 5^2$ mod 63
= 125 * 125 * 25 mod 63
= -1 * -1 * 25 mod 63
= 25 mod 63

Find the remainder when 5^{116} is divided by 63.

63 is relatively prime to 5, therefore, we can apply Carmichael's theorem.
λ (63) = 6. 116 = 2 mod 6.
5^{116} mod 63
= 5^2 mod 63
= 25 mod 63

Conclusion. Generally, Mr. Carmichael runs faster than Mr. Euler. If divisor is of the form p^n where p is an odd prime then both run at equal speed. In one line, from today onwards, do use Carmichael's Theorem.

Find the remainder when 2^{2002} is divided by 1001. posted by **Sri KLR**

1001 is relatively prime to 2, therefore we can apply Carmichael's theorem.
λ (1001) = 60. 2002 = 22 mod 60.

2^{2002} mod 1001
= 2^{22} mod 1001
= 1024 * 1024 * 4 mod 1001
= 23 * 23 * 4 mod 1001
= 2116 mod 1001
= 114 mod 1001

Find the remainder when $3^{2002} + 5^{2002}$ is divided by 26. posted by **Total Gadha**

Both 3 and 5 are relatively prime to 26, therefore we can apply Carmichael's theorem.

Both 3 and 5 are relatively prime to 26, therefore we can apply Carmichael's theorem.
$\lambda(26) = 12$. $2002 = 10 \mod 12$.

$3^{2002} + 5^{2002} \mod 26$
$= 3^{10} + 5^{10} \mod 26$
$= (27)^3 * 3 + (25)^5 \mod 26$
$= (1)^3 * 3 + (-1)^5 \mod 26$
$= 3 - 1 \mod 26$
$= 2 \mod 26$

Find the remainder when 5^{99} is divided by 66. **Quant Capsule - Division by Composite Numbers**
66 is relatively prime to 5, therefore we can apply Carmichael's theorem.
$\lambda(66) = 10$. $99 = 9 \mod 10$.
$5^{99} \mod 66$
$= 5^9 \mod 66$

According to Carmichael's theorem, $5^{10} = 1 \mod 66$
$5^9 * 5 = 1 \mod 66$
Let R be the remainder when 5^9 is divided by 66.
$R * 5 = 1 \mod 66$

$5R = 66m + 1$
$= 65m + m + 1$
LHS is a multiple of 5, therefore, RHS is a multiple of 5, therefore, m+1 is a multiple of 5, therefore, m=4.
$5R = 65*4 + 4 + 1$
$R = 13*4+1 = 53$

Hence, $5^9 = 53 \mod 66$.

Find the remainder when 55^{190} is divided by 153.
153 is relatively prime to 55, therefore we can apply Carmichael's theorem.
$\lambda(153) = 48$. $190 = 46 \mod 48$.
$55^{190} \mod 153$
$= 55^{46} \mod 153$

According to Carmichael's theorem, $55^{48} = 1 \mod 153$.
$55^{46} * 55^2 = 1 \mod 153$
$55^{46} * -35 = 1 \mod 153$
Let -R be the remainder when 55^{46} is divided by 153.
$-R * -35 = 1 \mod 153$

$35R = 153m + 1$
$= 140m + 13m + 1$
LHS is a multiple of 35, therefore, RHS is a multiple of 35, therefore, 13m+1 is a multiple of 35, therefore, 13m+1=35a.
$13m = 26a + 9a - 1$
LHS is a multiple of 13, therefore, RHS is a multiple of 13, therefore, 9a-1 is a multiple of 13, therefore, a=3.
$13m = 26*3 + 9*3 - 1$
$m = 2*3 + 2 = 8$

$35R = 140*8 + 13*8 + 1$
$R = 4*8 + 3 = 32 + 3 = 35$

Hence, $55^{190} = -35 \mod 153$ or $55^{190} = 120 \mod 153$.

Find the remainder when 39^{22} is divided by 7. **Quant Capsule - Euler's Theorem**
7 is relatively prime to 39, therefore we can apply Carmichael's theorem.
$\lambda(7) = \mathbf{6}$. $22 = 1 \mod \mathbf{3}$. (Why **3**? Why not **6**?)
$39^{22} \mod 7$
$= 4^{22} \mod 7$
$= 4^1 \mod 7$
$= 4 \mod 7$

MO#1

Find the remainder when b^K is divided by n where n is relatively prime to b.

If b is a perfect square AND two is a factor of $\lambda(n)$ then find the remainder K' when K is divided by $\lambda(n)/2$.
If b is a perfect cube AND three is a factor of $\lambda(n)$ then find the remainder K' when K is divided by $\lambda(n)/3$.
If b is a fourth power of some number AND four is a factor of $\lambda(n)$ then find the remainder K' when K is divided by $\lambda(n)/4$.
and so on.

The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

Find the remainder when 32^{134} is divided by 55.
55 is relatively prime to 32, therefore we can apply Carmichael's theorem.
$\lambda(55) = \mathbf{20}$. As 32 is 2 raised to **five** AND **five** is a factor of **20**, find the remainder K' when 134 is divided by

$\lambda(55) = 20$. As 32 is 2 raised to **five** AND **five** is a factor of **20**, find the remainder R when 134 is divided by $\lambda(55)$/**five**=4. 134 = 2 mod 4. The remainder when 32^{134} is divided by 55 is equal to the remainder when 32^2 is divided by 55.

32^{134} mod 55
= 32^2 mod 55
= 2^{10} mod 55
= 1024 mod 55
= 34 mod 55

Find the remainder when 21^{20} is divided by 37.

37 is relatively prime to 21, therefore we can apply Carmichael's theorem.

21^{20} mod 37
= $(-16)^{20}$ mod 37

$\lambda(37) = 36$. As $16=2^4$ AND 4 is a factor of 36, find the remainder when 20 is divided by $\lambda(37)/4=9$. 20 = 2 mod 9. The remainder when 21^{20} is divided by 37 is equal to the remainder when 21^2 is divided by 37.

21^{20} mod 37
= $(-16)^{20}$ mod 37
= $(-16)^2$ mod 37
= 256 mod 37
= 34 mod 37

Find the remainder when $37^{47^{57}}$ is divided by 16. Quant Capsule - Euler's theorem

$37^{47^{57}} \text{ mod } 16 = 5^{47^{57}} \text{ mod } 16$

16 is relatively prime to 5, therefore we can apply Carmichael's theorem.

$\lambda(16) = 4$. Now, find the remainder when 47^{57} is divided by 4.

$= 47^{57}$ mod 4
$= 3^{57}$ mod 4
$= (-1)^{57}$ mod 4
$= -1$ mod 4
$= 3$ mod 4 [By the way, according to MO#2, $3^{\text{Odd}} = 3$ mod 4.]

Therefore, $5^{47^{57}}$ and 5^3 leave the same remainder when divided by 16.

$5^{47^{57}}$ mod 16
$=5^3$ mod 16
$=25 * 5$ mod 16
$=9 * 5$ mod 16
$=13$ mod 16

Hence, $37^{47^{57}} = 13$ mod 16

What is the remainder when $20^{51^{97}}$ is divided by 17? posted by **Shivam Mehra**

$20^{51^{97}} \text{ mod } 17 = 3^{51^{97}} \text{ mod } 17$

17 is relatively prime to 3, therefore we can apply Carmichael's theorem.

$\lambda(17) = 16$. Now, find the remainder when 51^{97} is divided by 16.

51^{97} mod 16
$= 3^{97}$ mod 16

3 is relatively prime to 16, therefore we can apply Carmichael's theorem.

$\lambda(16) = 4$. Now, find the remainder when 97 is divided by 4.

$97 = 1$ mod 4.

Therefore, 3^{97} and 3^1 leave the same remainder when divided by 16.

3^{97} mod 16
$= 3^1$ mod 6
$= 3$ mod 6

Therefore, $3^{51^{97}}$ and 3^3 leave the same remainder when divided by 17.

$3^{51^{97}}$ mod 17
$=3^3$ mod 17
$=10$ mod 17

Hence, $20^{51^{97}} = 10$ mod 17.

Find the remainder when $97^{97^{97}}$ is divided by 11. posted by **Danger Daddu**

$97^{97^{97}}$ mod 11
$= 9^{97^{97}}$ mod 11

11 is relatively prime to 9, therefore we can apply Carmichael's theorem.

$\lambda(11) = 10$.

As $9=3^2$ AND 2 is a factor of $\lambda(11)=10$; according to MO#1, rather than finding the remainder when 97^{97} is divided by 10, we'll find the remainder when 97^{97} is divided by 10/2=5.

97^{97} mod 5
$= 2^{97}$ mod 5
$= 2^1$ mod 5 [$\lambda(5) = 4$. $97 = 1$ mod 4.]
$= 2$ mod 5

Therefore, $9^{97^{97}}$ and 9^2 give the same remainder when divided by 11.

$9^{97^{97}}$ mod 11
$= 9^2$ mod 11
$= 81$ mod 11
$= 4$ mod 11

Hence, $97^{97^{97}} = 4$ mod 11

Find the remainder when 3^{340} is divided by 341.
341 is relatively prime to 3, therefore we can apply Carmichael's theorem.
$\lambda(341) = 60$. $340 = 40$ mod 60.
3^{340} mod 341
$= 3^{40}$ mod 341 (Now, who's gonna calculate this for ~~me~~?)

To find the remainder R when b^K is divided by n,
- Split the original divisor into two (or three or so) parts, say p and q, such that HCF[p, q]=1 (and n=p*q).
- Then find the individual remainders say R_p and R_q when b^K is divided by each of these parts.
- Solve $R=px+R_p=qy+R_q$ to get the final remainder R.

Find the remainder when 3^{340} is divided by 341.
341=11*13. HCF[11, 13]=1. Both 11 and 13 are relatively prime to 341, therefore we can apply Carmichael's theorem.

$\lambda(11) = 10$. $340 = 0$ mod 10.
3^{340} mod 11
$= 3^0$ mod 11
$= 1$ mod 11
The final remainder is of the form R=11x+1.

$\lambda(13) = 12$. $340 = 4$ mod 12.
3^{340} mod 13
$= 3^4$ mod 13
$= 81$ mod 13
$= 3$ mod 13
The final remainder is of the form R=13y+3.

R=11x+1=13y+3
11x=11y+2y+2
LHS is a multiple of 11, therefore, RHS is a multiple of 11, therefore, 2y+2 is a multiple of 11, therefore, y=10.

R=13*10+3=133.

Hence, $3^{340} = 133$ mod 341.

Find the remainder when 3^{1001} is divided by 1001. posted by **Ankit Kheterpal**
1001=7*11*13. $\lambda(7)=6$. $\lambda(11)=10$. $\lambda(13)=12$.
Let's take 1001=91*11. HCF[91, 11]=1. $\lambda(91)=12$. $\lambda(11)=10$.
(If we take 1001=77*13 then we'll end up with larger values $\lambda(77)=30$ and $\lambda(13)=12$.)

$\lambda(91) = 12$. $1001 = 5$ mod 12.
3^{1001} mod 91
$= 3^5$ mod 91
$= 81 * 3$ mod 91
$= -10 * 3$ mod 91
$= -30$ mod 91
The final remainder is of the form R=91x-30.

$\lambda(11) = 10$. $1001 = 1$ mod 10.
3^{1001} mod 11
$= 3^1$ mod 11
The final remainder is of the form R=11y+3.

R=11y+3=91x-30

11y=91x-33
=88x+3x-33
LHS is a multiple of 11, therefore, RHS is a multiple of 11, therefore, 3x is a multiple of 11, therefore, x=0.

R=91*0-30=-30.

Hence, 3^{1001} = -30 mod 1001 or 3^{1001} = 971 mod 1001.

"Find the remainder when b^K is divided by n." equals **"Find the units digit of b^K in base b."** Why?
A number written in base 10 can be converted to any base B by first dividing the number by B and then dividing the successive quotient by B. The remainders thus obtained, written in reverse order, give the equivalent number in base B.

Let's convert $(56)_{10}$ to base 7.

$$\begin{array}{r|rl} 7 & 56 & \\ \hline & 8 & \mathbf{0} \\ \hline & 1 & 1 \\ & & 1 \end{array}$$

$(56)_{10} = (110)_7$
As you can **see**, we write the first remainder as a last digit of the converted number. Therefore, if we divide any number by base B, then the remainder thus obtained is the units digit of the converted number in base B.

Hence, What is the remainder when b^K is divided by n? and
What is the units digit of b^K in base b?
both are the same puzzles.

Find the units digit of 32^{32} in base 11.
All in all, we need to find the remainder when 32^{32} is divided by 11.
11 is relatively prime to 32, therefore we can apply Carmichael's theorem. λ(11)=10. 32 = 2 mod 10.

32^{32} mod 11
= 10^{32} mod 11
= 10^2 mod 11
= 1 mod 11

Hence, the units digit of 32^{32} in base 11 is 1.

Find the last digit of $41^{43^{45}}$ in base 16.
It's 9.

MO#2

In base b, if both b and b/2 are even, then $(b/2+1)^{ODD}$ ends in **single digit** (b/2+1) and $(b/2+1)^{EVEN}$ ends in 1.

i.e. if both b and b/2 are even, the remainder when $(b/2+1)^{ODD}$ divided by b is (b/2+1) and the remainder when $(b/2+1)^{EVEN}$ divided by b is 1.

If both b and b/2 are even then $(b/2+1)^{ODD}$ = (b/2+1) mod b
$(b/2+1)^{EVEN}$ = 1 mod b

For example, 5^{ODD} = 5 mod 8
5^{EVEN} = 1 mod 8.

What is the remainder when $41^{43^{45}}$ is divided by 16?
b=16=Even. b/2=8=Even. b/2+1=8+1=9. 43^{45}=Odd^{Odd}=Odd.

$41^{43^{45}}$ mod 16
= $9^{43^{45}}$ mod 16
= 9^{Odd} mod 16
= 9 mod 16

MO#3

In base b, if b is even and b/2 is odd, $(b/2)^{Natural\ Number}$ ends in **single digit** b/2.

i.e. if b is even and b/2 is odd, the remainder when $(b/2)^{Natural\ Number}$ divided by b is b/2.

If b is even and b/2 is odd then $(b/2)^{Natural\ Number}$ = b/2 mod b.

For example, $5^{Natural\ Number}$ = 5 mod 10.

What is the remainder when $15^{15^{15}}$ is divided by 30?
b=30=Even. b/2=15=Odd.
$15^{15^{15}}$ mod 30

$= 15^{\text{Natural Number}} \bmod 30$
$= 15 \bmod 30$

> The modulo order e of b (mod n) is always a factor of λ(n).
>
> To find the modulo order e of b (mod n)
> First find all the factors of λ(n).
> Then find the smallest factor e such that $b^e = 1 \bmod n$.

Find the modulo order of 2 (mod 7).
7 is relatively prime to 2. λ(7)=6. The factors of 6 are 1, 2, 3 and 6. Therefore, the modulo order of 2 (mod 7) is 1 or 2 or 3 or 6.

$2^1 \bmod 7 = 2 \bmod 7$
$2^2 \bmod 7 = 4 \bmod 7$
$2^3 \bmod 7 = 1 \bmod 7$

Hence, the modulo order of 2 (mod 7) is 3.

MO#4

> In base n, if b^K ends in **single digit** (n-1), then b^{2K} ends in 1.
>
> i.e. if the remainder when b^K divided by n is (n-1), then the remainder when b^{2K} divided by n is 1.
>
> If $b^K = -1 \bmod n$
> then $b^{2K} = +1 \bmod n$

Find the modulo order of 19 (mod 100).
100 is relatively prime to 19. λ(100)=20. The factors of 20 are 1, 2, 4, 5, 10 and 20. Therefore, the modulo order of 19 (mod 100) is 1 or 2 or 4 or 5 or 10 or 20.

$19^1 \bmod 100 = 19 \bmod 100$
$19^2 \bmod 100 = 61 \bmod 100$
$19^4 \bmod 100 = 61*61 \bmod 100 = 21 \bmod 100$
$19^5 \bmod 100 = 21*19 \bmod 100 = 99 \bmod 100 = -1 \bmod 100$

Therefore, $19^{2*5} = +1 \bmod 100$

Hence, 10 is the modulo order of 19 (mod 100).

MO#1 Reloaded

> The modulo order e of b (mod n) is always factor of λ (n).
>
> If b is a perfect square AND two is a factor of λ(n) then e is a factor of λ(n)/2.
> If b is a perfect cube AND three is a factor of λ(n) then e is a factor of λ(n)/3.
> If b is a fourth power of some number AND four is a factor of λ(n) then e is a factor of λ(n)/4.
> and so on.

Find the total number of all natural numbers n for which 111 divides 16^n - 1, where n is less than 1000. posted by **Software Engineer**
111 is relatively prime to 16. λ(111)=36. As $16=2^4$ AND 4 is a factor of 36, the modulo order e of 16 (mod 111) is a factor of 36/4=9. The factors of 9 are 1, 3 and 9. Therefore, the modulo order of 16 (mod 111) is 1, 3 or 9.

$16^1 \bmod 111 = 16 \bmod 111$
$16^3 \bmod 111 = 256 * 16 \bmod 111 = 34 * 16 \bmod 111 = 100 \bmod 111$

The only remaining possibility is 16^9, therefore the remainder when 16^9 divided by 111 must be 1.
$16^9 = 1 \bmod 111$ (without calculating it)

Therefore, according to Carmichael's Theorem,
$16^9 - 1 = 0 \bmod 111$
$16^{9*2} - 1 = 0 \bmod 111$
$16^{9*3} - 1 = 0 \bmod 111$
and so on.

The sequence formed by the exponents is an Arithmetic Progression:- 9, 18, 27, ... E
where E is the last term and it is less than 1000.

For the last term E,
$9 + (n-1)*9 < 1000$
$9n < 1000$
$n < 111.1$
$n = 111$
Hence, n can assume 111 distinct values such that 111 divides 16^n - 1 and n is less than 1000.

Hence, n can assume 111 distinct values such that 111 divides $16^n - 1$ and n is less than 1000.

If e is the modulo order of b (mod n), then $(b^1 + b^2 + b^3 + ... + b^e)$ is divisible by n.
Similarly, since $\lambda(n)$ is a multiple of e, $(b^1 + b^2 + b^3 + ... + b^{\lambda(n)})$ is divisible by n.

$(b^1 + b^2 + b^3 + ... + b^e) = 0 \mod n$
$(b^1 + b^2 + b^3 + ... + b^{\lambda(n)}) = 0 \mod n$

What is the remainder when $19^0 + 19^1 + 19^2 + ... + 19^{9001}$ is divided by 100?
100 is relatively prime to 19. $\lambda(100)=20$. Therefore, $(19^1 + 19^2 + ... + 19^{20})$ is divisible by 100.

$19^0 + (19^1 + 19^2 + 19^3 + ... + 19^{20})$
$+ (19^{21} + 19^{22} + 19^{23} + ... + 19^{40})$
$+ (19^{41} + 19^{42} + 19^{43} + ... + 19^{60})$
+..
$+ (19^{9001})$ mod 100
$= (1 + 0 + 0 + 0 + ... + 19^{9001})$ mod 100
$= (1 + 19^1)$ mod 100 [9001 = 1 mod 20]
= 20 mod 100

What is the remainder when $19^0 + 19^1 + 19^2 + ... + 19^{91}$ is divided by 100?
100 is relatively prime to 19. $\lambda(100)=20$. The factors of 20 are 1, 2, 4, 5, 10 and 20. Therefore, the modulo order of 19 (mod 100) is 1 or 2 or 4 or 5 or 10 or 20.

19^1 mod 100 = 19 mod 100
19^2 mod 100 = 61 mod 100
19^4 mod 100 = 61*61 mod 100 = 21 mod 100
19^5 mod 100 = 21*19 mod 100 = 99 mod 100 = -1 mod 100

Therefore, 19^{2*5} = +1 mod 100. Therefore, 10 is the modulo order of 19 (mod 100).

Therefore, $(19^1 + 19^2 + ... + 19^{10})$ is divisible by 100.
91 = 1 mod 10. Therefore, $(19^1 + 19^2 + ... + 19^{90})$ is divisible by 100.

$19^0 + (19^1 + 19^2 + 19^3 + ... + 19^{90}) + 19^{91}$ mod 100
$= 1 + (0) + 19^1$ mod 100 [91 = 1 mod 20]
= 20 mod 10
= 0 mod 10

So far we have solved some puzzles like 'Find the remainder when b^K is divided by n where n is relatively prime to b'. Now, let's solve some puzzles like 'Find the remainder when b^K is divided by n where n is **NOT** relatively prime to b'.

MO#5

In base b, if b is even and b/2 is odd, $(b/2+1)^{\text{Natural Number}}$ ends in **single digit** (b/2+1).

i.e. if b is even and b/2 is odd, the remainder when $(b/2+1)^{\text{Natural Number}}$ divided by b is (b/2+1).

If b is even and b/2 is odd then $(b/2+1)^{\text{Natural Number}} = (b/2+1) \mod b$.

For example, $6^{\text{Natural Number}} = 6 \mod 10$.

What is the remainder when 4^{96} is divided by 6? A. 3 B. 2 C. 4 D. 0 (CAT 2003)
b=6=Even. b/2=3=Odd. b/2+1=3+1=4.
$4^{\text{Natural Number}} = 4 \mod 6$.
Hence, (C).

Find the remainder when b^K is divided by n where n is NOT relatively prime to b.
As n is not relatively prime to b, there must be some highest common factor that divides both b and n.
Let p = HCF[b, n] and q = n/p.

After performing this operation, there are two possible possibilities:-
Either p and q are relatively prime to each other
Or p and q are NOT relatively prime to each other.

Possibility#1 p and q are relatively prime to each other

Carmichael#1

Find the remainder when b^K is divided by n where n is not relatively prime to b.

Find p=HCF[b, n] and q=n/p.

If p and q are relatively prime to each other
then Find the remainder K' when K is divided by $\lambda(q)$.
If $K' \neq 0$

If $K' > 0$

The remainder when b^K is divided by n is equal to the remainder when $b^{K'}$ is divided by n.

Otherwise

The remainder when b^K is divided by n is equal to the remainder when $b^{\lambda(q)}$ is divided by n.

Find the remainder when 2^{1990} is divided by 1990. posted by **Rajarshi Guha**
1990 is not relatively prime to 2, therefore we can't apply Carmichael's theorem.

p=HCF[2, 1990]=2 and q=1990/2=995.
As p=2 and q=995 are relative prime to each other, we can apply Carmichael#1.

$\lambda(995) = 396$. $1990 = 10 \bmod 995$.
The remainder when 2^{1990} is divided by 1990 is equal to the remainder when 2^{10} is divided by 1990.

$2^{1990} \bmod 1990$
$= 2^{10} \bmod 1990$
$= 1024 \bmod 1990$

The number 84^{86} when converted to base 210 ends in digit ____. posted by **Software Engineer**
210 is not relatively prime to 84, therefore we can't apply Carmichael's theorem.

p=HCF[84, 210]=42 and q=210/42=5.
As p=42 and q=5 are relative prime to each other, we can apply Carmichael#1.

$\lambda(5) = 4$. $86 = 2 \bmod 4$.
The remainder when 84^{86} is divided by 210 is equal to the remainder when 84^2 is divided by 210.

$84^{86} \bmod 210$
$= 84^2 \bmod 210$
$= 126 \bmod 1990$

Hence, the required **single digit number** is **126** in base 210. (If IIMs ever ask this question in CAT, one possible option will be **6**.)

Find the remainder when 12^{600} is divided by 100.
100 is not relatively prime to 12, therefore we can't apply Carmichael's theorem.

p=HCF[12, 100]=4 and q=100/4=25.
As p=4 and q=25 are relative prime to each other, we can apply Carmichael#1.

$\lambda(25)=20$. $600 = \mathbf{0 \bmod 20}$.
The remainder when 12^{600} is divided by 100 is equal to the remainder when $\mathbf{12^{20}}$ is divided by 100.

$12^{20} \bmod 100$
$= 4^{20} * 3^{20} \bmod 100$
$= 4^{20} * 3^{20} \bmod 100$ (HCF[3, 100]=1, $\lambda(100) = 20$, $3^{20} = 1 \bmod 100$)
$= 76 * 01 \bmod 100$ (According to MO#1, $4^{20} \bmod 100 = 4^{10} \bmod 100 = 2^{20} \bmod 100 = 76 \bmod 100$)
$= 76 \bmod 100$

Therefore, $12^{600} = 76 \bmod 100$.

Note: In Carmichael#1,
- p always divides b, because p is a factor of b. Therefore, the final remainder is of the form R=p*x.
- As HCF[b, q]=1 we can apply the Carmichael's Theorem to get the remainder R_q when b^K is divided by q, therefore, the final remainder is also of the form R=qy+ R_q.

Therefore, the final remainder R when b^K is divided by n is of the form $R=p*x=q*y+R_q$

Carmichael#1 Reloaded

Find the remainder when b^K is divided by n where n is not relatively prime to b.

Find HCF[b, n]=p and q=n/p.

If p and q are relatively prime to each other
then Find the remainder R_q when b^K is divided by q.
Solve $R=px=qy+R_q$ to get the final remainder R.

Find the remainder when 12^{1350} is divided by 68.
68 is not relatively prime to 12, therefore we can't apply Carmichael's theorem.

p=HCF[12, 68]=4 and q=68/4=17.
As p=4 and q=17 are relative prime to each other, we can apply Carmichael#1 Reloaded.

Now, find the remainder when 12^{1350} is divided by q=17. $\lambda(q)=\lambda(17)=16$. $1350 = 6 \bmod 16$.
$12^{1350} \bmod 17$
$= 12^6 \bmod 17$
$= 144 * 144 * 144 \bmod 17$

= 8 * 8 * 8 mod 17
= 64 * 8 mod 17
= 13 * 8 mod 17
= 2 mod 17

Now, R=4x=17y+2
=16y+y+2
LHS is a multiple of 4, therefore, RHS is a multiple of 4, therefore, y+2 is a multiple of 4, therefore, y=2.
R=17*2+2=36

Therefore, 12^{1350} = 36 mod 68.

Find the remainder when 2^{1990} is divided by 1990. posted by **Rajarshi Guha**
1990 is not relatively prime to 2, therefore we can't apply Carmichael's theorem.

p=HCF[2, 1990]=2 and q=1990/2=995.
As p=2 and q=995 are relative prime to each other, we can apply Carmichael#1 Reloaded.

Now, find the remainder when 2^{1990} is divided by q=995. λ(995) = 396. 1990 = 10 mod 995.
2^{1990} mod 995
= 2^{10} mod 995
= 29 mod 995

Now, R=2x=995y+29
=497y+y+28+1
LHS is a multiple of 2, therefore, RHS is a multiple of 2, therefore, y+1 is a multiple of 2, therefore, y=1.
R=995*1+29=1024

Therefore, 2^{1990} = 1024 mod 1990.

Find the remainder when 12^{600} is divided by 100.
100 is not relatively prime to 12, therefore we can't apply Carmichael's theorem.

p=HCF[12, 100]=4 and q=100/4=25.
As p=4 and q=25 are relative prime to each other, we can apply Carmichael#1 Reloaded.

Now, find the remainder when 12^{600} is divided by q=25. λ(q)=λ(25)=20. 600 = 0 mod 20.
12^{600} mod 25
= 12^{0} mod 25
= 1 mod 25

Now, R=4x=25y+1
=24y+y+1
LHS is a multiple of 4, therefore, RHS is a multiple of 4, therefore, y+1 is a multiple of 4, therefore, y=3.
R=25*3+1=76

Therefore, 12^{1350} = 76 mod 68.

The number 84^{86} when converted to base 210 ends in digit ____. posted by **Software Engineer**
210 is not relatively prime to 84, therefore we can't apply Carmichael's theorem.

p=HCF[84, 210]=42 and q=210/42=5.
As p=42 and q=5 are relative prime to each other, we can apply Carmichael#1 Reloaded .

λ(q)=λ(5)=4. 86 = 2 mod 4.

= 84^{86} mod 5
= $(-1)^{86}$ mod 5
= 1 mod 5

Now, R=42x=5y+1
5y=40x+2x-1
LHS is a multiple of 5, therefore, RHS is a multiple of 5, therefore, 2x-1 is a multiple of 5, therefore, x=3.

R=42*3=126.

Hence, the required **single digit number** is **126** in base 210. (If IIMs ever ask this question in CAT, one possible option will be **6**.)

Find the remainder when b^K is divided by n where n is NOT relatively prime to b.
As n is not relatively prime to b, there must be some highest common factor that divides both b and n.
Let p = HCF[b, n] and q = n/p.

After performing this operation, there are two possible possibilities:-
Either p and q are relatively prime to each other
Or p and q are NOT relatively prime to each other.

Possibility#2 p and q are NOT relatively prime to each other
If p and q are not relatively prime to each other, then we'll assign some **new values** to p and q such that HCF of p and q becomes 1.

Let H be the HCF of b and n, H=HCF[b, n].
Now, split the divisor n into two divisors p and q such that (i.e. n=p*q)

- p is a multiple of H
- HCF[H, q]=1

Now, p and q are relatively prime to each other.

For example,
Find the remainder when 22^{67} is divided by 100.

p=HCF[22, 100]=2 and q=100/2=50.
As p and q are not relatively prime to each other, we can't apply Carmichael#1. Now, we'll assign some new values to both p and q such that HCF of p and q becomes 1.

H=HCF[22, 100]=2.
Now, split n=100 into two divisors p and q such that p is a multiple of H=2 and HCF[H, q]=1 (and 100=p*q).
(p, q)=(4, 25).
Now, p=4 and q=25 are relatively prime to each other.

Carmichael#2

Find the remainder when b^K is divided by n where n is not relatively prime to b.

First try to apply **Carmichael#1**; if it can't be applied then

Find H=HCF[b, n].
Split the divisor n into two divisors p and q such that p is a multiple of H and HCF[H, q]=1 (and n=p*q).
Find the remainder R_q when b^K is divided by q.
Find the positive integer m such that $H^m=p$.

If K ≥ m
    Solve $R=px=qy+R_q$ to get the final remainder R.
Otherwise
    Solve $R=Hx=qy+R_q$ to get the final remainder R.

Find the remainder when 2^{2004} is divided by 2004. posted by **Dipankar Gosh**
2004 is not relatively prime to 2, therefore we can't apply Carmichael's theorem.

p=HCF[2, 2004]=2 and q=2004/2=1002.
As p=2 and q=1002 are NOT coprime, we can't apply Carmichael#1.

Now, H=HCF[2, 2004]=2. New values:- (p, q)=(4, 501).

Now, find the remainder when 2^{2004} is divided by q=501.
λ(q)=λ(501)=166. 2004 = 12 mod 166.

2^{2004} mod 501
= 2^{12} mod 501
= 1024 * 4 mod 501
= 22 * 4 mod 501
= 88 mod 501

H=2 and p=4, therefore, $2^2=4$, therefore m=2.

As K=2004 ≥ m=2
R=4x=501y+88
    =500y + y + 88.
LHS is a multiple of 4, therefore, RHS is a multiple of 4, therefore, y is a multiple of 4, therefore, y=0.
R=501*0+88=88

Therefore, 2^{2004} = 88 mod 2004.

Find the remainder when 22^{1352} is divided by 52.
52 is not relatively prime to 22, therefore we can't apply Carmichael's theorem.

p=HCF[22, 52]=2 and q=52/2=26.
As p=2 and q=26 are NOT relative prime to each other, we can't apply Carmichael#1.

Now, H=HCF[22, 52]=2. New values:- (p, q)=(4, 13).

Now, find the remainder when 22^{1352} is divided by q=13.
22^{1350} mod 13
= 9^{1350} mod 13
= 9^2 mod 13   [λ(q)=λ(13)=12. As $9=3^2$ AND 2 is a factor of λ(13)=12, 1352 = 2 mod (12/2).]
= 3 mod 13

H=2 and p=4, therefore, $2^2=4$, therefore m=2.

As K=1352 ≥ m=2
R=4x=13y+3
=12y+y+3
LHS is a multiple of 4, therefore, RHS is a multiple of 4, therefore, y+3 is a multiple of 4, therefore, y=1.
R=13*1+1=14

Therefore, $22^{1352} = 14 \bmod 52$.

Summary

Find the remainder when b^K is divided by n.

IF n is relatively prime to b
Apply **Carmichael's Theorem**

IF n is not relatively prime to b
Find p=HCF[b, n] and q=n/p.

IF p and q are relatively prime to each other
Apply **Carmichael#1 Reloaded** (or **Carmichael#1**)

Else Apply **Carmichael#2**

Consider the set $S=\{17^0, 17^1, 17^2, 17^3, \ldots, 17^{2009}\}$.
(1). Each member of set T, a subset of S, leaves the same remainder 1 when divided by 26. How many members are there in T?