Application of congruence relation

Ex: 01

Find the remainder of the division of $a = 1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$ by 7.

$$
\begin{array}{r|l}
7 & 1395 \,(199 \\
 & \underline{7} \\
 & 69 \\
 & \underline{63} \\
 & 65 \\
 & \underline{63} \\
 & 2
\end{array}
\qquad
\begin{array}{r|l}
7 & 675 \,(96 \\
 & \underline{63} \\
 & 45 \\
 & \underline{42} \\
 & 3
\end{array}
\qquad
\begin{array}{r|l}
7 & 12 \,(1 \\
 & \underline{7} \\
 & 5
\end{array}
\qquad
\begin{array}{r|l}
7 & 17 \,(2 \\
 & \underline{14} \\
 & 3
\end{array}
\qquad
\begin{array}{r|l}
7 & 22 \,(3 \\
 & \underline{21} \\
 & 1
\end{array}
$$

$a = 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod 7$

$\equiv 16 \cdot 27 + 15 \pmod 7$

$\equiv 2 \cdot 6 + 1 \pmod 7$

$\equiv 12 + 1 \pmod 7$

$\equiv 5 + 1$

$\equiv 6 \pmod 7$

(Ans)

Example 2: Find the remainder of the division of $a = 53 \cdot 47 \cdot 51 \cdot 43$ by 56

$\equiv (-3) \cdot (-9) \cdot (-5) \cdot (-13) \pmod{56}$

$\equiv 1755 \pmod{56}$

$\equiv 19 \pmod{56}$

(Ans)

Euler's Theorem

$k^{\phi(n)} \equiv 1 \pmod{n}$

) $k^{P-1} \equiv 1 \pmod{P}$

) $\phi(Pq) = (P-1)(q-1)$

) $\phi(p^k) = p^{k}\cancel{\left(1-\frac{1}{p}\right)} = p^k - p^{k-1}$

$\phi(300) = \phi(2^2 \cdot 3 \cdot 5^2)$

$= \phi(2^2)\,\phi(3)\,\phi(5^2)$

$= \cancel{\phi}(2^2-2^1)\,\cancel{\phi}(3^1-3^0)\,\cancel{\phi}(5^2-5^1)$

$= 60$

Number Theory

Compute the remainder

$$\text{rem}\left(24989^{184637} \cdot 673459^{8447}, 15\right)$$

$\text{rem}(24989, 15) = 14$

$\text{rem}(673459, 15) = 4$

$\left(14^{184637} \cdot 4^{8447}\right)$

$\text{rem}(14^1, 15) = 14$	$\text{rem}(4, 15) = 4$
$\text{rem}(14^2, 15) = 1$	$\text{rem}(4^2, 15) = 1$
$\text{rem}(14^3, 15) = 14$	$\text{rem}(4^3, 15) = 4$
$\text{rem}(14^3, 15) = 1$	$\text{rem}(4^3, 15) = 1$

$\left(14^{184637} \cdot 4^{8447}\right)$

$= 14 \cdot 4$

$= 56$

$\text{rem}(56, 15) = 11$.

(Ans) .

CT Q secA

(2) $\text{rem}\left(\left(22215^{3456789} + 7777921\right)^{5555} 37^{6666666} + 22217^{3456789}, 18\right)$

$\text{rem}(3^1, 18) = 3$

$\text{rem}(3^2, 18) = 9$

$\text{rem}(3^3, 18) = 9$

$\text{rem}(3^4, 18) = 9$

$\text{rem}(3^5, 18) = 9$

$\text{rem}(13^1, 18) = 13$

$\text{rem}(13^2, 18) = 7$

$\text{rem}(13^3, 18) = 1$

$\text{rem}(13^4, 18) = 13$

$\text{rem}(13^5, 18) = 7$

$\text{rem}(13^6, 18) = 1$

$\text{rem}(5^1, 18) = 5$

$\text{rem}(5^2, 18) = 7$

$\text{rem}(5^3, 18) = 17$

$\text{rem}(5^4, 18) = 13$

$\text{rem}(5^5, 18) = 11$

$\text{rem}(5^6, 18) = 1$

$\text{rem}(5^7, 18) = 5$

$\text{rem}(5^8, 18) = 7$

$a = 100$
$b = 500$

find lcm using max $lcm(a,b) = ?$

Ans: $a = 2 \times 50 = 2 \times 2 \times 25 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$b = 2 \times 2 \times 125 = 2 \times 2 \times 5 \times 25 = 2 \times 2 \times 5 \times 5 \times 5 = 2^2 \times 5^3$

$$Lcm\ max = 2^{max(2,2)}\ 5^{max(2,3)}$$
$$= 2^2 \cdot 5^3$$
$$= 4 \cdot 125$$
$$= 500.$$

$a = 10$, $b = 25$, $ab = 250$.

Find $gcd(10, 25) = ?$
$LCD(10, 25) = ?$

~~gcd~~

Ans: $10 = 2 \times 5$
$5 = \cancel{5} \times 5 = 5^2$

$\Rightarrow gcd(2^{min(1,0)} \cdot 5^{min(1,2)})$

$\Rightarrow$ ~~gcd~~ $(2^0 \cdot 5^1)$

$\Rightarrow 2^0 \cdot 5^1$

$\Rightarrow 1 \cdot 5$

$\Rightarrow 5$

$LCD = 2^{max(1,0)} \cdot 5^{max(1,2)}$

$= 2^1 \cdot 5^2$

$= 2 \cdot 25$

$= 50$.

(Ans).

Find gcd(2231, 847) by Euclid algorithm

Ans:

$\Rightarrow gcd(847, rem(2231, 899)) = 537$

$\Rightarrow gcd(537, rem(847, 537)) = 310$

$\Rightarrow gcd(310, rem(537, 310)) = 227$

$\Rightarrow gcd(227, rem(310, 227)) = 83$

$\Rightarrow gcd(83, rem(227, 83)) = 61$

$\Rightarrow gcd(61, rem(83, 61)) = 22$

$\Rightarrow gcd(22, rem(61, 22)) = 17$

$\Rightarrow gcd(17, rem(22, 17)) = 5$

$\Rightarrow gcd(5, rem(27, 5)) = 2$

$\Rightarrow gcd(2, rem(5, 2)) = 1$

$\Rightarrow gcd(1, rem(2, 1))$

$\Rightarrow 1.$

(Ans).

Ct Ques A section

$m = \cancel{\beta}\ 2^{9}\ 5^{24}\ 7^{4}\ 11^{7}$

$n = 2^{3}\ 7^{22}\ 11^{211}\ 19^{7}$

$P = 2^{5}\ 3^{4}\ 7^{6042}\ 19^{30}$

find $\gcd(m, n, p)$.

Ans:

$m = 2^{9}\ 3^{0}\ 5^{24}\ 7^{4}\ 11^{7}\ 19^{0}$

$n = 2^{3}\ 3^{0}\ 5^{0}\ 7^{22}\ 11^{211}\ 19^{7}$.

$P = 2^{5} . 3^{4}\ 5^{0}\ 7^{6042}\ 11^{0}\ 19^{30}$

$\gcd = (m, n, p)$

$= 2^{\min(9, \min(3,5))}$

$= 2^{\min(9,3)}$

$= 2^{3}$

$= 8$

(4) Prove that,

if $a \equiv b \pmod{n}$

$c \equiv d \pmod{n}$

then $ac \equiv bd \pmod{n}$

$a \equiv b \pmod{n}$ if $rem(a,n) = rem(b,n)$

assume, $a = 29$, $b = 15$, $n = 7$.

Ans: (a) $7 \overline{)29}(4$
$\underline{28}$
1

(b) $7 \overline{)15}(2$
$\underline{14}$
1

So, $a \equiv b$

assume,

$c = 36$ $d = 22$ $n = 7$

(c) $7 \overline{)36}(5$
$\underline{35}$
1

(d) $7 \overline{)22}(3$
$\underline{21}$
1

So, $c \equiv d$.

$a \times c$

29×36

$= 1044$

$b \times d$

15×22

$= 330$

$7 \overline{)1044}(149$
$\underline{1043}$
1

$7 \overline{)330}(47$
$\underline{329}$
1

So, $ac \equiv bd$.

$rem((9+7)1+17, 18))$

$= rem(16+17, 18)$

$= rem(33, 18)$

$= 15$

(Ans)

③ $n^{13} \equiv n \pmod n$ (prove)

not possible why

↓

n mod n .

CSE 401 (Ackermann function)

$A(1,1) = ?$

$= A(1-1, A(1, 1-1))$

$= A(0, A(1,0))$

$= A(0, A(1-1, 1))$

$= A(0, A(0,1))$

$= A(0, 1+1)$

$= A(0, 2)$

$= 2+1$

$= 3$

$A(2,1) = ?$

$= A(2-1, A(2, 1-1))$

$= A(1, A(2,0))$

$= A(1, A(2-1, 1))$

$= A(1, A(1,1))$

$= A(1, A(1-1, A(1, 1-1)))$

$= A(1, A(0, A(1,0)))$

$= A(1, A(0, A(1-1, 1)))$

$= A(1, A(0, A(0, 1)))$

$= A(1, A(0, 1+1))$

$= A(1, A(0, 2))$

$= A(1, 2+1)$

$= A(1, 3)$

$= A(1-1, A(1, 3-1))$

$= A(0, A(1, 2))$

$= A(0, A(0, A(1,1)))$

$= A(0, A(0, A(1-1, A(1, 0))))$

$= A(0, A(0, A(0, A(1-1, 1))))$

$= A(0, A(0, A(0, A(0, 1))))$

$= A(0, A(0, A(0, 1+1)))$

$= A(0, A(0, 3))$

$= A(0, 4)$

$= 5.$

Probability

CT/

Ques : N coins are tossed simultaneously. Predict the probability of getting at least 2 heads.

If $n = 2$,

Sample space = {{H H}, {H, T}, {T H}, {T, T}}.

= 4.

Sample point = {H, H}

= 1.

$\therefore$ Probability = $\dfrac{\text{Sample point}}{\text{Sample point}} = \dfrac{1}{4}$.

If $n = 3$,

Sample space = {HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}

= 8

Sample point = {HHH, HHT, HTH, THH}

= 4

$\therefore$ Probability = $\dfrac{\text{sample point}}{\text{Sample space}} = \dfrac{4}{8} = \dfrac{1}{2}$.