Date.

PSEUDORANDOM NUMBERS

Formula

$x_{n+1} = (a x_n + c) \bmod m$

let $x_0 = 3$, $a = 7$, $c = 4$, $m = 9$

Solution:

when $n = 0$

$x_{0+1} = (a x_0 + c) \bmod m$

$x_1 = (7 * 3 + 4) \bmod 9 = 25 \bmod 9 = 7$

$\boxed{x_1 = 7}$

when $n = 1$

$x_{1+1} = (a x_1 + c) \bmod m$

$x_2 = (7 * 7 + 4) \bmod 9 = 53 \bmod 9 = 8$

$\boxed{x_2 = 8}$

when $n = 2$

$x_{2+1} = (a x_2 + c) \bmod m$

$x_3 = (7 * 8 + 4) \bmod 9 = 60 \bmod 9 = 6$

$\boxed{x_3 = 6}$

when $n = 3$

$x_{3+1} = (a x_3 + c) \bmod m$

$x_4 = (7 * 6 + 4) \bmod 9 = 46 \bmod 9 = 1$

$\boxed{x_4 = 1}$

when $n = 4$

$x_{4+1} = (a x_4 + c) \bmod m$

$x_5 = (7 * 1 + 4) \bmod 9 = 11 \bmod 9 = 2$

$\boxed{x_5 = 2}$

So on ....

HASHING FUNCTION

Formula

$h(K) = K \bmod m$

m = memory locations , K = Keys (values)

$K = 42, 53, 65, 21, 30, 69, 56, 36, 28, 44$

$\Rightarrow \boxed{m = 10}$

$h(42) = 42 \bmod 10 = 2$
$h(53) = 53 \bmod 10 = 3$
$h(65) = 65 \bmod 10 = 5$
$h(21) = 21 \bmod 10 = 1$
$h(30) = 30 \bmod 10 = 0$
$h(69) = 69 \bmod 10 = 9$
$h(56) = 56 \bmod 10 = 6$ → $6+1 = 7$
$h(36) = 36 \bmod 10 = 6$ → By Applying linear Probing
$h(28) = 28 \bmod 10 = 8$
$h(44) = 44 \bmod 10 = 4$

$h(k, i) = (h(k) + i) \bmod m$

Keys	30	21	42	53	44	65	56	36	28	69
m	0	1	2	3	4	5	6	7	8	9

ENCRYPTION FUNCTION:

$f(P) = (P + K) \bmod 26$

when $K = 3$

$f(P) = (P + 3) \bmod 26$

"UNIVERSITY" Encrypted Message

For U; $f(20) = (20+3) \bmod 26 = 23 \bmod 26 = 23$ (X)
For N; $f(13) = (13+3) \bmod 26 = 16 \bmod 26 = 16$ (Q)
For I; $f(8) = (8+3) \bmod 26 = 11 \bmod 26 = 11$ (L)
For V; $f(21) = (21+3) \bmod 26 = 24 \bmod 26 = 24$ (Y)
For E; $f(4) = (4+3) \bmod 26 = 7 \bmod 26 = 7$ (H)
For R; $f(17) = (17+3) \bmod 26 = 20 \bmod 26 = 20$ (U)
For S; $f(18) = (18+3) \bmod 26 = 21 \bmod 26 = 21$ (V)
For I; $f(8) = (8+3) \bmod 26 = 11 \bmod 26 = 11$ (L)
For T; $f(19) = (19+3) \bmod 26 = 22 \bmod 26 = 22$ (W)
For Y; $f(24) = (24+3) \bmod 26 = 27 \bmod 26 = 1$ (B)

Decrypted Message: "XQLYHUVLWB"

Date

DECRYPTION FUNCTION:

$f^{-1}(P) = (P - K) \bmod 26$

when $K = 5$

$f^{-1}(P) = (P - 5) \bmod 26$

Decrypted Message is
"JCFR"

For J; $f(9) = (9-5) \bmod 26 = 4 \bmod 26 = 4$ (E)
For C; $f(2) = (2-5) \bmod 26 = -3 \bmod 26 = 23$ (X)
For F; $f(5) = (5-5) \bmod 26 = 0 \bmod 26 = 0$ (A)
For R; $f(17) = (17-5) \bmod 26 = 12 \bmod 26 = 12$ (M)

Encrypted Message "EXAM"

G.C.D "Greatest common Divisor" (HCF)

$24 = 2 \times 2 \times 2 \times 3$
$36 = 2 \times 2 \times 3 \times 3$

$GCD = 2 \times 2 \times 3 = 12.$

$17 = 1 \times 17$
$22 = 2 \times 11$

$\boxed{GCD = 1}$

L.C.M -

$24 = 2 \times 2 \times 2 \times 3$
$36 = 2 \times 2 \times 3 \times 3$

L.C.M = Common × Uncommon
$= (2 \times 2 \times 3) \times (2 \times 3) = 12 \times 6$
$= 72.$

Date

$G.C.D\ (a,b) = P_1^{\min(a_1,b_1)}\ P_2^{\min(a_2,b_2)} \cdots P_n^{\min(a_n,b_n)}$

$L.C.M\ (a,b) = P_1^{\max(a_1,b_1)}\ P_2^{\max(a_2,b_2)} \cdots P_n^{\max(a_n,b_n)}$

$120 : 2\times2\times2\times3\times5 = 2^3 . 3 . 5$

$500 : 2\times2\times5\times5\times5 = 2^2 . 5^3 . 3^0 \qquad \therefore 3^0 = 1$

$Gcd\ (120, 500) = 2^{\min(3,2)} . 3^{\min(1,0)} . 5^{\min(1,3)}$

$= 2^2 . 3^0 . 5^1 = 4\times1\times5 = 20.$

$Lcm\ (120, 500) = 2^{\max(3,2)} . 3^{\max(1,0)} . 5^{\max(1,3)}$

$= 2^3 . 3^1 . 5^3 = 8\times3\times125 = 3{,}000.$

$GCd\ (95256, 432) = 2^{\min(3,4)} . 3^{\min(5,3)} . 7^{\min(2,0)}$

$(2^3 3^5 7^2, 2^4, 3^3) = 2^3 . 3^3 . 7^0 = 8*27*1 = 216.$

$L.C.M\ (95256, 432) = 2^{\max(3,4)} . 3^{\max(5,3)} . 7^{\max(2,0)}$

$(2^3 . 3^5 . 7^2, 2^4 . 3^3) = 2^4 * 3^5 * 7^2 = 16*243*49 = 190512.$

Date.

Euclidean Algorithm

Compute. Gcd (120, 500):

Gcd (a, b)

∵ Greater number will be dividend,
∵ Smaller number will be divisor.

$a = qd + r$ Division Algorithm

$500 = (\ )(120) + (\ )$

$500 = (4)(120) + (20)$

$120 = (\ )(20) + (\ )$

$120 = (6)(20) + (0)$

↓
stop

Gcd (120, 500) = 20 Ans

x —— x —— x —— x —— x —— x ——

Compute.
Gcd(91, 287)

$a = qd + r$

$287 = (3)(91) + 14$

$91 = (6)(14) + (7)$

$14 = (2)(7) + 0$

↓
stop

Gcd (91, 287) = 7 Ans

Gcd as linear Combinations

Bezout Theorem

$$\gcd(a,b) = \underline{s}a + \underline{t}b$$

Bezout Coefficients

~~Show~~ Gcd (6,14) as linear combination:

Sol First apply Euclidean algorithm to calculate the gcd (a,b)

$a = qd + r$

$14 = (2)(6) + 2$

$6 = (3)(2) + 0$

$\gcd(6, 14) = 2$

Now rewrite equation in terms of r

$2 = (1)(14) - (2)(6)$

$2 = \underbrace{1 \cdot 14 + (-2)}_{\text{Bezout coefficient}} \cdot 6$

x — x — x — x — x — x — x — x — x — x

Show gcd (252, 198) = 18 as linear combination of 252 and 198

Sol

$a = qd + r$

$252 = (1)(198) + 54$

$198 = (3)(54) + 36$

$54 = (1)(36) + 18$

$36 = (2)(18) + 0$

Now rewrite equation in terms of r

$54 = 1 \cdot 252 - 1 \cdot 198$ — iii

$36 = 1 \cdot 198 - 3 \cdot 54$ — ii

$18 = 1 \cdot 54 - 1 \cdot 36$ — i

Now Substitute eqn (ii) & (iii) in (i)

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

$18 = \underbrace{1 \cdot 54 - 1 \cdot 198 + 3 \cdot 54} = 4 \cdot 54 - 1 \cdot 198$

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

$18 = 4 \cdot 252 - 5 \cdot 198$

$\boxed{18 = (4)(252) + (-5)(198)}$ Ans

1 <u>Linear Congruencies</u>

$$ax \equiv b \pmod m \qquad \text{Find } x.$$

Solve for x : $3x \equiv 4 \pmod 7$.

Sol: First we have find inverse of a.

Here, $a = 3$, $b = 4$, $m = 7$

· To compute first check that $\gcd(a, m) = 1$.

$\gcd(a, m) = \gcd(3, 7) = 1$

$a = qd + r$

$7 = (2)(3) + 1$ → Hence inverse exists

Now we can calculate inverse like,

$$\gcd(a, m) = 1 = as + tm$$

Now $1 = 1 \cdot 7 - 2 \cdot 3$

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

$\gcd(3,7) = 1 = t\ m + s\ a$

inverse can be make positive by adding mod value.

$\Rightarrow \bar{a} = -2$, $m = 7$

Hence $\bar{a} = -2 + 7 = 5$

Now if inverse is correct we can check that

$\because a\bar{a} \equiv 1 \pmod m$

$3 \times 5 \equiv 1 \pmod 7$

$\boxed{15 \equiv 1 \pmod 7}$

Hence correct.

Now finally finding x.

Now multity $\bar{a}$ both side

$$3x \equiv 4 \pmod 7$$

$$\cancel{3} * 5x \equiv 4*5 \pmod 7$$

$$x \equiv 20 \pmod 7$$

$$\boxed{x \equiv 6}$$ Ans

~~We can check the~~ we can also verify the value of x. .

Put $x = 6$

~~Multiply 6 both si~~

$$3x \equiv 4 \pmod 7$$

$$3*6 \equiv 4 \pmod 7$$

$$\boxed{18 \equiv 4 \pmod 7}$$ Hence verified

Q10

Sol Show that 937 is an inverse of 13 modulo 2436

Gc.d (a, m) = (13, 2436)

$a = qd + r$	
$2436 = (187)(13) + 5$	$1 = 3 - 2.1$
$13 = (2)(5) + 3$	$\underline{2} = 5 - 3.1$
$5 = (1)(3) + 2$	$\underline{3} = 13 - 2.5$
$3 = (1)(2) + 1$	$5 = 2436 - 187.13$

$1 = 3-2.1 \Rightarrow 1 = 3 - 1.(5-3.1) = 3-1.5 + 3.1$

$1 = 3.2 - 1.5 = 2.(13-2.5) - 1.5 = 2.13 - 4.5 - 1.5$

$1 = 2.13 - 5.5 = 2.13 - 5(2436 - 187.13)$

$1 = 2.13 - 5.2436 + 935.13$

$1 = (937)(13) + (-5)(2436)$

$\underline{937}$ $\downarrow$ is an inverse

Hence Proved.

⑥ Solve linear congruences using modular inverse.

ⓐ $19x = 4 \pmod{141}$

first we have to find inverse of 19

Sol

$a = dq + r$	
$141 = (19)(7) + 8$	$1 = 3 - 2\cdot1$
$19 = 8\cdot2 + 3$	$2 = 8 - 3\cdot2$
$8 = 3\cdot2 + 2$	$3 = 19 - 8\cdot2$
$3 = 2\cdot1 + 1$	$8 = 141 - 19\cdot7$

$$1 = 3 - 2\cdot1 = 3 - 1\cdot(8 - 3\cdot2) = 3\cdot3 - 8\cdot1$$

$$1 = 3\cdot(19 - 8\cdot2) - 8\cdot1 = 3\cdot19 - 6\cdot\underbrace{8 - 8}\cdot1 = 3\cdot19 - 7\cdot8$$

$$1 = 3\cdot19 - 7(141 - 19\cdot7) = 3\cdot19 - 7\cdot141 + 49\cdot19$$

$$1 = \underbrace{52}_{\text{Inverse}}\cdot19 + (-7)(141)$$

Thus $52\cdot19 \equiv 1 \pmod{141}$, hence 52 is an inverse of 19.

Now multiply 52 both side.

$$\cancel{52}\cdot\cancel{19}x \equiv 52*4 \pmod{141}$$

$$x = 208 \bmod 141$$

$$\boxed{x = 67}$$

It follows that the solution are the integers x satisfying

$$x = (52\cdot19x - 7\cdot141x) \equiv 208 \equiv 67 \pmod{141}$$

$x \equiv 2 \pmod 3$; $x \equiv 1 \pmod 4$; $x \equiv 3 \pmod 5$

Given : $a_1 = 2$, $m_1 = 3$; $a_2 = 1$, $m_2 = 4$; $a_3 = 3$, $m_3 = 5$

Find : $m = ?$; $M_1, M_2, M_3 = ?$; $y_1, y_2, y_3 = ?$

1st we find m ; $m = m_1 * m_2 * m_3 = 3 \times 4 \times 5 = 60$

Now $M_1 = \frac{m}{m_1} = \frac{60}{3} = 20$; $M_2 = \frac{m}{m_2} = \frac{60}{4} = 15$; $M_3 = \frac{60}{5} = 12$

Now y_1

$y_1 = 20 \bmod 3$

$a = dq + r$

$20 = 3 * 6 + 2$	$1 = 3 - 2.1$
$3 = 2(1) + 1$	$2 = 20 - 3.6$

$1 = 3 - 1.(20 - 3.6)$

$1 = 3 - 1 \cdot 20 + 3.6$

$1 = 7.3 + \underline{(-1)}(20)$

$\bar{a} + m$

Hence $-1 + 3 = 2$ is an inverse

Now y_2.

$y_2 = 15 \bmod 4$

$a = dq + r$

$15 = 4 * 3 + 3$	$1 = 4 - 3.1$
$4 = 3(1) + 1$	$3 = 15 - 4.3$

$1 = 4 - 1.(15 - 4.3) = 4 - 15 + 4.3$

$1 = \underline{(-1)}(15) + 4.4$

$\bar{a} + m$

Here $-1 + 4 = 3$ is an inverse

Now y_3

$y_3 = 12 \bmod 5$

$a = dq + r$

$12 = (5)(2) + 2$	$1 = 5 - 2.2$
$5 = (2)(2) + 1$	$2 = 12 - 5.2$

$1 = 5 - 2.(12 - 5.2)$

$1 = 5 - 2.12 + 4.5 = \underline{(-2)}(12) + 5.5$

Now $\bar{a} + m$

$-2 + 5 = 3$ is an inverse

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x = (2 * 20 * 2) + (1 * 15 * 3) + (3 * 12 * 3)$

$x = 80 + 45 + 108 = 233 \bmod 60$

$\boxed{x = 53}$

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

Sol Given $a_1 = 2, m_1 = 3$; $a_2 = 3, m_2 = 5$; $a = 2$, $m\,7$

find $x = ?$ $y_1 = ?$, $y_2 = ?$, $y_3 = ?$ $M_1, M_2, M_3, m = ?$

Let $m = m_1 * m_2 * m_3$

$$\boxed{m = 3 * 5 * 7 = 105}$$

Now,

$M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$; $M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

$x = 233 \bmod 105$

$\boxed{x = 23}$ Answer

Now,

for y_k we have to find inverse of $M_k \bmod m_k$

where $k = 1, 2, 3$ - - - . $y_k = \overline{M_k} \bmod m_k$

$y_1 = \underset{\downarrow \text{inverse}}{\underline{35}} \bmod 3$

$a = qd + r$

$35 = (11)(3) + 2$

$3 = (1)(2) + 1$

$2 = (1)(2) + 0$

$\rightarrow 1 = 3 - 2 \cdot 1$

$2 = 35 - 11 \cdot 3$

$1 = 3 - 1 \cdot (35 - 11 \cdot 3)$

$1 = 3 - 1 \cdot 35 - 11 \cdot 3$

$1 = -10 \cdot 3 - 1 \cdot 35$

$1 = (-1)(35) + (-10)(3)$

Inverse can't be negative

So add m into it

$-1 + 3 = 2$ is an

$y_2 = 21 \bmod 5$

$a = qd + r$

$21 = (4)(5) + 1$

$5 = (5)(1) + 0$

$\Rightarrow 1 = \underset{\downarrow}{(1)} \cdot 21 + (4)(5)$

is an inverse

$y_3 = 15 \bmod 7$

$a = dq + r$

$15 = (7)(2) + 1$

$7 = (1)(7) + 0$

$\Rightarrow 1 = (1) \cdot 15 + (7)(-2)$

is an inverse

Q//

$x \equiv 4 \pmod 5$
$x \equiv 6 \pmod 8$
$x \equiv 8 \pmod 9$

<u>Given</u>: $a_1 = 4, m_1 = 5, a_2 = 6, m_2 = 8$
$a_3 = 8, m_3 = 9$
find: $m = ?, M_1 = ?, M_2 = ?, M_3 = ?$
$y_1 = ?, y_2 = ?, y_3 = ?$

1st we find m; $m = m_1 * m_2 * m_3 = 5 \times 8 \times 9 = 360$

$M_1 = \frac{m}{m_1} = \frac{360}{5} = 72$; $M_2 = \frac{m}{m_2} = \frac{360}{8} = 45$; $M_3 = \frac{m}{m_3} = \frac{360}{\cancel{8}9} = 40$

Now $y_1, y_2, y_3 = ?$
$y_k = \overline{M_k} \bmod m$

<u>For y_1 = ?</u>

inverse??

$y_1 = \overline{72} \bmod 5$

$a = qd + r$
$72 = (14)(5) + 2$
$(5) = (2)(2) + 1$

$\Rightarrow 1 = 5 - 2.2$; $2 = 72 - 14.5$
$1 = 5 - 2(72 - 14.5)$
$1 = 5 - 2.72 + 28.5 = 29(5) + 72(-2)$

since
-2 is negative, hence have to add $m = 5$

So, $-2 + 5 = 3$ is an inverse

<u>For y_2</u>:

inverse

$y_2 = \overline{45} \bmod 8$

$a = qd + r$
$45 = (5)(8) + 5$
$8 = (1)(5) + 3$
$5 = (1)(3) + 2$
$3 = (1)(2) + 1$

$1 = 3 - 2.1$; $2 = 5 - (1)(3)$
$3 = 8 - (1)(5)$; $5 = 45 - 5.8$

Now

$1 = 3 - 2(1) = 3 - (1)(5 - 1.3)$
$1 = 3 - 5 + 1.3 = 2.3 - 5.1$
$1 = 2(8 - 5.1) - 5.1 = 2.8 - 5.2 - 5.1$
$1 = 2.8 - 5.3 = 2.8 - 3(45 - 5.8)$
$1 = 2.8 - 3.45 + \cancel{1}5.8 = 17.8 + (-3)(45)$

Since -3 so we have to add m, Therefore $-3 + 8 = 5$ is an inverse

<u>For y_3</u>:

$y_3 = \overline{40} \bmod 9$

$a = qd + r$

$40 = (4)(9) + 4$
$9 = (2)(4) + 1$
$4 = (4)(1) + 0$

$4 = 40 - 4.9$
$1 = 9 - 2.4$

$1 = 9 - 2(40 - 4.9) = 9 - 2.40 + 8.9$
$1 = 9.9 - 2.40$

inverse $= -2 + 9 = 7$

Putting values into formula

$x = 4454 \bmod 360$

$\boxed{x = 134}$

Fermat's Little Theorem

$\because a^{P-1} \equiv 1 \pmod P$ $\therefore P$ is Prime

Find $2^{50} \bmod 17$

Sol

$2^{17-1} \equiv 1 \pmod{17} \Rightarrow \boxed{2^{16} = 1 \pmod{17}}$

$\Rightarrow 2^{50}_{\bmod 17} \equiv 2^{16\times3+2} \bmod (17)$ ~~brea~~ $a = qd + r$

$50 = 16\times3 + 2$

$\equiv (2^{16})^3 \cdot 2^2 \pmod{17}$

$\equiv (1)^3 \cdot 4 \bmod 17$

$\equiv 4$ Ans

Find $4^{532} \bmod 11$

Sol

$4^{11-1} \equiv 1 \pmod{11} \Rightarrow \boxed{4^{10} \equiv 1 \pmod{11}}$

$\Rightarrow 4^{532} \bmod 11 \equiv 4^{10\times53+2} \bmod 11$

$\equiv (4^{10})^{53} \cdot 4^2 \bmod 11$

$\equiv (1)^{53} \cdot 4^2 \bmod 11$

$\equiv 16 \bmod 11$

$\equiv 5$ Ans

Date:

Find $5^{300} \bmod 7$

Sol

$$5^{7-1} \equiv 1 \pmod 7 \Rightarrow \boxed{5^6 \equiv 1 \pmod 7}$$

$$\begin{aligned}
5^{300} \bmod 7 &\equiv 5^{6\times 50+0} \bmod 7 \\
&\equiv (5^6)^{50} \cdot 5^0 \bmod 7 \\
&\equiv (1)^{50} \cdot 1 \bmod 7 \\
&\equiv 1 \bmod 7 \equiv 1
\end{aligned}$$

Ans

Find $7^{222} \bmod 11$

Sol:

$$7^{11-1} \equiv 1 \pmod{11} \Rightarrow \boxed{7^{10} \equiv 1 \pmod{11}}$$

$$\begin{aligned}
7^{222} \bmod 11 &\equiv 7^{22\times 10+2} \bmod 11 \\
&\equiv (7^{10})^{22} \cdot 7^2 \bmod 11 \\
&\equiv (1)^{22} \cdot 49 \bmod 11 \\
&\equiv 49 \bmod 11 \\
&\equiv 5
\end{aligned}$$

Ans