Fast Modular Exponentiation

$3^{100} \bmod 15$

(1) $(100)_{10} = (??)_2 = (1100100)_2$

(2)

1	1	0	0	1	0	0
3	12	9	6	3	9	6

(3) $3^2 \bmod 15 = 9 \bmod 15 = 9.$
$9 \times 3 \bmod 15 = 27 \bmod 15 = 12.$

(4) $12^2 \bmod 15 = 144 \bmod 15 = 9.$

(5) $9^2 \bmod 15 = 81 \bmod 15 = 6$

(6) $6^2 \bmod 15 = 36 \bmod 15 = 6$
$6 \times 3 \bmod 15 = 18 \bmod 15 = 3$

(7) $3^2 \bmod 15 = 9.$

(8) $9^2 \bmod 15 = 81 \bmod 15 = 6$

$\therefore 3^{100} \bmod 15 = 6$

Randall Hayman

Fermat's theorem:

If p is a prime number then

x^{p-1} ~~mod~~ $\equiv 1 \pmod{37}$

eg. $40^{110} \bmod 37$.

$40 \equiv 3 \pmod{37}$

$\therefore 40^{110} \bmod 37 = 3^{110} \bmod 37$

By Fermat's Little Theorem.

$3^{36} \equiv 1 \pmod{37}$

$110 = 3(36) + 2$

$3^{110} = 3^{3(36)+2}$

$= (3^{36})^3 \cdot 3^2$

$= 1^3 \cdot 3^2$

$= 9$

$3^{94} \pmod{17}$

$94 = 64 + 16 + 8 + 4 + 2$

$3^2 = 9 \pmod{17} = 9.$

$3^4 = 81 = \cancel{81m}$

$3^4 \pmod{17} = 81 \bmod 17 = 13, \quad 17 - 13 = -4$

$3^8 \bmod 17 = (3^4)^2 \bmod 17 = (-4)^2 = 16 \bmod 17 \equiv -1$

$3^{16} \bmod 17 = (3^8)^2 \bmod 17 \equiv (-1)^2 \equiv 1$

$3^{64} \bmod 17 = (3^{16})^4 \bmod 17 \equiv 1^4 \bmod 17 = 1$

$3^{94} \bmod 17 = 3^{(64+16+8+4+2)} \bmod 17$

$= \cancel{(3^{64})}$

$= (3^{64} \bmod 17)(3^{16} \bmod 17)(3^8 \bmod 17).$
$(3^4 \bmod 17)(3^2 \bmod 17)$

$= (1)(1)(-1)(-4)(9) \bmod 17$

$= 36 \bmod 17 = \cancel{3}$

$= 2.$

$3^{1000} \pmod{26}$

$3^2 = 9 \pmod{26} = 9$

$3^3 = 27 \mod 26 = 1$

$1000 = 3(333) + 1$

$3^{1000} = 3^{[3(333)+1]}$

$\equiv (3^3)^{333} \cdot 3^1$

$\equiv (27)^{333} \cdot 3^1$

$= 1 \cdot 3$

$= 3$