Basic Maths for DSA

cire of Erathostherus Erry nurky as print O \$1 not prime toom 1×0

GCD=HCF Euclids algorithm G(P(a,b) = G(P(a,b))eg 12, 8 G(P(12-8,6) OT CD (4,8) GCD (8-4. 67(8(0,4)

For Modulo do

(a+b)./. m=[a./.m+b./.m]./.m $(a * b) \cdot J \cdot m = (a \cdot l \cdot m) * (b \cdot l \cdot m)$ (a/b) · /· m => lade force Fast Esponential $a^{b} = \frac{b/2}{2}$ $a^{b/2} = \frac{b/2}{2}$ $a^{b/2} = \frac{2}{2}$ $a^{b/2} = \frac{2}{2}$ $a^{b/2} = \frac{2}{2}$