Note Title 5/6/2016

HW5 #12 $e = 109$

$N = 221 = 13 \cdot 17$

$\phi = (13-1)(17-1) = 12 \cdot 16 = 144 + 48 = 192.$

decryption key d: is $e \cdot d \bmod \phi = 1.$

$d \cdot 109 \bmod 192 = 1.$

if $\gcd(109, 192) \neq 1 \Rightarrow$ no d.

message m: $m^{109} \bmod 221 = c.$

$c^d \bmod 221 = m.$

HW5 #10

$(46)^{39} \bmod 11$

$39 = 32 + 4 + 2 + 1$

mod 11

$46^1 \bmod 11 \quad 46^2 \quad 46^4 \quad 46^8 \quad 46^{16} \quad 46^{32}$

$46 \bmod 11 = 2 \quad 2^2 \bmod 11 = 4 \quad 4^2 \bmod 11 = 5 \quad 5^2 \bmod 11 = 3 \quad 3^2 \bmod 11 = 9 \quad 9^2 \bmod 11 = 4$

$2 \cdot 4 \cdot 5 \cdot 4 \bmod 11 = (8 \bmod 11)(20 \bmod 11) \bmod 11$

$= 8 \cdot 9 \bmod 11 =$

$72 \bmod 11 = \boxed{6}$

$(46)^{39} = 46^{32+4+2+1} = 46^{32} \cdot 46^4 \cdot 46^2 \cdot 46^1$

$39 = (1\,0\,0\,1\,1\,1)_2$

$2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$

$2^5 = 32$ $2^2 = 4 > 1$

HW4 #5 if $a|b$ then $a|(bc)$

$b = a \cdot n$ $bc = c \cdot a \cdot n$

bc multiple of a.

$a|bc$.

Example $a|bc$ $a \nmid b$ $a \nmid c$.

$b = 4$ $a = 6$ $6|36 = 4 \cdot 9$.

$c = 9$

$6 \nmid 4$ $6 \nmid 9$.

9c HW 5 $(DDDDDDDD)_{16}$

$(3|3|3|3|3|3|3|3)_4$.

D → base 4

13 → 3 1

4's 1's

13 mod 4 = 1

13 div 4 = 3

$4^{(2)} = 16$

base 7 → base 8

$(362)_7$ → decimal.

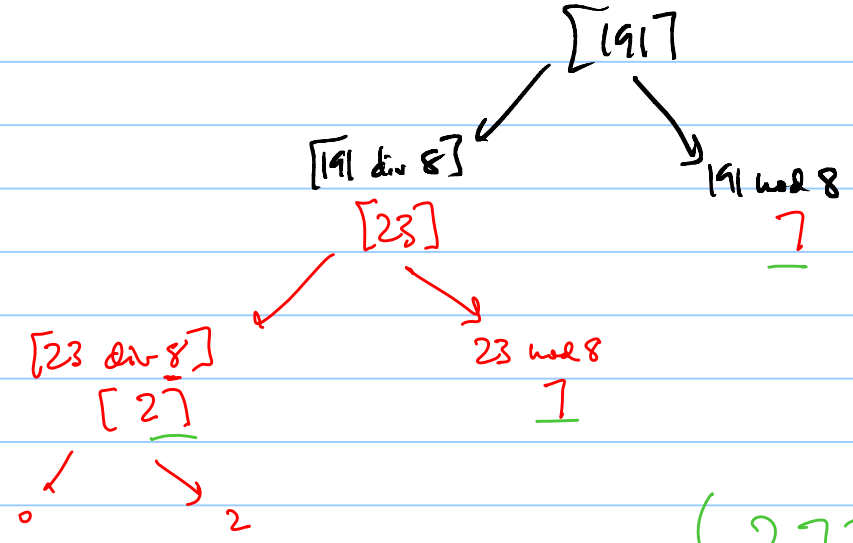
7^2 7^1 7^0

$3 \cdot 7^2 + 6 \cdot 7^1 + 2 \cdot 7^0 = 147 + 42 + 2 = 191$

191 → base 8.

$23 \cdot 8 + 7 = 191$

$191 \rightarrow$ base 8



$(277)_8 = 191.$

$(12012201)_3 \rightarrow$ base 9

$3+2$

$(5\ 1\ 8\ 1)_9.$

$3^2 = 9$

---

multiplicative inv of 53 mod 71

$d \cdot 53 \bmod 71 = 1.$

$\gcd(71, 53) = 1.$ $\quad 1 = s \cdot 53 + t \cdot 71$

71	53	18	17	1
		1	2	1

$1 = 18 - 17$

$17 = 53 - 2 \cdot 18$

$18 = 71 - 53.$

$1 = 18 - 17 = 18 - (53 - 2 \cdot 18) = 18 - 53 + 2 \cdot 18$

$= -53 + 3 \cdot 18 = -53 + 3(71 - 53)$

$= -53 + 3 \cdot 71 - 3 \cdot 53$

$= 3 \cdot 71 - 4 \cdot 53$

$-4 \bmod 71 = \boxed{67}$

Check: $67 \cdot 53 \bmod 71 = 1$

$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$

$p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n}$