Slide 85

Verificare la divisibilità di 119, 120 per 2, 3, 5, 7, 9, 11, 13, 19, 23

119 non è divisibile per 2, 120 divisibile per 2
119 non è divisibile per 3, 120 divisibile per 3
119 non è divisibile per 5, 120 è divisibile per 5

questo è divisibile

$119 \bmod 10 = 9 \qquad 119/10 = 11 \qquad q - 2r = 11 - 2(9) = -7$

$120 \bmod 10 = 0 \qquad 120/10 = 12 \qquad q - 2r = 12 - 2(0) = 12$

questo non è divisibile per 7

119 è divisibile per 7, 120 non è divisibile per 7

$S(119) = 1+1+9 = 1+1 = 2 \neq 9$
$S(120) = 1+2+0 = 3 \neq 9$
non sono divisibili per 9

119 non è divisibile per 9, 120 non è divisibile per

$q - r$ divisibilità per 11

CASO 119: $11 - 9 = 2$ non è divisibile per 11
CASO 120: $12 - 0 = 12$ non è divisibile per 11

$q + 4r$ divisibilità per 13

non è divisibile per 13

119: $11 + 4(9) = 47 \rightarrow 47 = \underbrace{4}_{r} \cdot 10 + \underbrace{7}_{q} \rightarrow 4 + 4(7) = 32$

120: $12 + 4(0) = 12$ → non è divisibile per 13

$9-5x$ divisibilità per 17

$119 \rightarrow 11-5(9)=-34$ è divis per 17

$120 \rightarrow 12-5(0)=12$ non divis per 17

$9+2x$ divisibilita per 19

$119: 11+2(9)=29$ non div per 19

$120: 12+2(0)=12$ non div per 19

$9+7x$ divisibilita per 23

$119: 11+7(9)=74$ non div per 23

$120: 12+2(0)=12$ non div per 23

SLIDE 133

$23 \equiv 3 \mod 5$

$$\mathbb{Z}_5 \{ \overset{20}{0}, \overset{21}{1}, \overset{22}{2}, \overset{23}{3}, 4 \}$$

$55 \mod 9 \equiv 1 \mod 9$

$$\mathbb{Z}_5 \{ \underset{54}{0}, \underset{55}{1}, 2, 3, 4, 5, 6, 7, 8 \}$$

$55 \mod 9 \equiv -8 \mod 9$

$$\mathbb{Z}_5 \{ \underset{54}{0}, \underset{55}{1}, 2, 3, 4, 5, 6, 7, 8 \}$$

Inverso di $49 \mod 23$

$\varphi(23) = 23 - 1 = 22$

$$\mathbb{Z}_{22} = \{ 0, \underset{46}{1}, \underset{47}{2}, \underset{48}{3}, 4 \dots, 22 \}$$

$49 \cdot x \equiv 1$

$49 \equiv 3 \mod 23 \rightarrow 3^{22-1} \mod 23 \rightarrow (3^3)^7 \mod 23$

$(27)^7 \mod 23 = \underbrace{(4)^7}_{} \mod 23$

$$\mathbb{Z}_{23} = \{ 0, 1, 2, 3, \underset{27}{4}, 5 \dots 23 \}$$

$$\mathbb{Z}_{23} = \{ 16, 17, \underset{-5}{\overset{27}{18}}, 19, 20, 21, 22, 23 \}$$

$4^3 \cdot 4^3 \cdot 4^1 \mod 23$

dovrebbe essere 18 ma prendiamo l'indice partendo dalla fine

$64 \cdot 64 \cdot 4 \mod 23$

$-5 \cdot -5 \cdot 4 \mod 23 = 100 \mod 23 = 8$

numero di eulero

Con n numero primo $\varphi(n) = n-1$

Con n prodotto di numeri primi $\varphi(15) = (3-1)\cdot(5\cdot 1)$

$= 2 \cdot 4 = 8$

Con n multiplo di un numero primo

$\varphi(8) = 2^3 - 2^2 = 8 - 4 = 4$