## CSS322 – Number Theory Notes

15: 1,3,5,15 16: 1,2,4,8,16  
15 = 
$$3 \times 5$$
 16 =  $2^4$   
 $gcd(15,16) = 1$   
15,16 relatively prime  
 $22 = 2 \times 11$   
 $145 = 5 \times 29$ 

Figure 1: Divisors, Greatest Common Divisor and Relatively Prime; Lecture 10

Figure 2: Modular Addition and Subtraction; Lecture 10

Figure 3: Modular Multiplication and Division; Lecture 10

$$2_8: 5^2 = 1 \pmod{8}$$
 $160 \mod 8 = (10 \times 16) \mod 8$ 
 $= [(0 \mod 8) \times (16 \mod 8)] \mod 8$ 
 $= [2 \times 0] \mod 8$ 
 $= 0$ 

Figure 4: Expanding with modular arithmetic properties 1; Lecture 10

$$||^{7} \mod 13 = (||^{4} \times ||^{2} \times ||^{1}) \mod 13$$

$$= [(||^{4} \mod ||^{3}) \times (||^{2} \mod ||^{3}) \times (|| \mod ||^{3})] \mod ||^{3}$$

$$= [(||^{2})^{2} \mod ||^{3}) \times (||^{2} \mod ||^{3}) \times (||^{1})] \mod ||^{3}$$

$$= [(||^{2})^{2} \mod ||^{3}) \times (||^{4}) \times (||^{1})] \mod ||^{3}$$

$$= [(||^{4})^{2} \mod ||^{3} \times ||^{4} \times ||^{1}] \mod ||^{3}$$

$$= [||^{3} \times ||^{4} \times ||^{1}] \mod ||^{3}$$

$$= ||^{3} \times ||^{4} \times ||^{3}$$

$$= |^{3} \times ||^{4} \times ||^{3}$$

Figure 5: Expanding with modular arithmetic properties 2; Lecture 10

Figure 6: Euler's Totient Examples; Lecture 10

$$a = 5$$
,  $b = 6$   $g\omega(5,6) = 1$   
 $\phi(5\times6) = \phi(30)$   
 $= \phi(5) \times \phi(6)$   
 $= 4 \times 2$   
 $= 8$   
 $p = 7$ ,  $q = 11$   
 $\phi(77) = \phi(7) \times \phi(11)$   
 $= 6 \times 10$   
 $= 60$   
 $\phi(143) = \phi(11) \times \phi(13)$   $11 \times 13 = 143$   
 $= 10 \times 12$   
 $= 120$ 

Figure 7: Totient of two factors; Lecture 11

97 | 
$$^{121}$$
 mod |  $^{143}$  = 97  $^{121}$  mod |  $^{143}$  = 97  $^{121}$  mod |  $^{143}$  =  $^{120}$   $^{121}$  mod |  $^{121}$  =  $^{120}$ 

Figure 8: Euler's Theorem Example; Lecture 11

$$3^5 \mod 5 = 3$$

$$a^6 \mod p = a$$

$$3^3 \mod 3 = 0$$

$$= 0 = 3 \pmod{3}$$

Figure 9: Fermat's Theorem Example; Lecture 11

Ordinary arthmetic:  

$$2^6 = 64$$
  
 $\log_2(64) = 6$   
Modular arthmetic:  
 $3^2 \mod 7 = 2$   
 $\log_{3,7}(2) = 2$   
 $3^3 \mod 7 = 6$   
 $\log_{3,7}(6) = 3$   
 $\log_{3,7}(5) = 5$   
 $3^5 \mod 7 = 5$   
 $\log_{2,7}(4) = 2 \text{ or } 5$   
 $2^{2.5} \mod 7 = 4$ 

Figure 10: Discrete Logarithm Examples; Lecture 11

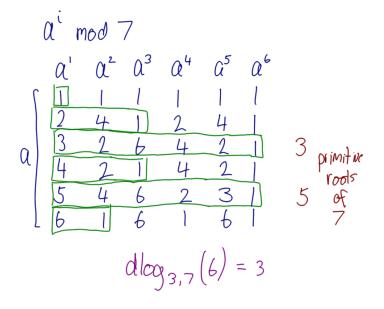


Figure 11: Primitive Roots mod 7; Lecture 11

$$\emptyset(23) = 23 - 1 = 22$$
 $|49|^{133} \mod |6| = |49|^{132+1} \mod |6| = |49|$ 
 $d\log_{2,19}(3) = 13$ 
 $2^{\frac{13}{2}} \mod 19 = 3$ 

Fermat's:  $\alpha^{p} \mod p = \alpha$ 

Evlers:  $\alpha^{\phi(n)+1} \mod n = \alpha$ 
 $\emptyset(161) = \emptyset(23 \times 7)$ 
 $= \emptyset(23) \times \emptyset(7)$ 
 $= 132$ 
 $|20398|^{1306973} \mod 130926|$ 

Figure 12: Number Theory Examples; Lecture 11