CSS441 – Number Theory Notes

16: 1, 2, 4, 8, 16 $\quad 16 = 2^4$

24: 1, 2, 3, 4, 6, 8, 12, 24 $\quad 24 = 2^3 \times 3$

gcd(16, 24) = 8

15: 1, 3, 5, 15 $\quad 15 = 3 \times 5$

gcd(16, 15) = 1 $\quad$ 15, 16 relatively prime

$22 = 2 \times 11$

$145 = 5 \times 29$

Figure 1: Divisibility and Primes; Lecture 09

$13 \bmod 10 = 3$

$13 \equiv 3 \pmod{10}$

$Z_{10} = \{0, 1, 2, 3, \dots 9\}$

Z_{10}

$4+3=7$

$4+7=1$

$AI(3) = 7$

since $3+7=0$

$4-7 = 4 + AI(7)$

$= 4+3$

$= 7$

$2-6 = 2 + AI(6) = 2+4 = 6$

$5-3 = 5 + AI(3) = 5+7 = 2$

Normal

$7-3=4$

$7+(-3)=4$

$(+3)+(-3)=0$

$\therefore AI(3) = -3$

Figure 2: Modular Addition and Subtraction; Lecture 09

Z_{10}	a	$AI(a)$
	0	0
	1	9
	2	8
	3	7
	4	6
	5	5
	6	4
	7	3
	8	2
	9	1

Figure 3: Additive Inverse; Lecture 09

$\mathbb{Z}_8$

$3 \times 2 = 6$

$3 \times 4 = 4 \qquad (3 \times 4) \bmod 8 = 12 \bmod 8 = 4$

$5 \div 3 = 5 \times MI(3)$

$\underline{3} \times 3 = 1 \qquad MI(3) = 3$

$5 \div 3 = 5 \times 3 = 7$

$6 \div 4 = 6 \times MI(4)$

$(\_ \times 4) \bmod 8 = 1$

Normal

$8 \div 3 = 8 \times \frac{1}{3}$

$3 \times \frac{1}{3} = 1$

$\therefore MI(3) = \frac{1}{3}$

Figure 4: Modular Multiplication and Division; Lecture 09

$\mathbb{Z}_8$											
a	0	1	2	3	4	5	6	7			4
$MI(a)$	x	1	x	3	x	5	x	7			

$\mathbb{Z}_{10}$											
a	0	1	2	3	4	5	6	7	8	9	4
$MI(a)$	x	1	x	7	x	x	x	3	x	9	

$\gcd(1,10) = \gcd(3,10) = \gcd(7,10) = \gcd(9,10) = 1$

Figure 5: Multiplicatve Inverse; Lecture 09

$\mathbb{Z}_8$

$$\begin{aligned} 132 \bmod 8 &= [(12 \bmod 8) \times (11 \bmod 8)] \bmod 8 \\ &= [\ 4 \times 3\ ] \bmod 8 \\ &= 4 \end{aligned}$$

$\mathbb{Z}_{13}$

$$\begin{aligned} 11^7 \bmod 13 &= (11^4 \times 11^3) \bmod 13 \\ &= [((11^2)^2 \bmod 13) \times (11^2 \bmod 13) \times (11^1 \bmod 13)] \bmod 13 \\ &= [\ 4^2 \bmod 13 \times 4 \times 11\ ] \bmod 13 \\ &= (3 \times 4 \times 11) \bmod 13 \\ &= 132 \bmod 13 \\ &= 2 \end{aligned}$$

Figure 6: Simplified Multiplication; Lecture 09

Relatively prime with 4:

gcd(4,1) = 1 ✓

gcd(4,2) = 2 ✗

gcd(4,3) = 1 ✓

2 numbers < 4

$\phi(4) = 2$

$\phi(8) = 4$

$\phi(10) = 4$

$\phi(9) = 6$

$\phi(13) = 12$

$\phi(29) = 28$

$\phi(7) = 6$

$\phi(5) = 4$

$\phi(35) = \phi(7 \times 5) = \phi(7) \times \phi(5)$

1	2	3	4	5	6	7	8
✓	✓	✗	✓	✓	✗	✓	✓

$= 6 \times 4$

$= 24$

Figure 7: Euler's Totient; Lecture 09

Fermat's theorem: $a^p \equiv a \pmod{p}$

p is prime

$3^5 \bmod 5 = 3$

$3^3 \bmod 3 = 0$ $\quad 3 \equiv 0$

Euler's theorem: $a^{\phi(n)+1} \equiv a \pmod{n}$

$97^{121} \bmod 143 = 97$

$\phi(143) = \phi(11 \times 13)$ $\quad 11 \times 13 = 143$

$= \phi(11) \times \phi(13)$

$= 10 \times 12$

$= 120$

Figure 8: Fermats Theorem and Eulers Theorem; Lecture 11

Ordinary arithmetic:

$$2^6 = 64 \qquad 3^4 = 81$$

$$\log_2(64) = 6 \qquad \log_3(81) = 4$$

Modular arithmetic:

$$3^2 \bmod 7 = 2$$

$$\mathrm{dlog}_{3,7}(2) = 2$$

$$\mathrm{dlog}_{3,7}(6) = 3$$

$$3^3 \bmod 7 = 6$$

$$\mathrm{dlog}_{2,7}(4) = 2 \text{ or } 5$$

$$2^2 \bmod 7 = 4 \quad \checkmark$$

$$2^5 \bmod 7 = 4 \quad \checkmark$$

Figure 9: Discrete Logarithm; Lecture 11

$$a^i \bmod 7 = x \qquad \mathrm{dlog}_{a,7}(x) = i$$

a	a^1	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

3 and 5 are primitive roots of 7

Figure 10: Primitive Roots; Lecture 11

$$\phi(23) = 22$$

$$149^{133} \bmod 161 =$$

$$\text{dlog}_{2,19}(3) = 13 \qquad 2^{13} \bmod 19 = 3$$

$$1203981^{1306973} \bmod 1309261 =$$

Figure 11: Number Theory Examples; Lecture 11