CSS322 – Number Theory Notes

15 : 1, 3, 5, 15 16: 1, 2, 4, 8, 16

$15 = 3^1 \times 5^1$ $16 = 2^4$

$\gcd(15, 16) = 1$

15, 16 relatively prime

$22 = 2 \times 11$

$145 = 5 \times 29$

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

$13 \bmod 10 = 3$

$13 \equiv 3 \pmod{10}$

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$

$\mathbb{Z}_{10}$:

$4+3=7$

$4+7=1$

$AI(3) = 7$

$3+7 = 0 \pmod{10}$

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

$= 4+3$

$= 7$

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

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

a	$AI(a)$
0	0
1	9
2	8
3	7
4	6
5	5
6	4
7	3
8	2
9	1

Normal

$7-3=4$

$7+(-3)=4$

$+3$ additive inverse of -3

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

Figure 2: Modular Addition and Subtraction; Lecture 10

$\mathbb{Z}_8$

$(3 \times 2) \bmod 8 = 6 \bmod 8$
$= 6$

$3 \times 4 = 4$

$5 \div 3 = 5 \times MI(3)$
$= 5 \times 3$ $\quad 3 \times 3 \bmod 8 = 1$
$= 7$

$6 \div 4 = 6 \times MI(4)$
$\times$ $\quad 4 \times \_ \bmod 8 = 1$

Normal
$8 \div 3 = 8 \times \frac{1}{3}$
$3 \times \frac{1}{3} = 1$
multiplicative inverse

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

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

Figure 3: Modular Multiplication and Division; Lecture 10

$\mathbb{Z}_8$: $5^2 = 1 \pmod 8$

$160 \bmod 8 = (10 \times 16) \bmod 8$
$= [(10 \bmod 8) \times (16 \bmod 8)] \bmod 8$
$= [\ 2 \times 0\ ] \bmod 8$
$= 0$

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

$$
\begin{aligned}
11^7 \bmod 13 &= (11^4 \times 11^2 \times 11^1) \bmod 13 \\
&= [(11^4 \bmod 13) \times (11^2 \bmod 13) \times (11 \bmod 13)] \bmod 13 \\
&= [((11^2)^2 \bmod 13) \times (121 \bmod 13) \times (11)] \bmod 13 \\
&= [(121^2 \bmod 13) \times (4) \times (11)] \bmod 13 \\
&= [(4^2) \bmod 13 \times 4 \times 11] \bmod 13 \\
&= [3 \times 4 \times 11] \bmod 13 \\
&= 132 \bmod 13 \\
&= 2
\end{aligned}
$$

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

Relatively prime with 4:

$\gcd(1,4) = 1$ ✓

$\gcd(2,4) = 2$ ✗

$\gcd(3,4) = 1$ ✓

2 numbers < 4 are RP with 4

$\phi(4) = 2$

$\phi(9) = 6$

1	2	3	4	5	6	7	8
✓	✓	✗	✓	✓	✗	✓	✓

$\phi(7) = 6$

$\phi(13) = 12$

$\phi(p) = p-1$

$\phi(5) = 4$

$$
\begin{aligned}
\phi(35) &= \phi(7 \times 5) \\
&= \phi(7) \times \phi(5) \\
&= 6 \times 4 \\
&= 24
\end{aligned}
$$

Figure 6: Euler's Totient Examples; Lecture 10

$$a = 5, \quad b = 6 \qquad \gcd(5,6) = 1$$

$$\begin{aligned}
\phi(5 \times 6) &= \phi(30) \\
&= \phi(5) \times \phi(6) \\
&= 4 \times 2 \\
&= 8
\end{aligned}$$

$$p = 7, \quad q = 11$$

$$\begin{aligned}
\phi(77) &= \phi(7) \times \phi(11) \\
&= 6 \times 10 \\
&= 60
\end{aligned}$$

$$\begin{aligned}
\phi(143) &= \phi(11) \times \phi(13) \qquad 11 \times 13 = 143 \\
&= 10 \times 12 \\
&= 120
\end{aligned}$$

Figure 7: Totient of two factors; Lecture 11

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

$$a^{\phi(n)+1} \bmod n = a$$

$$\begin{aligned}
\phi(143) &= \phi(11) \times \phi(13) \\
&= 120
\end{aligned}$$

Figure 8: Euler's Theorem Example; Lecture 11

$$3^5 \bmod 5 = 3$$

$$a^p \bmod p = a$$

$$\underbrace{3^{3^k} \bmod 3 \equiv 0}_{\equiv} \qquad 0 \equiv 3 \pmod 3$$

Figure 9: Fermat's Theorem Example; Lecture 11

Ordinary arithmetic:

$$2^6 = 64$$

$$\log_2(64) = 6$$

Modular arithmetic:

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

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

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

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

$$\text{dlog}_{3,7}(5) = 5$$

$$3^5 \bmod 7 = 5$$

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

$$2^{2,5} \bmod 7 = 4$$

Figure 10: Discrete Logarithm Examples; Lecture 11

$a^i \bmod 7$

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

primitive roots of 7

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

Figure 11: Primitive Roots mod 7; Lecture 11

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

$$149^{133} \bmod 161 = 149^{132+1} \bmod 161 = 149$$

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

Fermat's: $a^{p} \bmod p = a$

Euler's: $a^{\phi(n)+1} \bmod n = a$

$$\begin{aligned}\phi(161) &= \phi(23 \times 7)\\ &= \phi(23) \times \phi(7)\\ &= 132\end{aligned}$$

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

Figure 12: Number Theory Examples; Lecture 11