CSS322 – Number Theory Notes

$15 = 3 \times 5$

$15: 1, 3, 5, 15$

$24: 1, 2, 3, 4, 6, 8, 12, 24$

$24 = 2 \times 2 \times 2 \times 3$

$= 2^3 \times 3^1$

Figure 1: Divisors (Factors) Examples; Lecture 08

$$13 \equiv 3 \pmod{10}$$

$\mathbb{Z}_{10}$ mod 10 Normal

$4+3=7$ $4+3=7$

$4+7=1$ $7-3=4$

$AI(3)=7$ $7+(-3)=4$

$3+7 \bmod 10 = 0$

$$\begin{aligned} 4-7 &= 4+AI(7) \\ &= 4+3 \\ &= 7 \end{aligned}$$

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

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

Figure 2: Addition and Subtraction in Modular Arithmetic; Lecture 08

$\mathbb{Z}_8$

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

$3 \times 4 = 4$

$\mathbb{Z}_8$ $MI(3) = 3$ $MI(2) = X$

$MI(5) = 5$

$\mathbb{Z}_{10}$

$MI(3) = 7$

Figure 3: Multiplication in Modular Arithmetic; Lecture 08

mod 8 :

a	1	2	3	4	5	6	7
MI(a)	1	x	3	x	5	x	7

$\gcd(3,8) = 1$

3 & 8 are RP

$$2 \div 3 = 2 \times MI(3) = 2 \times 3 = 6$$

$$2 \div 4 = \times$$

Figure 4: Division in Modular Arithmetic; Lecture 09

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

$$2^3 \bmod 7 = 1$$

$$11^7 \bmod 13 = (11^4 \times 11^2 \times 11^1) \bmod 13$$
$$= ((11^2)^2 \times 11^2 \times 11^1) \bmod 13$$
$$= ((121)^2 \times 121 \times 11) \bmod 13$$
$$= [(121^2 \bmod 13) \times (121 \bmod 13) \times (11 \bmod 13)] \bmod 13$$
$$= [4^2 \bmod 13 \times 4 \times 11] \bmod 13$$
$$= [3 \times 4 \times 11] \bmod 13$$
$$= 132 \bmod 13$$
$$= 2$$

Figure 5: Expansion for Multiplication and Exponentiation; Lecture 09

$3^5 \bmod 5 = 3$

$a^p \equiv a \pmod{p}$

$p = 5$

$a = 3 \qquad 3^5 = 243$

$243 \bmod 5 = 3$

Figure 6: Fermats Theorem Example; Lecture 09

$\phi(8) = 4$

1 2 3 4 5 6 7

$\phi(9) = 6$

1 2 3 4 5 6 7 8

$\phi(23) = 22$

$\phi(5) = 4$

1 2 3 4

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

Figure 7: Eulers Totient Function; Lecture 09

$$4362^{61} \bmod 77 = 4362^{\phi(77)+1} \bmod 77$$

$$a^{\phi(n)+1} \bmod n = a \qquad = 4362$$

$$n = 77 \qquad \phi(n) = 60$$

Figure 8: Eulers Theorem Example; Lecture 09

$$2^6 = 64 \qquad \log_2(64) = 6$$

$$2^{13} \bmod 19 = 3$$

$$d\log_{2,19}(3) = 13$$

Figure 9: Discrete Logarithm Example; Lecture 09

mod 7: $a^i \bmod 7$

a \ i	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1

3 primitive root

Figure 10: Primitive Root Example; Lecture 10

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

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

$$\mathrm{dlog}_{2,7}(4) = X$$

Figure 11: Discrete Log Example; Lecture 10