Kelsey Neis, neis@umn.edu
CSCI 5421 - HW 3

31.5
1

Find all solutions to $X = 4 \pmod 5$ and $X = 5 \pmod{11}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
n mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3
n mod 11	0	1	2	3	4	5	6	7	8	9	10	0	1	2

n	14	15	16	17	18	19	20	21	22	23	24	25	26	27
n mod 5	4	0	1	2	3	4	0	1	2	3	4	0	1	2
n mod 11	3	4	5	6	7	8	9	10	0	1	2	3	4	5

n	28	29	30	31	32	33	34	35	36	37	38	39	40
n mod 5	3	4	0	1	2	3	4	0	1	2	3	4	0
n mod 11	6	7	8	9	10	0	1	2	3	4	5	6	7

n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
n mod 5	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
n mod 11	8	9	10	0	1	2	3	4	5	6	7	8	9	10	0

Assuming x must satisfy $X \equiv 4 \bmod 5$ and $X \equiv 5 \bmod 11$ at once, the solution will be 49 and $49 + m \cdot 55$, since the pattern repeats itself with an interval of 55.

2

find all x that leave remainders 1, 2, 3 when divided by $\underbrace{9, 8, 7}_{\text{pairwise relatively prime}}$

Chinese remainder theorem provides correspondence b/w a system of equations modulo a set of coprime moduli

$n = 9 \cdot 8 \cdot 7 = 504$

$a \longleftrightarrow (a_1, a_2, a_3)$, $a_i = a \bmod n_i$ for $i = 1, 2, 3$

$a \equiv 1 \bmod 9$
$a \equiv 2 \bmod 8$
$a \equiv 3 \bmod 7$

$m_i = n_1 \cdot n_2 \cdot n_3$, $j \neq i$

$c_i = m_i (m_i^{-1} \bmod n)$

$a \equiv (a_1 c_1 + a_2 c_2 \cdots + a_k c_k) \pmod n$

a	.... ? ....
$x \bmod 9$	.... 1 ....
$x \bmod 8$	.... 2 ....
$x \bmod 7$	.... 3 .....

Concretely:

$m_1 = n_2 \cdot n_3 = 56 = 2 \bmod 9 \rightarrow C_1 = 56(m_1^{-1} \bmod n)$

$m_2 = n_1 \cdot n_3 = 63 = 7 \bmod 8 \rightarrow C_2 = 63(m_2^{-1} \bmod n)$

$m_3 = n_1 \cdot n_2 = 72 = 2 \bmod 7 \rightarrow C_3 = 72(m_3^{-1} \bmod n)$

$2 \times 5 = 10 = 1 \bmod 9 \rightarrow m_1^{-1} = 5$

$7 \times 7 = 49 = 1 \bmod 8 \rightarrow m_2^{-1} = 7$

$2 \times 4 = 8 = 1 \bmod 7 \rightarrow m_3^{-1} = 4$

$C_1 = 56 \cdot 5 = 280$

$C_2 = 63 \cdot 7 = 441$

$C_2 = 72 \cdot 4 = 288$

$a = 1 \cdot 280 + 2 \cdot 441 + 3 \cdot 288 = 2026 = 10 \bmod 504$

$\boxed{10,\ 10 + m \cdot 504 \text{ for any integer } m}$

3

Argue if $\gcd(a,n)=1$, then $(a^{-1} \bmod n) \longleftrightarrow ((a_1^{-1} \bmod n_1), (a_2^{-1} \bmod n_2) \ldots)$

31.27 $a \longleftrightarrow (a_1, a_2, \ldots, a_k)$, $a \in \mathbb{Z}_n$, $a_i \in \mathbb{Z}_{n_i}$

$a_i = a \bmod n_i$

31.32: $a \equiv a_i \bmod n_i$,

- Since a and n are coprime, every element in $\mathbb{Z}_n^*$ has an inverse, which maps uniquely to $\mathbb{Z}_{n_i}^*$.
- If there is a bijection between $a \bmod n \longleftrightarrow a_i \bmod n_i$ with addition, multiplication, and subtraction, then there must be a bijection for division, and thus for inverse.

31.6

1

i	0	1	2	3	4	5	6	7	8	9	10	11	12 ...
1^i mod 11	1	1	2	3	4	5	6	7	8	9	10	0	1
2^i mod 11	1	2	4	8	5	10	9	7	3	6	1	2	...
3^i mod 11	1	3	9	5	4	1	3	9	5	4	1	3	...
4^i mod 11	1	4	5	9	3	1	4	5	9	3	1	4	...
5^i mod 11	1	5	3	4	9	1	5	3	4	9	1	5	...
6^i mod 11	1	6	3	7	9	10	5	8	4	2	1	6	...
7^i mod 11	1	7	5	2	3	10	4	6	9	8	1	7	...
8^i mod 11	1	8	9	6	4	10	3	2	5	7	1	8	...
9^i mod 11	1	9	4	3	5	1	9	4	3	5	1	9	...
10^i mod 11	1	10	1	10	1	10	1	10	1	10	1	10	...

↳ 2 is a primitive root, $o(2) = 10$

X	1	2	3	4	5	6	7	8	9	10
$\text{ind}_{11,2} X$	0	1	1.58	2	2.32	2.58	2.8	3	3.16	3.32

2

To reverse the modular-exponentiation algorithm, let's compare what happens when we add a 0 or 1 to the end of a binary string to what happens when we add a 0 or 1 to the beginning:

forwards: $a^{1} \xrightarrow{sq} a^{1\underline{0}} \xrightarrow{\times a} a^{1\underline{1}} \xrightarrow{sq} a^{11\underline{0}} \dots$

Backwards: $a^{0} \xrightarrow{\times a} a^{00} \xrightarrow{\times a} a^{10} \xrightarrow{sq} a^{\underline{0}10} \xrightarrow{sq}$

$$a^{0} \xrightarrow{\times a} a^{00} \xrightarrow{sq} a^{10} \xrightarrow{\times a} a^{010} \xrightarrow{sq} a^{110}$$

$$a^{2} \qquad\qquad a^{6}$$

So we can reverse the operations, meaning when $b_i = 0$,

$c = c+1$ and $d = a \cdot d$

and when $b_i = 1$, $c = 2c$ and $d = d \cdot d$

```
Modular-Exponentiation-Reversed(a, b, n):
    c = 0
    d = 1
    let <b_0, b_1, ...., b_k> be binary rep. of b
    for i = 0 to k:
        c = c+1
        d = (d·a) mod n
        if b_i == 1
            c = 2c
            d = (d·d) mod n
    return d
```

$\llcorner$

3.

In the example where $d = 7$, the inverse of a mod 561 is 560, because it is the first power where $7^c = 1$ mod 561.
So, given any number $\in \mathbb{Z}_n^*$, we can find its inverse by recording the value of C when $d=1$.

31.7

(3) $P_A(M_1) = M_1^e \bmod n \qquad P_A(M_2) = M_2^e \bmod n$

By the Chinese Remainder theorem ($ab \bmod n \Leftrightarrow a_i b_i \bmod n_i$)

$P_A(M_1)P_A(M_2) = M_1^e M_2^e \bmod n \Leftrightarrow$

$P_A(M_1 M_2) = (M_1 M_2)^e \bmod n = M_1^e M_2^e \bmod n$

Given someone knows how to decrypt 1% of the messages, they can obtain the exponent e from 1% of the messages can perform the mapping from C to M, $S_A(P_A(M))$.

Since $\mathbb{Z}_n$ is cyclic, all they would need to do is, given an encrypted message $P(M) = M^e \bmod n$, choose a random encrypted message and multiply them together to get $P(M_1 M_2)$. Repeat until a point is reached that is in the subset (1%) that can be decrypted, obtaining e. Compute its inverse, d, and raise $P(M)$ to d to get M.

31.8

Prove: If x is non-trivial sqrt of 1, then:

$$\gcd(x+1, n) \mid n \quad \text{and} \quad \gcd(x+1, n) \neq 1$$
$$\gcd(x-1, n) \mid n \quad \text{and} \quad \gcd(x-1, n) \neq 1$$

non-trivial sqrt means:

$x^2 - 1 = 0 \pmod{n}$ has solution not ± 1

$x^2 - 1 = 0$ can be rewritten as:

$$(x+1)(x-1) = 0$$

If x cannot be ± 1, then $(x+1)$ and $(x-1)$ are two numbers when multiplied, is a divisor of n

Since $x \neq 0$, it follows that there is some number, not 1 that satisfies $\gcd(x \pm 1, n)$