10.10.'22

CS6008: Cryptograph and Network Security.
Assignment

Akshara.M.S
2019103004

1. Why is gcd $(n, n+1) = 1$ for two consecutive integers n, $n+1$

Let's say n has a divisor q for which $n/q = p$, $p \in \mathbb{Z}$

If we divide $n+1$ by q, we obtain $\frac{n+1}{q} = p + 1/q$, thus for all $q \neq 1$ (since (gcd $(1, q) = 1$), $n+1$ will not be divisible by q

Therefore gcd $(n, n+1) = 1$

2. Using fermat's theorem, find $3^{201} \bmod 11$.

Fermat's theorem states that if p is prime and a is a positive integer, not divisible by p, then $a^{p-1} = 1 \bmod p$

$3^{201} \bmod 11 = (3^{10})^{20} \cdot 3^{1} \bmod 11$

$(3^{10}) \bmod 11 = 1$

$= (1)^{20} 3 \bmod 11$

$= 3 \bmod 11$

$= 3$ //

3. Using Fermat's theorem Find a number between 0 and 72 with a congruent to 9794 modula 73

According to Fermat's theorem

$a \equiv 9794 \bmod 73$

$\equiv 12$

$a \equiv 12$ //

4. Use Fermat's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29 (You should not use any brute force searching)

From fermat's theorem

$$x^{28} = 1 \bmod 29$$

Raising both side to the power of 3

$$x^{84} = 1 \bmod 29$$

then multiply by x on both sides

$$x^{85} = x(1 \bmod 29)$$

$$x \equiv 6 \bmod 29$$

$$x \equiv 6$$

5. Use Euler's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35.

$$x^{85} = 6 \bmod 35 \quad \text{—— ①}$$

As $35 = 5 \times 7$. $\gcd(5, 7) = 1$

$$① \Rightarrow x^{85} = 6 \bmod 5 = 1$$

As $\phi(5) = 4$ $85 = 1 \bmod 4$

$$x = 1 \bmod 5 \quad \text{—— ②}$$

$$② \Rightarrow x^{85} = 6 \bmod 7$$

As $\phi(7) = 6$ $85 = 1 \bmod 6$

$$x = 6 \bmod 7 \quad \text{—— ③}$$

3

$$x = 1 \bmod 5$$

$$x = 6 \bmod 7$$

$$1 + 5k = 6 \bmod 7$$

$$5k = 5 \bmod 7$$

$$k = 1 \bmod 7$$

$$k = 1 + 7m$$

$1+5(1+7m) = 1+5+35m$

$= 6+35m$

$a = 6$ //

6\. It can be shown that $\gcd(m, n) = 1$ then $\phi(m, n) = \phi(m)\phi(n)$
Determine the following

(a) $\phi(41)$

41 is a prime number

$\phi(41) = 40$

(b) $\phi(27) = \phi(3^3)$

$= 3^3 - 3^2$

$= 27 - 9$

$= 18$

(c) $\phi(231) \Rightarrow \phi(3) \times (\phi(7)) \times \phi(11)$

$= 2 \times 6 \times 10$

$= 120$

(d) $\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11)$

$= \phi(2^3 - 2^2) \times 4 \times 10$

$= (8-4) \times 4 \times 10$

$= 160$

n	ϕ
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10

7\. If n is composite and passes miller-rabin test for base a, then n is a strong pseudoprime to a base a, Show than 2047 is a strong pseudoprime to the base 2

$n = 2047$

$a = 2$

$n - 1 = 2046 = 2 \times 1023$

$m = 1023, k = 1$

$T = 2^{1023} \mod 2047$

$2^1 \mod 2047 = 2$

$2^2 \mod 2047 = 4$

$2^4 \mod 2047 = 16 = (4)^2$

$2^8 \mod 2047 = (16)^2 = 256$

$2^{16} \mod 2047 = (256)^2 = 32$

$2^{32} \mod 2047 = (32)^2 = 1024$

$2^{64} \mod 2047 = (1024)^2 = 512$

$2^{128} \mod 2047 = (512)^2 = 128$

$2^{256} \mod 2047 = (128)^2 = 8$

$2^{512} \mod 2047 = (8)^2 = 64$

$2^{1024} \mod 2047 = (64)^2 = 2$

$T = 2^{1023} \mod 2047$

$1023 = 512 + 256 + 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$

$= (64 \times 8 \times 128 \times 512 \times 1024 \times 32 \times 256 \times 16 \times 4 \times 2) \mod 2047$

$= 1$

$T = 1 \Rightarrow$ Hence composite

2047 is a strong composite pseudoprime to base 2

8. The example used by Sun-Tsu was

$x = 2 \mod 3$

$x = 3 \mod 5$

$x = 2 \mod 7$

Solve for x.

Let's take $x = 2 \mod 3$

$x = 3 \mod 5$

$$2+3k = 3 \bmod 5$$
$$3k = 1 \bmod 5$$
$$k = (3^{-1}) \bmod 5$$
$$k = 2+5l$$

$$2+3k = 2+3(2+5l)$$
$$= 2+6+15l$$
$$= 8+15l$$

$$x \equiv 8 \bmod 15$$

Let's take $x = 8 \bmod 15$, $x = 2 \bmod 7$

$$2 \bmod 7 = 2+7k$$
$$2+7k = 8 \bmod 15$$
$$7k = 6 \bmod 15$$
$$k = (7^{-1})^{6} \bmod 15$$
$$k = (13).(6) \bmod 15$$
$$k = 78 \bmod 15$$
$$k = 3 \bmod 15$$
$$k = 3+15l$$

$$2+7k = 2+7(3+15l)$$
$$= 2+21+105l$$
$$= 23+105l$$

$$x \equiv 23 \bmod 105$$

$$x = 23.$$

9. If the day in the question is the xth (counting from and including the first monday)

$$x = 1+2k_1$$
$$x = 2+3k_2$$
$$x = 3+4k_3$$

$x = 4 + k4$

$x = 5 + 6k5$

$x = 6 + 5k6$

$x = 7k_7$

① $x \equiv 1 \mod 2$

② $x = 2 \mod 3$

③ $x \equiv 3 \mod 4$

④ $x \equiv 4 \mod 1$

⑤ $x \equiv 5 \mod 6$

⑥ $x \equiv 6 \mod 5$

⑦ $x \equiv 0 \mod 7$

① and ③ are congruent.

② and ⑤ are congruent

While considering equation 3

$x \equiv 3 \mod 4 \mid 7 \mod 8 \mid 8\ 11 \mod 12$

While considering equation 5

$x \equiv 5 \mod 6 \mid 11 \mod 12$

So equation 3 and 5 are congruent

$x = 4 \mod 1$, so ignore equation 4

Therefore

$x = 11 \mod 12$

$x = 6 \mod 5$

$x = 0 \mod 7$

Let's take $x = 11 \mod 12$

$x = 6 \mod 5$

$6 \mod 5 = 1 + 5k$

$1 + 5k = 11 \mod 12$

$5k = (11 - 1) \mod 12$

$5k = 10 \mod 12$

$k = (10) \mod 12 \Rightarrow (5^{-1})\ 10 \mod 12$

$= 50 \mod 12$

$= 2 \mod 12 = 2 + 12l$

$$1+5k=(1+5(2+12l))$$
$$=1+10+60l$$
$$=11+60l$$

$x = 11 \bmod 60l$

Let's take $x = 11 \bmod 60$ and $x = 0 \bmod 7$

$$0 \bmod 7 = 0+7k$$
$$7k = 11 \bmod 60$$
$$k = (7^{-1})(11) \bmod 60$$
$$= 43.(11)(\bmod 60)$$
$$= 473 \bmod 60$$

$k = 53 \bmod 60$

$k = 53 + 60l$

$$0+7k = 0+7(53+60l)$$
$$= 371 + 420l$$

$x = 371 \bmod 420$

The first x satisfying the condition is 371

$\therefore x = 371$

10. Find all primitive roots of 25

$$\phi(25) = \phi(5^2) = 5^2 - 5^1 = 20$$

According to Euler's theorem

$$a^{20} = 1 \bmod 25$$

$$Z_{25} = \{0, 1, 2 \ldots 24\}$$

for Z_5, primitive roots are 2, 3

if g is primitive root, $g+p$ may / may not be primitive

7, 8, 12, 13, 17, 18, 22, 23

7 and 18 are not primitive roots because their power are not distinct

Hence primitive roots are

2, 3, 8, 12, 13, 17, 22, 23.