Modulo Table

0 modulo 15 is 0	10 modulo 15 is 10	20 modulo 15 is 5
1 modulo 15 is 1	11 modulo 15 is 11	21 modulo 15 is 6
2 modulo 15 is 2	12 modulo 15 is 12	22 modulo 15 is 7
3 modulo 15 is 3	13 modulo 15 is 13	23 modulo 15 is 8
4 modulo 15 is 4	14 modulo 15 is 14	24 modulo 15 is 9
5 modulo 15 is 5	15 modulo 15 is 0	25 modulo 15 is 10
6 modulo 15 is 6	16 modulo 15 is 1	26 modulo 15 is 11
7 modulo 15 is 7	17 modulo 15 is 2	27 modulo 15 is 12
8 modulo 15 is 8	18 modulo 15 is 3	28 modulo 15 is 13
9 modulo 15 is 9	19 modulo 15 is 4	29 modulo 15 is 14
30 modulo 15 is 0	40 modulo 15 is 10	50 modulo 15 is 5
31 modulo 15 is 1	41 modulo 15 is 11	51 modulo 15 is 6
32 modulo 15 is 2	42 modulo 15 is 12	52 modulo 15 is 7
33 modulo 15 is 3	43 modulo 15 is 13	53 modulo 15 is 8
34 modulo 15 is 4	44 modulo 15 is 14	54 modulo 15 is 9
35 modulo 15 is 5	45 modulo 15 is 0	55 modulo 15 is 10
36 modulo 15 is 6	46 modulo 15 is 1	56 modulo 15 is 11
37 modulo 15 is 7	47 modulo 15 is 2	57 modulo 15 is 12
38 modulo 15 is 8	48 modulo 15 is 3	58 modulo 15 is 13
39 modulo 15 is 9	49 modulo 15 is 4	59 modulo 15 is 14
60 modulo 15 is 0	70 modulo 15 is 10	80 modulo 15 is 5
61 modulo 15 is 1	71 modulo 15 is 11	81 modulo 15 is 6
62 modulo 15 is 2	72 modulo 15 is 12	82 modulo 15 is 7
63 modulo 15 is 3	73 modulo 15 is 13	83 modulo 15 is 8
64 modulo 15 is 4	74 modulo 15 is 14	84 modulo 15 is 9
65 modulo 15 is 5	75 modulo 15 is 0	85 modulo 15 is 10
66 modulo 15 is 6	76 modulo 15 is 1	86 modulo 15 is 11

67 modulo 15 is 7 68 modulo 15 is 8 69 modulo 15 is 9	77 modulo 15 is 2 78 modulo 15 is 3 79 modulo 15 is 4	87 modulo 15 is 12 88 modulo 15 is 13 89 modulo 15 is 14
90 modulo 15 is 0 91 modulo 15 is 1 92 modulo 15 is 2 93 modulo 15 is 3 94 modulo 15 is 4 95 modulo 15 is 5 96 modulo 15 is 6 97 modulo 15 is 7 98 modulo 15 is 8 99 modulo 15 is 9		

0 modulo 11 is 0 1 modulo 11 is 1 2 modulo 11 is 2 3 modulo 11 is 3 4 modulo 11 is 4 5 modulo 11 is 5 6 modulo 11 is 6 7 modulo 11 is 7 8 modulo 11 is 8 9 modulo 11 is 9	10 modulo 11 is 10 11 modulo 11 is 0 12 modulo 11 is 1 13 modulo 11 is 2 14 modulo 11 is 3 15 modulo 11 is 4 16 modulo 11 is 5 17 modulo 11 is 6 18 modulo 11 is 7 19 modulo 11 is 8	20 modulo 11 is 9 21 modulo 11 is 10 22 modulo 11 is 0 23 modulo 11 is 1 24 modulo 11 is 2 25 modulo 11 is 3 26 modulo 11 is 4 27 modulo 11 is 5 28 modulo 11 is 6 29 modulo 11 is 7
30 modulo 11 is 8 31 modulo 11 is 9 32 modulo 11 is 10 33 modulo 11 is 0 34 modulo 11 is 1 35 modulo 11 is 2	40 modulo 11 is 7 41 modulo 11 is 8 42 modulo 11 is 9 43 modulo 11 is 10 44 modulo 11 is 0 45 modulo 11 is 1	

36 modulo 11 is 3 37 modulo 11 is 4 38 modulo 11 is 5 39 modulo 11 is 6		

Question 1 (4.5 points)

Let $G = \{g^2 \text{ for all } g \in Z_{11}^*\} = \{1, 3, 4, 5, 9\}$ be a subset of Z_{11}^*. $= \{1, 2, \ldots, 10\}$

(a) Let . represents multiplication modulo 11. Create the multiplication table of G with . as the operation.

(b) Prove that $(G, .)$ is a group.

Hint: Prove that there is an identity element. Prove that for each element, there is a unique inverse. Prove that the group is closed under operation. Prove that the elements of the group sastisfy associativity.

(c) Let $\bar{G}$ be the set of all elements in Z_{11}^* that are not in G. Show that $\bar{G}$ is not a group.

Let H be an abelian group.

Show that $G = \{h^2$ for all $h \in G\}$ is a group.

(set of squares in H forms a group)

---

1) Identity element: $1 \in H$. $1^2 = 1 \in G$.

2) closure. $\forall a, b \in G$, we want to show that $a \cdot b \in G$.

proof: $a = x^2$, $x \in H$

$b = y^2$, $y \in H$

$a \cdot b = x^2 y^2 = (xy)^2 \in G$.

3) unique inverse. $\forall a \in G$, $\exists b \in G$ s.t. $a \cdot b = b \cdot a = 1$.

proof: $a = x^2$, $x \in H$

$b = (x^{-1})^2$, $x^{-1} \in H$

$a \cdot b = x^2 \cdot (x^{-1})^2 = (x \cdot x^{-1})^2 = 1$

$b \cdot a = (x^{-1})^2 \cdot (x)^2 = (x^{-1} \cdot x)^2 = 1$

4) associativity: H is a group. $G \subseteq H$. Associativity follows from H.

① $\mathbb{Z}_{11}^*$. The set of squares form a group of order $5 = \frac{10}{2}$

The squares generate a subgroup of order 5.

② Any integer which is a square can not be a generator in $\mathbb{Z}_p^*$.

4 is a square, $4 = 2^2$

4 can't be a generator of $\mathbb{Z}_p^*$.

What is the order of 4?

Note that $2^{2\left(\frac{p-1}{2}\right)} \equiv 1 \mod p$, for odd prime by Fermat's.

and $\frac{p-1}{2}$ is an integer.

We have $4^{\frac{p-1}{2}} \equiv 1 \mod p$

Hence, order 4 is a divisor of $\frac{p-1}{2} < p-1$.

Question 2 (6.5 points)

(a) Compute the order of 2 in Z_3^*. Is 2 a generator of Z_3^*?

(b) Compute the order of 3 in Z_5^*. Is 3 a generator of Z_5^*?

(c) Compute the order of $(2,3) \in Z_3^* \times Z_5^*$. Is $(2,3)$ a generator of $Z_3^* \times Z_5^*$?

(d) Compute the element x in Z_{15}^* such that

$x \equiv 2 \bmod 3$ and

$x \equiv 3 \bmod 5$

(e) What's the order of x in Z_{15}^*?

(f) Let p, q be distinct odd primes. Prove that no element in $Z_p^* \times Z_q^*$ has order equal to the order of $Z_p^* \times Z_q^*$.

Hint: What's the order of $Z_p^* \times Z_q^*$? What's the order of $(a,b) \in Z_p^* \times Z_q^*$ in terms of the order of a and the order of b?

(g) Let p, q be distinct odd primes. Is Z_{pq}^* a cyclic group? Justify your answer.

(a) $2^2 = 4 \equiv 1 \bmod 3$

order of 2 is 2.

$|\mathbb{Z}_3^*| = 2$.

2 is a generator

(b) $3^2 = 9 \equiv 4 \bmod 5$

$3^3 = 4 \times 3 = 12 \equiv 2 \bmod 5$

$3^4 = 2 \times 3 = 6 \equiv 1 \bmod 5$

order of 3 is 4

$|\mathbb{Z}_5^*| = 4$

3 is a generator

(c) $(2,3)^2 = (2^2, 3^2) = (1,4)$

$(2,3)^3 = (2,3) \cdot (1,4) = (2,2)$

$(2,3)^4 = (2,3) \cdot (2,2) = (1,1)$

order of $(2,3)$ is 4.

$|\mathbb{Z}_3^* \times \mathbb{Z}_5^*| = |\mathbb{Z}_3^*| \times |\mathbb{Z}_5^*| = 2 \times 4 = 8$

$(2,3)$ is not a generator.

(d) $x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

In $\mathbb{Z}_{15}^*$

For $x \equiv 3 \bmod 5$, $x = 3, 8, 13, \ldots$

x ✗ ✓

$x = 8$

(e) order of 8 in $\mathbb{Z}_{15}^*$.

$\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$

$8 \longmapsto (2, 3)$

order of 8 is the order of $(2,3)$

which is 4

(f) $\text{ord}((a,b)) = \dfrac{\text{ord}(a) \cdot \text{ord}(b)}{\gcd(\text{ord}(a), \text{ord}(b))} = \text{lcm}(\text{ord}(a), \text{ord}(b))$

proof: for $(a,b)^x = 1$

we must have $a^x = 1$ and $b^x = 1$

$(a^x \equiv 1 \bmod 3)$ and $(b^x \equiv 1 \bmod 5)$

x must be a multiple of order of a

x must be a multiple of order of b

The smallest such x is least common multiple of order of a and order of b.

f) No element in $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ has order equal to $(p-1)(q-1)$ where p and q are odd distinct primes.

---

proof: $ord((a,b)) = \frac{ord(a) \cdot ord(b)}{gcd(ord(a), ord(b))}$

Let a be a generator of $\mathbb{Z}_p^*$.

Let b be a generator of $\mathbb{Z}_q^*$.

$ord((a,b)) = \frac{(p-1)\cdot(q-1)}{gcd(p-1, q-1)}$

p and q are odd primes.

$2 \mid gcd(p-1, q-1)$

$ord(a,b) < (p-1)(q-1)$

All other elements of $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ are of the form (a^i, b^j) and $ord((a^i, b^j))$ is a divisor of $ord((a,b))$.

Hence, $ord(a^i, b^j) < (p-1)(q-1)$.

g) False because of (f)

Theorem

If p, q are distinct odd primes.

Then $\mathbb{Z}_{pq}^*$ is not cyclic.

Theorem

$\mathbb{Z}_n^*$ is cyclic for only the following values:

$n = 2, 3, 4, p^k, 2p^k$, p is odd prime.

Question 3 (2 points)

Recall that an isomorphism ϕ is a bijective map from a group $(G, *)$ to a group $(H, .)$ such that $\phi(g * h) = \phi(g).\phi(h)$.

For a group element k, we write the inverse of k has k^{-1}.

Prove that for all $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$.

This means: $g \longrightarrow \phi(g)$

$g^{-1} \longrightarrow \phi(g)^{-1}$

$e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \cdot \phi(g^{-1})$

$e_H = \phi(e_G) = \phi(g^{-1} * g) = \phi(g^{-1}) \cdot \phi(g)$

By definition of inverse, $\phi(g^{-1})$ is $\phi(g)^{-1}$

a is inverse of b if

$a \cdot b = b \cdot a = e$

Question 4 (3 points)

Recall the Diffie-Hellman Key Exchange protocol and the discrete logarithm problem.

algorithm is summarized in Table 2.2.

Public parameter creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.	
Private computations	
Alice	**Bob**
Choose a secret integer a. Compute $A \equiv g^a \pmod{p}$.	Choose a secret integer b. Compute $B \equiv g^b \pmod{p}$.
Public exchange of values	
Alice sends A to Bob $\longrightarrow$ A	
B $\longleftarrow$ Bob sends B to Alice	
Further private computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	

Table 2.2: Diffie–Hellman key exchange

(a) Eve observes the public exchange of values A and B. Suppose Eve able to solves the discrete logarithm problem for the value of a from A. Does Eve needs to solve the discrete logarithm problem for the value of b from B to get the shared secret value? Justify your answer.

(b) Suppose the order of g is a prime q. If Alice chooses integer q as the value of a, then can Eve finds out the shared secret value without solving the discrete logarithm problem? If so, what's the value of A? Justify your answer.

a) Eve sees A, $A = g^a \bmod p$.

If Eve solves a, the secret shared value is B^a.

b) $a = q$

$A = g^q \bmod p = 1$

The secret shared value is $A^b = 1^b = 1$.

Eve doesn't have to solve DLP.

Public parameter creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.	
Private computations	
Alice	**Bob**
Choose a secret integer a. Compute $A \equiv g^a \pmod{p}$.	Choose a secret integer b. Compute $B \equiv g^b \pmod{p}$.
Public exchange of values	
Alice sends A to Bob $\longrightarrow$ A	
B $\longleftarrow$ Bob sends B to Alice	
Further private computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	

Table 2.2: Diffie–Hellman key exchange

(c) Suppose the order of g is $p-1$. If Eve observes that the value A sent by Alice to Bob is g^{-1}, can Eve easily find out the secret integer a of Alice without solving the discrete logarithm problem? If so, what's the value of a? Justify your answer.

(d) In order to make the Diffie-Hellman Key Exchange protocol to be secure, we should always choose a large value of g. For example, we should not choose $g = 2$ over $g = p-1$ because the discrete logarithm problem with $g = 2$ is easier to solve compared to when $g = p-1$ since 2 is smaller than $p-1$. True or False.

(c) $\text{ord}(g) = p-1$

$A = g^{-1} = g^a \mod p$

$a = -1 \mod p-1$

$a = p-2$

$g^a = A \mod p$

Running time based on $\text{ord}(g)$

Not the value of g.

(d) False.

When $g = p-1$,

$\text{ord}(g) = \text{ord}(p-1) = 2$ because

$(p-1)^2 = p^2 - 2p + 1 \mod p$

$= 1$

So, $p-1$ is a bad choice for g!

Question 5 (4 points)

When witness is found, output composite. When input p is a prime. There is no witness.

Recall the algorithms for primality testing.

(a) Let p be an odd prime. Given the input p (for which you want to test primality), there is a possibility that Fermat's Little primality test will output that p is a composite. True or False? False.

(b) Let n be a Carmichael number. Given the input n (for which you want to test primality) and any positive integer k (for which the number of bases are chosen to test if the base is a witness), there is a possibility that Fermat's little primality test will output that n is a composite. True or False? False. Carmichael is composite and no witness.

(c) Let n be a Carmichael number. Given the input n (for which you want to test primality) and any positive integer k (for which the number of bases are chosen to test if the base is a witness), Miller-Rabin's primality test will always output that n is a composite. True or False? False.

(d) Let n be a composite integer. Given the input n (for which you want to test primality) and any positive integer k (for which the number of bases are chosen to test if the base is a witness).

If Miller Rabin test outputs that n is probably prime, then Fermat's little test will not output that n is composite. In other words, if Miller Rabin test failed to conclude that n is composite, then Fermat's little test will also fail to conclude that n is composite. True or False? false.