1

1.22

a

Let $m \in \mathbb{Z}$. Suppose m is odd. What integer between 1 and $m-1$ is equal to $2^{-1} \bmod m$?

✓ **Answer** ⌄

$\frac{m+1}{2} \equiv 2^{-1} \mod m$

b

More generally, suppose $m = 1 \bmod b$. What integer between 1 and m is equal to $b^{-1} \bmod m$? Verify your answer to part (b) with $b = 6$ and $m = 31$.

✓ **Answer**

$m \equiv 1 \mod b$

$\exists n \in \mathbb{N} : nb = m - 1$

$n = \frac{m-1}{b} \in \mathbb{N}$

$\frac{m-1}{b} \equiv b^{-1} \mod m$

1.32

For each of the following primes p and numbers a, compute $a^{-1} \pmod p$ in two ways:

1. The extended Euclidean algorithm
2. The fast power algorithm and Fermat's little theorem.

a

$p = 47$ and $a = 11$

i

✓ **Answer**

$mp + na = 1$

x	y	N
1	0	47

x	y	N
0	1	11
1	-4	3
-3	13	2
4	-17	1
-11	47	0

$na \mod p = 1$
$n \equiv -17 \equiv 30 \mod p$
$n = 30 = a^{-1}$

ii

✓ **Answer**

$a^p \equiv a^{-1} \mod p$
$47 = 2^5 + 2^3 + 2^2 + 1$

k	$a^{2^k} \mod p$
0	11
1	27
2	24
3	12
4	3
5	9

$a^{32}a^8a^4a = 28512 \equiv 30 = a^{-1} \mod p$

b

$p = 587$ and $a = 345$

i

✓ **Answer**

$mp + na = 1$

x	y	N
1	0	587

x	y	N
0	1	345
1	-1	242
-1	2	103
3	-5	36
-7	12	31
10	-17	5
-67	114	1

$na \mod p = 1$

$n \equiv -114 \mod p$

$n = 114 = a^{-1}$

ii

Answer

$a^p \equiv a^{-1} \mod p$

$587 = 2^9 + 2^6 + 2^3 + 1$

k	$a^{2^k} \mod p$
0	345
1	451
2	299
3	177
4	218
5	564
6	529
7	429
8	310
9	419

$a^{512}a^{64}a^{8}a = 114 = a^{-1} \mod p$

1.34

Recall that g is called a primitive root modulo p if all the powers of g give nonzero elements of $\mathbb{F}_p$.

a

For which of the following primes is 2 a primitive root modulo p?

i

7

Answer

$2, 4, 1 \to 3$

Not a primitive root

ii

13

Answer

$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 \to 12$

Primitive root

iii

19

Answer

$2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1 \to 18$

Primitive root

iv

23

Answer

$2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1 \to 11$

Not a primitive root

b

For which of the following primes is 3 a primitive root modulo p?

i

5

✓ **Answer**

$3, 4, 2, 1 \to 4$

Primitive root

ii

7

✓ **Answer**

$3, 2, 6, 4, 5, 1 \to 6$

Primitive root

iii

11

✓ **Answer**

$3, 9, 5, 4, 1 \to 5$

Not a primitive root

iv

17

✓ **Answer**

$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1 \to 16$

Primitive root

c

Find a primitive root for each of the following primes: $(\mathrm{i})\ 23$, $(\mathrm{ii})\ 29$, $(\mathrm{iii})\ 41$, $(\mathrm{iv})\ 43$

i

23

✓ **Answer**

$a = 5$

$5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1 \to 22$

ii

29

✓ **Answer**

$a = 2$

$2, 4, 8, 16, 3, 6, 12, 24, 19, 9, 18, 7, 14, 28, 27, 25, 21, 13, 26, 23, 17, 5,$
$10, 20, 11, 22, 15, 1 \to 28$

iii

41

✓ **Answer**

$a = 6$

$1, 6, 36, 11, 25, 27, 39, 29, 10, 19, 32, 28, 4, 24, 21, 3, 18, 26, 33, 34, 40,$
$35, 5, 30, 16, 14, 2, 12, 31, 22, 9, 13, 37, 17, 20, 38, 23, 15, 8, 7, 1 \to 40$

iv

43

✓ **Answer**

$a = 3$

$1, 3, 9, 27, 38, 28, 41, 37, 25, 32, 10, 30, 4, 12, 36, 22, 23,$
$26, 35, 19, 14, 42, 40, 34, 16, 5, 15, 2, 6, 18, 11, 33, 13, 39,$
$31, 7, 21, 20, 17, 8, 24, 29, 1 \to 42$

d

Find all the primitive roots $\bmod 11$. Verify that there are exactly $\phi(10)$ of them.

✓ **Answer**

$\phi(10) = |\{1, 3, 7, 9\}| = 4$

$a = 2, 6, 7, 8$

Sources

Wrote and utilized the following code to help find primitive roots:

```
P ← 11
J ← ∵⊂ P (+2⇡(-1P))

# Calculate next number: prev P_A
q ← ◿:⊙(⊏0) ×⊙(⊏1.)

# Duplicate each item as many times as necessary
R ← ≡(↯ -1 ⊏ 0.) J

# Scan sequences
S ← ≡(⬚1\q) R

# Check if is Primitive root
T ← ≡(× ⊃(=2 /+ =1|=1 ⊣)) S

# Reconstruct primitive roots
I ← +2 ⊚ T

I
```