hw2

November 4, 2023

Q1. Use Euclid's algorithm to find the inverse of 31 and 9 in Z_{1025}.

[14]:
```
def extended_gcd(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = extended_gcd(b % a, a)
        return int(g), int(y - (b // a) * x), int(x)

qa, qb = 31, 9
qz = 1025
_, ax, _ = extended_gcd(qa, qz)
_, bx, _ = extended_gcd(qb, qz)
print(f"{qa} * {ax} % 1025 = {(qa * ax) % qz}\n{qb} * {bx} % 1025 = {(qb * bx)
 ↪% qz}")
```

```
31 * 496 % 1025 = 1
9 * 114 % 1025 = 1
```

A1. The inverse of 31 and 9 in Z_{1025} are 496 and 114 respectively.

Q2. Find x such that $x \equiv 3 \pmod{17}$, $x \equiv 9 \pmod{121}$, and $x \equiv 13 \pmod{129}$.

[50]:
```
from itertools import combinations

def product(m: list[int]) -> int:
    total = 1
    for n in m:
        total *= n
    return int(total)

def is_all_coprime(m: list[int]):
    checks = combinations(m, 2)
    for check in checks:
        if extended_gcd(*check)[0] != 1:
            return False
    return True

a = [3, 9, 13]
```

```
n = [17, 121, 129]
M = product(n)

x = 0
for ai, ni in zip(a, n):
    mi = M // ni
    si = extended_gcd(ni, mi)[2]
    x += (ai * si * mi)
x = x % M

print("All a_i and n_i are unique with each other.")
print(f"All n_i are coprime with each other: {is_all_coprime(n)}")
print(f"x = {x}")
for ai, ni in zip(a, n):
    print(f"{x} % {ni} == {ai}: {x % ni == ai}")
```

```
All a_i and n_i are unique with each other.
All n_i are coprime with each other: True
x = 195061
195061 % 17 == 3: True
195061 % 121 == 9: True
195061 % 129 == 13: True
```

A2. $x = 195061$

Q3. Identify all the generators of the cyclic group Z_{29}^*.

[71]:
```
from math import gcd
def is_coprime(a: int, b: int):
    return gcd(a, b) == 1

def get_z_s(z: int) -> set[int]:
    return set(filter(lambda x: is_coprime(x, z), range(z)))

def is_generator(x: int, z: int, z_s: set[int] | None = None, debug: bool =␣
↪False):
    if z_s is None:
        z_s = get_z_s(z)

    if x not in z_s:
        return False

    n: int = x
    generated: set[int] = set([x])
    for _ in range(len(z_s)):
        n = (n * x) % z
        if n in generated:
            break
```

```
        else:
            generated.add(n)

    if debug:
        print(x, generated)
    return z_s == generated

z29_s = get_z_s(29)
generators = set(filter(lambda x: is_generator(x, 29, z29_s, debug=True),␣
 ↪z29_s))
generators
```

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

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

[71]:
```
{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}
```

A3. The generators of Z_{29}^* are 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, and 27.

Q4. Let p_1, p_2, p_3 be three distinct prime numbers. Identify $\phi(p_1^2)$ and $\phi(p_1 p_2 p_3)$.

A4.

$\phi(p_1^2) = p_1^2 - p_1$ because out of the integers between 1 and p_1^2, only the multiples of p_1 (of which there are p_1) are *not* coprime with p_1^2.

$\phi(p_1 p_2 p_3) = \phi(p_1)\phi(p_2)\phi(p_3) = (p_1 - 1)(p_2 - 1)(p_3 - 1)$

[81]:
```
print(f"{len(get_z_s(7*7))=}, {(7*7)-7=}")
print(f"{len(get_z_s(2*3*5))=}, {1*2*4=}")
```

```
len(get_z_s(7*7))=42, (7*7)-7=42
len(get_z_s(2*3*5))=8, 1*2*4=8
```