Number Theory - Homework 2

Philip Warton

January 29, 2021

Problem 8

Find every equivalence class mod 7 that satisfies the condition.

(a)

$\boxed{|x| \leqslant 3}$

$$\{0, 1, 2, 3\}$$

(b)

$\boxed{x \text{ is odd}}$

$$\{1, 3, 5, 6\}$$

(c)

$\boxed{x \text{ is divisible by } 3}$

$$\{0, 3, 6\}$$

(d)

$\boxed{x \text{ is prime}}$

$$\{2, 3, 5\}$$

Problem 9

(a)

$\boxed{k \in \mathbb{Z} \implies k^2 \equiv 0 \text{ (mod 4) or } k^2 \equiv 1 \text{ (mod 4)}}$

Proof. Let $k \in \mathbb{Z}$ be arbitrary. Then we know that mod 4, k is equivalent to either 0, 1, 2, or 3. Then we can square each of these equivalence classes, and find that the only results will be 0 or 1.

$$\begin{aligned} 0^2 &\equiv 0 \\ 1^2 &\equiv 1 \\ 2^2 &\equiv 0 \\ 3^2 &\equiv 1 \end{aligned}$$

$\square$

(b)

$\boxed{\text{If } m \equiv 3 \pmod 4 \text{ then } m \text{ cannot be expressed as the sum of two squares in } \mathbb{Z}}$

Proof. Suppose that m can be expressed as the sum of two squares, that is,

$$a^2 + b^2 = m$$

However, from there we know a^2 and b^2 are equivalent to 0 or 1, thus their sum mod 4 will be equivalent to one of the following

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 2 \end{aligned}$$

Since none of these are 3, we say that m is not equivalent to 3 (mod 4). □

Problem 10

$\boxed{\text{Find } 35^{-1} \in \mathbb{Z}_{97}}$

First we assume that 35 is a unit element mod 97, and is therefore invertible. Then we use the extended euclidean algorithm to find the multiplicative inverse.

$$\begin{aligned} 97 &= (2)35 + 27 \\ 35 &= (1)27 + 8 \\ 27 &= (3)8 + 3 \\ 8 &= (2)3 + 2 \\ 3 &= (1)2 + 1 \end{aligned}$$

$$\begin{aligned} 3 - 2 &= 1 \\ 3 - (8 - (2)3) &= 1 \\ (3)3 - 8 &= 1 \\ (3)(27 - (3)8) - 8 &= 1 \\ (3)27 - (10)8 &= 1 \\ (3)27 - (10)(35 - 27) &= 1 \\ (13)27 - (10)35 &= 1 \\ (13)(97 - (2)35) - (10)35 &= 1 \\ (13)97 - (36)35 &= 1 \end{aligned}$$

From here we can say $(-36)(35) = (-13)97 + 1 \implies (-36)(35) \equiv 1 \pmod{97}$. So then we say that $-36 \equiv 61$ is the multiplicative inverse of 35 mod 97.

Problem 11

$\boxed{\text{Find the } 1 \leqslant x \leqslant 10 \text{, find the order of } x \text{ mod 11. Which of these } x \text{ are primitive roots?}}$

$$
\begin{aligned}
1^1 &\equiv 1 \pmod{11} \\
2^{10} &\equiv 1 \qquad \vdots \\
3^5 &\equiv 1 \\
4^5 &\equiv 1 \\
5^5 &\equiv 1 \\
6^{10} &\equiv 1 \\
7^{10} &\equiv 1 \\
8^{10} &\equiv 1 \\
9^5 &\equiv 1 \\
10^2 &\equiv 1
\end{aligned}
$$

We have primitive roots $\{2, 6, 7, 8, 10\}$.

Problem 12

Show that for every natural number $n, 3^{2n+5} + 2^{4n+1}$ is divisible by 7.

Proof. We use the property that $a \equiv b \pmod{n}$ implies that $ac \equiv bc \pmod{n}$. Then, looking at $\mathbb{Z}_7$ we write the following:

$$
\begin{aligned}
3^{2n+5} + 2^{4n+1} &\equiv (3^5)3^{2n} + (2)2^{4n} \\
&\equiv (5)3^{2n} + (2)2^{4n} \\
&\equiv (5)(3^2)^n + (2)(2^4)^n \\
&\equiv (5)2^n + (2)2^2 \\
&\equiv 7(2^n) \equiv 0 \pmod{7}
\end{aligned}
$$

□

Problem 13

Code:

```
def smallest_prime_factor(n):
    if n % 2 == 0:
        return 2
    else:
        x = 3
        while True:
            if n % x == 0:
                return x
            x = x + 2

print(smallest_prime_factor(594088117))
print(smallest_prime_factor(346132737927421))
```

Output:

```
7
592759
```

Problem 14

Code:

```
def compute_order(a, n):
    if a % n == 1:
        return 1
    for i in range(2,n):
        if a^i % n == 1:
            return i

print(compute_order(17, 100))
print(compute_order(100001, 11111))
```

Output:

```
20
540
```

Problem 15

Code:

```
primes = [101,103,107]

def find_smallest_primitive_root(n):
    for a in range(1, n):
        if compute_order(a, n) == n - 1:
            return a

for p in primes:
    print(find_smallest_primitive_root(p))
```

Output:

```
2
5
2
```