Winter 2021 MTH 440/540 Homework 2

Instructions. Due via Gradescope on Friday January 29. Solutions must be typed. Problems not marked with * are required for everyone. Problems marked with $*$ are required for 540 students and are optional challenge problems for 440 students (they will not be graded for 440 students). Use Sage only on problems which explicitly say to use Sage; solve all other problems "by hand" and show your calculations.)

8. For each part, find a complete set S of congruence class representatives modulo 7 satisfying the stated property. (You do not have to explain your answers for this problem.)

(a) Every element x of S satisfies $|x| \leq 3$.

$S = \{-3, -2, -1, 0, 1, 2, 3\}$

(b) Every element of S is odd.

$S = \{1, 3, 5, 7, 9, 11, 13\}$

(c) Every element of S is divisible by 3.

$S = \{0, 3, 6, 9, 12, 15\}$

(d) Every element of S is prime.

$S = \{2, 3, 5, 7, 11, 13, 29\}$

9.

(a) Show that if $k \in \mathbb{Z}$, then either $k^2 \equiv 0 \pmod 4$ or $k^2 \equiv 1 \pmod 4$.

Let $k \in \mathbb{Z}$ be arbitrary. Modular arithmetic is compatible with exponentiation, such that $a \equiv b \pmod n \implies a^m \equiv b^m \pmod n$ for any non-negative integer m. Given some k, k is congruent to either $0 \pmod 4$, $1 \pmod 4$, $2 \pmod 4$, or $3 \pmod 4$. If we now square each side, we have 4 possible cases:

$k^2 \equiv 0^2 \pmod 4 \equiv 0 \pmod 4$
$k^2 \equiv 1^2 \pmod 4 \equiv 1 \pmod 4$
$k^2 \equiv 2^2 \pmod 4 \equiv 4 \pmod 4 \equiv 0 \pmod 4$
$k^2 \equiv 3^2 \pmod 4 \equiv 9 \pmod 4 \equiv 1 \pmod 4$

In all cases, we have either $k^2 \equiv 0 \pmod 4$ or $k^2 \equiv 1 \pmod 4$.

(b) Show that if $m \equiv 3 \pmod 4$, then m cannot be expressed as the sum of two squares in $\mathbb{Z}$.

From above, we know the square of any $k \in \mathbb{Z}$ is either $0 \pmod 4$ or $1 \pmod 4$. Without loss of generality, there are three cases when summing two squares $\pmod 4$: both are congruent to 0 (mod 4), both are congruent to 1 (mod 4), or one square is congruent to either. We can then show for each case,

$0 \pmod 4 + 0 \pmod 4 \equiv (0 + 0) \pmod 4 \equiv 0 \pmod 4$
$0 \pmod 4 + 1 \pmod 4 \equiv (0 + 1) \pmod 4 \equiv 1 \pmod 4$
$1 \pmod 4 + 1 \pmod 4 \equiv (1 + 1) \pmod 4 \equiv 2 \pmod 4$

We can then see that the sum of two squares may only be $[0]_4$, $[1]_4$, or $[2]_4$, so if we are given some $m \in \mathbb{Z}$ such that $m \equiv 3$ (mod 4), it is impossible to express m as the sum of two squares in $\mathbb{Z}$.

10. Find $x \in \mathbb{Z}$ such that $35x \equiv 1 \pmod{97}$.

We can re-frame this as finding the inverse of $35 \pmod{97}$. We can do this by applying Euclid's extended algorithm. First, to find $\gcd(35, 97)$:

$97 = 2 \cdot 35 + 27$
$35 = 1 \cdot 27 + 8$
$27 = 3 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

The remainder before the final step is 1, so we have $\gcd(35, 97) = 1$. We may now carry out the extended part of the algorithm:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1(8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8$
$1 = 3(27 - 3 \cdot 8) - 1 \cdot 8 = 3 \cdot 27 - 10 \cdot 8$
$1 = 3 \cdot 27 - 10(35 - 1 \cdot 27) = 13 \cdot 27 - 10 \cdot 35$
$1 = 13(97 - 2 \cdot 35) - 10 \cdot 35 = 13 \cdot 97 - 36 \cdot 35$

So we have $1 \equiv (-36) \cdot 35 \pmod{97}$, so -36 is the inverse of 35 mod 97. We can then take $x = -36 + 97n \; \forall n \in \mathbb{Z}$.

11. For each $1 \leq x \leq 10$, find the order of x modulo 11. Which of these x are primitive roots?
To find the order of each x, we work through progressive powers of x until $x \equiv 1 \pmod{11}$. For the sake of saving on notation, $x \equiv y \implies x \equiv y \pmod{11}$.

$x = 1:$
$1^1 \equiv 1 \implies O_{11}(1) = 1$

$x = 2:$

$2^1 \equiv 2$
$2^2 \equiv 2 \cdot 2 \equiv 4$
$2^3 \equiv 2 \cdot 4 \equiv 8$
$2^4 \equiv 2 \cdot 8 \equiv 16 \equiv 5$
$2^5 \equiv 2 \cdot 5 \equiv 10$
$2^6 \equiv 2 \cdot 10 \equiv 20 \equiv 9$
$2^7 \equiv 2 \cdot 9 \equiv 18 \equiv 7$
$2^8 \equiv 2 \cdot 7 \equiv 14 \equiv 3$
$2^9 \equiv 2 \cdot 3 \equiv 6$
$2^{10} \equiv 2 \cdot 6 \equiv 12 \equiv 1 \implies O_{11}(2) = 10$

$x = 3:$

$3^1 \equiv 3$
$3^2 \equiv 3 \cdot 3 \equiv 9$
$3^3 \equiv 3 \cdot 9 \equiv 27 \equiv 5$
$3^4 \equiv 3 \cdot 5 \equiv 15 \equiv 4$
$3^5 \equiv 3 \cdot 4 \equiv 12 \equiv 1 \implies O_{11}(3) = 5$

$x = 4:$

$4^1 \equiv 4$

$4^2 \equiv 4 \cdot 4 \equiv 16 \equiv 5$

$4^3 \equiv 4 \cdot 5 \equiv 20 \equiv 9$

$4^4 \equiv 4 \cdot 9 \equiv 36 \equiv 3$

$4^5 \equiv 4 \cdot 3 \equiv 12 \equiv 1 \implies O_{11}(4) = 5$

$x = 5:$

$5^1 \equiv 5$

$5^2 \equiv 5 \cdot 5 \equiv 25 \equiv 3$

$5^3 \equiv 5 \cdot 3 \equiv 15 \equiv 4$

$5^4 \equiv 5 \cdot 4 \equiv 20 \equiv 9$

$5^5 \equiv 5 \cdot 9 \equiv 45 \equiv 1 \implies O_{11}(5) = 5$

$x = 6:$

$6^1 \equiv 6$

$6^2 \equiv 6 \cdot 6 \equiv 36 \equiv 3$

$6^3 \equiv 6 \cdot 3 \equiv 18 \equiv 7$

$6^4 \equiv 6 \cdot 7 \equiv 42 \equiv 9$

$6^5 \equiv 6 \cdot 9 \equiv 54 \equiv 10$

$6^6 \equiv 6 \cdot 10 \equiv 60 \equiv 5$

$6^7 \equiv 6 \cdot 5 \equiv 30 \equiv 8$

$6^8 \equiv 6 \cdot 8 \equiv 48 \equiv 4$

$6^9 \equiv 6 \cdot 4 \equiv 24 \equiv 2$

$6^{10} \equiv 6 \cdot 2 \equiv 12 \equiv 1 \implies O_{11}(6) = 10$

$x = 7:$

$7^1 \equiv 7$

$7^2 \equiv 7 \cdot 7 \equiv 49 \equiv 5$

$7^3 \equiv 7 \cdot 5 \equiv 35 \equiv 2$

$7^4 \equiv 7 \cdot 2 \equiv 14 \equiv 3$

$7^5 \equiv 7 \cdot 3 \equiv 21 \equiv 10$

$7^6 \equiv 7 \cdot 10 \equiv 70 \equiv 4$

$7^7 \equiv 7 \cdot 4 \equiv 28 \equiv 6$

$7^8 \equiv 7 \cdot 6 \equiv 42 \equiv 9$

$7^9 \equiv 7 \cdot 9 \equiv 63 \equiv 8$

$7^{10} \equiv 7 \cdot 8 \equiv 56 \equiv 1 \implies O_{11}(7) = 10$

$x = 8:$

$8^1 \equiv 8$

$8^2 \equiv 8 \cdot 8 \cdot 64 \equiv 9$

$8^3 \equiv 8 \cdot 9 \cdot 72 \equiv 6$

$8^4 \equiv 8 \cdot 6 \equiv 48 \equiv 4$

$8^5 \equiv 8 \cdot 4 \equiv 32 \equiv 10$

$8^6 \equiv 8 \cdot 10 \equiv 80 \equiv 3$

$8^7 \equiv 8 \cdot 3 \equiv 24 \equiv 2$

$8^8 \equiv 8 \cdot 2 \equiv 16 \equiv 5$

$8^9 \equiv 8 \cdot 5 \equiv 40 \equiv 7$
$8^{10} \equiv 8 \cdot 7 \equiv 56 \equiv 1 \implies O_{11}(8) = 10$

$x = 9:$
$9^1 \equiv 9$
$9^2 \equiv 9 \cdot 9 \equiv 81 \equiv 4$
$9^3 \equiv 9 \cdot 4 \equiv 36 \equiv 3$
$9^4 \equiv 9 \cdot 3 \equiv 27 \equiv 5$
$9^5 \equiv 9 \cdot 5 \equiv 45 \equiv 1 \implies O_{11}(9) = 5$

$x = 10:$
$10^1 \equiv 10$
$10^2 \equiv 10 \cdot 10 \equiv 100 \equiv 1 \implies O_{11}(10) = 2$

12. Show that for all $n \geq 1$, $3^{2n+5} + 2^{4n+1}$ is divisible by 7.

We start with the base case $n = 1$:
$3^{2(1)+5} + 2^{4(1)+1} \pmod 7 \equiv 3^7 + 2^5 \pmod 7 \equiv 2187 \pmod 7 + 32 \pmod 7 \equiv 3 \pmod 7 + 3 \pmod 7 \equiv 7 \pmod 7 \equiv 0 \pmod 7$
So we see the property holds for $n = 1$. Now assume $3^{2n+5} + 2^{4n+1} \pmod 7 \equiv 0$ for some $n \in \mathbb{N}$. We then see
$3^{2(n+1)+5} + 2^{4(n+1)+1} \pmod 7 \equiv 3^{2n+5+2} + 2^{4n+1+4} \pmod 7 \equiv 3^{2n+5} \cdot 3^2 + 2^{4n+1} \cdot 2^4 \pmod 7 \equiv 3^{2n+5} \cdot 3^2 \pmod 7 + 2^{4n+1} \cdot 2^4 \pmod 7 \equiv 3^{2n+5} \cdot 9 \pmod 7 + 2^{4n+1} \cdot 16 \pmod 7 \equiv 3^{2n+5} \cdot 2 \pmod 7 + 2^{4n+1} \cdot 2 \pmod 7 \equiv 2 \cdot (3^{2n+5} + 2^{4n+1}) \pmod 7 \equiv 2 \cdot 0 \pmod 7 \equiv 0,$
so the $n + 1$th term is divisible by 7 as well. By the principle of induction, $3^{2n+5} + 2^{4n+1}$ is divisible by 7 for all $n \geq 1$. ☠

13. Write a program in Sage which inputs an integer $n \geq 2$, and outputs the smallest prime factor of n. You may use Sage's `is_prime()` command, but do not use powerful commands such as `factor()` to find the prime divisors of n. Use your program to find the smallest prime factors of 6594088117 and 346132737927421.

```
def least_prime_factor(n):
    if is_prime(n): return n
    if n % 2 == 0: return 2
    len = int(sqrt(n)) + 1
    factors = [0] * len

    # factors[i] == 0 denotes prime, 1 denotes composite

    # prime seive
    for i in range(2, len):
        if factors[i] == 0:
            if n % i == 0: return i
            for j in range(2 * i, len, i):
                factors[j] = 1


print(least_prime_factor(6594088117))
print(least_prime_factor(346132737927421))
```

```
> 1487
> 592759
```

The least prime factors of 6594088117 and 346132737927421 are 1487 and 592759, respectively.

14. Write a program in Sage which inputs integers a and n with $n \geq 1$ and $\gcd(a, n) = 1$, and outputs the order of a modulo n, according to the following simple algorithm: successively test $a^1, a^2, a^3, \ldots$ until the first k occurs for which $a^k \equiv 1 \pmod{n}$, and report that the number k is the order of a modulo n. Test your program by finding the order of 17 modulo 100 and the order of 10001 modulo 11111.

```
def order_mod_n(a, n):
    k = 1
    check = a
    while k <= n:
        if check % n == 1: return k
        check = (check * a) % n
        k = k + 1
    return -1 # no result catch

print(order_mod_n(17, 100))
print(order_mod_n(10001, 11111))

> 20
> 1080
```

The order of 17 $\pmod{100}$ is 20 and the order of 10001 $\pmod{11111}$ is 1080.

15. For each of the primes $p = 101, 103, 107$, use your Sage program from problem **14** to find the smallest positive primitive root modulo p.

```
primes = [101, 103, 107]
for p in primes:
    a = 2
    while order_mod_n(a, p) != p - 1:
        a = a + 1
    print(a)

> 2
> 5
> 2
```

The smallest primitive roots modulo $101, 103, 107$ are $2, 5, 2$ respectively.
$\mathcal{K}$