Number Theory: Diophantine Equations and Orders

1.
Factoring Tricks

Common Factoring Tricks

- polynomial factoring
  - $x^3 - 3x^2 - 4x + 12$
- completing the rectangle / Simon's Favorite Factoring Trick
  - $xy+3x-2y-6=10$ x,y are positive integers
  - $xy^2 + xy - 2y^2 - 6x - 2y + 6 = 0$ x,y are integers

Cubics

- $(x+y)(y+z)(z+x) = 2xyz + (x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2)$
- $(x+y+z)^3 = x^3 + y^3 + z^3 + 6xyz + 3(x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2)$
- $(x+y+z)(x^2+y^2+z^2) = x^3 + y^3 + z^3 + (x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2)$

- $(x+y+z)^3 = x^3 + y^3 + z^3 + 3(x+y)(y+z)(z+x)$
- $(x+y+z)^3 = (x+y+z)(x^2+y^2+z^2) + 2(x+y)(y+z)(z+x) + 2xyz$

2. Bounding

The idea is to create inequalities from a set of equations.

Example #1

$$x^3 + y^3 = 1$$

$$x^4 + y^4 = 1$$

Example #2: 2021 AMO #1

Let a, b and c be positive integers. Vaughan arranges abc identical white unit cubes into an $a \times b \times c$ rectangular prism and paints the outside of the prism red. After disassembling the prism back into unit cubes, he notices that the number of faces of the unit cubes that are red is the same as the number that are white.

Find all values that the product abc could take.

3. Orders

Powers of 2 mod 5

- $2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 3, \quad 2^4 \equiv 1, \quad 2^5 \equiv 2, \quad 2^6 \equiv 2$
- We say **the order of 2 mod 5** is **4**, because 2^4 is the first time $2^d \equiv 1 \bmod 5$.

What is **the order of 3 mod 5**?

- $3^1 \equiv 3, \quad 3^2 \equiv 4 \equiv -1, \quad \ldots \quad 3^4 \equiv 1$

Definition of an Order

- Let d be the order of a mod p.
- Then, **d is the minimal solution to x** in **$a^x \equiv 1 \bmod p$**.

What is **the order of 3 mod 37**?

- $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27$, $3^4 \equiv 7$, $3^5 \equiv 21$, $3^6 \equiv 26$,
- $3^7 \equiv 4$, $3^8 \equiv 12$, $3^9 \equiv 36 \equiv -1$, … $3^{18} \equiv 1$

Euler's Theorem

- $a^{\varphi(n)} \equiv 1 \pmod{n}$
- $\varphi(n) = n * \Pi (1-1/p)$
  - $\varphi(15) = \varphi(3*5) = 15 * (1-⅓) * (1-⅕) = 15 * ⅔ * ⅘ = 8$
  - $\varphi(18)$?
    - $\varphi(2*3^2) = 18 * (1-½) * (1-⅓) = 18 * ½ * ⅔ = 6$

- If d is the order, then $a^d \equiv 1 \pmod{n}$. By Euler's Theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$. **Therefore, d divides φ(n).**

Prime Mods

- Whenever we're dealing with orders, mod primes work the best.
  - Why? For one, orders become much easier to calculate/express. Also, same goes for $\varphi(n)$. (Recall Euler's Theorem.)
  - Also, for a prime p modulus, there exist a *primitive root* g, such that **the order of g mod p is p-1**.
    - $\{1, 2, 3, \ldots, p\} = \{g^1, g^2, g^3, \ldots g^{p-1}\}$

Practice: *Repunits*

- A *repunit* is a number consisting only of the digit 1, such as 111 and 11111. Find the smallest repunit divisible by 21.

Summary

- 3 Classic Number Theory Methods:
  - Factoring Tricks
  - Bounding
  - Orders
- $\varphi(n)$ is a common late-AMC / mid-late AIME topic as well
- orders on the AMC come up indirectly (as in the practice problem in the preceding slide)
  - for the AMC, just knowing that they exist and the special case for prime modulus is enough