MATH 430 Fall 2020

Midterm 1

QILIN YE

Due by Sep 14th 2020 11:59 PM PST on Gradescope

Instructions: Midterm 1 is open notes and open textbook but closed to internet searches. Calculators are allowed though not needed. You are required to do the exam by yourself and not take the help of any person. Make sure you write down proper steps and reasons, mention any theorem/result you use in your solutions etc. Correct solutions but with unjustified/poorly reasoned claims will not receive full credit.

Answer all questions (5×10 points)

1. Let a, b, N, K all be integers > 1. Given that $gcd(a^N, b^K) = 1$, find $gcd(a, b)$. Explain your answer with reasons.
2. Show that 8007 is NOT a sum of three squares. Explain your answer with reasons (Hint: Think mod 8)
3. Solve for x where $16x + 10 \cong 46 \mod 37$. Show neat steps
4. Find three consecutive integers, the first of which is divisible by a square, the second by a cube and the third by a fourth power. Show neat steps.
5. For some integer, $n > 1$, you are given than $2^{10} \cong 1 \mod n$ and $3^5 \cong 1 \mod n$. Find a value i where $0 \leq i \leq n-1$ so that
$$6(2^{2019} + 3^{2019}) \cong i \mod n.$$
Explain your answer with reasons.

1) Suppose $gcd(a,b) = n > 1$, then we have $n \mid a$ and $n \mid b$. Therefore

$n \mid a \Rightarrow n \mid a^N$ and $n \mid b \Rightarrow n \mid b^K$.

Hence $n > 1$ is a common divisor of a^N and b^K, Contrary to $gcd(a^N, b^K) = 1$.

Therefore $gcd(a,b) = 1$.

2) Computing the remainders of squares when divided by 8 by brute force:

In $\mathbb{Z}/8\mathbb{Z}$.

$[0]^2 = [0] = [0]$

$[1]^2 = [1] = [1]$

$[2]^2 = [4] = [4]$

$[3]^2 = [9] = [1]$

$[4]^2 = [16] = [0]$

$[5]^2 = [25] = [1]$

$[6]^2 = [36] = [4]$

$[7]^2 = [49] = [1]$.

and $[8007] = [8000 + 7] = [7]$.

Since it's impossible to get $[7]$ (or $[15]$) as a sum of three elements in the set $\{[0], [1], [4]\}$ (with replacement so that each can be picked multiple times), we conclude that 8007 can't be written as the sum of 3 squares.

3. $16x + 10 \equiv 46 \pmod{37} \Leftrightarrow 16x \equiv 36 \equiv -1 \pmod{37}$.

Then, for some $y \in \mathbb{Z}$ we have

$$16x + 37y = -1$$
$$\Rightarrow 16(-x) + 37(-y) = 1.$$

Since $gcd(16, 37) = 1$. there will be solutions. Now apply Euclid's Algorithm.

$37 = 16 \times 2 + 5 \Rightarrow 5 = 16 \times (-2) + 37 \times 1$

$16 = 5 \times 3 + 1 \Rightarrow 1 = 16 \times 1 + 5 \times (-3)$

$= 16 \times 1 + 16 \times 6 + 37 \times (-3)$

$= 16 \times 7 + 37 \times (-3)$.

Hence $16 \times 7 + 37 \times (-3) = 1 \Rightarrow 16 \times (-7) = 37 \times (-3) - 1$.

$\Rightarrow 16 \times (-7) \equiv -1 \pmod{37}$

$\Rightarrow 16 \times (-7) + 10 \equiv 9 \equiv 46 \pmod{37}$

$\Rightarrow$ Set of solutions $= \{-7 + 37k, k \in \mathbb{Z}\}$

$= \{30 + 37k, k \in \mathbb{Z}\}$

4. For simplicity let's make the divisors as small as possible:

4th power $\rightarrow 2^4 = 16$, cube: $3^3 = 27$, square: $5^2 = 25$.

Suppose the largest number among the three is n, then

$$\begin{cases} 25 \mid n-2 \\ 27 \mid n-1 \\ 16 \mid n \end{cases} \Rightarrow \begin{cases} n \equiv 2 \pmod{25} & ① \\ n \equiv 1 \pmod{27} & ② \\ n \equiv 0 \pmod{16} & ③ \end{cases}$$

By the Chinese Remainder Theorem,

we first find x such that $\begin{cases} x \equiv 2 \pmod{25} \\ 27 \cdot 16 \mid x. \end{cases}$

Note in $\mathbb{Z}/25\mathbb{Z}$, $[27 \cdot 16] = [432] = [7]$.

Since $[7] \times [7] = [49] = [-1]$, we know $[7] \times [-14] = [2]$.

Hence let $x = (-14) \cdot 27 \cdot 16 = -6048$.

Now find b such that $\begin{cases} b \equiv 1 \pmod{27} \\ 25 \cdot 16 \mid b. \end{cases}$

In $\mathbb{Z}/27\mathbb{Z}$, $[25 \cdot 16] = [400] = [-5]$.

Note that $[-5][16] = [-80] = [1]$, hence let $b = 16 \cdot 25 \cdot 16 = 6400$.

Finally, find c such that $\begin{cases} c \equiv 0 \pmod{16} \\ 25 \cdot 27 \mid c. \end{cases}$

Obviously we can let $c = 16 \cdot 25 \cdot 27 = 400 \cdot 27 = 10800$.

Then $a + b + c = 11152$ is the number we want.

Furthermore, $11152 - lcm(25, 27, 16) = 352$ also works.

Verification: $\begin{cases} 350 = 25 \times 14 \\ 351 = 27 \times 13 \\ 352 = 16 \times 22. \end{cases}$

Hence one solution is $\{350, 351, 352\}$.

5. From $2^{10} \equiv 3^5 \equiv 1 \pmod{n}$ we know

$n \mid 1023$ and $n \mid 242$.

Since $1023 = 3 \times 11 \times 30$. $242 = 2 \times 11^2$.

if $n > 1$ then the only possibility is $n = 11$.

In $\mathbb{Z}/11\mathbb{Z}$, we have

$[6(2^{2019} + 3^{2019})]$

$= [6(2^{2010+9} + 3^{2015+4})]$

$= [6 \cdot 2^{2010} \cdot 2^9 + 6 \cdot 3^{2015} \cdot 3^4]$

$= [6][2^9] + [6][3^4]$.

$= [6][6] + [6][4]$

$= [60]$

$= [5]$.

Hence $i = 5$.