Math 362 Assignment 2

Due: Wednesday, October 2

- Answer all questions. Each question is worth 5 marks. Full marks will be awarded only for answers that are both mathematically correct and coherently written.
- Please consider the markers and write neatly and legibly! I have instructed the markers to ignore work they cannot read. (And I won't read it, either.)

1. Squares:

   (a) The prime power decomposition (ppd) of an integer $n \geq 2$ is given by $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. Give a necessary and sufficient condition for n to be a square.

   (b) Which integers n, where $2 \leq n \leq 20$, can be written as the sum of **two** squares? For example, $9 = 0^2 + 3^2$. Express each such integer as such a sum. Also give the ppd of n.

   (c) Show that if $n \equiv 3 \pmod 4$, then n cannot be written as the sum of the squares of two integers. (**Remember this result!**)

   (d) Which integers n, where $2 \leq n \leq 20$, can be written as the sum of **three** squares? For example, $5 = 0^2 + 1^2 + 2^2$. Express each such integer as such a sum.

   (e) What do the numbers in (d) that cannot be expressed as the sum of three squares have in common? (Think of a property that is not shared by any other number from 2 to 20.)

Answer

(a) The integer $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ is square if and only if each e_i is even and positive.

(b)
$$\begin{array}{rrr} 2 = 1^2 + 1^2 & 4 = 2^2 = 0^2 + 2^2 & 5 = 1^2 + 2^2 \\ 8 = 2^3 = 2^2 + 2^2 & 9 = 3^2 = 0^2 + 3^2 & 10 = 2 \cdot 5 = 1^2 + 3^2 \\ 13 = 2^2 + 3^2 & 16 = 2^4 = 0^2 + 4^2 & 17 = 1^2 + 4^2 \\ 18 = 2 \cdot 3^2 = 3^2 + 3^2 & 20 = 2^2 \cdot 5 = 2^2 + 4^2 & \end{array}$$

(c) If $n \equiv 3 \pmod 4$, then n is odd. Suppose, to the contrary, that a and b are integers such that $n = a^2 + b^2$. Then one of a and b is even, the other one odd. Assume without loss of generality that a is even and b is odd. Then $a \equiv 0$ or $2 \pmod 4$, so $a^2 \equiv 0 \pmod 4$, while $b \equiv 1$ or $3 \pmod 4$, so $b^2 \equiv 1 \pmod 4$. But then

$$3 \equiv n \equiv 0 + 1 \equiv 1 \pmod 4,$$

which is impossible because 4 does not divide $3 - 1 = 2$. Therefore n cannot be written as the sum of the squares of two integers.

(d) Any integer that can be written as the sum of two squares can be written as the sum of three squares – just add (another) 0^2. The integers that cannot be written as the sum of two squares, but **can** be written as the sum of three squares, are below.

$$3 = 1^2 + 1^2 + 1^2 \qquad 6 = 2 \cdot 3 = 1^2 + 1^2 + 2^2 \qquad 11 = 1^2 + 1^2 + 3^2$$
$$12 = 2^2 \cdot 3 = 2^2 + 2^2 + 2^2 \qquad 14 = 2 \cdot 7 = 1^2 + 2^2 + 3^2 \qquad 19 = 1^2 + 3^2 + 3^2$$

(e) Only two integers remain, namely 7 and 15. They are both congruent to 7 (mod 8).

2. (a) Given that n is a positive integer, determine the least residue of $2485234^n \pmod 9$.

(b) Given that $k \equiv 3 \pmod 5$, determine the least residue of $2k^2 + 19^3 \pmod 5$.

(c) Given that $k \equiv 3 \pmod 8$, determine the least residue of $5k^{333} + 23^{123} \pmod 8$.

Answer

(a) Since $2485234 \equiv 1 \pmod 9$, the least residue of $2485234^n \pmod 9$ is $\boxed{1}$ for all $n \geq 1$.

(b) Since $k \equiv 3 \pmod 5$ and $19 \equiv -1 \pmod 5$, $2k^2 + 19^3 \equiv 2(3)^2 - 1 \equiv -3 \equiv 2 \pmod 5$. The least residue is $\boxed{2.}$

(c) Since $k \equiv 3 \pmod 8$ and $23 \equiv -1 \pmod 8$,

$$5k^{333} + 23^{123} \equiv 5(3)^{333} + (-1)^{123} \equiv -3(3)^{333} - 1 \equiv -(3^2)^{167} \equiv -1 - 1 \equiv 6 \pmod 8.$$

The least residue is $\boxed{6.}$

3. Solve the congruences

(a) $7x \equiv 13 \pmod{15}$

(b) $8x \equiv 12 \pmod{28}$

(c) $13x \equiv 352 \pmod{1261}$.

Answer

(a) Since $(7, 15) = 1$, the congruence has exactly one solution. Since

$$7x \equiv 13 \equiv 28 \pmod{15}$$

(and again since $(7, 15) = 1$), $\boxed{x = 4.}$

(b) Since $(8, 28) = 4$ and $4|12$, the congruence has four solutions. Simplifying, we get

$$2x \equiv 3 \equiv 10 \pmod{7},$$

so that $x \equiv 5 \pmod{7}$ because $(2, 7) = 1$. The solutions are $\boxed{x \in \{5, 12, 19, 26\}.}$

(c) Since $1261 = 13 \times 97$ and $352 = 2^5 11$, $(13, 1261) = 13$ (or you could use the Euclidean algorithm). Since $13 \nmid 352$, the congruence has no solutions.

4. A school has between 500 and 800 students who registered to participate in sports days to raise money for charity. On Sports Day 1, they all play tennis. Each tennis team consists of four students, two to play singles matches, and a pair to play doubles matches. So they are grouped into teams of size four, but three students are left over. On Sports Day 2, they all play cricket. Each cricket team consists of 11 students. So they are grouped into teams of size 11, but nine students are left over. On Sports Day 3, they all play rugby. Each rugby team consists of 15 students. So they are grouped into teams of size 15, and no students are left over.

   How many students registered to participate in sports days?

   Answer

   Suppose x students registered for sports days. The only important information from the above paragraph is

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 9 \pmod{11} \\ x &\equiv 0 \pmod{15}. \end{aligned}$$

   Since $4, 11$ and 15 are pairwise relatively prime, the system has a unique solution, modulo $4 \cdot 11 \cdot 15$ (by the Chinese Remainder Theorem).

   From the third congruence, $x \equiv 0 \pmod{15}$. Hence there exists $a \in \mathbb{Z}$ such that $x = 15a$. From the first congruence, $15a \equiv 3a \equiv 3 \pmod{4}$, hence $a \equiv 1 \pmod{4}$, since $(3, 4) = 1$.

   Say $a = 4b + 1$, $b \in \mathbb{Z}$. Substituting in the equation for x, we get $x = 15(4b + 1) = 60b + 15$. From the second congruence, $x \equiv 9 \pmod{11}$. Therefore $60b + 15 \equiv 5b + 4 \equiv 9 \pmod{11}$. Therefore $5b \equiv 5 \pmod{11}$, and since $(5, 11) = 1$, we see that $b \equiv 1 \pmod{11}$. Say $b = 11c + 1$, $c \in \mathbb{Z}$.

   Then $x = 60b + 15 = 60(11c + 1) + 15 = 660c + 75$.

   Choosing $c = 1$ (the only value that would give a number between 500 and 800, we see that $\boxed{735}$ students registered for sports days.

5. The same school as above has between 150 and 200 students who have registered for grade 12 chemistry, grade 12 physics and grade 11 math. The grade 12 chemistry lab can only accommodate 12 students at a time, the physics lab can accommodate 20 students at a time, and the math classroom with computers can accommodate 36 students at a time. When the administrative assistant groups these students in classes of size 12, 20 or 36, seven students are always left over.

   How many students registered to take these three subjects?

   Answer

   Suppose x students registered to take these subjects. The information above gives the congruences

$$x \equiv 7 \pmod{12}$$
$$x \equiv 7 \pmod{20}$$
$$x \equiv 7 \pmod{36}.$$

   Since $x \equiv 7 \pmod{36}$ implies that $x \equiv 7 \pmod{12}$, we can ignore the congruence $x \equiv 7 \pmod{12}$.

   Also, $x \equiv 7 \pmod{20}$ implies that $x \equiv 2 \pmod{5}$. Say $x = 5a + 2,\ a \in \mathbb{Z}$.

   Substitution in the third congruence gives $5a + 2 \equiv 7 \pmod{36}$, so $a \equiv 1 \pmod{36}$ since $(5, 36) = 1$. Say $a = 36b + 1,\ b \in \mathbb{Z}$. Then $x = 5(36b + 1) + 2 = 180b + 7$. The only value of b that gives a number between 150 and 200 is $b = 1$, thus $\boxed{187}$ students registered for these subjects.

6. Use Fermat's Theorem to determine the least residue of

   (a) $3^{311} \pmod{23}$

   (b) $24^{36n+3} + 11 \pmod{19}$, where $n \in \mathbb{N}$.

   Answer

   (a) Since 23 is prime and $(3, 23) = 1$, $3^{22} \equiv 1 \pmod{23}$. Since $311 = 14 \cdot 22 + 3$,

$$3^{311} \equiv (3^{22})^{14} 3^3 \equiv 3^3 \equiv 4 \pmod{23}.$$

   The least residue is $\boxed{4.}$

   (b) Since $24 \equiv 5 \pmod{19}$ and 19 is prime (and $(5, 19) = 1$), $5^{18} \equiv 1 \pmod{19}$. Therefore

$$24^{36n+3} + 11 \equiv (5^{18})^{2n} \cdot 5^3 + 11 \equiv 6 \cdot 5 + 11 \equiv 3 \pmod{19}.$$

   The least residue is $\boxed{3.}$

7. (a) What is the remainder when 2019^{2019} is divided by 22? (No long stories!)

   (b) What is the remainder when $2019^{2019} \cdot 18!$ is divided by 247?

Answer

(a) Since $2019 \equiv 9-1-2 \equiv 6 \pmod{11}$ and 11 is prime, $2019^{10} \equiv 6^{10} \equiv 1 \pmod{11}$. Hence

$$2019^{2019} \equiv (6^{10})^{201} \cdot 6^9 \equiv 2 \pmod{11}.$$

Hence $2019^{2019} \equiv 2$ or $13 \pmod{22}$. But 2019^{2019} is odd, hence $2019^{2019} \equiv 13 \pmod{22}$. The remainder is $\boxed{13.}$

(b) Let $x = 2019^{2019} \cdot 18!$.

Note that $247 = 13 \times 19$. Since $13|18!$, $x \equiv 0 \pmod{13}$.

Since 19 is prime, $18! \equiv -1 \pmod{19}$.

Also, $2019 \equiv 5 \pmod{19}$ and $2019 = 112 \cdot 18 + 3$. Hence

$$x \equiv 2019^{2019} \cdot 18! \equiv (5^{18})^{112} 5^3 (-1) \equiv -5^3 \equiv -11 \equiv 8 \pmod{19}.$$

Say $x = 19a+8$, where $a \in \mathbb{Z}$, and substitute in the congruence $x \equiv 0 \pmod{13}$. This gives

$$19a \equiv 6a \equiv -8 \equiv 5 \equiv 18 \pmod{13}$$

and since $(6, 13) = 1$, $a \equiv 3 \pmod{13}$. Therefore $a = 13b+3$, $b \in \mathbb{Z}$, from which it follows that

$$x = 19a + 8 = 19(13b + 3) + 8 = 247b + 65.$$

The remainder is $\boxed{65.}$