

Peize Liu  
*St. Peter's College*  
*University of Oxford*

**Problem Sheet 1**  
**ASO: Number Theory**

April 29, 2020

**Question 1**

Let  $a$  be the positive integer and suppose that in its decimal expansion it has 7 digits:  $a = a_0 + 10a_1 + \cdots + 10^6a_6$ . Show that  $a$  is divisible by 7 if and only if  $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6$  is divisible by 7.

*Proof.* We have:

$$10 \equiv 3 \pmod{7}$$

$$10^2 \equiv 3^2 \equiv 2 \pmod{7}$$

$$10^3 \equiv 2 \cdot 3 = 6 \equiv -1 \pmod{7}$$

$$10^4 \equiv 2^2 = 4 \equiv -3 \pmod{7}$$

$$10^5 \equiv 4 \cdot 3 \equiv -2 \pmod{7}$$

$$10^6 \equiv 2 \cdot 4 \equiv 1 \pmod{7}$$

$$\text{Hence } a \equiv 0 \iff a_0 + 10a_1 + \cdots + 10^6a_6 \equiv 0 \iff a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 \equiv 0 \pmod{7}.$$

✓ 10/10

□

**Question 2**

Find a positive integer  $x$  such that  $x \equiv 3 \pmod{4}$ ,  $2x \equiv 5 \pmod{9}$  and  $7x \equiv 1 \pmod{11}$ .

*Proof.* Observe that  $2x \equiv 5 \pmod{9} \implies 10x \equiv 25 \pmod{9} \implies x \equiv 7 \pmod{9}$  and  $7x \equiv 1 \pmod{11} \implies 21x \equiv 3 \pmod{11} \implies -x \equiv 3 \pmod{11} \implies x \equiv 8 \pmod{11}$ .

We have  $x \equiv 3 \pmod{4}$ ,  $x \equiv 7 \pmod{9}$  and  $x \equiv 8 \pmod{11}$ , where 4, 9 and 11 are pairwise coprime. By Chinese Remainder Theorem  $x$  exists and is unique up to congruence class of  $396\mathbb{Z}$ . We shall follow the procedure described in the notes below Theorem 2.2.

Let  $Q_1 = 99$ ,  $Q_2 = 44$  and  $Q_3 = 36$ . Since  $Q_1 \equiv -1 \pmod{4}$ , we have  $m_1Q_1 \equiv 1 \pmod{4}$  where  $m_1 = 3$ . Since  $Q_2 \equiv -1 \pmod{9}$ , we have  $m_2Q_2 \equiv 1 \pmod{9}$  where  $m_2 = 8$ . Since  $Q_3 \equiv 3 \pmod{11}$ , we have  $m_3Q_3 \equiv 1 \pmod{11}$  where  $m_3 = 4$ .

Hence we can put  $x = 3m_1Q_1 + 7m_2Q_2 + 8m_3Q_3 = 4507$ . The smallest positive  $x$  is  $x = 151$ .

✓ 10/10

□

**Question 3**

Find the smallest positive integer  $x$  such that  $x \equiv 11 \pmod{59}$  and  $x \equiv 29 \pmod{71}$ .

*Proof.* Let  $Q_1 = 71$  and  $Q_2 = 59$ .  $Q_1$  and  $Q_2$  are coprime. We shall find the inverse of  $Q_1$  in  $Q_2\mathbb{Z}$  by Euclidean Algorithm and hence the inverse of  $Q_2$  in  $Q_1\mathbb{Z}$ .

$$71 = 1 \cdot 59 + 12$$

$$59 = 4 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$11 = 11 \cdot 1$$

Hence

$$1 = 12 - 11$$

$$= 12 - (59 - 4 \cdot 12) = 5 \cdot 12 - 59$$

$$= 5 \cdot (71 - 59) - 59 = 5 \cdot 71 - 6 \cdot 59$$

And we obtain that  $5Q_1 \equiv 1 \pmod{59}$  and  $-6Q_2 \equiv 1 \pmod{71}$ . We can put  $x = 11 \cdot 5 \cdot 71 + 29 \cdot (-6) \cdot 59 = -6361$ . Such  $x$  is unique up to congruence class of  $4189\mathbb{Z}$ . The smallest positive  $x$  is  $x = -6361 + 2 \cdot 4189 = 2017$ .  $\square$  10/10

#### Question 4

Show that  $2^{340} \equiv 1 \pmod{341}$ . Comment on this in connection with Fermat's Little Theorem.

*Proof.* Observe that  $2^{10} = 1024 = 1 + 3 \cdot 341$ . Hence  $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} = 1 \pmod{341}$ .

It is tempting to apply Fermat's Little Theorem directly to obtain the result. This is incorrect, however, since  $341 = 11 \cdot 31$  is not prime. An indirect way to prove the result using Fermat's Little Theorem is as follows:

Let  $x_1 = 2^{11}$ . Since  $x_1 \notin 31\mathbb{Z}$  and  $31 \in \mathbb{Z}$  is prime, by Fermat's Little Theorem we have  $2^{340} = 2^{10} x_1^{30} \equiv 1 \pmod{31}$ . We have used the fact that  $2^5 = 32 \equiv 1 \pmod{31}$ . Let  $x_2 = 2^{34}$ . Since  $x_2 \notin 11\mathbb{Z}$  and  $11 \in \mathbb{Z}$  is prime, by Fermat's Little Theorem  $2^{340} = x_2^{10} \equiv 1 \pmod{11}$ . By Chinese Remainder Theorem, there is a well-defined ring isomorphism  $\varphi : \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z} \rightarrow \mathbb{Z}/341\mathbb{Z}$  given by  $(x + 11\mathbb{Z}, x + 31\mathbb{Z}) \mapsto x + 341\mathbb{Z}$  for  $x \in \mathbb{Z}$ . Hence we conclude that  $2^{340} \equiv 1 \pmod{341}$ .  $\square$

*slightly overkill.*  
Simply use  $a \equiv b \pmod{q_1} \wedge a \equiv b \pmod{q_2} \Rightarrow a \equiv b \pmod{q_1 q_2}$   
 $\wedge (q_1, q_2) = 1$  10/10

#### Question 5

Let  $n := (6t + 1)(12t + 1)(18t + 1)$  with  $6t + 1$ ,  $12t + 1$  and  $18t + 1$  all prime numbers. Prove that

$$a^{n-1} \equiv 1 \pmod{n}$$

whenever  $(a, n) = 1$ . Comment on this in connection with Fermat's Little Theorem.

*Proof.* Since  $\gcd(a, n) = 1$ ,  $a$  is coprime with  $6t + 1$ ,  $12t + 1$ , and  $18t + 1$ . By Fermat's Little Theorem, we have:

$$a^{6t} \equiv 1 \pmod{6t + 1}$$

$$a^{12t} \equiv 1 \pmod{12t + 1}$$

$$a^{18t} \equiv 1 \pmod{18t + 1}$$

Notice that  $n - 1 = (6t + 1)(12t + 1)(18t + 1) - 1 = (6 \cdot 12 \cdot 18)t^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)t^2 + (6 + 12 + 18)t$  is divisible by  $18t$ . Therefore we have

$$a^{n-1} \equiv 1 \pmod{6t + 1}$$

$$a^{n-1} \equiv 1 \pmod{12t + 1}$$

$$a^{n-1} \equiv 1 \pmod{18t + 1}$$

By Chinese Remainder Theorem, we conclude that  $a^{n-1} \equiv 1 \pmod{n}$ .  $\square$  10/10

#### Question 6

Show that if  $x$  is an integer then  $x^{10} \in \{-1, 0, 1\} \pmod{25}$ .

*Proof.* By Lemma 3.6 in the notes,  $(\mathbb{Z}/25\mathbb{Z})^\times$  is a cyclic group, whose order is  $|(\mathbb{Z}/25\mathbb{Z})^\times| = \phi(25) = 20$ . For  $x \in \mathbb{Z}$ , let  $\bar{x}$  be the image under the projection  $\mathbb{Z} \rightarrow \mathbb{Z}/25\mathbb{Z}$ .

If  $\bar{x}^{10} = \bar{0}$ , then  $x^{10} \equiv 0 \pmod{25}$ . If  $\bar{x}^{10} = \bar{1}$ , then  $x^{10} \equiv 1 \pmod{25}$ . If  $\bar{x}^{10} \neq \bar{1}$  and  $\bar{x}^{10} \neq \bar{0}$ , then  $(\bar{x}^{10})^2 = \bar{1}$  implies that  $\bar{x}^{10}$  has order 2 in  $(\mathbb{Z}/25\mathbb{Z})^\times$ . As a cyclic group,  $(\mathbb{Z}/25\mathbb{Z})^\times$  has a unique element of order 2, which is  $-\bar{1}$ . It follows that  $x^{10} \equiv -1 \pmod{25}$ .  $\square$  10/10

#### Question 7

For which  $N$  is the following true: if you take an  $N$  digit number, reverse its digits and then add the result to the original number, you always get a multiple of 11?

*Proof.* This is true if only if  $N$  is even. ✓

For a  $N$ -digit number  $a$ , we can express it as  $a = \sum_{n=0}^{N-1} a_n 10^n$ . Let  $\tilde{a} = \sum_{n=0}^{N-1} a_n 10^{N-1-n}$  be the number obtained by reversing its digits. We have:

$$a + \tilde{a} = \sum_{n=0}^{N-1} a_n (10^n + 10^{N-1-n})$$

Therefore

$$a + \tilde{a} = \sum_{n=0}^{N-1} a_n ((-1)^n + (-1)^{N-1-n}) \pmod{11}$$

If  $N$  is even, then  $n$  and  $N-1-n$  differ in parity. It follows that  $(-1)^n + (-1)^{N-1-n} = 0$ . Hence  $a + \tilde{a} \in 11\mathbb{Z}$ . Conversely, if  $N$  is odd, we consider  $a = 10^{N-1}$ . Then  $a + \tilde{a} = 10^{N-1} + 1 \equiv (-1)^{N-1} + 1 = 2 \pmod{11}$ .  $a + \tilde{a} \notin 11\mathbb{Z}$ . 10/10 □

### Question 8

Find all primes  $p$  for which the map  $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  defined by  $\phi(x) = x^{13}$  is a group homomorphism.

*Proof.* The map  $\phi$  satisfies that  $\phi(0) = 0$  and  $\phi(1) = 1$ . It follows that  $\phi \in \text{End}(\mathbb{Z}/p\mathbb{Z})$  is a group homomorphism if and only if  $\phi = \text{id}_{\mathbb{Z}/p\mathbb{Z}}$ .  $x \neq 0$

Since  $p$  is prime,  $\mathbb{Z}/p\mathbb{Z}$  is a field. Then  $x^{13} \equiv x \pmod{p}$  implies that  $x^{12} \equiv 1 \pmod{p}$ . Hence  $\text{ord}_p(x) \mid 12$ . Since  $(\mathbb{Z}/p\mathbb{Z})^\times$  is the cyclic group  $C_{p-1}$ , it follows that  $(p-1) \mid 12$ . The primes satisfying this condition are 2, 3, 5, 7, 13. 10/10 □

### Question 9

Find all four-digit numbers  $N$  such that, when written in decimal, the last four digits of any power of  $N$  are the same as the digits of  $N$ .

*Proof.* Suppose that  $N^m$  and  $N$  have the same last four digits. In particular  $N^2$  and  $N$  have the same last four digits. Hence  $N^2 \equiv N \pmod{10^4}$  or  $10^4 \mid N(N-1)$ .  $10^4 = 2^4 \cdot 5^4$ . Exactly one of  $N$  and  $N-1$  is divisible by 2 and one divisible by 5. There are only two possibilities:

$$\begin{cases} N \equiv 0 \pmod{16} \\ N \equiv 1 \pmod{625} \end{cases} \quad \text{or} \quad \begin{cases} N \equiv 1 \pmod{16} \\ N \equiv 0 \pmod{625} \end{cases}$$

Notice that  $625 = 39 \cdot 16 + 1$ . By Chinese Remainder Theorem, the second case implies that  $N \equiv 625 \pmod{10^4}$ . This is impossible since  $N$  has exactly four digits. For the first case,  $N$  is given by:

$$N = 1 \cdot (625 - 39) \cdot 16 + 0 \cdot 1 \cdot 625 = 9376$$


For  $N = 9376$ ,  $N^2 \equiv N \pmod{10^4}$ . Inductively we have  $N^m \equiv N \pmod{10^4}$  for  $m \in \mathbb{Z}_+$ . 10/10 □

### Question 10


For each of the following properties, show that there are infinitely many positive integers  $n$  which do *not* have that property.

- (i)  $n$  is the sum of at most 3 squares;

- (ii)  $n$  is the sum of at most 8 sixth powers;
- (iii)  $n$  is the sum of at most 11 tenth powers;
- (iv)  $n$  is the sum of at most 15 fourth powers;
- (v)  $n$  is the sum of at most 7 positive seventh powers.

*Proof.* (i) We claim that  $n$  does not satisfy the property if  $n \in 8\mathbb{Z} + 7$ . 

Suppose that  $n = \sum_{i=1}^3 n_i^2$  for some  $n_i \in \mathbb{Z}$ . Notice that  $n^2 \in \{0, 1, 4\} \pmod{8}$  for any  $n \in \mathbb{Z}$ . Hence  $\sum_{i=1}^3 n_i \in \{0, 1, 2, 3, 4, 5, 6\} \pmod{8}$ . But  $n \equiv 7 \pmod{8}$ , which is a contradiction. Hence  $n$  does not satisfy the property. Since  $8\mathbb{Z} + 7$  is an infinite set, we conclude that there are infinitely many integers that does not satisfy the property.

(ii) We claim that  $n$  does not satisfy the property if  $n \in 9\mathbb{Z} \setminus 27\mathbb{Z}$ . 

Suppose that  $n = \sum_{i=1}^8 n_i^6$  for some  $n_i \in \mathbb{Z}$ . By Lemma 3.6 in the notes,  $(\mathbb{Z}/9\mathbb{Z})^\times$  is the cyclic group  $C_6$ . For  $m \in \mathbb{Z}$ , if  $m \in 3\mathbb{Z}$ , then  $m \equiv 0 \pmod{9} \implies m^6 \equiv 0 \pmod{9}$ . If  $m \notin 3\mathbb{Z}$ , then  $\bar{m} \in (\mathbb{Z}/9\mathbb{Z})^\times$ . Therefore  $\bar{m}^6 \equiv 1 \pmod{9}$ , since the order of the elements in  $C_6$  divides 6. It follows that  $n_i^6 \in \{0, 1\} \pmod{9}$  for each  $i$ . In particular,  $n = \sum_{i=1}^8 n_i^6 \equiv 0 \pmod{9}$  only if  $n_i^6 \equiv 0 \pmod{9}$  for each  $i$ . But

$$n_i^6 \equiv 0 \pmod{9} \implies 3 \mid n_i \implies 3^6 \mid n_i^6 \implies 3^6 \mid n = \sum_{i=1}^8 n_i^6$$

contradicting that  $n \notin 27\mathbb{Z}$ . Hence  $n$  does not satisfy the property. Since  $9\mathbb{Z} \setminus 27\mathbb{Z}$  is an infinite set, we conclude that there are infinitely many integers that does not satisfy the property.

(iii) We claim that  $n$  does not satisfy the property if  $n \in 25\mathbb{Z} + 13$ .

Suppose that  $n = \sum_{i=1}^{11} n_i^{10}$  for some  $n_i \in \mathbb{Z}$ . By Question 6 we know that  $n_i^{10} \in \{-1, 0, 1\} \pmod{25}$ . In particular,

$$n = \sum_{i=1}^{11} n_i^{10} \in \{-11, -10, \dots, 10, 11\} = \{0, 1, \dots, 10, 11, 14, 15, \dots, 24\} \pmod{25}$$

But  $n \equiv 13 \pmod{25}$  by definition. Hence  $n$  does not satisfy the property. Since  $25\mathbb{Z} + 13$  is an infinite set, we conclude that there are infinitely many integers that does not satisfy the property.

(iv) First we claim that 31 does not satisfy the property. Suppose that there exists  $n_1, \dots, n_{15} \in \mathbb{Z}$  such that  $31 = \sum_{i=1}^{15} n_i^4$ . Note that  $n_i^4 \geq 0$ . We must have  $31 \geq n_i^4 \implies |n_i| \in \{0, 1, 2\}$  for each  $i$ . And there is exactly one  $|n_i| = 2$ . A direct calculation may verify that it is impossible to express 31 as such combination.

Next we shall use induction to prove that  $31 \cdot 16^n$  does not satisfy the property for  $n \in \mathbb{N}$ . We have proven the base case.

For the induction case, suppose that  $31 \cdot 16^{n-1}$  does not have the property. By Lemma 3.7 in the notes, we have  $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4$ . For  $m \in 2\mathbb{Z}$ ,  $m^4 \equiv 0 \pmod{16}$ . For  $m \notin 2\mathbb{Z}$ ,  $m \in (\mathbb{Z}/16\mathbb{Z})^\times$ . Since every element of  $(\mathbb{Z}/16\mathbb{Z})^\times$  has order at most 4,  $m^4 \equiv 1 \pmod{16}$ . Hence  $m^4 \in \{0, 1\} \pmod{16}$  for any  $m \in \mathbb{Z}$ . Therefore

$$31 \cdot 16^n = \sum_{i=1}^{15} n_i^4 \implies \forall i \in \{1, \dots, 15\} : n_i^4 \equiv 0 \pmod{16} \implies \forall i \in \{1, \dots, 15\} : n_i \in 2\mathbb{Z}$$

Then  $31 \cdot 16^n = 16 \cdot \sum_{i=1}^{15} \left(\frac{n_i}{2}\right)^4 \implies 31 \cdot 16^{n-1} = \sum_{i=1}^{15} \left(\frac{n_i}{2}\right)^4$ . It follows that  $31 \cdot 16^{n-1}$  is a sum of 15 fourth powers of integers. Contradiction. Hence  $31 \cdot 16^n$  does not satisfy the property, completing the induction.

Finally,  $\{31 \cdot 16^n : n \in \mathbb{Z}\}$  is an infinite set. There are infinitely many integers that does not satisfy the property.

(v) There is a combinatorial method of doing this problem. Suppose for contradiction that there exists  $m$  integers that does not satisfy the property. Consider an integer  $n < k^7$  for large enough  $k \in \mathbb{Z}$ . If  $n$  satisfies the property,

then  $n = \sum_{i=1}^7 n_i^7$ , where  $n_i \in \{0, \dots, k-1\}$ . Hence  $n_i^7 \in \{0, 1, 2^7, \dots, (k-1)^7\}$ . Since each  $n_i^7$  has  $k$  possible values, it follows from simple combinatorics that  $\sum_{i=1}^7 n_i^7$  has at most  $\binom{k+6}{7}$  different values.

Let  $\varphi(k)$  be the number of integers less than  $k^7$  that does not satisfy the property. Then we have shown that

$$\varphi(k) \geq p(k) := k^7 - \binom{k+6}{7} = \left(1 - \frac{1}{7!}\right) k^7 + p_6(k)$$

where  $p_6 \in \mathbb{Z}[x]$  is a polynomial of degree at most 6. It follows that  $\varphi(k) \rightarrow \infty$  as  $k \rightarrow \infty$ . Therefore there exists  $N \in \mathbb{N}$  such that  $\varphi(N) > m$ , which is a contradiction. We conclude that there are infinitely many integers that does not satisfy the property.

□

10/10