Math 261 — Exercise sheet 6

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: October 31, 2018

Answers are due for Wednesday 31 October, 11AM.

The use of calculators is allowed.

Exercise 6.1: A huge number! (25 pts)

For this exercise, remember that every integer is congruent mod 9 *to the sum of its digits.*

Let $A = 4444^{4444}$, let B be the sum of the digits of A, let C be the sum of the digits of B, and finally let D be the sum of the digits of C.

1. (15 pts) Compute D mod 9.
2. (7 pts) Prove that $D \leqslant 14$.

   Hint: Start with the upper bound $A < 10000^{5000} = 10^{20000}$.
3. (3 pts) What is the exact value of D (as opposed to just mod 9)?

Solution 6.1:

1. Since every integer is congruent mod 9 to the sum of its digits, we have $D \equiv C \equiv B \equiv A \pmod 9$, so we can just as well compute A mod 9.

   Now $4444 \equiv 16 \equiv -2 \pmod 9$, so $A \equiv (-2)^{4444} \pmod 9$. Now -2 and 9 are coprime, so by Fermat's little theorem we have $(-2)^{\phi(9)} \equiv 1 \pmod 9$. We have $\phi(9) = 6$, so we can replace the exponent 4444 by anything congruent to it mod 6. Since $4444 \equiv 4 \pmod 6$, we deduce that $A \equiv (-2)^4 = 16 \equiv 7 \pmod 9$.

2. We are going to estimate roughly the size of D. First of all, we have

   $$A < 10000^{5000} = 10^{20000},$$

   so A has at most 20000 digits, so

   $$B \leqslant 9 \times 20000 = 180000.$$

   So either B has 6 digits and the first one is a 1, or it has 5 digits or less; either way

   $$C \leqslant 1 + 6 \times 9 = 55.$$

   Therefore C has at most 2 digits and the first one is at most 5, so

   $$D \leqslant 5 + 9 = 14.$$

3. Since we know that $D \equiv 7 \pmod 9$ and that $D \leqslant 14$, we conclude that in fact $D = 7$.

Exercise 6.2: Primitive roots mod 43 (35 pts)

1. (5 pts) Suppose you choose an element of $(\mathbb{Z}/43\mathbb{Z})^\times$ at random. What is the probability that this element is a primitive root? In other words, what is the proportion of elements of $(\mathbb{Z}/43\mathbb{Z})^\times$ that are primitive roots?

2. (15 pts) Find a primitive root $g \in (\mathbb{Z}/43\mathbb{Z})^\times$.

3. (10 pts) What is the multiplicative order of g^{261}, where g is the primitive root found in the previous question?

Solution 6.2:

1. Since 43 is prime, primitive roots exist. More precisely, there are exactly $\phi(\phi(43)) = \phi(42) = 12$ of them. Compared to the $\phi(43) = 4$ elements of $(\mathbb{Z}/43\mathbb{Z})^\times$, that's a proportion $12/42 = 2/7$ that are primitive roots.

2. We are just going to try values of g until we find one. Since $42 = 2 \cdot 3 \cdot 7$, we know that g is a primitive root if and only if $g^{2\cdot 3} = g^6$, $g^{2\cdot 7} = g^{14}$, and $g^{3\cdot 7} = g^{21}$ are all $\neq 1$.

   Obviously $g = 1$ is not a primitive root (quite the opposite!), so let us try $g = 2$. We compute in $\mathbb{Z}/43\mathbb{Z}$ that

   $$2^6 = 64 = 21 \neq 1,$$

   but

   $$2^{14} = (2^7)^2 = (2 \cdot 21)^2 = 42^2 = -1^2 = 1$$

   so 2 is not a primitive root.

   Let us try $g = 3$:

   $$3^6 = 3^4 3^2 = 81 \cdot 9 = -5 \cdot 9 = -45 = -2 \neq 1,$$

   $$3^{14} = 3^2 3^6 3^6 = 9 \cdot -2 \cdot -2 = 36 = -7 \neq 1,$$

   $$3^{21} = 3 \cdot 3^6 3^{14} = 3 \cdot -2 \cdot -7 = 42 = -1 \neq 1$$

   so $g = 3$ is one of the 12 primitive roots.

3. Since g is a primitive root, it has order $\phi(43) = 42$. Thus

   $$MO(g^{261}) = \frac{MO(g)}{\gcd(MO(g), 261)} = \frac{42}{\gcd(42, 261)} = \frac{42}{3} = 14.$$

Exercise 6.3: A multiplicative sequence (40 pts)

The goal of this exercise is to understand the behavior of the sequence $x_n = 2^n$ in $\mathbb{Z}/40\mathbb{Z}$.

1. (3 pts) Why cannot we say that x_n is periodic mod 40 "as usual"?

2. (12 pts) Find a formula for the values of x_n mod 5 in terms of n. You answer should have the form "if n is like this, then $x_n =$ this; if n is like that, then $x_n =$ that; if …".

3. (10 pts) Find a formula for the values of x_n mod 8 in terms of n.

   Hint: Compute x_n for $n \leqslant 4$ "by hand".

4. (15 pts) Deduce a formula for x_n mod 40. What is the period? What is the length of the "tail"?

   Hint: 中国剩余定理.

Solution 6.3:

1. We know that the sequence $1, x, x^2, \cdots$ is periodic for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, but 2 is not invertible mod 40 (their gcd is 2) so this argument does not apply.

2. Now 2 is invertible mod 5, so we know that 2^n mod 5 is periodic, of period dividing $\phi(5) = 4$ by FlT. Let us see: in $\mathbb{Z}/5\mathbb{Z}$, we have $x_0 = 1$, $x_1 = 2$, $x_2 = 4 = -1$, $x_3 = -2$, and $x_4 = -4 = 1 = x_0$. So the period is exactly 4 (in other words 2 is a primitive root in $\mathbb{Z}/5\mathbb{Z}$) and

$$x_n \bmod 5 = \begin{cases} 1 & \text{if } n \equiv 0 \bmod 4, \\ 2 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 2 \bmod 4, \\ -2 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

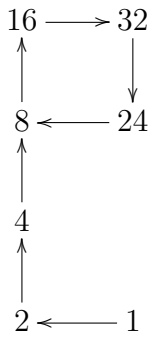
3. Since 2 is not invertible mod 8, the theory seen in class does not apply. Let us compute a few terms anyway. Mod 8, we have $x_0 = 1$, $x_1 = 2$, $x_2 = 4$, and $x_3 = 8 = 0$. So $x_n \equiv 0 \bmod 8$ for all $n \geqslant 3$. Thus

$$x_n \bmod 8 = \begin{cases} 1 & \text{if } n = 0 \\ 2 & \text{if } n = 1, \\ 4 & \text{if } n = 2, \\ 0 & \text{if } n \geqslant 3. \end{cases}$$

4. The hint is to use CRT. Indeed, for $n \geqslant 3$ we have $x_n \equiv 0 \bmod 8$ whereas x_n mod 5 is given by the formula found in question 2. By putting this information together, we can deduce x_n mod 40 for $n \geqslant 3$; and for $n < 3$ we can just compute x_n by hand. We find

$$x_n \bmod 40 = \begin{cases} 1 & \text{if } n = 0 \\ 2 & \text{if } n = 1, \\ 4 & \text{if } n = 2, \\ 8 & \text{if } n \geqslant 3 \text{ and } n \equiv 3 \bmod 4, \\ 16 & \text{if } n \geqslant 3 \text{ and } n \equiv 0 \bmod 4, \\ 32 & \text{if } n \geqslant 3 \text{ and } n \equiv 1 \bmod 4, \\ 24 & \text{if } n \geqslant 3 \text{ and } n \equiv 2 \bmod 4. \end{cases}$$

   We see that we have a tail of length 3, after which we enter a cycle of length 4.



The exercises below are not mandatory. They are not worth any points, and are given here for you to practice. The solutions will be made available with the solutions to the other exercises.

Exercise 6.4: More primitive roots

1. Find a primitive root for $\mathbb{Z}/7\mathbb{Z}$. Justify your answer in detail.

2. Same question for $\mathbb{Z}/11\mathbb{Z}$.

3. Same question for $\mathbb{Z}/23\mathbb{Z}$.

Solution 6.4:

1. Fermat's little theorem tells us that every $x \in (\mathbb{Z}/7\mathbb{Z})^\times$ has order dividing $7-1 = 6 = 2 \times 3$. Therefore, x is a primitive root iff. it satisfies $x^2 \neq 1$ and $x^3 \neq 1$.

   Let us try $x = 2$. We have $2^2 = 4 \neq 1$, but $2^3 = 8 = 1$ so 2 is not a primitive root (in fact, since $2 \neq 1$ it does not have order 1, and since 3 is prime, the identity $2^3 = 1$ tells us that the multiplicative order of 2 is 3).

   Let us try again, with $x = 3$. We find $3^2 = 9 \neq 1$ and $3^3 = 27 = -1 \neq 1$, so 3 is a primitive root.

   Remark: we know that there are in fact $\phi(6) = 2$ primitive roots; the other one is $3^{-1} = 5$.

2. We have $11 - 1 = 10 = 2 \times 5$, so we are looking for an $x \neq 0$ such that $x^2 \neq 1$ and $x^5 \neq 1$.

   Let us try $x = 2$. This time we are luckier: we have $2^2 = 4 \neq 1$ and $2^5 = 32 = -1 \neq 1$, so 2 is a primitive root.

   Remark: we know that there are in fact $\phi(10) = 4$ primitive roots; they are the 2^m where $m \in (\mathbb{Z}/10\mathbb{Z})^*$, in other words, 2, 8, 7, and 6.

3. We have $23 - 1 = 22 = 2 \times 11$, so we are looking for an $x \neq 0$ such that $x^2 \neq 1$ and $x^{11} \neq 1$.

   Let us try $x = 2$. Bad luck: we have $2^2 = 4 \neq 1$, but $2^{11} = 1$, so 2 is a not primitive root.

   Let us try again with $x = 3$: we have $3^2 = 9 \neq 1$, but again $3^{11} = 1$, so 3 is not a primitive root either.

   The next value is $x = 4$, however we can see directly that $4^{11} = (2^2)^{11} = 2^{22} = (2^{11})^2 = 1$, so 4 is not going to work either.

   But let us not give up! For $x = 5$ we have $5^2 = 25 = 2 \neq 1$, and $5^{11} = -1 \neq 1$, so 5 is a primitive root.

   Remark: we know that there are in fact $\phi(22) = 10$ primitive roots; they are the 5^m where $m \in (\mathbb{Z}/22\mathbb{Z})^*$. Also, to compute x^{11}, it is a good idea to write something like $x^1 1 = x \times (x^5)^2$, and to reduce mod 23 at every step.

Final remarks: in $\mathbb{Z}/p\mathbb{Z}$, we can only have $x^2 = 1$ when $x = \pm 1$. So as long as we did not consider $x = -1$ ($x = 1$ would be really too silly), we didn't have to care

about x^2 being $\neq 1$. Also, we have $x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = \pm 1$; this explains why $x^{\frac{p-1}{2}} = -1$ whenever x is a primitive root.

Exercise 6.5: Even more primitive roots

Let $p \in \mathbb{N}$ be prime, and let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root.

1. Let $a \in \mathbb{Z}$. Give a necessary and sufficient condition on a for g^a to be a primitive root in $\mathbb{Z}/p\mathbb{Z}$.

2. Prove that if a is prime, then g^a is a primitive root in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \not\equiv 1 \pmod{a}$.

3. Show that the previous assertion is no longer valid when a is not assumed to be prime, by finding a counterexample.

4. Is every primitive root of $\mathbb{Z}/p\mathbb{Z}$ of the form g^a for some $a \in \mathbb{Z}$? Justify your answer.

Solution 6.5:

1. By definition of g, the multiplicative order of g is $p-1$. As a consequence, for every a the multiplicative order of g^a is $\frac{p-1}{\gcd(p-1,a)}$. Therefore, g^a is a primitive root iff. a and $p-1$ are coprime.

2. By the previous question, g^a is a primitive root iff. $p-1$ and a are coprime. Since a is prime, this is equivalent to a not dividing $p-1$, which is equivalent to p not being congruent to 1 mod a.

3. In view of the previous questions, we will get a counterexample if we can find a and p such that a does not divide $p-1$ and yet $\gcd(a, p-1) \neq 1$, i.e. such that $1 < \gcd(p-1, a) < a$.

   So for instance we can take $a = 4$, $p = 7$. Indeed, we then have that $p \not\equiv 1 \pmod{a}$, and yet the multiplicative order of g^a is $\frac{6}{\gcd(4,6)} = 3 < 6$. (To be even more concrete, we can take $g = 3$ as in the previous exercise, and then $g^a = 3^4 = 81 = 11 = 4$ is not a primitive element since $4^3 = 64 = 1 + 63 = 1$.)

4. Yes, simply because by definition of primitive roots, every nonzero element of $\mathbb{Z}/p\mathbb{Z}$, primitive root or not, is of the form g^a for some $a \in \mathbb{N}$.

Exercise 6.6

Prove that $2^{3n+5} + 3^{n+1}$ is divisible by 5 for all $n \in \mathbb{N}$.

Solution 6.6

Since $2 \in (\mathbb{Z}/5\mathbb{Z})^\times$, its multiplicative order mod 5 is a divisor of 4 (in fact, it can be checked by the methods of exercise 4.1 that its order is exactly 4, i.e. 2 is a primitive root mod 5), so 2^m mod 5 only depends on m mod 4. And since $3n+5$ mod 4 only depends on n mod 4, we have that 2^{3n+5} mod 5 only depends on n mod 4.

Similarly, the multiplicative order of 3 mod 5 divides 4 (its in is fact again exactly 4), so 3^m mod 5 only depends on m mod 4, and so 3^{n+1} mod 5 only depends on n mod 4. As a result, the expression $2^{3n+5} + 3^{n+1}$ mod 5 only depends on n mod 4.

Thus all we have to do is check that $2^{3n+5} + 3^{n+1} \equiv 0 \pmod 5$ for 4 values of n **representing all 4 elements of** $\mathbb{Z}/4\mathbb{Z}$, such as $0, 1, 2, 3$, or even cleverer, $-1, 0, 1, 2$.

Other solution: instead of checking for 4 values of n, which is easy but still a bit tedious, we can directly compute that $3n + 5 \equiv -n + 1 \bmod 4$, so that

$$2^{3n+5} \equiv 2^{-n+1} \equiv 2 \times 3^n \pmod 5$$

since 3 is the inverse of 2 mod 5; as a result, we have

$$2^{3n+5} + 3^{n+1} \equiv 2 \times 3^n + 3 \times 3^n = 5 \times 3^n \equiv 0 \pmod 5.$$

Exercise 6.7: Another really big number

Compute the remainder of $16^{2^{1000}}$ when divided by 7.

Solution 6.7:

We want to reduce $16^{2^{1000}} \bmod 7$.

We have $16 \equiv 2 \pmod 7$, so $16^{2^{1000}} \equiv 2^{2^{1000}} \pmod 7$. Next, we see that $2^3 \equiv 1 \pmod 7$, so $2^m \bmod 7$ only depends on $m \bmod 3$ (we are using the fact that the multiplicative order of 2 mod 7 divides 3; actually it is exactly 3). So we want to reduce $2^{1000} \bmod 3$. This is easy: we have $2 \equiv -1 \pmod 3$, so $2^{1000} \equiv (-1)^{1000} \equiv 1 \pmod 3$. Conclusion:

$$16^{2^{1000}} \equiv 2^{2^{1000}} \equiv 2^1 \equiv 2 \pmod 7,$$

so the remainder is 2.

Exercise 6.8: Possible orders

1. Let $n \in \mathbb{N}$. Explain why the additive order of any $x \in \mathbb{Z}/n\mathbb{Z}$ is a divisor of n, and prove that for any $d \mid n$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ of order d.

2. Let $p \in \mathbb{N}$ be a prime. Explain why the multiplicative order of any $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a divisor of $p - 1$, and prove that for any $d \mid (p - 1)$, there exists an $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order d.

3. Let $n \in \mathbb{N}$. Is it true that for any $d \mid \phi(n)$, there exists an $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ of multiplicative order d?

4. Suppose that $n \in \mathbb{N}$, and that there exists an $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ of multiplicative order $n - 1$. Prove that n must be prime.

Solution 6.8:

1. For all x, we have $nx = 0x = 0$ so the additive order of x divides n. If $d \mid n$, then we can consider $x = \frac{n}{d} \in \mathbb{Z}/n\mathbb{Z}$, and it is clear that $mx = 0 \in \mathbb{Z}/n\mathbb{Z}$ precisely when $d \mid m$, so this x is of additive order exactly d.

2. By Fermat's little theorem, the multiplicative order of x divides $\phi(p)$, and $\phi(p) = p - 1$ since p is prime. Let now $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root (there exists at least one since p is prime), then by definition $g^m = 1$ iff. $(p - 1) \mid m$. So if $d \mid (p - 1)$, then $x = g^{\frac{p-1}{d}}$ satisfies

$$x^m = 1 \iff g^{\frac{p-1}{d}m} = 1 \iff (p-1) \mid \frac{p-1}{d}m \iff d \mid m,$$

which shows that the multiplicative order of x is exactly d.

3. No. In fact, this is false when $d = \phi(n)$: in this case, such x are precisely primitve roots, and those do not exist for most n.

4. Since $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ is invertible, all its powers are also invertible (of inverse the same power of the inverse of x). But x has multiplicative order $n-1$, so the sequence of its power is periodic of period exactly $n-1$, so x has $n-1$ distinct powers. So we have at least $n-1$ invertibles in $\mathbb{Z}/n\mathbb{Z}$. But in $\mathbb{Z}/n\mathbb{Z}$ there are n elements, and clearly 0 cannot be invertible[1], so we see that all nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ are invertible. This means that $\mathbb{Z}/n\mathbb{Z}$ is a field, so n must be prime.

[1]Well, technically 0 is invertible in $\mathbb{Z}/1\mathbb{Z}$. But on the other hand, the order of any element is at least 1, so $n-1 \geqslant 1$ so we must have $n \geqslant 2$ in this exercise. But I should have made that clear in the question.