Math 261 — Exercise sheet 4

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 17, 2017

Answers are due for Monday 16 October, 11AM.

The use of calculators is allowed.

Exercise 4.1: Primitive roots (24pts)

1. (8pts) Find a primitive root for $\mathbb{Z}/7\mathbb{Z}$. Justify your answer in detail.
2. (8pts) Same question for $\mathbb{Z}/11\mathbb{Z}$.
3. (8pts) Same question for $\mathbb{Z}/23\mathbb{Z}$.

Solution 4.1:

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; by exercise 4.2, 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; by exercise 4.2, 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 4.2: More primitive roots (32 pts)

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

1. (8 pts) 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. (8 pts) 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. (8 pts) Show that the previous assertion is no longer valid when a is not assumed to be prime, by finding a counterexample.

4. (8 pts) 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 4.2:

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 4.3: (24 pts)

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

Solution 4.3:

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 $3n + 5 \equiv -n + 1$ mod 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 4.4: A really big number (20 pts)

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

Hint: This number is so large that most calculators and computers won't be able to help you, but congruences and multiplicative orders will...

Solution 4.4:

We want to reduce $16^{2^{1000}}$ mod 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 mod 7 only depends on m mod 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} mod 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.

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

Exercise 4.5: Largest possible orders

1. Prove that for every $n \in \mathbb{N}$, and for every $x \in \mathbb{Z}/n\mathbb{Z}$, the additive order of x is at most n.

2. Prove that for every $n \in \mathbb{N}$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ whose additive order is exactly n.

3. Prove that for every $n \in \mathbb{N}$, and for every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative order of x is at most $\phi(n)$.

4. Find an $n \in \mathbb{N}$ such that every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ has multiplicative order $< \phi(n)$.

Solution 4.5:

1. We have $x + x + \cdots + x$ (n times) $= nx = 0x = 0$, so the additive order of x divides n.

2. Remember that the additive order of x is the smallest $m \in \mathbb{N}$ such that $mx = 0 \in \mathbb{Z}/n\mathbb{Z}$. So if we take $x = 1$, then we have $mx = 0$ iff. $m = 0$ iff. $n \mid m$, so the additive order of 1 is n. (In fact, we can show similarly that the additive order of any *invertible* element of $\mathbb{Z}/n\mathbb{Z}$ is exactly n, and that conversely the only elements of additive order n are the invertibles.)

3. The multiplicative order of x is the smallest $m \in \mathbb{N}$ such that $x^m = 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$. We have $x^{\phi(n)} = 1$ by Fermat's little theorem, so the multiplicative order of x divides $\phi(n)$.

4. We can take $n = 8$: then every $x \in (\mathbb{Z}/8\mathbb{Z})^\times$ satisfies $x^2 = 1$, so is of order $\leqslant 2$, whereas $\phi(8) = 4 > 2$.

Exercise 4.6: 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 4.6:

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 $d = \phi(n)$, as we saw at the end of the previous exercise.

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.