Introduction to number theory
Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html

Version: January 11, 2021

Answers are due for Monday October 26th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Euler*

Compute $\phi(2020)$.

Solution 1

In order to use the formulas for ϕ, we must factor 2020. W see easily that $2020 = 2^2 \times 5 \times 101$; and since neither 2 nor 3 nor 5 nor 7 divides 101, we conclude that 101 is prime since it is not divisible by any prime $\leq \sqrt{101} < 11$. So we can conclude that

$$\phi(2020) = \phi(2^2 \times 5 \times 101) = \phi(2^2) \times \phi(5) \times \phi(101) = 2 \times 4 \times 100 = 800$$

as $\phi(p^v) = p^{v-1}(p-1)$ for p prime; in particular $\phi(p) = p - 1$ (this reflects that for p prime, only 0 is not invertible in $\mathbb{Z}/p\mathbb{Z}$).

Exercise 2 *A really large number*

What is the remainder of $22^{7^{2020}}$ when divided by 17?
Just to be clear: a^{b^c} *means* $a^{(b^c)}$, *as opposed to* $(a^b)^c = a^{bc}$.

Solution 2

We want to reduce $22^{7^{2020}}$ mod 17.

First, we have $22 \equiv 5 \bmod 17$, so $22^{7^{2020}} \equiv 5^{7^{2020}} \bmod 17$.

Next, by Fermat we know that since $\gcd(5, 17) = 1$, $5^{\phi(17)} \equiv 1 \bmod 17$, so the value of $5^m \bmod 17$ only depends on $m \bmod \phi(17)$. As 17 is prime, we have $\phi(17) = 17 - 1 = 16$, so we want to determine $7^{2020} \bmod 16$.

Again by Fermat, since $\gcd(7, 16) = 1$, we have $7^{\phi(16)} \equiv 1 \bmod 16$, so $7^m \bmod 16$ only depends on $m \bmod \phi(16)$. And as $16 = 2^4$, we have $\phi(16) = 2^{4-1}(2-1) = 8$.

So we now want to determine 2020 mod 8. That one is easy, we find that $2020 \equiv 4 \bmod 8$.

So $7^{2020} \equiv 7^4 \bmod 16$. In order to compute that, we begin by $7^2 = 49 \equiv 1 \bmod 16$, whence $7^4 = (7^2)^2 \equiv 1^2 = 1 \bmod 16$.

Thus $5^{7^{2020}} \equiv 5^1 = 5 \bmod 17$. Conclusion:

$$22^{7^{2020}} \equiv 5 \bmod 17,$$

so the remainder is 5.

These were the only mandatory exercises, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises.

Exercise 3 *An inverse*

1. Use the Euclidean algorithm to determine if 47 is invertible mod 111, and to find its inverse if it is.

2. Solve the equation $47x \equiv 5 \bmod 111$ in $\mathbb{Z}/111\mathbb{Z}$.

Solution 3

1. We know that 47 is invertible mod 111 if and only if 47 and 111 are coprime. If they are, we need to look for u and $v \in \mathbb{Z}$ such that $47u + 111v = 1$; indeed, u will then be an inverse of 47 mod 111. To find u and v, we either spot them directly[1], or we use the Euclidean algorithm. This algorithm will also tell us if the gcd of 47 and 111 is not 1, so let's apply it:

$$\begin{aligned} 111 &= 2 \times 47 + 17 \\ 47 &= 2 \times 17 + 13 \\ 17 &= 13 + 4 \\ 13 &= 3 \times 4 + 1 \end{aligned}$$

   So the gcd is 1, so 47 is invertible mod 111. To find it, we write

$$\begin{aligned} 1 &= 13 - 3 \times 4 \\ &= 13 - 3(17 - 13) = 4 \times 13 - 3 \times 17 \\ &= 4(47 - 2 \times 17) - 3 \times 17 = 4 \times 47 - 11 \times 17 \\ &= 4 \times 47 - 11 \times (111 - 2 \times 47) = 26 \times 47 - 11 \times 111, \end{aligned}$$

   whence 26 mod 111 is the inverse of 47 mod 111.

2. Since 47 is invertible mod 111, the only solution is

$$x = 5 \times 47^{-1} = 5 \times 26 = 130 \equiv 19 \bmod 111.$$

[1] It can happen sometimes, but here there are no obvious candidates

Exercise 4 *More inverses*

1. Fix $n \in \mathbb{N}$, let $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ be invertible, and let $y \in \mathbb{Z}/n\mathbb{Z}$ be the inverse of x. Prove that x^2, $-x$, and y are also invertible, and find their inverses.

2. Find all the elements of $(\mathbb{Z}/15\mathbb{Z})^\times$, and give the inverse of each of them. What is $\phi(15)$?

   Hint: Use the previous question to save your effort!

Solution 4

1. We are tempted to write

$$\frac{1}{x^2} = \left(\frac{1}{x}\right)^2 = y^2, \quad \frac{1}{-x} = -\frac{1}{x} = -y, \quad \frac{1}{y} = \frac{1}{1/x} = x,$$

   and to conclude that x^2, $-x$, and y are invertible, of respective inverses y^2, $-y$, and x. Let us check:

$$x^2y^2 = (xy)^2 = 1^2 = 1, \quad (-x)(-y) = xy = 1, \quad yx = xy = 1$$

   since $xy = 1$ as y is the inverse of x. This proves that our intuition is correct.

2. The elements of $\mathbb{Z}/15\mathbb{Z}$ can be represented by $-7, -6, \cdots, 5, 6, 7$. Among these, the invertible ones are the ones that are coprime with 15, namely $-7, -4, -2, -1, 1, 2, 4, 7$. That's 8 of them, so $\phi(15) = 8$.

   NB we could have determined $\phi(15)$ directly from the factorisation of 15: since $15 = 3 \times 5$, we have $\phi(15) = 15(1 - 1/3)(1 - 1/5) = 8$. But since the question was asking to list the elements of $(\mathbb{Z}/15\mathbb{Z})^\times$, it was simpler to just count them!

   Let us now match each element with its inverse, Obviously, 1 and -1 are their own inverses. Also, the inverse of 2 is $8 = -7$ since $2 \cdot 8 = 16 = 1$ in $\mathbb{Z}/15\mathbb{Z}$. By the previous question, we immediately get that the inverses of 4, -2 and -7 are respectively $(-7)^2 = 49 = 4$, $- - 7 = 7$, and 2. It is now easy to complete the following table:

x	-7	-4	-2	-1	1	2	4	7
x^{-1}	2	-4	7	-1	1	-7	4	-2

Exercise 5 *A system of congruences*

Find an integer $x \in \mathbb{Z}$ such that $x \equiv 12 \bmod 7$ and $x \equiv 7 \bmod 12$.

Solution 5

This is Chinese remainders: as 12 and 7 are coprime, we have a 1:1 correspondence

$$\mathbb{Z}/84\mathbb{Z} \longleftrightarrow \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \tag{中}$$

and we are looking for a pre-image of $(12 \bmod 7, 7 \bmod 12)$ under this correspondence.

Let us start by finding u and v such that $7u + 12v = 1$. Either we spot them right away, or we use the Euclidean algorithm:

$$\begin{aligned} 12 &= 7 + 5 \\ 7 &= 5 + 2 \\ 5 &= 2 \times 2 + 1 \end{aligned}$$

whence

$$1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = 3 \times 5 - 2 \times 7 = 3(12 - 7) - 2 \times 7 = 3 \times 12 - 5 \times 7.$$

So, under the correspondence (中), $3 \times 12 = 36$ is a preimage of $(1 \bmod 7, 0 \bmod 12)$, and $-5 \times 7 = -35$ is a preimage of $(0 \bmod 7, 1 \bmod 12)$. As a result, since

$$\begin{aligned} (12 \bmod 7, 7 \bmod 12) &= (5 \bmod 7, 7 \bmod 12) \\ &= 5 \times (1 \bmod 7, 0 \bmod 12) + 7 \times (0 \bmod 7, 1 \bmod 12), \end{aligned}$$

a preimage for $(12 \bmod 7, 7 \bmod 12)$ is $x = 5 \times 36 + 7 \times -35 = -65$.

Remark: Of course, any integer congruent to $-65 \bmod 84$ *works (for instance, 19). In fact, the Chinese remainder theorem tells us that the solutions are exactly the numbers that are congruent to* $-65 \bmod 84$*; no more, no less.*

Exercise 6 *Primes mod 6*

1. Let p be a prime number which is neither 2 nor 3. Prove that either $p \equiv 1 \bmod 6$ or $p \equiv -1 \bmod 6$.

2. Prove that there are infinitely many primes p such that $p \equiv -1 \bmod 6$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$*. Let* $N = 6p_1 \cdots p_k - 1$*, and consider a prime divisor of* N*.*

3. Why does the same proof fail to show that there are infinitely may primes p such that $p \equiv 1 \bmod 6$?

4. *Dirichlet's theorem on primes in arithmetic progressions*, which is way beyond the scope of this course, states that for all coprime positive integers a and b, there are infinitely many primes p such that $p \equiv a \bmod b$; in particular, there are in fact infinitely many primes p such that $p \equiv 1 \bmod 6$. Why, in the statement of this theorem, is it necessary to assume that a and b are coprime?

Solution 6

1. If p is neither 2 nor 3, then $p \nmid 6$, so p and 6 are coprime. But the only invertibles in $\mathbb{Z}/6\mathbb{Z}$ are ± 1 (either see it by inspection of all 6 elements, or use the fact that $\phi(6) = 2$), so we must have $p \equiv \pm 1 \bmod 6$.

2. Suppose that $p_1, \cdots, p_k$ are the only such primes, and let $N = 6p_1 \cdots p_k - 1$. Clearly, neither 2 nor 3 divide N (since $N \equiv -1 \bmod 6$), so the primes dividing N are all $\equiv \pm 1 \bmod 6$ by the previous question. If they were all $\equiv +1 \bmod 6$,

then N, their product, would also be $\equiv +1 \bmod 6$, which is not the case. So at least one of them, say p, is $\equiv -1 \bmod 6$. But this p cannot be one of $p_1, \cdots, p_k$, else we would have $p \mid (6p_1 \cdots p_k - N) = 1$. We therefore have reached a contradiction.

3. We could suppose by contradiction that $p_1, \cdots, p_k$ are the only primes $\equiv 1 \bmod 6$, and consider a prime divisor of $N = 6p_1 \cdots p_k - 1$ (or $N = 6p_1 \cdots p_k + 1$). Such a prime could not be any of the p_i for the same reason as above, but there is no reason why it would have to be $\equiv 1 \bmod 6$; indeed, nothing prevents the divisors of N from being all $\equiv -1 \bmod 6$. So we are stuck.

4. If $p \equiv a \bmod b$, then $p = bx + a$ for some $x \in \mathbb{Z}$, so $\gcd(a, b) \mid p$; and obviously, if $\gcd(a, b) > 1$, this can only happen for at most one prime p (exactly one if $\gcd(a, b) = p$ is itself prime, and none else).

Exercise 7 *Inverse Euler*

The goal of this exercise is to find all integers $n \in \mathbb{N}$ such that $\phi(n) = 4$.

1. Prove that if $p \in \mathbb{N}$ is a prime and $v \in \mathbb{N}$ is such that $p^v \mid n$, then $(p-1)p^{v-1} \mid \phi(n)$.

   Hint: When p is prime, what is $\phi(p^v)$?

2. Using the previous question, prove that if $\phi(n) = 4$, then n cannot be divisible by a prime $p \geq 7$. Also prove that $3^2,\ 5^2 \nmid n$.

3. Find all n such that $\phi(n) = 4$.

   Hint: Think in terms of the factorisation of n. You should find that there are four such n — but you are required to prove this as part of this question!

Solution 7

1. Let $p^{v'}$ be the exact power of p that divides n, so that $v' = v_p(n) \geq v$ and we may write $n = p^{v'} m$ with $\gcd(p^{v'}, m) = 1$. Since ϕ is multiplicative, $\phi(n) = \phi(p^{v'})\phi(m)$ is divisible by $\phi(p^{v'}) = (p-1)p^{v'-1}$, whence also by $(p-1)p^{v-1}$ since $v' - 1 \geq v - 1$.

2. Let $p^v \mid n$, then by the previous question $(p-1)p^{v-1} \mid \phi(n) = 4$, so in particular $p - 1 \leq 4$, i.e. $p \leq 5$. Besides, if $v = 2$, then we get $(p-1)p \mid 4$, so $p \mid 4$, so $p = 2$. In other words, we cannot have $p^2 \mid n$ unless $p = 2$.

3. According to the previous question, the only possible prime factors of n are 2, 3, and 5; and 3 and 5 cannot be repeated factors. So we must have $n = 2^a 3^b 5^c$ for $a \geq 0$ and $b, c = 0$ or 1. Since ϕ is multiplicative and since powers of distinct primes are coprime, we must then have $4 = \phi(n) = \phi(2^a)\phi(3^b)\phi(5^c)$. Now observe that
$$\phi(2^a) = \left\{ \begin{array}{ll} 1, & \text{if } a = 0, \\ 2^{a-1}, & \text{if } a \geq 1, \end{array} \right.$$

$$\phi(3^b) = \begin{cases} 1, & \text{if } b = 0, \\ 2, & \text{if } b = 1, \end{cases}$$

and

$$\phi(5^c) = \begin{cases} 1, & \text{if } c = 0, \\ 4, & \text{if } c = 1. \end{cases}$$

These observations clearly imply that the only combinations of (a, b, c) for which $\phi(n) = 4$ correspond to $n = 2^3$, $2^2 3$, 5, or $2 \cdot 5$.

In conclusion, we have exactly four solutions: $n = 5$ or 8 or 10 or 12.

Exercise 8 *More inverse Eulers*

This exercise is a bit more difficult, but still doable. The questions are independent from each other.

1. Using the fact that $2018 = 2 \times 1009$ and that 1009 is prime, prove that there is no $n \in \mathbb{N}$ such that $\phi(n) = 2018$.

   Hint: Suppose 1009 *is a factor of* $\phi(n)$*. Where can this factor come from?*

2. Prove that for all $m \in \mathbb{N}$, there are at most finitely many[2] $n \in \mathbb{N}$ such that $\phi(n) = m$.

   Hint: Try to bound the prime factors of n *in terms of* m*.*

3. Prove that $\phi(n)$ is even for all $n \geq 3$.

   Hint: Start with the case when n *is a prime power.*

Solution 8

1. Suppose n is such that $\phi(n) = 2018 = 2 \cdot 1009$. Factoring $n = \prod p_i^{v_i}$ with the p_i distinct primes and the $v_i \geq 1$, we get that

   $$1009 \mid 2018 = \phi(n) = \prod \phi(p_i^{v_i})$$

   since ϕ is multiplicative. Since 1009 is prime, Euclid's lemma tells us that 1009 must divide one of the factors $\phi(p_i^{v_i}) = (p_i - 1)p_i^{v_i - 1}$, and then another use of Euclid gives us $1009 \mid (p_i - 1)$ or $1009 \mid p_i^{v_i - 1}$. We are now going to prove that neither of these can happen.

   Indeed, if $1009 \mid (p_i - 1)$, then $p_i \equiv 1 \bmod 1009$, so $p_i = 1 + 1009x$ for some integer $x \geq 0$. Actually, $1 + 1009x$ is not prime for $x = 0$ nor for $x = 1$, and not for $x = 2$ either since $1 + 1009 \cdot 2 = 2019$ si divisible by 3 (sum of digits). So we must have[3] $x \geq 3$. But then $p_i > 3 \cdot 2018$, which is absurd since the fact that $(p_i - 1) \mid \phi(p_i^{v_i}) \mid \phi(n) = 2018$ implies that $p_i - 1 \leq 2018$.

   And if $1009 \mid p_i^{v_i - 1}$, then by uniqueness of factorisation we must have $p_i = 1009$ and $v_i = 2$; but this is absurd since in this case $\phi(p_i^{v_i}) = (p_i - 1)p_i = 1008 \cdot 1009$ is clearly way too large to divide $\phi(n) = 2018$.

   So we have reached a contradiction, which means that no such n exists.

[2] This means either finitely many or none.

[3] Actually, a computer search shows that the smallest x such that $1 + 1009x$ is prime is $x = 10$.

2. Fix m, and let n be such that $\phi(n) = m$. Let p be a prime factor of n, and let $v = v_p(n)$ be the corresponding exponent, so that $n = p^v q$ with $q \in \mathbb{N}$ coprime to p. Then $m = \phi(n) = \phi(p^v)\phi(q)$ is divisible by $\phi(p^v) = (p-1)p^{v-1}$, so $(p-1)p^{v-1} \leq m$. This forces $p - 1 \leq m$, i.e. $p \leq m + 1$. and also shows that v cannot be arbitrarily large.

   So n has finitely many possible prime factors (the primes $\leq m+1$), and for each such prime p, $v_p(n)$ is bounded. So n has finitely many possible factorisations, i.e. there are finitely many candidates for such n.

   Remark: This is enough to prove that there are at most finitely many n such that $\phi(n) = m$, but of course, we have been rather sloppy, and as result we have probably grossly overestimated the number of such n. Estimating this number precisely would be much more complicated, cf. the previous exercise for instance!

3. Since $n \geq 3$, $n \neq 1$, so n has at least one prime factor p. Write again $n = p^v q$, where $v = v_p(n)$ so that $\gcd(p, q) = 1$. Then $(p-1)p^{v-1} = \phi(p^v) \mid \phi(n)$.

   Now clearly $p - 1$ is even, except if $p = 2$. So we are done if we can take $p \neq 2$. In other words, the only case for which we have not yet proved that $\phi(n0$ is even is the case where $n = 2^v$ is a power of 2. But since $n \geq 3$, we have $v \geq 2$, so $\phi(n) = \phi(2^v) = 2^{v-1}$ is again even as $v - 1 > 0$.

Exercise 9 *Divisibility criteria*

Let $n \in \mathbb{N}$.

1. Prove that n is congruent mod 9 to the sum of its digits. In other words, if $n_0, n_1, n_2, \cdots$ are the digits of n from right to left, so that

   $$n = n_0 + 10n_1 + 100n_2 + \cdots = \sum_i n_i 10^i,$$

   then $n \equiv n_0 + n_1 + n_2 + \cdots \bmod 9$.

2. Prove that $9 \mid n$ iff. 9 divides the sum of digits of n.

3. Find a similar criterion to test whether $11 \mid n$.

Solution 9

The key is the following observation: if $n_0, n_1, n_2, \cdots$ are the digits of n from right to left, so that

$$n = n_0 + 10n_1 + 100n_2 + \cdots = \sum n_i 10^i,$$

and since $10 \equiv 1 \bmod 9$, we have

$$n = \sum n_i 10^i \equiv \sum n_i 1^i = \sum n_i \bmod 9;$$

in other words, n is congruent to the sum of its digits (mod 9). In particular, this congruence also holds mod 3 since $3 \mid 9$.

So we have

$$9 \mid n \iff n \equiv 0 \bmod 9 \iff \sum n_i \equiv 0 \bmod 9 \iff 9 \mid \sum n_i$$

and

$$3 \mid n \iff n \equiv 0 \bmod 3 \iff \sum n_i \equiv 0 \bmod 3 \iff 3 \mid \sum n_i.$$

For divisibility by 11, we notice that $10 \equiv -1 \bmod 11$, so that

$$n = \sum n_i 10^i \equiv \sum n_i (-1)^i = n_0 - n_1 + n_2 - n_3 + \cdots \bmod 11.$$

As a result, $11|n$ if and only if the expression

$$n_0 - n_1 + n_2 - n_3 + \cdots,$$

which we may call the *alternate* sum of digits of n, is divisible by 11.

Exercise 10 *A huge number!*

In this exercise, you may use the fist question of the previous exercise: 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. Compute $D \bmod 9$.
2. Prove that $D \leq 14$.

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

Solution 10

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

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

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 $D \equiv 7 \bmod 9$ and that $D \leq 14$, we conclude that in fact $D = 7$.

Exercise 11 *Primitive roots mod 43*

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

3. What is the multiplicative order of g^{2020}, where g is the primitive root found in the previous question?

4. Prove that every primitive root in $(\mathbb{Z}/43\mathbb{Z})^\times$ is a power of g.

5. For which $m \in \mathbb{Z}$ is g^m a primitive root?

Solution 11

1. Since 43 is prime, primitive roots exist. More precisely, there are exactly $\phi(\phi(43)) = \phi(42) = 12$ of them. Compared to the $\phi(43) = 42$ 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
   $$MO(g^{2020}) = \frac{MO(g)}{\gcd(MO(g), 2020)} = \frac{42}{\gcd(2 \times 3 \times 7, 2^2 \times 5 \times 101)} = \frac{42}{2} = 21.$$
   In particular, g^{2020} is not a primitive root since $21 < 42$.

4. Since g is a primitive root, every element of $(\mathbb{Z}/43\mathbb{Z})^\times$ is a power of g; in particular this includes the primitive roots. And this has nothing to do with 43!

5. We know that $MO(g^m) = \frac{42}{\gcd(42,m)}$, so g^m is a primitive root iff. $MO(g^m) = 42$ iff. m is coprime to 42.

Exercise 12 *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 12

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, when we see Legendre symbols in chapter 3, we'll see that 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 13 *A multiplicative sequence*

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

1. Why cannot we say that t_n is periodic mod 40 "as usual"?
2. Find a formula for the values of t_n mod 5 in terms of n. You answer should have the form "if n is like this, then $t_n =$ this; if n is like that, then $t_n =$ that; if ...".
3. Find a formula for the values of t_n mod 8 in terms of n.

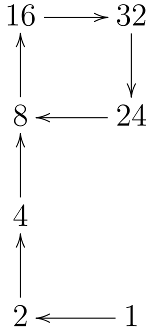
   Hint: Compute t_n for $n \leq 4$ "by hand".
4. Deduce a formula for t_n mod 40. What is the period? What is the length of the "tail"?

   Hint: 中國餘數定理.

Solution 13

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 Fermat's little theorem. Let us see: in $\mathbb{Z}/5\mathbb{Z}$, we have $t_0 = 1$, $t_1 = 2$, $t_2 = 4 = -1$, $t_3 = -2$, and $t_4 = -4 = 1 = t_0$. So the period is exactly 4 (in other words 2 is a primitive root in $\mathbb{Z}/5\mathbb{Z}$) and
$$t_n \bmod 5 = \begin{cases} 1 & \text{if } n \equiv 0 \bmod 4, \\ 2 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 2 \bmod 4, \\ -2 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$
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 $t_0 = 1$, $t_1 = 2$, $t_2 = 4$, and $t_3 = 8 = 0$. So $t_n \equiv 0 \bmod 8$ for all $n \geqslant 3$. Thus
$$t_n \bmod 8 = \begin{cases} 1 & \text{if } n = 0 \\ 2 & \text{if } n = 1, \\ 4 & \text{if } n = 2, \\ 0 & \text{if } n \geqslant 3. \end{cases}$$
4. The hint is to use CRT. Indeed, for $n \geqslant 3$ we have $t_n \equiv 0 \bmod 8$ whereas t_n mod 5 is given by the formula found in question 2. By putting this information together, we can deduce t_n mod 40 for $n \geqslant 3$; and for $n < 3$ we can just compute t_n by hand. We find
$$t_n \bmod 40 = \begin{cases} 1 & \text{if } n = 0 \\ 2 & \text{if } n = 1, \\ 4 & \text{if } n = 2, \\ 8 & \text{if } n \geqslant 3 \text{ and } n \equiv 3 \bmod 4, \\ 16 & \text{if } n \geqslant 3 \text{ and } n \equiv 0 \bmod 4, \\ 32 & \text{if } n \geqslant 3 \text{ and } n \equiv 1 \bmod 4, \\ 24 & \text{if } n \geqslant 3 \text{ and } n \equiv 2 \bmod 4. \end{cases}$$

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



Exercise 14 *A divisibility relation*

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

Solution 14

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 that its order is exactly 4, i.e. 2 is a primitive root mod 5), so $2^m \bmod 5$ only depends on $m \bmod 4$. And since $3n + 5 \bmod 4$ only depends on $n \bmod 4$, we have that $2^{3n+5} \bmod 5$ only depends on $n \bmod 4$.

Similarly, the multiplicative order of 3 mod 5 divides 4 (its in is fact again exactly 4), so $3^m \bmod 5$ only depends on $m \bmod 4$, and so $3^{n+1} \bmod 5$ only depends on $n \bmod 4$. As a result, the expression $2^{3n+5} + 3^{n+1} \bmod 5$ only depends on $n \bmod 4$. Thus all we have to do is check that $2^{3n+5} + 3^{n+1} \equiv 0 \bmod 5$ 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

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

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

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

Exercise 15 *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 15

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 primitive 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[4], 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.

[4] 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.