

Solving discrete problems — Math 2020, Spring 2005

Homework 4 Solutions

The solutions to the questions are in boxes.

1. Make multiplication and division tables for the integers modulo n for $n = 2, 3, 4, 5, 6, 7, 8$.

In the following tables, a is the variable in the left column, and b the variable in the top row. Remember that $a/b \equiv c \pmod n$ means that c is some integer with $a \equiv bc \pmod n$.

	0	1
0	0	0
1	0	1
$a \times b \pmod 2$		

	0	1
0	0	0
1	-	1
$a/b \pmod 2$		

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1
$a \times b \pmod 3$			

	0	1	2
0	0	0	0
1	-	1	2
2	-	2	1
$a/b \pmod 3$			

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1
$a \times b \pmod 4$				

	0	1	2	3
0	0	0	0	0
1	-	1	-	3
2	-	2	1	2
3	-	3	-	1
$a/b \pmod 4$				

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1
$a \times b \pmod 5$					

	0	1	2	3	4
0	0	0	0	0	0
1	-	1	3	2	4
2	-	2	1	4	3
3	-	3	4	1	2
4	-	4	2	3	1
$a/b \pmod 5$					

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1
$a \times b \pmod 6$						

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	-	1	-	-	-	5
2	-	2	1	-	2	4
3	-	3	-	1	-	3
4	-	4	2	-	1	2
5	-	5	-	-	-	1
$a/b \pmod 6$						

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1
$a \times b \pmod 7$							

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	-	1	4	5	2	3	6
2	-	2	1	3	4	6	5
3	-	3	5	1	6	2	4
4	-	4	2	6	1	5	3
5	-	5	6	4	3	1	2
6	-	6	3	2	5	4	1
$a/b \pmod 7$							

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1
$a \times b \pmod 8$								

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	-	1	-	3	-	5	-	7
2	-	2	1	6	-	2	7	6
3	-	3	-	1	-	7	-	5
4	-	4	2	4	1	4	2	4
5	-	5	-	7	-	1	-	3
6	-	6	7	2	-	6	1	2
7	-	7	-	5	-	3	-	1
$a/b \pmod 8$								

Important point:

A multiplication table for $\mathbf{Z}/N\mathbf{Z}$ should include all elements of $\mathbf{Z}/N\mathbf{Z}$ to be complete. Since $\mathbf{Z}/N\mathbf{Z}$ has N elements, which are (represented by) the numbers $0, 1, 2, \dots, N - 1$, these tables should have N rows and columns. If you give more columns, this is OK but unnecessary.

For example, modulo 5, the numbers 3 and 8 are the same, so a mod 5 table does not need columns for both 3 and 8, since they would be the same—see the following table.

In the following table, you can see how the 5×5 block repeats itself:

	0	1	2	3	4	5	6	7	8	9	5	6
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	0	1	2	3	4	0	1
2	0	2	4	1	3	0	2	4	1	3	0	2
3	0	3	1	4	2	0	3	1	4	2	0	3
4	0	4	3	2	1	0	4	3	2	1	0	4
5	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	2	3	4	0	1	2	3	4	0	1
7	0	2	4	1	3	0	2	4	1	3	0	2
8	0	3	1	4	2	0	3	1	4	2	0	3
9	0	4	3	2	1	0	4	3	2	1	0	4
5	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	2	3	4	0	1	2	3	4	0	1
7	0	2	4	1	3	0	2	4	1	3	0	2
8	0	3	1	4	2	0	3	1	4	2	0	3
9	0	4	3	2	1	0	4	3	2	1	0	4
$a \times b \pmod 5$												

2. For an integer n , we define $\mathbf{Z}/n\mathbf{Z}$ to be the set of integers modulo n , so we can write $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \dots, n - 1\}$.

The rules of addition on $\mathbf{Z}/n\mathbf{Z}$ are modulo n .

Now we set

$$\mathbf{Z}/n\mathbf{Z}^\times = \{x : x \in \mathbf{Z}/n\mathbf{Z} \text{ and } \gcd(x, n) = 1\}.$$

Here the gcd is computed in the usual way as for integers.

A. Prove the following result: If n, a and b are integers, and if $a \equiv b \pmod n$, then $\gcd(a, n) = \gcd(b, n)$.

Parts of the following proof are written out in blue; these parts are supposed to describe possible thinking processes for arriving at the proof; you don't need to write these out in your proof. Note that to prove something, you have to know what you're talking about, which means knowing and using the definitions; to emphasise this I've written definition in red. The importance of definitions is why some professors force you to memorise them.

Proof: [Use the hypothesis, $a \equiv b \pmod n$, and write out what this means, i.e., use the definition.] If $a \equiv b \pmod n$ then $a - b$ is divisible by n . [Now use the definition of divisible.] This means that for some integer q we have $a - b = qn$. Rearranging this, we have $a = b + qn$. [Now we have used the hypothesis to write down a concrete relationship between the quantities a and b ; this can be used to tackle the conclusion].

By substituting $a = b + qn$, we get

$$\gcd(a, n) = \gcd(b + qn, n). \quad (\star)$$

[Bearing in mind that we want to show that $\gcd(a, n) = \gcd(b, n)$, now we have to relate the quantity $\gcd(b + qn, n)$ to $\gcd(b, n)$. Note that $\gcd(b + qn, n)$ is already closer to $\gcd(b, n)$ than $\gcd(a, n)$, since it explicitly involves the quantity b , so we are probably on the right way to a proof.]

[Use the definition of gcd.] If $d = \gcd(b, n)$, then $d|b$ and $d|n$, i.e., [by definition of divisible], there are integers k, j such that $b = kd$ and $n = jd$. [Now we've dealt with what $d = \gcd(b, n)$ means, we turn to the quantity $\gcd(b + qn, n)$, and consider how we can relate this to $\gcd(b + qn, n)$.] From $b = kd$ and $n = jd$, we get $b + qn = kd + jd = (k + j)d$, which means [by definition of divisible] that $d|(b + qn)$; since we already have $d|n$, this means [by definition of gcd] that $d|\gcd(b + qn, n)$, i.e., [recalling how we defined d]

$$\gcd(b, n) | \gcd(b + qn, n). \quad (*)$$

[We actually want to show $\gcd(b, n) = \gcd(b + qn, n)$, one way to do this would be to show $\gcd(b + qn, n) | \gcd(b, n)$, since if u, v are two integers, $u|v$ and $v|u$ implies that $u = v$. There are various ways to achieve $\gcd(b + qn, n) | \gcd(b, n)$; one is to notice this will work in pretty much the same way as $\gcd(b, n) | \gcd(b + qn, n)$. This can be expressed in various ways; one is the following.]

[Now use the definition of gcd.] If $d = \gcd(b + qn, n)$, then $d|b + qn$ and $d|n$, i.e., [by definition of divisible], there are integers k', j' such that $b + qn = k'd$ and $n = j'd$. So we get $b = (b + qn) - qn = k'd - j'qd = (k' - j'q)d$, which means [by definition of divisible] that $d|b$; since we already have $d|n$, this means [by definition of gcd] that $d|\gcd(b, n)$, i.e., [recalling how we defined d]

$$\gcd(b + qn, n) | \gcd(b, n). \quad (\dagger)$$

So from (*) and (†) we must have $\gcd(b + qn, n) = \gcd(b, n)$. Combining this with (★), we get to the conclusion $\gcd(a, n) = \gcd(b, n)$.

B. Find the number of elements in $\mathbf{Z}/n\mathbf{Z}^\times$ for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$.

Note, if A is a set, the number of elements in A is usually written as $\#A$ or $|A|$. E.g., $\#(\mathbf{Z}/11\mathbf{Z})^\times = 10$.

To find $\mathbf{Z}/N\mathbf{Z}^\times$, just write out elements of $\mathbf{Z}/N\mathbf{Z}$, and cross out those which do not have $\gcd(x, N) = 1$:

$$\begin{aligned} (\mathbf{Z}/2\mathbf{Z})^\times &= \{\emptyset, 1\} \Rightarrow \#(\mathbf{Z}/2\mathbf{Z})^\times = 1 \\ (\mathbf{Z}/3\mathbf{Z})^\times &= \{\emptyset, 1, 2\} \Rightarrow \#(\mathbf{Z}/3\mathbf{Z})^\times = 2 \\ (\mathbf{Z}/4\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3\} \Rightarrow \#(\mathbf{Z}/4\mathbf{Z})^\times = 2 \\ (\mathbf{Z}/5\mathbf{Z})^\times &= \{\emptyset, 1, 2, 3, 4\} \Rightarrow \#(\mathbf{Z}/5\mathbf{Z})^\times = 4 \\ (\mathbf{Z}/6\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5\} \Rightarrow \#(\mathbf{Z}/6\mathbf{Z})^\times = 2 \\ (\mathbf{Z}/7\mathbf{Z})^\times &= \{\emptyset, 1, 2, 3, 4, 5, 6\} \Rightarrow \#(\mathbf{Z}/7\mathbf{Z})^\times = 6 \\ (\mathbf{Z}/8\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7\} \Rightarrow \#(\mathbf{Z}/8\mathbf{Z})^\times = 4 \\ (\mathbf{Z}/9\mathbf{Z})^\times &= \{\emptyset, 1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8\} \Rightarrow \#(\mathbf{Z}/9\mathbf{Z})^\times = 6 \\ (\mathbf{Z}/10\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9\} \Rightarrow \#(\mathbf{Z}/10\mathbf{Z})^\times = 4 \end{aligned}$$

C. Prove that if p is prime, then $\mathbf{Z}/p\mathbf{Z}^\times$ has $p - 1$ elements.

We have already seen that $\mathbf{Z}/p\mathbf{Z}$ has elements $0, 1, \dots, p-1$. (Or as equivalence classes, $[0], [1], \dots, [p-1]$.) So since $\mathbf{Z}/p\mathbf{Z}^\times$ is a subset of $\mathbf{Z}/p\mathbf{Z}$, we just need to check which of these elements is coprime to p . 0 is not in $\mathbf{Z}/p\mathbf{Z}^\times$, since $\gcd(0, p) = p$. For an integer a with $1 \leq a \leq p$, we must have $\gcd(a, p) = 1$, since if $d|a$ and $p|p$, since p is prime, $d = 1$ or p , and since $d|a$ and $a < p$ we must have $d < p$, so the only possibility is $d = 1$. So $\gcd(a, p) = 1$, so all of $1, 2, \dots, p-1$ (or their equivalence classes, which are all difference) are in $(\mathbf{Z}/p\mathbf{Z})^\times$, so $(\mathbf{Z}/p\mathbf{Z})^\times$ has $p - 1$ elements.

D. What can you say about the number of elements in $\mathbf{Z}/n\mathbf{Z}^\times$ when n is not prime?

If m is not prime, then there must be some prime p dividing m , and $1 < p < m$. The set $\mathbf{Z}/m\mathbf{Z}$ has elements $0, 1, \dots, m-1$. Of these, at least 0 and p are not in $\mathbf{Z}/m\mathbf{Z}^\times$, since $\gcd(0, m) = m \neq 1$ and $\gcd(p, m) = p \neq 1$. So we can say that $\#\mathbf{Z}/m\mathbf{Z}^\times \leq m - 2$.

E. Find the number of elements in $(\mathbf{Z}/2^n\mathbf{Z})^\times$ for $n = 1, 2, 3, 4$ do you notice a pattern?

As before, to find $\mathbf{Z}/N\mathbf{Z}^\times$, just write out elements of $\mathbf{Z}/N\mathbf{Z}$, and cross out those which do not have $\gcd(x, N) = 1$:

$$\begin{aligned} (\mathbf{Z}/2\mathbf{Z})^\times &= \{\emptyset, 1\} \Rightarrow \#(\mathbf{Z}/2\mathbf{Z})^\times = 1 \\ (\mathbf{Z}/4\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3\} \Rightarrow \#(\mathbf{Z}/4\mathbf{Z})^\times = 2 \\ (\mathbf{Z}/8\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7\} \Rightarrow \#(\mathbf{Z}/8\mathbf{Z})^\times = 4 \\ (\mathbf{Z}/16\mathbf{Z})^\times &= \{\emptyset, 1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15\} \Rightarrow \#(\mathbf{Z}/16\mathbf{Z})^\times = 6 \end{aligned}$$

You should notice the pattern $\#(\mathbf{Z}/2^n\mathbf{Z})^\times = 2^{n-1}$.

This is not hard to prove — half of the elements from 0 to $2^n - 1$ are odd, and so not divisible by 2 , and coprime to 2^n , which is only divisible by the prime 2 . These elements must be in $(\mathbf{Z}/2^n\mathbf{Z})^\times$. The other half are even, so are not coprime to 2^n , and so not in $(\mathbf{Z}/2^n\mathbf{Z})^\times$. So exactly half of the integers $0, 1, \dots, 2^n$ are in $(\mathbf{Z}/2^n\mathbf{Z})^\times$, so this set has $\frac{1}{2}2^n = 2^{n-1}$ elements.

F. Find the number of elements in $(\mathbf{Z}/(3 \times 5)\mathbf{Z})^\times$, $(\mathbf{Z}/(2 \times 5)\mathbf{Z})^\times$ and $(\mathbf{Z}/(3 \times 7)\mathbf{Z})^\times$. Do you notice any pattern? How many elements do you think are in $(\mathbf{Z}/(p \times q)\mathbf{Z})^\times$ for p and q primes, with $p \neq q$.

In the same way as before (crossing out elements not in the set), we can show that $\#(\mathbf{Z}/15\mathbf{Z})^\times = 6$, $\#(\mathbf{Z}/10\mathbf{Z})^\times = 4$, and $\#(\mathbf{Z}/21\mathbf{Z})^\times = 12$.

For primes p, q , the numbers from 1 to pq which are divisible by p are $p, 2p, 3p, \dots, qp$; the numbers which are divisible by q are $q, 2q, 3q, \dots, qp$. The first list has $q + 1$ numbers, and the second list has $p + 1$ numbers. In the first list, since q is prime, only 0 and pq are divisible by q . In the second list, since p is prime, only 0 and pq are divisible by p . So we have $q - 1$ elements: $p, 2p, 3p, \dots, (q - 1)p$ which are divisible by p , but not q , and we have $p - 1$ elements: $q, 2q, 3q, \dots, (p - 1)q$ which are divisible by q , but not p , and 1 element pq divisible by q and p . This gives $p - 1 + q - 1 + 1 = p + q - 1$ elements from 1 to pq which are not coprime to pq . These elements are distinct elements of $\mathbf{Z}/pq\mathbf{Z}$ which will not be in $\mathbf{Z}/pq\mathbf{Z}^\times$. There are pq elements from 1 to pq , which represent exactly the elements of $\mathbf{Z}/pq\mathbf{Z}$.

So there are $pq - (p + q - 1) = pq - p - q + 1 = (p - 1)(q - 1)$ elements in $\mathbf{Z}/pq\mathbf{Z}^\times$.

G. For integers n, a , find a condition on a so that $1/a \pmod n$ exists.

(To spot a pattern, use the tables computed in question 1, and more tables if necessary).

Either from examples or thinking hard about this, you should spot that if $1/a \pmod n$ exists, then $\gcd(n, a) = 1$. (For this question you only need to make this observation, no proof was required.)

To prove this, note that $x = 1/a \pmod n$ means $ax \equiv 1 \pmod n$, so $ax - 1 = n$, so $\gcd(a, n) = \gcd(a, ax - 1) = 1$, (since if $d|a$ and $d|ax - 1$, then d divides ax and $ax - 1$, so d divides $ax - (ax - 1) = 1$, so $d = 1$).

Conversely, if $\gcd(a, n) = 1$, then for some u, v , we have $au + nv = 1$, so $au - 1 = -nv$ so $au \equiv 1 \pmod n$, so we can take $u \equiv 1/a \pmod n$.

So in fact, $1/a \pmod n$ exists if and only if $\gcd(a, n) = 1$.

3. Can you find an example of a number m , which is not prime, and another number a so that $a^{m-1} \equiv 1 \pmod{m}$? If so, give an example, if not, why not?

The simplest possible example is to take $a = 1$. We always get $1^{m-1} = 1$, and so $1^{m-1} \equiv 1 \pmod{m}$. It's sufficient for you to give this as an example, since the question did not specify that $a \neq 1$.

But there are other examples even apart from this, but they are not easy to find, unless you know that for all a with $\gcd(a, m) = 1$, we have $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is the number of elements in $(\mathbf{Z}/m\mathbf{Z})^\times$. (The result $a^{\phi(m)} \equiv 1 \pmod{m}$ can be proved in a similar way to Fermat's little theorem, and is no more difficult, just needs some modifications of that proof.)

We saw in 2 part F above that if p and q are prime, then $\mathbf{Z}/pq\mathbf{Z}^\times = (p-1)(q-1)$, so the version of Fermat's little theorem for $m = pq$ says that if $\gcd(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Suppose we are in the case $m = pq$. This question asks if we can have $a^{pq-1} \equiv 1 \pmod{pq}$. If this was true, since we have that $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$, we would get $a^{(p-1)(q-1)} = a^{pq-p-q+1} = a^{pq-1}a^{-p-q+2} \equiv a^{-p-q+2} \equiv 1 \pmod{pq}$, so $a^{p+q-2} \equiv 1 \pmod{pq}$. Now we have $a^{p+q-2} \equiv 1 \pmod{pq}$ and $a^{pq-1} \equiv 1 \pmod{pq}$. Suppose $d = \gcd(pq-1, p+q-2)$. This means that there are some integers u, v with $d = u(pq-1) + v(p+q-2)$, so $a^d = a^{u(pq-1)+v(p+q-2)} = a^{u(pq-1)}a^{v(p+q-2)} = (a^{pq-1})^u(a^{p+q-2})^v \equiv 1^u 1^v \equiv 1 \pmod{pq}$. If $d = \gcd(pq-1, p+q-2) = 1$, then this would mean that $a = a^1 \equiv 1 \pmod{pq}$, which is the easy case we already knew about. For more interesting examples, we at least need to find prime p and q with $p+q-2$ and $pq-1$ having a common factor greater than 1. E.g., could these numbers both be divisible by 3? For this we'd need $p+q \equiv 2 \pmod{3}$ and $pq \equiv 1 \pmod{3}$, so we could take any p and q with $p \equiv q \equiv 1 \pmod{3}$.

E.g., try $p = 7$ and $q = 13$, so that $pq = 7 \times 13 = 91$. Then $p+q-2 = 18$, and $pq-1 = 90$. We have $\gcd(18, 90) = 18$. So, there might be some number a with $a^{18} \equiv 1 \pmod{91}$, and with $a \not\equiv 1 \pmod{91}$. To find out, we can just try all numbers from 2 to 91.

Try $a = 2$, we get $2^{18} = 91 \times 2880 + 64$, so $a = 2$ does not work.

Try $a = 3$, and we get $3^{18} = 387420489 = 4257368 \times 91 + 1$.

So $3^{18} \equiv 1 \pmod{91}$,

so $a = 3$ and $m = 91$ gives an example where m is not prime, and $3^{m-1} \equiv 1 \pmod{m}$.

Using the same technique you can find more examples.

If $a^{m-1} \equiv 1 \pmod{m}$ for all a with $1 \leq a \leq m-1$, can we conclude that m is prime? If so, prove this, if it's not true, give an example.

Note, I changed this question to ask you what you thought from examples, but not to try to give a proof, since we have not covered enough material. However, you should notice from examples that we never have $a^{m-1} \equiv 1 \pmod{m}$ for all a with $1 \leq a \leq m-1$ when m is not prime.

Here is a fairly simple proof:

If $a^{m-1} \equiv 1 \pmod{m}$ for all a with $1 \leq a \leq m-1$, then $a \times a^{m-2} \equiv 1 \pmod{m}$, so, using the result given in part G, $a \pmod{m}$ has an inverse, namely $1/a \equiv a^{m-2} \pmod{m}$. However, we saw that $a \pmod{m}$ has an inverse implies that $\gcd(a, m) = 1$. So if for all of a with $1 \leq a \leq m-1$ we have $a^{m-1} \equiv 1 \pmod{m}$, then for all a with $1 \leq a \leq m-1$ we have $\gcd(a, m) = 1$, which means that m is prime. So, if m is not prime, it can't happen that $a^{m-1} \equiv 1 \pmod{m}$ for all a with $1 \leq a \leq m-1$.

Note, even if we restrict to a which are coprime to m , we still don't generally get $a^{m-1} \equiv 1 \pmod{m}$, but this involves a generalisation of Fermat's little theorem to the non-prime case, and other results which we have not discussed.