Notes on Modular Arithmetic

Let $m$ and $n$ be integers, where $m$ is positive. Then, by the remainder formula, we can write $n = qm + r$ where $0 \leq r < m$ and $q$ is an integer. Instead of writing $n = qm + r$ every time, we use the congruence notation: we say that $n$ is congruent to $r$ modulo $m$ if $n = qm + r$ for some integer $q$, and denote this by

$$n \equiv r \pmod{m}.$$

If $n$ is an integer, then

For any integers $m$ and $n$, we write $n (\text{mod } m)$ to denote the remainder when $n$ is divided by $m$.

Since the remainder is between zero and $m$, the set $\{n (\text{mod } m) : n \in \mathbb{Z}\}$ is exactly the same as $\{0, 1, 2, \ldots, m - 1\}$ — these are all possible remainders when $n$ is divided by $m$. In this way, we introduce a new relation on the integers, namely congruence, which we denote by the symbol $\equiv$, this is the congruence or equivalence symbol. Two integers $a$ and $b$ are congruent modulo $m$, written $a \equiv b \pmod{m}$ if they have the same remainder when divided by $m$. For example, any two odd numbers are congruent modulo two, since the remainder when we divide them by two is 1. Note that $a \equiv b \pmod{m}$ is exactly the same as $a - b \equiv 0 \pmod{m}$. This last statement is the way to check whether $a$ and $b$ are congruent mod $m$: just check whether $a - b$ is divisible by $m$. When it is obvious what $m$ is, we will sometimes just write $a \equiv b$ instead of $a \equiv b \pmod{m}$.

The $\equiv$ symbol behaves very much like the $=$ symbol and the $\leftrightarrow$ symbol. The three basic properties (modulo any number $m$) are:

1. $a \equiv a$
2. $a \equiv b \leftrightarrow b \equiv a$
3. $a \equiv b \land b \equiv c \rightarrow a \equiv c$.

All these properties can be checked directly from the definition of $\equiv$. For example, to check the last property, note that $a \equiv b \leftrightarrow a - b \equiv 0 \leftrightarrow a - b = qm$ for some integer $q$, and $b \equiv c \leftrightarrow b - c \equiv 0 \leftrightarrow b - c = rm$ for some integer $r$, so

$$a - c = (a - b) - (b - c) = (q - r)m$$

which means $a - c \equiv 0$ or $a \equiv c$, proving (3).

Many of the usual rules of arithmetic apply when dealing with congruences. For example, $a \equiv b$ implies $ac \equiv bc$ and $a \pm c \equiv b \pm c$ for any integer $c$ — so we can multiply and add or subtract from both sides of a congruence. This allows us to introduce a new system of arithmetic on $\{0, 1, 2, \ldots, m - 1\}$ called modular arithmetic, and we denote this new system by $\mathbb{Z}_m$, the integers modulo $m$. We can imagine that the numbers $\{0, 1, 2, \ldots, m - 1\}$ are placed around a circle in increasing clockwise order, and then note that when we add numbers $a, b \in \{0, 1, 2, \ldots, m - 1\}$ in $\mathbb{Z}_m$, we imagine that we are starting at zero, and then moving $a + b$ steps around the circle, and this gives us $a + b \pmod{m}$. The same thing works for
multiplication: for example, $3a \pmod{m}$ (i.e. three times $a$ in $\mathbb{Z}_m$) is obtained by starting at 0 and then moving $3a$ steps clockwise around the circle. Subtraction is obtained by moving counterclockwise around the circle. Of course, this is just a pictorial representation; if we really want to find something like $111 \cdot 222 \pmod{246}$ then we use long division to find the remainder when $111 \cdot 222$ is divided by 246.

**Example.** Find $111 \cdot 222 \pmod{246}$. Well, first multiply 111 by 222 as integers: we get $111 \cdot 222 = 24642$. Now we have to divide by 246. Well by long division $24642 = 246 \cdot 100 + 42$, so the remainder is 42 when we divide 24642 by 246. Therefore $111 \cdot 222 \pmod{246} = 42$.

We could also try negative numbers: find $-11 \pmod{17}$. Since these numbers are small, we could visualize it using the circle: start at zero and move 11 steps counterclockwise. We arrive at 6, so $11 \pmod{17} = 6$. Let’s check it by long division: we see that $11 = (-1) \cdot 17 + 6$, so the remainder when we divide 17 by $-11$ is 6, confirming our result.

### Computing Large Congruences.

We can work out congruences using Fermat’s Theorem and/or a little bit of ingenuity. The main trick is often to replace parts of expressions mod $m$ with simpler expressions. Let’s do some examples.

**Examples.** To work out $6^{16} \pmod{5}$ is really easy. Notice that $6^{16} \equiv 1^{16} \equiv 1 \pmod{5}$, so the answer is $6^{16} \equiv 1 \pmod{5}$ and we didn’t even use Fermat. We could have used Fermat: since $6^4 \equiv 1 \pmod{5}$, we know $6^{16} \equiv 6^{4 \cdot 4} \equiv (6^4)^4 \equiv 1^4 \equiv 1 \pmod{5}$. Let’s work out $39^{41} \pmod{11}$ using Fermat; it applies since 11 is prime. Fermat gives $39^{10} \equiv 1$. So

$$39^{41} \equiv 39^{4 \cdot 10 + 1} \equiv 39 \equiv 6 \pmod{11}.$$ 

How about $39^{41} \pmod{12}$? We cannot use Fermat since 12 is not prime. Fortunately $39 \equiv 3 \pmod{12}$ so

$$(39)^{41} \equiv (3)^{41} \equiv 9 \cdot (3^3)^{13} \equiv 9 \cdot 3^{13} \equiv 9 \cdot 3^4 \cdot 3 \equiv 3^7 \equiv (3^3)^2 \cdot 3 \equiv 9 \cdot 3 \equiv 3 \pmod{12}.$$ 

We repeatedly replaced $3^3$ by 3 in this example, since 27 $\equiv 3 \pmod{12}$. What about $1115^{1111} \pmod{9}$? Since $1115 \equiv 8 \pmod{9}$, this is the same as $8^{1111} \pmod{9}$. Now $8^2 \equiv 1 \pmod{9}$ so we can repeatedly replace $8^2$ with 1. We can do that 1110/2 = 555 times until we’re left with $1^{555} \cdot 8^1$. So $1115^{1111} \equiv 8 \pmod{9}$. A summary of what we just said is given below:

---

**To find $a^b \pmod{m}$ when $m$ is prime, replace $a$ with the remainder when $a$ is divided by $m$, and replace $b$ with the remainder when $b$ is divided by $m-1$.**

**If $m$ is not prime, then to compute $a^b \pmod{m}$, look for powers of $a$ that are congruent to $s$, something small, mod $m$, and repeatedly replace these powers with $s$.**

---

Try the following on your own:

- $2^{81} \pmod{7}$
- $12^{81} \pmod{17}$
- $13^{13} \pmod{14}$
- $31^{41} \pmod{50}$
- $10^{10^{10}} \pmod{7}$
- $(-5)^{99} \pmod{8}$
Inverses

We have mentioned how multiplication, addition, and subtraction affect $\equiv$. But can we do division? In our usual arithmetic on rational numbers (i.e. fractions), the inverse of a fraction $n$ is just $q = 1/n$, which is still a fraction. In other words, it is the fraction $q$ such that $nq = 1$. In $\mathbb{Z}_m$, an inverse of a number $n$ is a number $q$ such that $nq \equiv 1 \pmod{m}$. But this no longer means that $q = 1/n$, since $1/n$ is not allowed in our set \{0,1,2,\ldots,m-1\}! So what is $q$, then? Let’s do some examples to see what $q$ could be.

Example. Suppose we’re working in $\mathbb{Z}_5$. Zero has no inverse, because there is no number $q$ such that $0 \cdot q \equiv 1$ (remember this would mean $1 - 0q = 1$ is divisible by 5, which is never true). The inverse of 1 is clearly 1, since $1 \cdot 1 \equiv 1$. The inverse of 2 is 3, since $2 \cdot 3 \equiv 1$. The inverse of 3 is 2, the inverse of 4 is 4, and so we’ve worked out the inverses of all numbers in $\mathbb{Z}_5$, apart from 0 which has no inverse. Let’s now try $\mathbb{Z}_6$. Zero has no inverse again, and the inverse of 1 is 1. What about 2? Well we can try all numbers in \{0,1,2,3,4,5\}, and none of them satisfies the definition of the inverse. So we say that 2 has no inverse. Similarly, 3 and 4 have no inverse. Now 5 has an inverse, namely 5, since $5 \cdot 5 = 25$ and $25 \equiv 1$.

We saw in the last example that some numbers in $\mathbb{Z}_m$ have inverses, and some don’t. How can we tell? Definitely zero never has an inverse, and 1 is the inverse of 1, but what about 2,3,\ldots,m-1? The following theorem gives us a complete answer:

**Theorem.** Let $n$ and $m > 1$ be positive integers. Then $n$ has an inverse in $\mathbb{Z}_m$ if and only if $\gcd(m,n) = 1$.

Numbers $m$ and $n$ such that $\gcd(m,n) = 1$ are called relatively prime numbers. So to check if $n$ has an inverse modulo $m$, we just have to check whether $m$ and $n$ are relatively prime. Fortunately, we know how to do that using the Euclidean Algorithm. But first, let’s show why the theorem is true:

**Proof.** If $\gcd(m,n) = 1$, then by a previous theorem, there are integers $\alpha$ and $\beta$ such that

$$1 = \alpha m + \beta n.$$  

This means

$$1 \equiv \alpha m + \beta n \pmod{m}.$$  

But $\alpha m \equiv 0$ modulo $m$, since $\alpha m$ is divisible by $m$, so we get $\beta n \equiv 1$ mod $m$. By definition, that means $\beta$ is the inverse of $n$. It is an exercise to show that if $n$ has an inverse, then $\gcd(m,n) = 1$.

If $n$ has an inverse in $\mathbb{Z}_m$, then the inverse is unique, and we denote it by $n^{-1}$. For example, in $\mathbb{Z}_5$ we saw that $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$. Why can’t a number $n$ have two inverses in $\mathbb{Z}_m$? Well, suppose for a contradiction that $q$ and $r$ are both inverses of $n$. Then $qn \equiv 1$ and $rn \equiv 1$. This means $(q - r)n \equiv 0$ in $\mathbb{Z}_m$, which means $m|(q - r)n$. But by the theorem, $\gcd(m,n) = 1$, so $m|(q - r)$. However $q, r$ are elements of $\mathbb{Z}_m$, so they are in \{0,1,2,\ldots,m-1\}. The only way $q - r$ could be divisible by $m$ is that $q - r = 0$, i.e. $q = r$. Therefore $n$ has a unique inverse.
To find the inverse of \( n \) in \( \mathbb{Z}_m \), the steps to take are: first make sure \( \gcd(m, n) = 1 \) by performing the Euclidean Algorithm. Whenever we perform step (2) in the algorithm, say we're looking at \( \gcd(a, b) \) and \( b = aq + r \) where \( 0 < r < a \), write out the working in full:

\[
\cdots = \gcd(a, b) = \gcd(a, b - aq) = \cdots
\]

At the end, if \( n \) has an inverse, we get \( \gcd(x, 1) \) for some \( x \), and since we always replace \( b \) by \( b - aq \) in step (2), we find the expression \( 1 = mx + ny \), and the number \( y \) is the inverse of \( n \). We make this definite with an example:

**Example.** Find \( 9^{-1} \) in \( \mathbb{Z}_{17} \). Well, we apply the above procedure: using the Euclidean Algorithm:

\[
\gcd(9, 17) = \gcd(9, (-1)17 + (2)9) = \gcd(9, 1) = 1.
\]

We deduce that \( 1 = (-1)17 + (2)9 \) so \( \beta = 2 \) and \( 9^{-1} = 2 \). If we check it, we indeed get \( 9 \cdot 2 \equiv 1 \) in \( \mathbb{Z}_{17} \). Now let's find \( 8^{-1} \) in \( \mathbb{Z}_{17} \).

\[
\gcd(8, 17) = \gcd(8, 17 - (2)8) = \gcd(8, 1) = 1.
\]

So \( 1 = 17 - (2)8 \) which means \( 8^{-1} \equiv -2 \mod 17 \). But we want the inverse in \( \mathbb{Z}_{17} \), so negative numbers are not allowed. We use \( -2 \equiv 15 \mod 17 \): so \( 8^{-1} = 15 \) in \( \mathbb{Z}_{17} \). If we check it, \( 8 \cdot 15 = 120 \) and since \( 120 = 17 \cdot 7 + 1 \), we have \( 8 \cdot 15 \equiv 1 \) in \( \mathbb{Z}_{17} \), as required.

**Modular Equations.**

- **Example.** Solve the equation \( 2x + 3 \equiv -1 \mod 15 \). Well this is the same as \( 2x \equiv -4 \mod 15 \) and since \( -4 \equiv 11 \mod 15 \) we get \( 2x \equiv 11 \mod 15 \). Therefore \( x \equiv 2^{-1} \cdot 11 \mod 15 \), and it remains to work out \( 2^{-1} \). Using the Euclidean Algorithm:

\[
\gcd(2, 15) = \gcd(2, 15 - 7 \cdot 2) = \gcd(2, 1) = 1,
\]

and therefore \( 1 = 15 - 7 \cdot 2 \) and so \( 2^{-1} \equiv -7 \mod 15 \). Now \( -7 \equiv 8 \mod 15 \), so \( 2^{-1} = 8 \mod 15 \). This gives \( x \equiv 88 \equiv 3 \mod 15 \); in other words, the solution is \( x = 3 \).

- **Example.** Solve the equation \( 121x \equiv 23 \mod 501 \). We have to work out \( 121^{-1} \) – at this point, we don’t even know if it exists – we have to check that \( \gcd(121, 501) = 1 \).

\[
\gcd(121, 501) = \gcd(121, 501 - 4 \cdot (121)) = \gcd(121 - 7 \cdot (501 - 4 \cdot (121)), 501 - 4 \cdot (121)) = \gcd(3, 1).
\]

Therefore

\[
1 = 501 - 4 \cdot (121) - 5 \cdot (121 - 7 \cdot (501 - 4 \cdot (121))) = -37 \cdot (121) + 36 \cdot 501
\]

so \( 121^{-1} \equiv -37 \equiv 464 \mod 501 \). Therefore

\[
x \equiv 121^{-1} \cdot 23 \equiv 464 \cdot 23 \mod 501
\]

and since \( 464 \cdot 23 = 10672 \), \( x \equiv 10672 \mod 501 \). But \( 10672 = 21 \cdot 501 + 151 \) using long division, so \( x = 151 \) is the final answer.