Modular Arithmetic

Table of Contents

1 Introduction

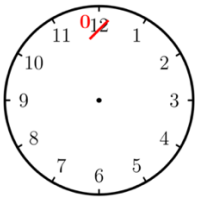
Modular arithmetic is a system of arithmetic for integers, which considers the remainder. In modular arithmetic, numbers "wrap around" upon reaching a given fixed quantity (this given quantity is known as the modulus) to leave a remainder.

Modular n (mod n) answers the question, what is the remainder left over when you take out groups of n? How many times does your modular number divide the number in question and what is the remainder? Remember, the remainder is your answer, not how many times you fit in.

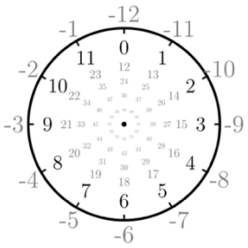
mod tells you how many values we have in mod and highest number in mod is always one less than mod number itself
So, mod n is the set {0,1,2,3,4,…n-1} i.e. the remainder when you divide by n
Note n≡ 0 in mod n since n divides n so that is why we don't go as far as n in the set

For example, mod3 is {0,1,2}.
There are 3 values in mod 3 and the highest number is 2.
3≡ 0 in mod 3, this is why we don't have 3 in the set, since it is already accounted for with 0

An intuitive way to understand modular arithmetic is with a 12-hour clock. We conduct the familiar addition of hours and replace 12 on the clock face by 0 (we say 12 is equivalent to zero and hence are in mod 12)



We wrap the number line around a circle such that all numbers with the same remainder from division by 12 are in the same position



If it is 10:00 now, then in 5 hours the clock will show 3:00 instead of 15:00. 3 is the remainder of 15 with a modulus of 12.

2 Basic simplification examples

Let's do some basic examples so you can better understand how this works.

2.1 Simplifying positive numbers

- What is $8\ (mod\ 5)$
  Way 1:
  Only allowed numbers {0,1,2,3,4}
  Divide 8 by 5 and consider remainder. $\frac{8}{5} = 1\ r\ 3$
  The remainder is 3
  So, $8 \equiv 3\ (mod\ 5)$

  Way 2:
  Keep subtracting multiples of 5 until end up in {0,1,2,3,4}
  $8 - 5 = 3$
  So, $8 \equiv 3\ (mod\ 5)$

- What is $19\ (mod\ 4)$?
  Way 1:
  Only allowed numbers {0,1,2,3}
  Divide 19 by 4 and consider remainder. $\frac{19}{4} = 4\ r\ 3$
  The remainder is 3
  So, $19 \equiv 3\ (mod\ 4)$

  Way 2:
  Keep subtracting multiples of 4 until end up in {0,1,2,3}
  $19 - 4(4) = 3$
  So, $19 \equiv 3\ (mod\ 4)$

- What is $53\ (mod\ 3)$?
  Way 1:
  Only allowed numbers {0,1,2}
  Divide 53 by 3 and consider remainder. $\frac{53}{3} = 17\ r\ 2$
  The remainder is 2
  So, $53 \equiv 2\ (mod\ 3)$

  Way 2:
  Keep subtracting multiples of 3 until end up in {0,1,2}
  $53 - 17(3) = 2$
  So, $53 \equiv 2\ (mod\ 3)$

2.2 Simplifying Negative Numbers

If dealing with negative number one way is to keep adding multiples of the mod since if "bumping up" by the mod - you're not changing the number since n in mod n is the same as zero.

- What is $-8\ (mod\ 5)$?
  Way 1:
  Consider positive 8
  One lot of 5 goes into 8 and gives a remainder of 3 so -3
  So we have -3
  But only allowed numbers {0,1,2,3,4}
  We can just keep adding 5 until you get into that positive interval from 0-4
  -3+5=2
  So, $-8 \equiv 2\ (mod\ 5)$

Way 2:
Start at -8 and keep adding multiples of 5 until you end up in {0,1,2,3,4}
$-8+2(5)=2$
So, $-8 \equiv 2 \pmod 5$

Way 3:
Ask yourself how far from the closest neg multiple of 5
2 away from -10
So, $-8 \equiv 2 \pmod 5$

- What is $-15 \pmod 8$?
  Way 1:
  Consider positive 15
  One lot of 8 goes into 8 and gives a remainder of 7 so -7
  So we have -7
  But the only allowed numbers are {0,1,2,3,4,5,6,7}
  You can just keep adding 8 until you get into that positive interval from 0-7
  -7+8=1
  So, 1 (mod 8)

  Way 2:
  Start at -15 and keep adding multiples of 8 until you end up in {0,1,2,3,4,5,6,7}
  $-15+2(8)=1$
  So, 1 (mod 8)

  Way 3:
  Ask yourself "how far from closest neg multiple of 8?"
  1 away from -16
  So, 1 (mod 8)

- Is $10 \equiv -2 \pmod 4$ a true statement?
  LHS is 2. On RHS we can start at -2 and add 4 to it which is the same as 2 mod 4
  $\therefore$ true

3 Interpretations

Now you understand how mod n works, let's define it slightly more formally.
$a \equiv b \ (mod\ n)$ says in the world of mod n, a and b are equivalently the same thing. We can interpret this in the following **three** ways

i. **They have the same "remainder" when they are divided by n where $n > 1$. We put in quotes since we may end up with negative remainder**
ii. **$a = kn + b$ for some k$\in \mathbb{Z}$**
iii. **$n|(a - b)$. This means n divides $(a - b)$ so $(a - b)$ is a multiple of n**

The first is the most natural way to know what mod means. The second is useful when trying to solve for an equation from a congruence (you change the congruence to an equation first) and the third is useful for proofs

Note: $a \equiv 0 \ (mod\ n)$ means a is a multiple of n, i.e. $a = kn$ for some k$\in \mathbb{Z}$

$\mathbf{10 \equiv 14 \ (mod\ 4)}$

Using the 3 interpretations above

i. $10 \div 4 = 2R2$
$14 \div 4 = 3R2$
So we have the same remainder 2

ii. $10 = ?\, 4 + 14$
$10 = -1(4) + 14$ so $k = -1$

iii. $4|(10 - 14)$ so $4|-4$ and this is true that 4 divides -4 since -4=4(-1) which is a multiple

4 Notations/Definitions

- Division
  $a|b$ means a divides b (a is a divisor/factor of b or b is a multiple of a)
  i.e. $b = az$ for some $z \in \mathbb{Z}$
- $\mathbb{Z}_n$ or $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$ (the integers mod n) = {0,1,2,3,4,…n-1}
- $\mathbb{Z}_n{}^*$ (integers mod n without 0) ={1,2,3,4,…n-1,}
- $(\mathbb{Z}_n)^\times$ (set of integers coprime to n i.e. the integers which are invertible mod n)
  If n is prime we get $(\mathbb{Z}_p)^\times$={1,2,…p-1}

$$(\mathbb{Z}_6)^\times = \{\mathbf{1}, \mathbf{5}\}$$
$$(\mathbb{Z}_5)^\times = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}\}$$

- Highest Common Factor
  If a, b are non-zero integers then the highest common factor (HCF) is the largest positive integer which divides $a \; and \; b$ and is denoted hcf (a,b). Some courses call this the greatest common divisor (GCD).
  If $hcf(a, b)$= 1 then $a \; and \; b$ are called coprime i.e. no factors in common. This can be written as hcf(a,b) = 1 iff a & b are coprime

5 Theorems/Algorithms/Lemmas

5.1 Division Theorem

Let $a, b \in \mathbb{Z}$, $b > 0$, then $\exists$ *unique integers* $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$.
Note: This can also be written as $a = qb + r$ (*)
This should make sense since $\frac{a}{b} = quotient + \frac{remainder}{b}$
If we re-arrange, we get $a = b(quotient) + remainder$ which is (*)

Consider 13 and 3
We can write this as $13 = 3 \times 4 + 1$
This can also we written as $\frac{13}{4} = 3 + \frac{1}{4}$

5.2 Euclid's Algorithm

Euclid's Algorithm is a method for finding the HCF/GCD of 2 positive integers by repeated division.
Note: There is no quick algorithm for working out if a number is prime.
You should always end up with +0 as your last remainder at the end if done correctly

- **Use Euclid's algorithm to find the HCF of 1169 and 560**

$1169 = 560 \times 2 + 49$
$560 = 49 \times 11 + 21$
$49 = 21 \times 2 + 7$ → HCF is last non-zero remainder
$21 = 7 \times 3 + 0$
$\Rightarrow$ HCF (1169, 560) = 7

- **Use Euclid's algorithm to find the HCF of 10414 and 9129**

$10414 = 9129 \times 1 + 1285$
$9129 = 1285 \times 7 + 134$
$1285 = 134 \times 9 + 79$
$134 = 79 \times 1 + 55$
$79 = 55 \times 1 + 24$
$55 = 24 \times 2 + 7$
$24 = 7 \times 3 + 3$
$7 = 3 \times 2 + 1$ → HCF is last non-zero remainder
$3 = 1 \times 3 + 0$
$\Rightarrow$ HCF (10414, 9129) = 1

Therefore 10,414 and 9129 are co-prime

5.3 Bezout's Lemma/Identity

Let a and b be non-integers with highest common factor d. Then there exist integers s *and* r such that $as + br = d$ i.e. $as + br = hcf(a, b)$
So, this is saying we can write the HCF of a and b as a linear combination of a and b. What does this mean. For example, $5 = 12 \times 1 - (8 \times 1)$ where 4 is written as a linear combination of 12 and 8 i.e the sum or difference of any integer times 12 and any integer times 8.

Why is Bezout's useful?
Say you want to write 2 as a linear combination of **6** and **8.** We know we can do this by Bezout's since the HCF(6,8) is 2.
This is easy to just spot straight away
$2 = \mathbf{8} \times 1 - \mathbf{6} \times 1$
What about when it is not easy to spot for any two numbers?
We can of course write out the multiple of each
6,12,18,24,…. AND 8,16,24,…

Then we can try and spot what combination of a pair of numbers (one from each list) subtracted will give us 2
However, this may be time consuming for larger numbers and we don't need to do this!
Bezout's Lemma guarantees the existence of these numbers, and we use the EXTENDED Euclid Algorithm to find them.

Method: We find the HCF using Euclid's algorithm and then work backwards from Euclid's algorithm with what is known as Extended Euclid's Algorithm. The examples below will make this method clear.

Use Euclid's algorithm to find the highest common factor d of 2406 and 330. Also find integers r and s such that $d = 2406r + 330s$

$2406 = 330 \times 7 + 96$
$330 = 96 \times 3 + 42$
$96 = 42 \times 3 + 12$
$42 = 12 \times 3 + 6$ → HCF is last non-zero remainder
$12 = 6 \times 2 + 0$
$\Rightarrow HCF(2406, 330) = 6$

$$so\ d = 6$$

If we extend Euclid's Algorithm, by re-arranging each step of the Euclidian Algorithm above we get

$2406 = 330 \times 7 + 96 \Rightarrow 96 = 2406 - 330 \times 7$
$330 = 96 \times 3 + 42 \Rightarrow 42 = 330 - 96 \times 3$
$96 = 42 \times 3 + 12 \Rightarrow 12 = 96 - 42 \times 3$
$42 = 12 \times 3 + 6 \Rightarrow 6 = 42 - 12 \times 3$ (*)
$12 = 6 \times 2 + 0$

Start from (*) and work your way upwards

$6 = 42 - 12 \times 3$
Replace the 12
$= 42 - (96 - 42 \times 2) \times 3$
Simplify by multiplying out and then grouping the 42's
$= 42 \times 7 - 96 \times 3$
Replace the 42
$= (330 - 96 \times 3) \times 7 - 96 \times 3$
Simplify by multiplying out and then grouping the 96's
$= 330 \times 7 - 96 \times 24$
Replace the 96
$= 330 \times 7 - (2406 - 330 \times 7) \times 24$
Simplify by multiplying out and then grouping the 330's
$= 330 \times 175 - 2406 \times 24$
So,
$6 = 175 \times 330 - 24 \times 2406$
$s = 175, r = -24$

5.4 Linear combinations (corollary of Bezout's)

More generally, the integers of the form $as + br$ are exactly the **multiples** of d, i.e. not necessarily equal to $hcf(a, b)$ but of any multiple of $hcf(a, b)$. Meaning, we can write any multiple of the hcf of a and b as a linear combination of a and b.
Formally we say, $as + br = y$ where $hcf(a, b)|y$ i.e. we can write y a and b as a linear combination of a and b iff $hcf(a, b)|y$

Take the last example in the section above where we wrote hcf(2406,330) as a multiple of 2406 and 330
We found that $6 = 175(330) - 24(2406)$
We can now extend this to any multiple of 6, let's choose 18.
So we want to write 18 as a multiple of 330 and 2406
$18 = 3[175(330) - 24(2406)]$
$18 = 525(330) - 72(2406)$
So, we have r and s such that $18 = 2406r + 330s$
$r = 525, s = -72$

Notice how we have just multiplied ours answer in the previous example by 3.

It should be stated that the Bezout's coefficients are not necessarily unique.

gcd(12,42) = 6
12 x (-10) + 42 x (3) = 6
12 x (-3) + 42 x (1) = 6
etc

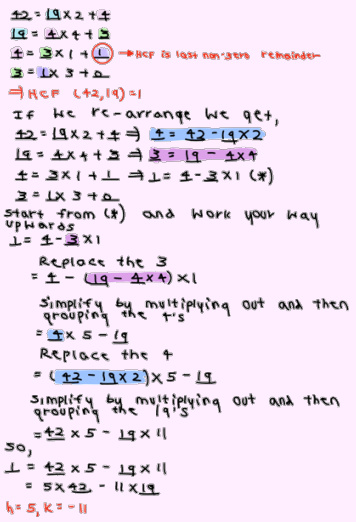
5.5 h-k Lemma

If a and b are coprime, then $\exists h, k$ such that $ah + bk = 1$. This is just Bezout's Lemma where the highest common factor is 1. The reverse is also true, ah + bk = 1 implies a,b are coprime.

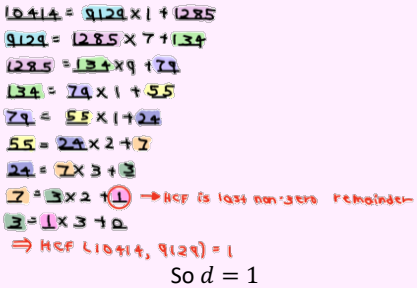
Write 1 as a linear combination of 5 and 7
This is easy to spot and doesn't need Euclid's Algorithm
$1 = 5 \times 3 - 7 \times 2$

How about when it isn't so easy to spot?

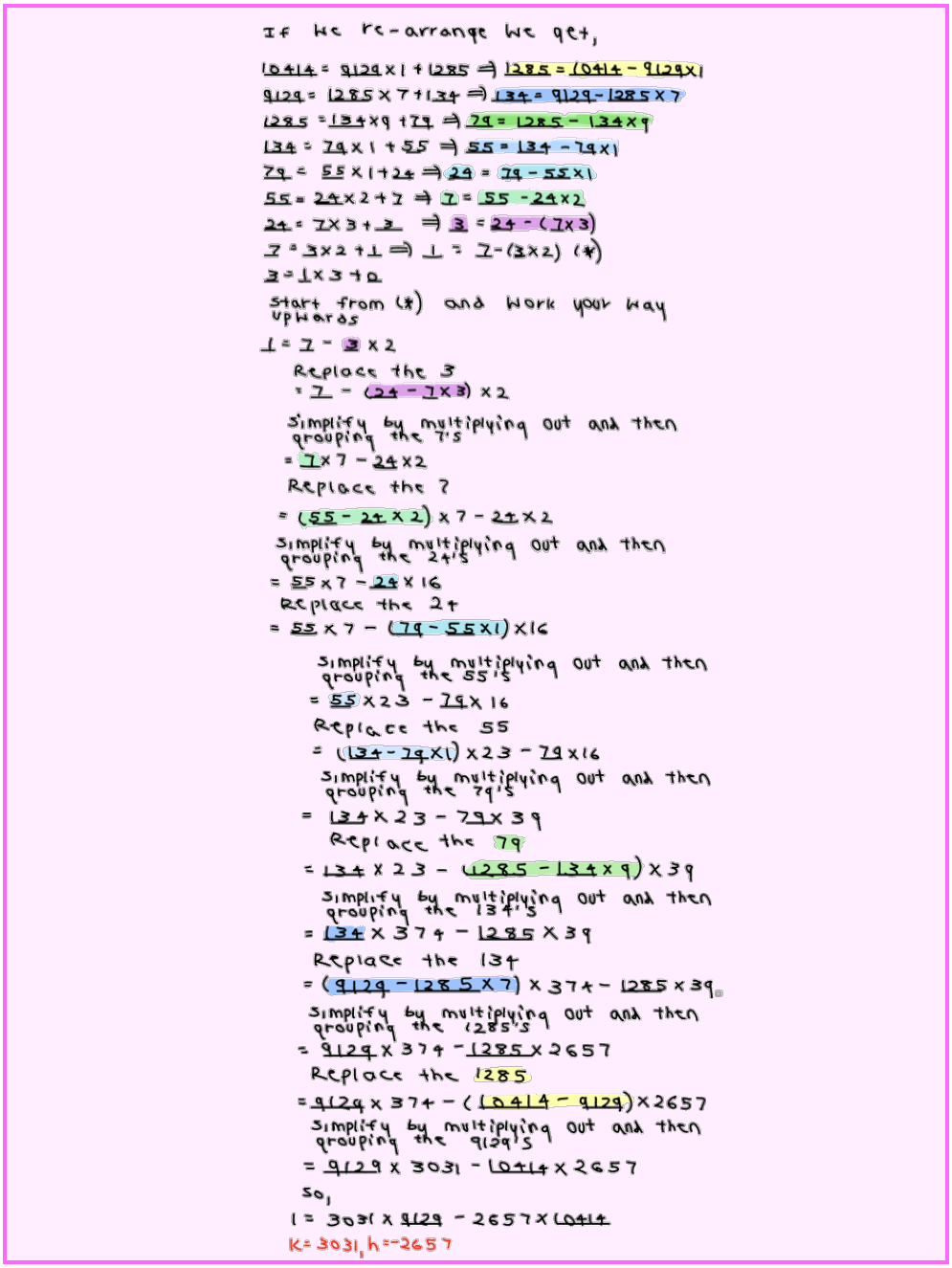
- ***Find integers h and k such that*** $42h + 19k = 1$



- ***Find integers h and k such that*** $d = 10414h + 9129k$



So $d = 1$



5.6 Chinese Remainder Theorem

If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers and if $a_1, a_2, \ldots, a_k$ are any integers, then the simultaneous congruences $x \equiv a_1 (mod\ m_1), x \equiv a_2 (mod\ m_2), \ldots, x \equiv a_k (mod\ m_k)$ have a solution and the solution is unique mod m, where $m = m_1 m_2, \ldots m_k$. Chinese Remainder theorem helps you solve these simultaneous equations of the form $x \equiv a_1 (mod\ m_1), x \equiv a_2 (mod\ m_2), \ldots, x \equiv a_k (mod\ m_k)$.

5.7 Fermat's Little Theorem

If p is prime, then for any integer a such that $a \not\equiv 0\ (mod\ p)$, then $a^{p-1} \equiv 1\ (\text{mod } p)$. For example, if a = 2 and p = 7, then 2^7 = 128, and 128 − 2 = 126 = 7 × 18 is an integer multiple of 7

5.8 Euler's Theorem (Euler Totient Theorem)

This is just a generalisation of Fermat's Little Theorem.

The Euler Totient function $\varphi(n)$ of a positive integer n greater than one is defined to be the number of positive integers less than n which are coprime to n.
We write this as
$\varphi(n)$ =number of elements in $(\mathbb{Z}_n)^\times = |(\mathbb{Z}_n)^\times|$
Euler's Theorem generalises Fermat's Theorem to the case where the modulus is not prime. It states that:
If n is a positive integer and hcf(n, a)=1 (i.e a is invertible mod n) then $a^{\varphi(n)} \equiv 1 \pmod n$

$$\boldsymbol{\varphi(6) = |\{1,5\}| = 2}$$
$$\boldsymbol{\varphi(8) = |\{1,3,5,7\}| = 4}$$

What is the easiest way to find $\varphi(n)$ for large n? We don't really want to have to count all the coprime elements.
There is a lemma that s if $n = p^a$ (where p is prime and a is a positive integer) then
$\varphi(n) = (p-1)p^{a-1}$
Note:
$\varphi(p) = (p-1)p^{1-1} = \mathrm{p} - 1$ (this is Fermat's Little Theorem)

6 Common types of Mod Calculation questions

6.1 $+, -, \times, \div$ mod n

You can usually use a calculator, but if not take note of the working below

- $7 \times 9 \ (mod\ 21)$
  $7 \times 9 = 63$
  How many 21's go into this? 3 exactly, with 0 remainder
  $= 0 \ (mod\ 21)$

- $85 \times 92 \ (mod\ 3)$
  Rather than do the calculation first like above, let's simplify each number mod 3
  $1 \times 2 \ (mod\ 3)$
  $= 2 \ (mod\ 3)$

- $10^{10} \ (mod\ 19)$
  10^{10} is too big to deal with
  $10^{10} = (10^2)^5 = (100)^5$
  $= (5)^5 \ (mod\ 19) = 5 \times 5^2 \times 5^2 = 5 \times 25 \times 25$
  $= 5 \times 6 \times 6 \ (mod\ 19) = 5 \times 36$
  $= 5 \times -2 \ (mod\ 19) = -10$
  $= 9 \ (mod\ 19)$

6.2 Finding Inverses mod n $a^{-1} \ (mod\ n)$

We need hcf (a, n)=1 to be able to find the inverse

Method: Use Euclid's Algorithm followed by h-k lemma and then reduce mod n

Use Euclid's algorithm to find the inverse of 3 in $\mathbb{Z}/71$

$3^{-1} \ (mod\ 71)$
hcf $(3, 71) = 1$ therefore inverse exists
$71 = 3 \times 23 + 2$
$3 = 2 \times 1 + 1$
so $1 = 3 - 2 \times 1$
$= 3 - (71 - 3 \times 23) \times 1$
$= 3 \times 24 - 71 \times 1$
Reduce mod 71
$\Rightarrow 1 = 3 \times 24 - 0$
$1 = 3 \times 24$
24 must be the inverse since this brings 3 back to the identity (1)
So $3^{-1} = 24 \ (mod\ 71)$

Note: With a small modulus you should be able to spot the inverse without having to apply the h-k lemma. Ask yourself what number in the set can you multiply with what you are trying to find the inverse of to get 1.

Exercises:
Use Euclid's algorithm to find the inverses of 6,13 and 23 in $\mathbb{Z}$ /175 (ans=146, 27, 137)
Find 43^{-1} $\mathbb{Z}_{53}{}^*$ (ans=37)
Find 3^{-1} $\mathbb{Z}_{17}{}^*$ (ans=6)
5^{-1} $\mathbb{Z}_{13}{}^*$ (ans=8)

6.3 Dealing with fractions mod n

$\frac{a}{b} = ab^{-1}$
If a is clearly divisible by b we can quickly divide. If not, we multiply a by the inverse of b to get rid of the fraction

Note: This is the same as solving $bx \equiv a \ mod \ n$ in section 6.4 below

Find $\frac{3}{4}$ $(mod\ 7)$

Need 4^{-1} (mod 7)

$7 = 4 \times 1 + 3$

$4 = 3 \times 1 + 1$

$1 = 4 - 3 \times 1$

$= 4 - (7 - 4 \times 1)$

$= 2 \times 4 - 7$

Mod 7 we get

$1 = 2 \times 4$

So $4^{-1} = 2$

$\frac{3}{4}$ (mod 7)

$= 3(4^{-1})$ (mod 7)

$= 3(2)$ (mod 7)

$= 6$ (mod 7)

6.4 Solving linear congruences of the form $ax \equiv b\ (mod\ n)$

How do we solve something familiar like $2x = 6$? We want to divide through by 2 to get x on its own. We have to be careful about doing so now that we are in a "mod world".
To see why consider $30 \equiv 42\ (mod\ 4)$
This is a true statement since both 30 and 42 are the same as 2 (mod 4)
Let's divide through by 6
$\frac{30}{6} \equiv \frac{42}{6}\ (mod\ 4)$
This gives $5 \equiv 7\ (mod\ 4)$ which means $1 \equiv 3\ (mod\ 4)$ which is obviously not true
Instead let's divide by 3
$\frac{30}{3} \equiv \frac{42}{3}\ (mod\ 4)$
This gives $10 \equiv 14\ (mod\ 4)$ which means $2 \equiv 2\ (mod\ 4)$ which is true
So, how do we know what we can divide by?
The first didn't work since hcf (4,6)$\neq 1$, but the second did work since $hcf(3,4) = 1$

There are 2 main types when solving $ax \equiv b\ (mod\ n)$

i. $hcf(a,n) = 1$ i.e. a is not a factor of n (a doesn't divide n)
$ax \equiv b\ (mod\ n)$
$x \equiv \frac{b}{a}\ mod(n)$ i.e. $x = a^{-1}b\ (mod\ n)$ **Notice how we don't divide the mod!**
Obviously working out $\frac{b}{a}$ is easy if a divides b in an obvious manner, but if it doesn't you need to find a^{-1} (mod n) first

ii. $hcf(a,n) \neq 1$ i.e. a is a factor of n (a divides n)
2 cases
   a) a is a factor of n, but not b ⇒ no solutions
   b) if a is a factor of both n and b ⇒ $x \equiv \frac{b}{a}\ mod\left(\frac{n}{a}\right)$

Examples of type i.

- $3x \equiv 3\ (mod\ 5)$

$3x \equiv 3$ (mod 5)

hcf (3,5) = 1

so can divide by 3 even though 5 not divisible by 3

$x \equiv \frac{3}{3}$ (mod 5)

$x \equiv 1$ (mod 5)

- $3x \equiv 9\ (mod\ 5)$

$3x \equiv 9 \pmod 5$

$hcf(3,5) = 1$

so can divide by 3 even though 5 not divisible by 3

$x \equiv \frac{9}{3} \pmod 5$

$x \equiv 3 \pmod 5$

- $5x \equiv 10 \pmod{71}$

$5x \equiv 10 \pmod{71}$

$hcf(5,71) = 1$

so can divide by 5 even though 71 not divisible by 3

$x \equiv \frac{10}{5} \pmod{71}$

$x \equiv 2 \pmod{71}$

If a doesn't divide b in an obvious manner then you can either try to spot the inverse or use h-k lemma to get the inverse

- $3x \equiv 4 \pmod{71}$

$3x \equiv 4 \pmod{71}$

$hcf(3,71) = 1$ so inverse exists

$x \equiv \frac{4}{3} \pmod{71}$

Not obvious what $\frac{4}{3}$ is

$\frac{4}{3} = 4(3^{-1})$

Lets find multiplicative inverse of 3 which is 3^{-1}

$71 = 3 \times 23 + 2$

$3 = 2 \times 1 + 1$

so $1 = 3 - 2 \times 1$

$= 3 - (71 - 3 \times 23) \times 1$

$= 3 \times 24 - 71 \times 1$

Reduce mod 71

$\Rightarrow 1 = 3 \times 24 - 0$

$1 = 3 \times 24$

24 must be the inverse since this brings 3 back to the identity (1)

So $3^{-1} = 24 \pmod{71}$

Now we can solve $3x \equiv 4 \pmod{71}$

$x \equiv 3^{-1}(4) \mod 71$

$\equiv 24(4) \mod 71$

$\equiv 96 \mod 71$

$\equiv 25 \mod 71$

Examples of type ii.

- $3x \equiv 3 \pmod 5$

$3x \equiv 3 \pmod 5$

$hcf(3,5) = 1$

so can divide by 3 even though 5 not divisible by 3

$x \equiv \frac{3}{3} \pmod 5$

$x \equiv 1 \pmod 5$

- $3x \equiv 9 \pmod 5$

$3x \equiv 9 \pmod 5$

$Hcf(3,5) = 1$

so can divide by 3 even though 5 not divisible by 3

$x \equiv \frac{9}{3} \pmod 5$

$x \equiv 3 \pmod 5$

- $5x \equiv 10 \ (mod\ 71)$

$5x \equiv 10 \pmod{71}$

$hcf(5, 71) = 1$

so can divide by 5 even though 71 not divisible by 3

$x \equiv \frac{10}{5} \pmod{71}$

$x \equiv 2 \pmod{71}$

If a doesn't divide b in an obvious manner then you can either try to spot the inverse or use h-k lemma to get the inverse

- $3x \equiv 4 \ (mod\ 71)$

$3x \equiv 4 \pmod{71}$

$hcf(3, 71) = 1$ so inverse exists

$x \equiv \frac{4}{3} \pmod{71}$

Not obvious what $\frac{4}{3}$ is

$\frac{4}{3} = 4(3^{-1})$

Lets find multiplicative inverse of 3 which is 3^{-1}

$71 = 3 \times 23 + 2$

$3 = 2 \times 1 + 1$

so $1 = 3 - 2 \times 1$

$= 3 - (71 - 3 \times 23) \times 1$

$= 3 \times 24 - 71 \times 1$

Reduce mod 71

$\Rightarrow 1 = 3 \times 24 - 0$

$1 = 3 \times 24$

24 must be the inverse since this brings 3 back to the identity (1)

So $3^{-1} = 24 \pmod{71}$

Now we can solve $3x \equiv 4 \pmod{71}$

$x \equiv 3^{-1}(4) \mod 71$

$\equiv 24(4) \mod 71$

$\equiv 96 \mod 71$

$\equiv 25 \mod 71$

- $5x \equiv 18 \ (mod\ 10)$

No solution

- $6x \equiv 18 \ (mod\ 72)$

$6x \equiv 18 \pmod{72}$

$hcf(6, 72) \neq 1$, but this doesn't matter since 6 goes into both 18 and 72 i.e. we can divide 18 and 72 by 6

$x \equiv 3 \pmod{12}$

- $2x \equiv 10 \ (mod\ 4)$

$2x \equiv 10 \pmod{4}$

$hcf(2, 4) \neq 1$, but doesn't matter since dividing modulus too

Reduce by mod 4

$x \equiv 5 \pmod{2}$

$x \equiv 1 \pmod{2}$

Little hidden "tricks" you may need to also use:

Can you reduce all terms mod to simplify first?

- $15x \equiv 2\ (mod\ 7)$

$15x \equiv 2 \pmod 7$
Reduce by mod 7 - don't even need to care about hcf(15,7)=1 here or whether can divide
$x \equiv 2 \pmod 7$

Can you divide ALL including modulus by a number?
If this then gives x on its own then done. If not proceed using type i. or ii. method

- $55x \equiv 44\ (mod\ 121)$

$55x \equiv 44 \pmod{121}$
hcf(55,121) ≠1
Also, we can't divide through by 55 since BOTH 44 and 121 are not multiples of 55
We can divide all by 11 through
$5x \equiv 4 \pmod{11}$
hcf(5,11) =1 so inverse exists
$x \equiv \frac{4}{5} \pmod{11}$ so $x \equiv 4(5^{-1}) \pmod{11}$
Need $5^{-1} \pmod{11}$
Don't need h-k (emma. $5 \times 9 = 45 \equiv 1 \pmod{11}$
so $5^{-1} \equiv 9$
$x \equiv 4(9) \pmod{11} = 36 \pmod{11} \equiv 3 \pmod{11}$

Note: could have just solved $55x \equiv 44 \pmod{121}$ from very beginning
$x \equiv \frac{44}{55} \pmod{121}$ so $x \equiv 44(55^{-1}) \pmod{121}$
Need $55^{-1} \pmod{121}$
$11 = 5 \times 2 + 1$
so $1 = 11 - 5 \times 2$
Reduce mod 11
$1 = -5 \times 2$
so $5^{-1} = -2 \pmod{11}$
$= 9 \pmod{11}$
so $5x \equiv 4 \pmod{11}$
becomes
$x \equiv 5^{-1}(4) \bmod 11$
$\equiv 9(4) \bmod 11$
$\equiv 36 \bmod 11$
$\equiv 3 \bmod 11$

- $18x \equiv 6\ (mod\ 72)$

$18x \equiv 6 \pmod{72}$
hcf(18 72) ≠1 so can't divide by 18
6 goes into all though, so can divide by 6
$3x \equiv 1 \pmod{12}$
hcf(3,12) ≠1 so we can't divide both 1 and 12 by 3, so we're stuck
∴ no solutions

You can also factor a number out from the left hand side so $ax \equiv b\ (mod\ n)$ becomes $*\ (cx) \equiv b\ (mod\ n)$. Now try and solve as type ii. with * and mod n and then type i. after with $cx = b (mod\ n)$

Exercises:
$43x \equiv 4\ (mod\ 53)$ (ans= 42 mod 53)
$3x \equiv 8\ (mod\ 17)$ (ans=14 mod 17)
$2x \equiv 5\ (mod\ 73)$ (ans=39 mod 73)
$4x \equiv 6\ (mod\ 104)$ (ans= no sol)
$18x \equiv 6\ (mod\ 102)$ (ans=6 mod 17)

6.5 Solving two or more congruences of the form $ax \equiv b\ (mod\ n)$

Solving 2 or more linear congruences $x \equiv b\ (mod\ n)$
There are 2 systematic ways to solve this
Way 1: Using Chinese remainder theorem
Way 2: Using def^n of modulus and substituting back

- $x \equiv 4\ (mod\ 8), x \equiv 3(mod\ 5)$

This is basically saying, what is the smallest positive integer so that when we divide it by 8 and 5 we get remainders of 4 and 3 respectively
This is easy to spot and is 28, but it is not always easy to spot, so we need a systematic way.

$x \equiv 4 \pmod 8$, $x \equiv 3 \pmod 5$

Way 1:

$x \equiv 4 \pmod 8$, $x \equiv 3 \pmod 5$

a, n, b, m

HCF(5, 8) = 1 so can find a solution by CRT

Apply h-k Lemma

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

So,

$1 = 3 - 2 \times 1$

$= 3 - (5 - 3 \times 1)$

$= 2 \times 3 - 5$

$= 2 \times (8 - 5 \times 1) - 5$

$= 2 \times 8 - 3 \times 5$

r, n, r, m

Solution form looks like

$x \equiv hnb + kma \pmod{nxm}$

$\equiv 2(8)(3) + (-3)(5)(4) \pmod{40}$

$\equiv -12 \pmod{40}$

$\equiv 28 \pmod{40}$

$x \equiv 28 \pmod{40}$

Way 2:

$x \equiv 4 \pmod 8$, $x \equiv 3 \pmod 5$

HCF(5, 8) = 1 so can find a solution by CRT

$x = 4 \pmod 8$ means $x = 8k + 4$ since when divide by 8 get remainder of 4

So $x = 8k + 4$ ①

Sub this into $x \equiv 3 \pmod 5$

$8k + 4 \equiv 3 \pmod 5$

$8k \equiv -1 \pmod 5$

mod out by 5

$3k \equiv 4 \pmod 5$

hcf(3, 5) = 1

Need to find $3^{-1} \bmod 5$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

So $1 = 3 - (2 \times 1)$

$= 3 - (5 - 3 \times 1)$

$= 2 \times 3 - 5$

Reduce mod 5

$1 = 2 \times 3$

So $3^{-1} = 2 \pmod 5$

$3k \equiv 4 \pmod 5$

$k \equiv 3^{-1}(4) \pmod 5$

$k \equiv 2(4) \pmod 5$

$k \equiv 8 \pmod 5$

$k = 3 \pmod 5$

So $k = 5l + 3$

Sub this into ①

$x = 8(5l + 3) + 4$

$x = 40l + 28$

This means $x \equiv 28 \pmod{40}$

- $x \equiv 1\ (mod\ 3), x \equiv 4(mod\ 5),\ x \equiv 6(mod\ 7)$

This is basically saying, what is the smallest positive integer so that when we divide it by 3,5, and 7 we get reminders of 1,4 and 6 respectively

$x \equiv 1 \pmod 3$ $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$

Way 1:

$x \equiv 1 \pmod 3$, $x \equiv 4 \pmod 5$

a b c d

HCF(3,5) = 1

Apply h-k lemma

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

so $1 = 3 - (2 \times 1)$

$= 3 - (5 - 3 \times 1)$

$= 2 \times 3 - 1 \times 5$

h k m n

Solution form looks like:

$x \equiv hmb + kna \pmod{nxm}$

$\equiv 2(3)(4) + (-1)(5)(1) \pmod{15}$

$\equiv 19 \pmod{15}$

$\equiv 4 \pmod{15}$

Now solve $x \equiv 4 \pmod{15}$, $x \equiv 6 \pmod 7$

a c b d

hcf(7,15) = 1

Apply h-k lemma

$15 = 2 \times 7 + 1$

$1 = 15 - 2 \times 7$

$= 1 \times 15 - 2 \times 7$

h k m n

Way 2:

$x \equiv 1 \pmod 3$, $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$

hcf(3,5) = 1, hcf(5,7) = 1, hcf(1,7) = 1 so can find a solution by CRT

Solve this using another method

$x \equiv 1 \mod 3$ means $x = 3k+1$ for $k \in \mathbb{Z}$ since when divide by 3 get a remainder of 1

$x = 3k+1$ ①

Sub $x = 3k+1$ into $x \equiv 4 \pmod 5$

$3k+1 \equiv 4 \pmod 5$

$3k \equiv 3 \pmod 5$

ok to divide by 3 since hcf(3,5) = 1

$k \equiv 1 \pmod 5$

This means $k = 5l+1$ for $l \in \mathbb{Z}$

plug into ①

$x = 3(5l+1)+1$

$x = 15l+4$ ②

Sub $x = 15l+4$ into $x \equiv 6 \pmod 7$

so $15l+4 \equiv 6 \pmod 7$

$15l \equiv 2 \pmod 7$

Simplify mod 7

$l \equiv 2 \pmod 7$

This means $l = 7m+2$ for $m \in \mathbb{Z}$

Sub this into ②

$k = 15(7m+2)+4$

$= 105m+34$

This means $x \equiv 34 \pmod{105}$

Solution form looks like

$x \equiv hmb + kna \pmod{nxm}$

$\equiv 1(15)(6) + (-2)(7)(4) \pmod{105}$

$\equiv 34 \pmod{105}$

So $x \equiv 34 \pmod{105}$

- $x \equiv 3 \ (mod\ 101^{1000})$, $x \equiv 3 \ (mod\ 7^{200})$
  This solution is easy to spot
  $x \equiv 3 \ (mod\ 101^{1000} \times 7^{200})$

The last example above should have shown you if $x \equiv a \ (mod\ n)$ and $x \equiv a \ (mod\ m)$ then we know answer is $x \equiv a \ (mod\ nm)$ straight away, don't need to do any work

Exercises:

$x \equiv 7 \ (mod\ 11)$ and $x \equiv 10 \ (mod\ 13)$ (ans =62 mod 143)

$x \equiv 1 \ (mod\ 23)$ and $x \equiv 5 \ (mod\ 31)$ (ans=346 mod 713)

$x \equiv 5 \ (mod\ 13)$ and $x \equiv 9 \ (mod\ 19)$ (ans=161 mod 247)

$x \equiv 1 \ (mod\ 25)$ and $x \equiv 2 \ (mod\ 19)$ (ans=401 mod 475)

$x \equiv 2 \ (mod\ 7)$, $x \equiv 5 \ (mod\ 11)$, $x \equiv 2 \ (mod\ 19)$ (ans=401 mod 1463)

$x \equiv 5\ (mod\ 7^{1000})$, $x \equiv 5\ (mod\ 5^{200})$ (ans $x \equiv 5\ \ (mod\ 7^{1000} \times 5^{200})$)

6.6 Simplifying powers of the form $a\hat{}b\ (mod\ n)$

Ideally we would like to type this into the calculator and simplify mod n. These numbers end up being far too big for the calculator to deal and often you're not allowed calculators on your university course anyway! Therefore, we need other methods.

3 methods:

i. n prime (call it p) AND (a,n)=1 ⟹use Fermat's
$a^{p-1} \equiv 1$

ii. n not prime AND (a,n)=1 ⟹use Euler's
If $n = p^a$ where $\varphi(n) = (p-1)p^{a-1}$, then $a^{\varphi(n)} \equiv 1$
Note: This works for n prime too. If n is prime this just becomes Fermat's as stated earlier since
$\varphi(n) = p - 1\ \ and\ \ a^{\varphi(n)} \equiv 1$ so $a^{p-1} \equiv 1$
So, it would be unnecessary to try and calculate using Euler Totient

iii. If (a,n)≠ 1, then use Chinese Remainder Theorem. First split up, simplify each using one of the methods above OR using the fact that if n|a^b then answer is $\equiv 0\ (mod\ n)$.
then use CRT after to bring together all the separate equations

Note: You cannot simplify the POWER first modulo the number, but it is sometimes helpful to simplify the base!
for example, $3^{173}\ (mod\ 4) = (-1)^{173}\ (mod\ 4) = -1$
Simplifying the power changes the question though, so we can't do it! The question would just be too easy if we could, right?
If you want to reduce the power, you can only do so in the following ways

- Split into more manageable powers first
  $3^{49}(mod\ 53) = (3^7)^7 = (2187)^7 = (14)^7\ (mod\ 53) = 105413504 = 2\ (mod\ 53)$
- use facts already stated in i. and ii. that
  $a^{n-1} \equiv 1$ (if n prime AND hcf $(a, n) = 1$)
  or
  $a^{\varphi(n)} \equiv 1$ (n not prime AND (a,n)=1)

  We use rules $x^a x^b = x^{a+b}\ or\ (x^a)^b = x^{ab}$ to help us involve these forms
  $5^{31}(mod\ 37) = 5^{36}5^{-5}\ \ (mod\ 37)$ is helpful since $5^{36} \equiv 1\ (mod\ 37)$

  $5^{300}(mod\ 11) = \ (5^{10})^{30}(mod\ 11)$ is helpful since $5^{10} \equiv 1\ (mod\ 31)$

- **$5^{300}(\mathbf{mod\ 11})$**

$5^{300} \pmod{11}$
hcf $(5, 11) = 1$ i.e. co-prime and 11 is prime
So can apply Fermat's Theorem
Fermat's Little Theorem ⇒ $5^{10} \equiv 1 \bmod 11$
Hint: Try and involve 5^{10}
$5^{300} = (5^{10})^{30}$
$= (1)^{30} \pmod{11}$
$= 1 \pmod{11}$

- **$5^{300}(\boldsymbol{mod\ 13})$**

$5^{300} \pmod{13}$
hcf $(5, 13) = 1$ i.e. coprime and 13 is prime
So can apply Fermat's Theorem
Fermat's Little Theorem ⇒ $5^{12} \equiv 1 \bmod 13$
$5^{300} = (5^{12})^{25}$
$= (1)^{25} \pmod{13}$
$= 1 \pmod{13}$

- **$5^{300}(\boldsymbol{mod\ 143})$**
  Hint: We can use above 2 results to help us

$5^{300} \pmod{143}$
$= 5^{300} \pmod{11 \times 13}$
So need to solve $x \equiv 5^{300} \bmod 11$, $x \equiv 5^{300} \bmod 13$
(already found $x \equiv 1 \bmod 11$; already found $x \equiv 1 \bmod 13$)
Need to now solve $x \equiv 1 \bmod 11$, $x \equiv 1 \bmod 13$ (a, n, k, m)
$\text{hcf}(11, 13) = 1$
$13 = 11 \times 1 + 2$
$11 = 2 \times 5 + 1$

$1 = 11 - 2 \times 5$
$= 11 - (13 - 11 \times 1) \times 5$
$= 6 \times 11 - 13 \times 5$
$= 6 \times 11 - 5 \times 13$ (k, n, k, m)

$x \equiv hna + kmb \pmod{n \times m}$
$= 6(11)(1) + (-5)(13)(1) \bmod 143$
$= 1 \bmod 143$

Note: didn't need to do any working once got to $x \equiv 1 \bmod 11$, $x \equiv 1 \bmod 13$
It is obvious the answer is $x \equiv 1 \bmod 143$

- $5^{2401} (mod\ 13)$

$5^{2401} \pmod{13}$
$\text{hcf}(2401, 13) = 1$ and 13 is prime
So can apply Fermat's Theorem
Fermat's little theorem $\Rightarrow 5^{12} \equiv 1 \pmod{13}$
Hint: Try and involve 5^{12}
$5^{2401} = (5^{12})^{200} \times 5^1$
$= (1)^{200} \times 5 \pmod{13}$
$= 5 \pmod{13}$

- $6^{422} (mod\ 43)$

$6^{422} \pmod{43}$
$\text{hcf}(6, 43) = 1$ and 43 is prime
So can apply Fermat's Theorem
Fermat's little theorem $\Rightarrow 6^{42} \equiv 1 \pmod{43}$
Hint: Try and involve 6^{42}
$6^{422} = (6^{42})^9 \times 6^2$
$= (1)^{10} \times 6^2 \pmod{43}$
$= 36 \pmod{43}$

- $10^{100} (mod\ 19)$

$10^{100} \pmod{19}$
$\text{hcf}(100, 19) = 1$ and 19 prime
So can apply Fermat's Theorem
Fermat's little theorem $\Rightarrow 10^{18} \equiv 1 \pmod{19}$
Hint: Try and involve 10^{18}
$10^{100} = (10^{18})^5 \times 10^{10} \pmod{19}$
$= (1)^5 \times 10^{10} \pmod{19}$
$= 10^{10} \pmod{19}$
Let's reduce mod 19 now (cleverly since number is big and usually not allowed a calculator)

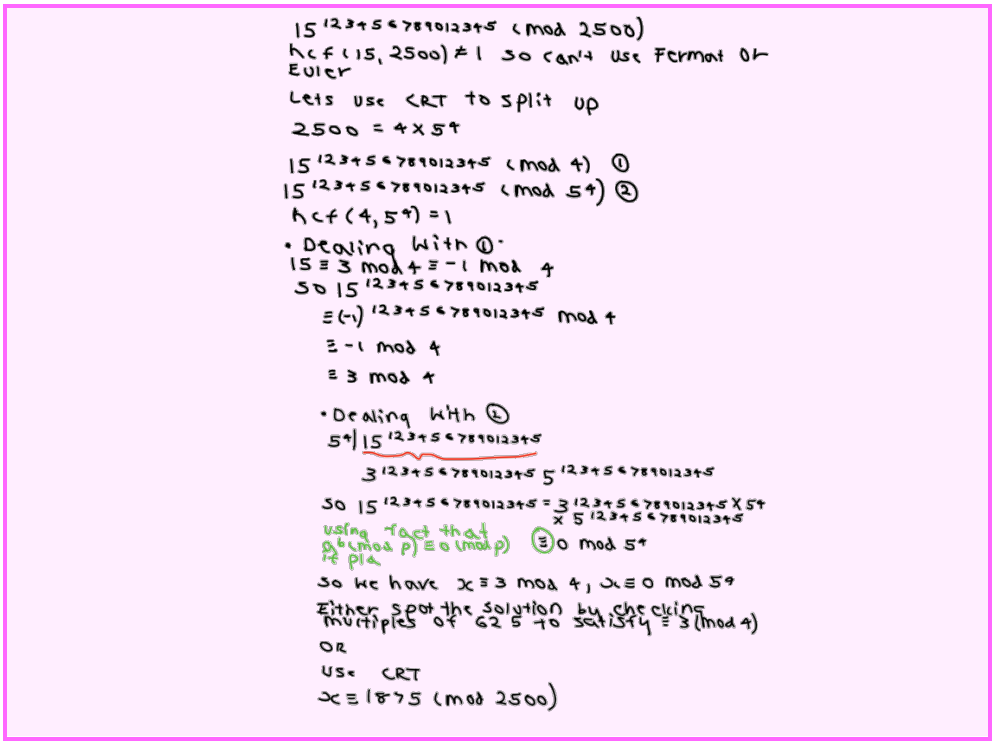
$10^{10} = (10^2)^5 \pmod{19}$
$= (100)^5 \pmod{19}$
$= 5^5 \pmod{19}$
$= 5 \times 5^2 \times 5^2 \pmod{19}$
$= 5 \times 25 \times 25 \pmod{19}$
$= 5 \times 6 \times 6 \pmod{19}$
$= 5 \times 36 \pmod{19}$
$= 5 \times -2 \pmod{19}$
$= -10 \pmod{19}$
$= 9 \pmod{19}$

- $11^{135246875003} (mod\ 2500)$

$11^{135246875003} \pmod{2500}$
$\text{hcf}(11, 2500) = 1$ BUT 2500 not prime so can't use Fermat's
$\text{hcf}(11, 2500) = 1$ so can use Euler-Totient though (2500 doesn't need to be prime)
$\varphi(2500) = \varphi(2^2 \times 5^4)$
$= \varphi(2^2)\varphi(5^4)$
$= (1)(2)^1(5)(5)^3$
$= 1000$

$x^{\varphi(n)} \equiv 1 \pmod{2500}$
$\Rightarrow x^{1000} \equiv 1 \pmod{2500}$
Consider the power 135246875003
$135246875003 \equiv 3 \pmod{1000}$
Hint: Involve 1000 as the power
$11^{135246875003} \equiv (11^{1000})\cdots \times 11^3$
$\equiv 1 \times 11^3 \pmod{2500}$
$\equiv 11^3 \pmod{2500}$
$\equiv 1331 \pmod{2500}$

- $15^{123456789012345} (mod\ 2500)$



Exercises:
$5^{2401} \pmod{13}$ (ans= 5 mod 13)
$6^{422} \pmod 3$ (ans=0 mod 3)
3^{158} $\mathbb{Z}_{17}{}^*$ (ans=2 mod 17)
5^{122} $\mathbb{Z}_{13}{}^*$ (ans=12 mod 13)
5^{1198} $\mathbb{Z}_{13}{}^*$ (ans=12 mod 13)

6.7 Solving x's to powers of the form $x\hat{}a \equiv b \pmod n$

Goal: Like usual, to get x on its own

How do we solve something basic like $x^{\frac{2}{3}} = 16$

We raise both sides to the power of $\frac{3}{2}$ to get x on its own

$\left(x^{\frac{2}{3}}\right)^{\frac{3}{2}} = 16^{\frac{3}{2}}$

$x = 64$

Keep this in mind when solving the types below.

There are 4 main methods you can use

i. n prime AND hcf$(b, \boldsymbol{n-1})$=1⟹use Fermat's.
Find b^{-1} (mod $n-1$) and raise both sides to this power. Simplify RHS using knowledge from 6.6 or just basic simplification. See way 2 in the Fermat examples below
Note: There is an alternative method to finding b^{-1}. Instead, we try and get the LHS as close as possible to $x^{p-1} = 1$. We very rarely use this method though. See way 1 in the Fermat examples below

ii. n not prime AND hcf(b, n)=1 AND (a, $\varphi(n)) = 1$ ⟹use Euler's.
Find b^{-1} $(mod\ \varphi(n))$ and raise both sides to this power. Simplify RHS using knowledge from 6.6 or just basic simplification
Obviously this works for n being prime too, but this is just Fermat's above so there is no need to use the Euler Totient function.
Note: You can also solve this like the alternative method above where we try and get as close as possible to $x^{\varphi(n)} = 1$. We also very rarely use this method and has not been used in any of the Euler examples below.

iii. n not prime ⟹ split up and one of the above methods on each and then use Chinese Remainder Theorem. First split up, simplify each using one of the methods above OR trial and error if the mod is small (when using the trial and error you can use the fact that if n$|a^b$ then answer is ≡ 0 $(mod\ n)$). Then use CRT after to solve all the separate equations

Note: If the power of x too big you may use the fact that $x^{p-1} = 1$ (if n prime) or $x^{\varphi(n)} = 1$ (n not prime) to reduce the power of x, before trying to find its inverse.
Do not just reduce the power by mod n though. This was mentioned in * in 6.6

- $x^{17} \equiv 3 \ (mod \ 53)$

$x^{17} \equiv 3 \pmod{53}$
Way 1: Apply Fermats
53 is prime
So can apply Fermat's Theorem
Fermat's little theorem $\Rightarrow x^{52} \equiv 1 \pmod{53}$
Hint: Try and get as close as possible to x^{52}
$x^{17} \equiv 3 \pmod{53}$
$(x^{17})^3 \equiv (3)^3 \pmod{53}$
$x^{51} \equiv 27 \pmod{53}$
Multiply both sides by x
$x^{51} \cdot x \equiv 27x \pmod{53}$
$\equiv 1$
$1 \equiv 27x \pmod{53}$
So now solving $27x \equiv 1 \pmod{53}$
$x \equiv 27^{-1}(1) \pmod{53}$
$x \equiv 27^{-1} \pmod{53}$ (*)
So let's find $27^{-1} \pmod{53}$
$hcf(27, 53) = 1$ so coprime
$53 = 27 \times 1 + 26$
$27 = 26 \times 1 + 1$
So, $1 = 27 - 26 \times 1$
$= 27 - (53 - 27 \times 1)$
$= 2 \times 27 - 53 \times 1$
Mod out by 53
$1 = 2 \times 27$
so $27^{-1} \equiv 2 \pmod{53}$
* becomes $x \equiv 2 \pmod{53}$

Way 2:
53 prime and $hcf(17, 53) = 1$
Need $17^{-1} \pmod{52}$
$52 = 17 \times 3 + 1$
$1 = 52 - 17 \times 3$
Reduce mod 52
$1 = -17 \times 3$
so $17^{-1} \equiv -3 \equiv 49 \pmod{52}$
$x^{17} \equiv 3 \pmod{53}$
$(x^{17})^{49} \equiv 3^{49} \pmod{53}$
$x \equiv (3^3)^7 \pmod{53}$
$\equiv (2187)^7 \pmod{53}$
$\equiv (14)^7 \pmod{53}$
$\equiv 10541350 4 \pmod{53}$
$\equiv 2 \pmod{53}$

- $x^{13} \equiv 2 \ (mod \ 53)$

$x^{13} \equiv 2 \pmod{53}$
Way 1: Apply Fermat's
53 is prime
So can apply Fermat's Theorem
Fermat's little theorem $\Rightarrow x^{52} \equiv 1 \pmod{53}$
Hint: Try and get as close as possible to x^{52}
$(x^{13})^4 \equiv (2^4) \pmod{53}$
$x^{52} \equiv 16 \pmod{53}$
$1 \equiv 16 \pmod{53}$
This isn't true
$\Rightarrow$ no solution
Way 2:
53 prime BUT $hcf(13, 52) \neq 1$ so can't use this method

- $x^5 \equiv 3 \ (mod \ 7)$

$x^5 \equiv 3 \pmod 7$

Way 1: Apply Fermats since 7 is prime

$x^6 \equiv 1 \pmod 7$

Hint: Try and get as close as possible to x^6

$x^5 x \equiv 3x \pmod 7$

$1 \equiv 3x \pmod 7$

$3x \equiv 1 \pmod 7$

hcf $(3,7) = 1$ so 3^{-1} exists

Need $3^{-1} \pmod 7$

$7 = 3 \times 2 + 1$

$3 = 1 \times 3 + 0$

so $1 = 7 - 3 \times 2$

Reduce mod 7

$1 = -3 \times 2$

$3^{-1} = -2 \pmod 7$

$x \equiv 3^{-1}(1) \pmod 7$

$\equiv (-2)(1) \pmod 7$

$\equiv -2 \pmod 7$

$\equiv 5 \pmod 7$

Way 2:

7 prime and hcf $(5,6) = 1$

Find $5^{-1} \bmod 6$

$6 = 5 \times 1 + 1$

$5 = 5 \times 1 + 0$

so $1 = 6 - 5 \times 1$

Reduce mod 6

$1 = -5 \times 1$

so $5^{-1} \equiv -1 \pmod 6$

$\equiv 5 \pmod 6$

Had $x^{5^{-1}} \equiv 3 \pmod 7$

$(x^5)^5 \equiv 3^5 \pmod 7$

$x \equiv 243 \pmod 7$

$\equiv 5 \pmod 7$

- $x^{461} \equiv 3 \ (mod\ 1358)$

$x^{461} \equiv 3 \pmod{1358}$

1358 not prime, so can use Euler's

1358

2×679

7×97

$\varphi(1358) = \varphi(2 \times 7 \times 97)$

$= \varphi(2)\varphi(7)\varphi(97)$

$= 1 \times 6 \times 96$

$= 576$

$(461, 576) = 1$ and $(3, 1358) = 1$

Want $461^{-1} \bmod 576$

$576 = 461 \times 1 + 115$

$461 = 115 \times 4 + 1$

so $1 = 461 - 115 \times 4$

$= 461 - (576 - 1 \times 461) \times 4$

$= 5 \times 461 - 4 \times 576$

reduce mod 576

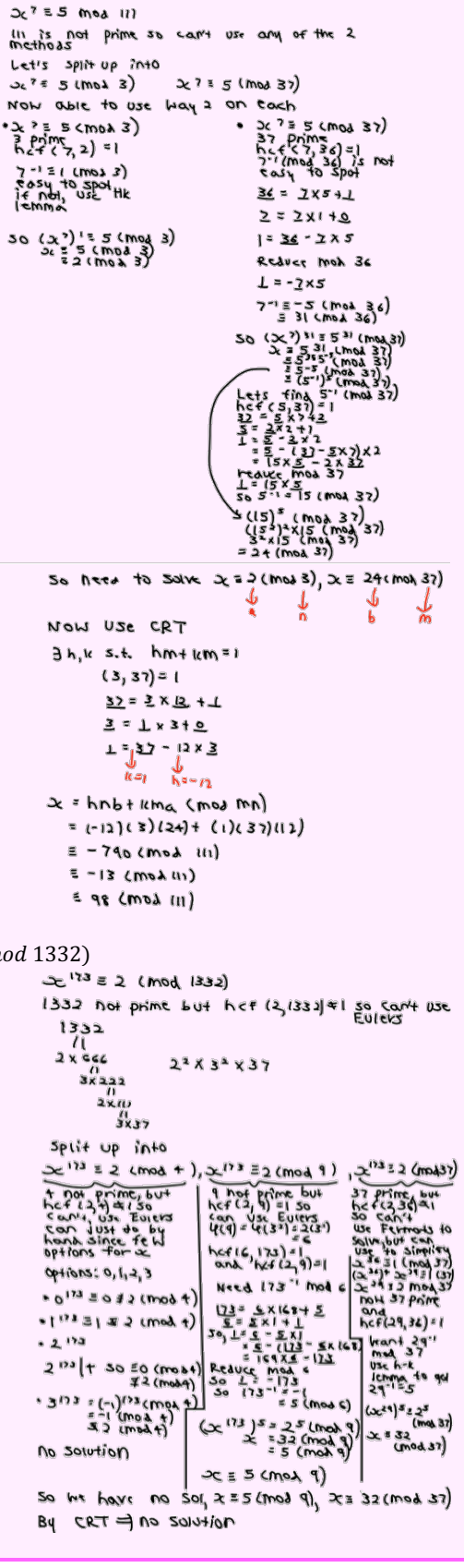
$\Rightarrow 1 = 5 \times 461$

so $461^{-1} = 5 \pmod{576}$

$(x^{461})^5 \equiv 3^5 \pmod{576}$

$\Rightarrow x \equiv 243 \pmod{1358}$

- $x^7 \equiv 5 \ (mod\ 111)$



- $x^{173} \equiv 2 \ (mod\ 1332)$

Exercises:
Find the inverse of 7 $(mod\ 12)$ and hence solve $x^7 \equiv 2\ (mod\ 13)$
$x^{11} \equiv 3\ (mod\ 17)$ (ans 10 mod 17)

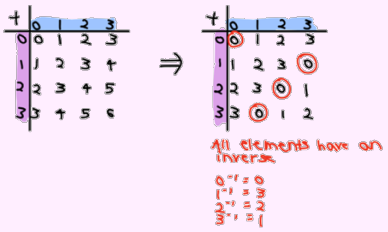
$x^5 \equiv 2\ (mod\ 17)$ (ans=15 mod 17)
$x^{17} \equiv 3\ (mod\ 53)$ (ans= 2 mod 53)
$x^{13} \equiv 2\ (mod\ 53)$ (ans=no solution)
$x^7 \equiv 2\ (mod\ 13)$ (ans 11 mod 13)
$x^{461} \equiv 3\ (mod\ 1358)$ (ans 243 mod 1358)
$x^{823} \equiv 2\ (mod\ 2015)$ (ans=128 mod 2015)
$x^{411} \equiv 11\ (mod\ 2001)$ (ans=1331 mod 2001)
$x^{1667} \equiv 2\ (mod\ 2500)$ Hint: Split up as mod (4x625). (ans= no solution)

7 Addition and Multiplication Composition/Cayley tables

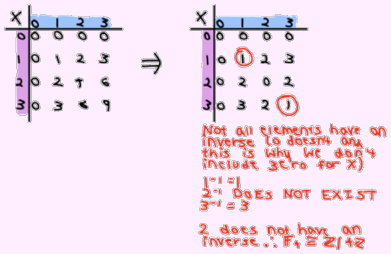
A binary operation in a finite set can completely be described by means of a table. This table is known as a composition table. The composition table helps us to verify most of the properties satisfied by the binary operations. An operation represented by the composition table will be binary, if every entry of the composition table belongs to the given set.

Composition tables contains all possible combinations of two elements with respect to the operation

- $\mathbb{Z}_4$ under addition and multiplication
  This set looks like {0,1,2,3}. Let's find all possible combinations for these elements
  Addition



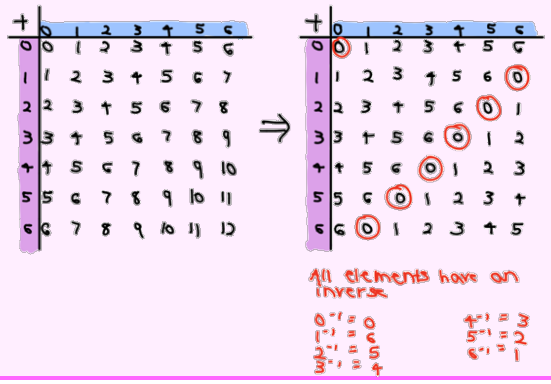
  Multiplication:



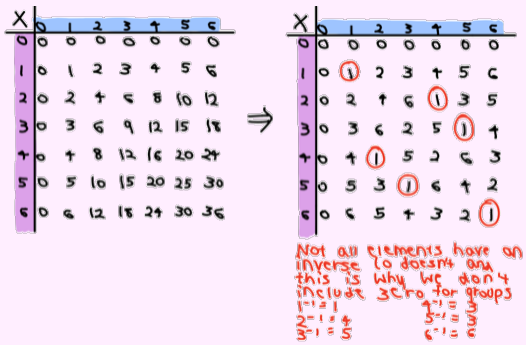
- Notice the symmetry across the diagonals since addition and multiplication are commutative
  It is not necessary to draw 2 tables for each. I have only done so to show the working

- $\mathbb{Z}_7$ under addition and multiplication
  This set looks like {0,1,2,3,4,5,6}. Let's find all possible combinations for these elements

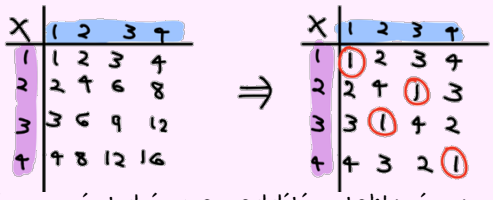
  Addition



Multiplication:

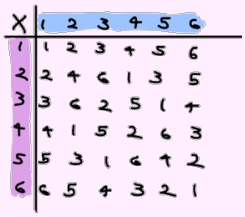


- $\mathbb{Z}_5^*$ under multiplication
  This set looks like {1,2,3, 4}. Let's find all possible combinations for these elements

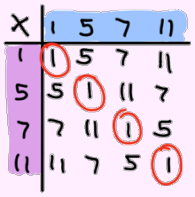


Note: There is no point doing an addition table since not all elements will be in the set

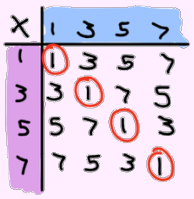
- $\mathbb{Z}_7^*$ under addition and multiplication
  This set looks like {1,2,3, 4, 5,6}. Let's find all possible combinations for these elements



- $(\mathbb{Z}/12)^\times$ under multiplication.
  This is the set {1,5,7,11}. Let's find all possible combinations for these elements



- $(\mathbb{Z}/18)^\times$ multiplication.
  This is the set {1,3,5,7}. Let's find all possible combinations for these elements



8 Fields

Ideally you should have knowledge of group theory and vector spaces before starting fields. The order normally taught is Group theory, then fields and then vector spaces. Fields are taught before vector spaces, since in order to define a vector space we need to know what a field is

8.1 Notation

$\mathbb{F}$ denotes a field
$\mathbb{F}_n = \{0,1,2,3,4, \ldots . n-1)$ where n is prime
Note: $\mathbb{F}_n \cong \mathbb{Z}/n\mathbb{Z}$ for n prime

8.2 Intuitive Definition

$\mathbb{F}$ is a set on which addition, subtraction, multiplication and division are defined and behave as the corresponding operations on rational and real numbers do i.e. set of numbers where you can add, subtract, multiply and divide.
A field is a mathematical object that on one hand is a relatively simple generalization of the ideas behind groups, but on the other will allow us to understand a variety of beautiful mathematical concepts and applications. We start here with the basics:
Common examples include
$\mathbb{R}$ Reals (decimals)
$\mathbb{C}$ (Complex numbers)
$\mathbb{Q}$ (Rationals)
$\mathbb{Z}$ is not a field since there is no multiplicative inverse for 2 or 3, For example we can't have $\frac{1}{2} \because \frac{1}{2} \notin \mathbb{Z}$
There are lots of other fields, even ones with only a finite number of elements called finite fields. Subtraction is the same as adding negatives and division is the same thing as multiplying by fractions, so we only need addition and multiplication. Subtraction and division are not separate composition laws

8.3 Formal Definition

A field is a set of elements {.....} with 2 operations $+$ and $\times$. We write $\mathbb{F} = (\mathbb{F}, +, 0, \times, 1)$
It satisfies the following properties

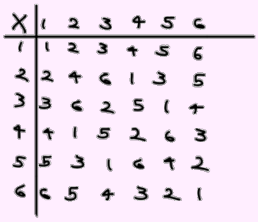
- Closure
  $+$: $\forall x, y \in \mathbb{F}, x + y \in \mathbb{F}$ i.e if you add any 2 elements of the set you get another element of the set
  $\times$: $\forall x, y \in \mathbb{F}, xy \in \mathbb{F}$ i.e if you multiply any 2 elements of the set you get another element of the set
  with 2 operations $+$ and $\times$
- Associative
  $+$: $(x + y) + z = x + (y + z) \ \forall x, y, z \in \mathbb{F}$
  $\times$: $(xy)z = x(yz) \ \forall x, y, z \in \mathbb{F}$
- Commutative: under addition and multiplication (if you omit zero since can't divide by 0)
  $+$: $x + y = y + x \ \forall x, y, \in \mathbb{F}$
  $\times$: $xy = yx \ \forall x, y \in \mathbb{F}$
  Table symmetrical about diagonal
- Identity
  $+$: $\exists 0 \in \mathbb{F}$, s.t. $0 + x = x \ \forall x \in \mathbb{F}$ (table row and column item is itself)
  $\times$: $\exists 1 \neq 0 \in \mathbb{F}$, s.t. $1 \times x = x \ \forall x \in \mathbb{F}$
- Inverse
  $+$: $\forall x \in \mathbb{F}$, $\exists -x \in \mathbb{F}$ s.t. $x + (-x) = 0$
  $\times$: $\forall x \neq 0 \in \mathbb{F}$, $\exists x^{-1} \in \mathbb{F}$ s.t. $x \times x^{-1} = 1$
- Distributive property: This connects addition and multiplication
  $\forall x, y, z \in \mathbb{F}, a(b + c) = (a \times b) + (a \times c)$

8.4 Fields versus Groups

In a sense, a field is pretty much a set F that is a commutative group in two ways at the same time: that is, it is a group with respect to addition, and it is also a group with respect to multiplication if you ignore the additive identity 0!
Every field is a group but not every group is a field. Fields require commutativity too and have 2 operations not just one!
A **group** has a SINGLE binary operation, usually called "multiplication" but sometimes called "addition", especially if it **is** commutative. A **field** has TWO binary operations, usually called "addition" and "multiplication". Both of them are always commutative. **Groups** model symmetries.

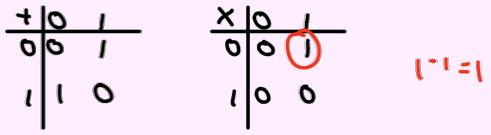
8.5 Examples

- Write down multiplication table for $\mathbb{F}_7{}^{\times}$ and find the inverse of each element
  Hint: all elements coprime to 7

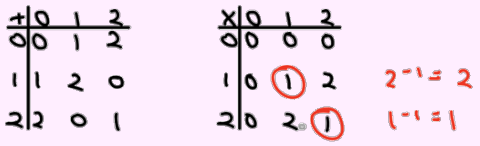


$1^{-1} = 1$
$2^{-1} = 4$
$3^{-1} = 5$
$4^{-1} = 2$
$5^{-1} = 3$
$6^{-1} = 6$

- Take $\mathbb{F}_2$, a field with 2 elements $\{0,1\}$
  Think: 0 ~ even integers
  1~ odd integers



- Take $\mathbb{F}_3$, a field with 3 elements $\{0,1,2\}$
  Think: 0 ={integers exactly divisible by 3}
  1 ={integers with remainder=1 mod 3}
  2 ={integers with remainder=2 mod 3}



- Consider the set {0,1,2,3} which are the remainders mod 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

This is not a field so not $\mathbb{F}_4$ since the element 2 does not have a multiplicative inverse

- Consider the set {0,1,2,3, 4} which are the remainders mod 5We will just look at the multiplication table this time

×	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

This is $\mathbb{F}_5$

Can you spot a pattern now?
$\mathbb{F}_n \cong \mathbb{Z}_n$ iff n is prime